



Prezes Rady Ministrów

Donald Tusk

Warszawa, dnia /elektroniczny znacznik czasu/

RM-0610-195-25
UC32

Pan Szymon HOŁOWNIA
Marszałek Sejmu

Szanowny Panie Marszałku,

na podstawie art. 118 ust. 1 Konstytucji Rzeczypospolitej Polskiej przedstawiam Sejmowi
projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz
niektórych innych ustaw.

Ma on na celu wykonanie prawa Unii Europejskiej.

Do prezentowania stanowiska Rządu w tej sprawie w toku prac parlamentarnych został
upoważniony Minister Cyfryzacji.

Z poważaniem

Donald Tusk

/podpisano kwalifikowanym podpisem elektronicznym/

Do wiadomości:
wnioskodawca

U S T A W A

z dnia

o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw¹⁾

Art. 1. W ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077 i 1222 oraz z 2025 r. poz. 1017 i 1069) wprowadza się następujące zmiany:

1) odnośnik nr 1 do tytułu ustawy otrzymuje brzmienie:

„¹⁾ Niniejsza ustawa wdraża dyrektywę Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniającą rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającą dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz. Urz. UE L 333 z 27.12.2022, str. 80).”;

2) do tytułu ustawy dodaje się odnośnik nr 2 w brzmieniu:

„²⁾ Niniejsza ustawa służy częściowemu stosowaniu rozporządzenia delegowanego Komisji (UE) 2024/1366 z dnia 11 marca 2024 r. uzupełniającego rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/943 poprzez ustanowienie kodeksu sieci dotyczącego zasad sektorowych w zakresie aspektów cyberbezpieczeństwa w transgranicznych przepływach energii elektrycznej (Dz. Urz. UE L 2024/1366 z 24.05.2024).”;

¹⁾ Niniejszą ustawą zmienia się ustawy: ustawę z dnia 8 marca 1990 r. o samorządzie gminnym, ustawę z dnia 21 marca 1991 r. o obszarach morskich Rzeczypospolitej Polskiej i administracji morskiej, ustawę z dnia 24 sierpnia 1991 r. o Państwowej Straży Pożarnej, ustawę z dnia 20 sierpnia 1997 r. o Krajowym Rejestrze Sądowym, ustawę z dnia 29 sierpnia 1997 r. – Ordynacja podatkowa, ustawę z dnia 5 czerwca 1998 r. o samorządzie województwa, ustawę z dnia 5 czerwca 1998 r. o samorządzie powiatowym, ustawę z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych, ustawę z dnia 24 maja 2000 r. o Krajowym Rejestrze Karnym, ustawę z dnia 21 grudnia 2000 r. o dozorze technicznym, ustawę z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej, ustawę z dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym, ustawę z dnia 28 kwietnia 2011 r. o systemie i informacji w ochronie zdrowia, ustawę z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej, ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych, ustawę z dnia 11 września 2019 r. – Prawo zamówień publicznych, ustawę z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa, ustawę z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej, ustawę z dnia 12 lipca 2024 r. – Prawo komunikacji elektronicznej oraz ustawę z dnia 12 lipca 2024 r. – Przepisy wprowadzające ustawę – Prawo komunikacji elektronicznej.

3) w art. 1:

- a) w ust. 1 w pkt 3 kropkę zastępuje się średnikiem i dodaje się pkt 4 w brzmieniu:
„4) zakres Krajowego planu reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę.”,
- b) w ust. 2 uchyla się pkt 1 i 2;

4) w art. 2:

- a) po pkt 3 dodaje się pkt 3a–3d w brzmieniu:
 - „3a) CSIRT sektorowy – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego, działający na poziomie sektora lub podsektora, ustanowiony przez organ właściwy do spraw cyberbezpieczeństwa dla danego sektora lub podsektora;
 - 3b) abonent nazwy domeny – podmiot będący stroną umowy o utrzymywanie nazwy domeny zawartej z rejestrem nazw domen najwyższego poziomu (TLD), za pośrednictwem podmiotu świadczącego usługi rejestracji nazw domen;
 - 3c) adres do doręczeń elektronicznych – adres, o którym mowa w art. 2 pkt 1 ustawy z dnia 18 listopada 2020 r. o doręczeniach elektronicznych (Dz. U. z 2024 r. poz. 1045 i 1841), wpisany do bazy adresów elektronicznych, o której mowa w art. 25 tej ustawy;
 - 3d) bezpieczeństwo systemów informacyjnych – odporność systemów informacyjnych, przy danym poziomie pewności, na zdarzenia naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy;”
- b) pkt 4 otrzymuje brzmienie:
 - „4) cyberbezpieczeństwo – cyberbezpieczeństwo w rozumieniu art. 2 pkt 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz. Urz. UE L 151 z 07.06.2019, str. 15, z późn. zm.²⁾), zwanego dalej „rozporządzeniem 2019/881”;”

²⁾ Zmiana wymienionego rozporządzenia została ogłoszona w Dz. Urz. UE L 2025/37 z 15.01.2025.

c) po pkt 4 dodaje się pkt 4a–4k w brzmieniu:

- „4a) cyberzagrożenie – cyberzagrożenie w rozumieniu art. 2 pkt 8 rozporządzenia 2019/881;
- 4b) dostawca sieci dostarczania treści – osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, która dostarcza treści i usługi cyfrowe do sieci rozproszonych geograficznie serwerów służących zapewnieniu wysokiej i łatwej dostępności tych treści i usług cyfrowych lub ich szybkiego dostarczania na rzecz użytkowników internetu w imieniu dostawców treści i usług, z wyłączeniem przedsiębiorców komunikacji elektronicznej;
- 4c) dostawca sprzętu lub oprogramowania – producenta, upoważnionego przedstawiciela, importera lub dystrybutora, w rozumieniu odpowiednio art. 2 pkt 3–6 rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 765/2008 z dnia 9 lipca 2008 r. ustanawiającego wymagania w zakresie akredytacji i uchylającego rozporządzenie (EWG) nr 339/93 (Dz. Urz. UE L 218 z 13.08.2008, str. 30, z późn. zm.³⁾), produktu ICT, usługi ICT lub procesu ICT;
- 4d) dostawca internetowej platformy handlowej – osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, która dostarcza internetową platformę handlową, o której mowa w art. 2 pkt 8 ustawy z dnia 30 maja 2014 r. o prawach konsumenta (Dz. U. z 2024 r. poz. 1796 oraz z 2025 r. poz. 1172);
- 4e) dostawca chmury obliczeniowej – osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, która świadczy usługę umożliwiającą dostęp do skalowalnego i elastycznego zbioru zasobów obliczeniowych do wspólnego wykorzystywania przez wielu użytkowników;
- 4f) dostawca usług DNS – podmiot, który świadczy dostępne publicznie rekurencyjne usługi rozpoznawania nazw domen na rzecz ogółu użytkowników końcowych internetu lub autorytatywne usługi rozpoznawania nazw domen do użytku ogółu użytkowników końcowych internetu, z wyjątkiem głównych serwerów nazw;

³⁾ Zmiana wymienionego rozporządzenia została ogłoszona w Dz. Urz. UE L 169 z 25.06.2019, str. 1.

- 4g) dostawca usługi centrum przetwarzania danych – osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, która świadczy usługę obejmującą struktury lub grupy struktur przeznaczone do scentralizowanego hostingu, zapewniania wzajemnego połączenia i eksploatacji produktów ICT, usług ICT lub procesów ICT służącego do świadczenia usług przechowywania, przetwarzania i transportu danych wraz ze wszystkimi obiektami i całą infrastrukturą, zapewniającymi dystrybucję energii elektrycznej i kontrolę środowiskową;
- 4h) dostawca usług zarządzanych – osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, która świadczy usługi związane z instalacją, eksploatacją lub konserwacją produktów ICT, usług ICT, procesów ICT lub systemów informacyjnych przez wsparcie lub aktywną administrację przeprowadzane u usługobiorcy na miejscu lub zdalnie;
- 4i) dostawca usług zarządzanych w zakresie cyberbezpieczeństwa – osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, która świadczy usługi polegające na realizacji lub wsparciu dla realizacji działań związanych z zarządzaniem ryzykiem w cyberbezpieczeństwie, w tym obsługę incydentów, testów bezpieczeństwa, audytów systemów informacyjnych, doradztwo;
- 4j) dostawca usług zaufania – dostawcę usług zaufania w rozumieniu art. 3 pkt 19 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE (Dz. Urz. UE L 257 z 28.08.2014, str. 73), zwanego dalej „rozporządzeniem 910/2014”;
- 4k) dostawca wyszukiwarki internetowej – osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, która świadczy usługę wyszukiwarki internetowej, o której mowa w art. 2 pkt 5 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/1150 z dnia 20 czerwca 2019 r. w sprawie propagowania sprawiedliwości i przejrzystości dla użytkowników biznesowych korzystających z usług pośrednictwa internetowego (Dz. Urz. UE L 186 z 11.07.2019, str. 57);”;

- d) pkt 5 otrzymuje brzmienie:

„5) incydent – zdarzenie, które ma lub może mieć niekorzystny wpływ na bezpieczeństwo systemów informacyjnych;”
- e) pkt 7 i 8 otrzymują brzmienie:

„7) incydent poważny – incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi przez podmiot kluczowy lub podmiot ważny, straty finansowe dla tego podmiotu lub wpływa na inne osoby fizyczne, osoby prawne, jednostki organizacyjne nieposiadające osobowości prawnej przez wywołanie poważnej szkody materialnej lub niematerialnej;

8) incydent w cyberbezpieczeństwie na dużą skalę – incydent, którego skutki przekraczają możliwości reagowania państwa lub który ma poważny wpływ na inne państwo członkowskie Unii Europejskiej;”
- f) po pkt 8 dodaje się pkt 8a w brzmieniu:

„8a) kierownik podmiotu kluczowego lub podmiotu ważnego – kierownik jednostki w rozumieniu art. 3 ust. 1 pkt 6 ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2023 r. poz. 120, z późn. zm.⁴⁾) kierujący podmiotem kluczowym lub podmiotem ważnym; w przypadku podmiotu kluczowego lub podmiotu ważnego będącego jednostką sektora finansów publicznych kierownikiem podmiotu jest kierownik, o którym mowa w art. 53 ust. 1 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2024 r. poz. 1530, z późn. zm.⁵⁾);”
- g) uchyla się pkt 9,
- h) po pkt 10 dodaje się pkt 10a w brzmieniu:

„10a) organizacja badawcza – osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, która prowadzi działalność, o której mowa w art. 4 ust. 2 pkt 2 lub ust. 3 ustawy z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce (Dz. U. z 2024 r. poz. 1571, z późn. zm.⁶⁾), z wyłączeniem podmiotów, o których mowa w art. 7 ust. 1 pkt 1–7 tej ustawy;”

⁴⁾ Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2023 r. poz. 295 i 1598, z 2024 r. poz. 619, 1685 i 1863 oraz z 2025 r. poz. 1218.

⁵⁾ Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2024 r. poz. 1572, 1717, 1756 i 1907 oraz z 2025 r. poz. 39 i 1180.

⁶⁾ Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2024 r. poz. 1871 i 1897 oraz z 2025 r. poz. 619, 620, 621, 622 i 1162.

- i) pkt 11 otrzymuje brzmienie:
„11) podatność – właściwości produktu ICT lub usługi ICT, które mogą być wykorzystane przez cyberzagrożenie;”;
- j) po pkt 11 dodaje się pkt 11a–11o w brzmieniu:
 - „11a) platforma sieci usług społecznościowych – usługę świadczoną drogą elektroniczną w rozumieniu przepisów ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2024 r. poz. 1513), która umożliwia użytkownikom końcowym łączenie się z innymi osobami oraz komunikowanie się i wymianę, udostępnianie i odkrywanie treści za pomocą wielu urządzeń;
 - 11b) podmiot finansowy – podmiot, o którym mowa w art. 2 ust. 1 lit. a–t rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniającego rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (Dz. Urz. UE L 333 z 27.12.2022, str. 1, z późn. zm.⁷⁾), zwanego dalej „rozporządzeniem 2022/2554”;
 - 11c) podmiot publiczny – podmiot wskazany w załączniku nr 1 lub 2 do ustawy w sektorze podmioty publiczne;
 - 11d) podmiot krytyczny – podmiot krytyczny w rozumieniu art. 2 pkt 1 dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylającej dyrektywę Rady 2008/114/WE (Dz. Urz. UE L 333 z 27.12.2022, str. 164), zwanej dalej „dyrektywą 2022/2557”;
 - 11e) podmiot świadczący usługi rejestracji nazw domen – rejestratora lub agenta działającego w imieniu rejestratorów, w tym dostawcę lub odsprzedawcę usług w zakresie prywatnej rejestracji lub pośrednictwa w rejestracji;
 - 11f) potencjalne zdarzenie dla cyberbezpieczeństwa – zdarzenie, które mogło mieć niekorzystny wpływ na bezpieczeństwo systemów informacyjnych, które jednak nie wystąpiło lub któremu udało się zapobiec;

⁷⁾ Zmiana wymienionego rozporządzenia została ogłoszona w Dz. Urz. UE L 2024/90177 z 12.03.2024.

- 11g) poważne cyberzagrożenie – cyberzagrożenie, które przez swoje właściwości techniczne może mieć poważny wpływ na bezpieczeństwo systemów informacyjnych lub użytkowników tych systemów przez wywołanie poważnej szkody materialnej lub niematerialnej;
- 11h) projekt – przedsięwzięcie realizowane w ramach programu, o którym mowa w art. 45a ust. 1, na podstawie umowy o dofinansowanie, zawieranej między beneficjentem a podmiotem udzielającym pomocy;
- 11i) poważny incydent związany z ICT – poważny incydent związany z technologiami informacyjno-komunikacyjnymi w rozumieniu art. 3 pkt 10 rozporządzenia 2022/2554;
- 11j) przedsiębiorca komunikacji elektronicznej – przedsiębiorcę komunikacji elektronicznej w rozumieniu art. 2 pkt 39 ustawy z dnia 12 lipca 2024 r. – Prawo komunikacji elektronicznej (Dz. U. poz. 1221 oraz z 2025 r. poz. 637 i 820);
- 11k) przedsiębiorca telekomunikacyjny – przedsiębiorcę telekomunikacyjnego w rozumieniu art. 2 pkt 40 ustawy z dnia 12 lipca 2024 r. – Prawo komunikacji elektronicznej;
- 11l) proces ICT – proces ICT w rozumieniu art. 2 pkt 14 rozporządzenia 2019/881;
- 11m) produkt ICT – produkt ICT w rozumieniu art. 2 pkt 12 rozporządzenia 2019/881;
- 11n) usługa ICT – usługę ICT w rozumieniu art. 2 pkt 13 rozporządzenia 2019/881;
- 11o) rejestr nazw domen najwyższego poziomu (TLD) – podmiot, któremu powierzono konkretną domenę najwyższego poziomu (TLD) i który odpowiada za zarządzanie nią, w tym za rejestrację nazw domen w ramach TLD oraz za jej techniczne funkcjonowanie, w tym za obsługę jej serwerów nazw, utrzymanie jej baz danych oraz dystrybucję plików strefowych TLD we wszystkich serwerach nazw, bez względu na to, czy którekolwiek z tych działań jest wykonywane przez sam podmiot czy zlecane na zewnątrz, ale z wyłączeniem sytuacji, w których rejestr wykorzystuje nazwy TLD wyłącznie do własnego użytku;”;
- k) pkt 14 otrzymuje brzmienie:
 - „14) system informacyjny – oznacza to:
 - a) system teleinformatyczny, o którym mowa w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących

zadania publiczne (Dz. U. z 2024 r. poz. 1557 i 1717 oraz z 2025 r. poz. 1006, 1019, 1158 i 1301), lub

b) urządzenie lub grupę połączonych urządzeń i oprogramowania zaprogramowanych w celu przetwarzania danych

– wraz z danymi przetwarzanymi w postaci elektronicznej;”,

l) po pkt 14 dodaje się pkt 14a w brzmieniu:

„14a) właściwy organ w rozumieniu rozporządzenia 2022/2554 – Komisję Nadzoru Finansowego w zakresie nadzoru przewidzianego rozporządzeniem 2022/2554;”,

m) uchyla się pkt 15–17;

5) po art. 2 dodaje się art. 2a w brzmieniu:

„Art. 2a. W przypadku podmiotu publicznego pod pojęciem usługi rozumie się także zadanie publiczne realizowane przez ten podmiot.”;

6) w art. 3 wyrazy „kluczowych i usług cyfrowych” zastępuje się wyrazami „przez podmioty kluczowe lub podmioty ważne”;

7) po art. 3 dodaje się art. 3a w brzmieniu:

„Art. 3a. W ramach obsługi incydentów podmiot krajowego systemu cyberbezpieczeństwa może w szczególności podejmować działania w celu wykrywania źródła lub dokonywania analizy aktywności, w tym ruchu sieciowego, powodujących wystąpienie incydentu zakłócającego świadczenie usług przez ten podmiot.”;

8) w art. 4:

a) pkt 1 i 2 otrzymują brzmienie:

„1) podmioty kluczowe;

2) podmioty ważne;”,

b) pkt 6 otrzymuje brzmienie:

„6) CSIRT sektorowe;”,

c) uchyla się pkt 7–16,

d) po pkt 17 dodaje się pkt 17a w brzmieniu:

„17a) Połączone Centrum Operacyjne Cyberbezpieczeństwa, zwane dalej „PCOC”;”,

9) w tytule rozdziału 2 wyrazy „operatorów usług kluczowych” zastępuje się wyrazami „podmiotów kluczowych lub podmiotów ważnych”;

10) art. 5 otrzymuje brzmienie:

„Art. 5. 1. Podmiotem kluczowym jest:

- 1) osoba fizyczna, osoba prawna albo jednostka organizacyjna nieposiadająca osobowości prawnej wskazana w załączniku nr 1 do ustawy, która przewyższa wymogi dla średniego przedsiębiorstwa określone w art. 2 ust. 1 załącznika I do rozporządzenia Komisji (UE) nr 651/2014 z dnia 17 czerwca 2014 r. uznającego niektóre rodzaje pomocy za zgodne z rynkiem wewnętrznym w zastosowaniu art. 107 i 108 Traktatu (Dz. Urz. UE L 187 z 26.06.2014, str. 1, z późn. zm.⁸⁾), zwanego dalej „rozporządzeniem 651/2014/UE”;
- 2) przedsiębiorca komunikacji elektronicznej, który co najmniej spełnia wymogi dla średniego przedsiębiorcy określone w art. 2 ust. 1 załącznika I do rozporządzenia 651/2014/UE albo je przewyższa;
- 3) dostawca usług zarządzanych w zakresie cyberbezpieczeństwa, który co najmniej spełnia wymogi dla małego albo średniego przedsiębiorcy określone w art. 2 ust. 1 załącznika I do rozporządzenia 651/2014/UE albo je przewyższa;
- 4) niezależnie od wielkości podmiotu:
 - a) dostawca usług DNS,
 - b) kwalifikowany dostawca usług zaufania w rozumieniu art. 3 pkt 20 rozporządzenia 910/2014,
 - c) podmiot krytyczny,
 - d) podmiot publiczny wskazany w załączniku nr 1 do ustawy w sektorze podmioty publiczne,
 - e) podmiot zidentyfikowany jako podmiot kluczowy na podstawie art. 7l ust. 2 pkt 1,
 - f) państwowa osoba prawna zidentyfikowana jako podmiot kluczowy na podstawie art. 7m,
 - g) podmiot, który nie jest przedsiębiorcą, a jest wskazany w załączniku nr 1 do ustawy z nazwy albo przez określenie jego rodzaju,

⁸⁾ Zmiany wymienionego rozporządzenia zostały ogłoszone w Dz. Urz. UE L 329 z 15.12.2025, str. 28, Dz. Urz. UE L 149 z 07.06.2016, str. 10, Dz. Urz. UE L 156 z 20.06.2017, str. 1, Dz. Urz. UE L 26 z 31.01.2018, str. 53, Dz. Urz. UE L 215 z 07.07.2020, str. 3, Dz. Urz. UE L 89 z 16.03.2021, str. 1, Dz. Urz. UE L 270 z 29.07.2021, str. 39, Dz. Urz. UE L 119 z 05.05.2023, str. 159, Dz. Urz. UE L 167 z 30.06.2023, str. 1 oraz Dz. Urz. UE L 2025/90138 z 13.02.2025.

- h) podmiot będący operatorem obiektu energetyki jądrowej, o którym mowa w art. 2 pkt 2 ustawy z dnia 29 czerwca 2011 r. o przygotowaniu i realizacji inwestycji w zakresie obiektów energetyki jądrowej oraz inwestycji towarzyszących (Dz. U. z 2025 r. poz. 1156),
- i) rejestr nazw domen najwyższego poziomu (TLD),
- j) podmiot świadczący usługi rejestracji nazw domen.

2. Podmiotem ważnym jest:

- 1) osoba fizyczna, osoba prawna albo jednostka organizacyjna nieposiadająca osobowości prawnej wskazana w załączniku nr 1 do ustawy, która spełnia wymogi dla średniego przedsiębiorcy określone w art. 2 ust. 1 załącznika I do rozporządzenia 651/2014/UE oraz która nie jest podmiotem kluczowym;
- 2) osoba fizyczna, osoba prawna albo jednostka organizacyjna nieposiadająca osobowości prawnej wskazana w załączniku nr 2 do ustawy, która spełnia wymogi dla średniego przedsiębiorcy określone w art. 2 ust. 1 załącznika I do rozporządzenia 651/2014/UE lub przewyższa te wymogi oraz która nie jest podmiotem kluczowym;
- 3) niekwalifikowany dostawca usług zaufania będący mikro-, małym lub średnim przedsiębiorcą, o którym mowa w art. 2 ust. 1 załącznika I do rozporządzenia 651/2014/UE;
- 4) przedsiębiorca komunikacji elektronicznej będący mikro- lub małym przedsiębiorcą, o którym mowa w art. 2 ust. 2 i 3 załącznika I do rozporządzenia 651/2014/UE;
- 5) podmiot będący inwestorem obiektu energetyki jądrowej, o którym mowa w art. 2 pkt 2 ustawy z dnia 29 czerwca 2011 r. o przygotowaniu i realizacji inwestycji w zakresie obiektów energetyki jądrowej oraz inwestycji towarzyszących, który uzyskał decyzję zasadniczą, o której mowa w art. 3a ust. 1 tej ustawy – niezależnie od jego wielkości;
- 6) podmiot zidentyfikowany jako podmiot ważny na podstawie art. 71 ust. 2 pkt 2;
- 7) podmiot, który nie jest przedsiębiorcą, a jest wskazany w załączniku nr 2 do ustawy z nazwy albo przez określenie jego rodzaju;
- 8) podmiot publiczny, który nie jest podmiotem kluczowym oraz jest samorządową jednostką budżetową, samorządowym zakładem budżetowym, samorządową instytucją kultury albo spółką wykonującą zadania o charakterze użyteczności publicznej w rozumieniu art. 1 ust. 2 ustawy z dnia 20 grudnia 1996 r. o gospodarce

komunalnej (Dz. U. z 2021 r. poz. 679), jeżeli realizuje zadanie publiczne z wykorzystaniem systemów informacyjnych.

3. Przy określaniu wymogów dla podmiotów, o których mowa w ust. 1 pkt 1–3, ust. 2 pkt 1–4, nie stosuje się art. 3 ust. 4 załącznika I do rozporządzenia 651/2014/UE.

4. Jeżeli podmiot, o którym mowa w ust. 1, spełnia wymogi zarówno dla podmiotu kluczowego, jak i dla podmiotu ważnego, to jest podmiotem kluczowym.

5. Jeżeli status podmiotu kluczowego lub podmiotu ważnego zależy od wielkości podmiotu, to przesłanki uznania za podmiot kluczowy lub podmiot ważny bada się według stanu na dzień sporządzenia sprawozdania finansowego.

6. Jeżeli podmiot spełnia wymogi do uznania za podmiot kluczowy, ponieważ przewyższa kryteria dla średniego przedsiębiorstwa zgodnie z art. 6 ust. 2–4 załącznika I do rozporządzenia 651/2014/UE, ale jego system informacyjny jest niezależny od systemów informacyjnych jego przedsiębiorstw powiązanych lub przedsiębiorstw partnerskich lub nie świadczy on usług wspólnie z jego przedsiębiorstwami powiązanymi lub przedsiębiorstwami partnerskimi, to nie jest podmiotem kluczowym.

7. Jeżeli podmiot spełnia wymogi do uznania za podmiot ważny, ponieważ spełnia kryteria dla średniego przedsiębiorstwa zgodnie z art. 6 ust. 2–4 załącznika I do rozporządzenia 651/2014/UE, ale jego system informacyjny jest niezależny od systemów informacyjnych jego przedsiębiorstw powiązanych lub przedsiębiorstw partnerskich lub nie świadczy on usług wspólnie z jego przedsiębiorstwami powiązanymi lub przedsiębiorstwami partnerskimi, to nie jest podmiotem ważnym.

8. Podmiot leczniczy, który nie jest przedsiębiorcą:

- 1) jest podmiotem ważnym, jeżeli zatrudnia od 50 do 249 osób;
- 2) jest podmiotem kluczowym, jeżeli zatrudnia co najmniej 250 osób.

9. Podmiot, o którym mowa w ust. 1 pkt 4 lit. h, staje się podmiotem kluczowym z dniem:

- 1) uzyskania zezwolenia na eksploatację, o której mowa w art. 4 ust. 1 pkt 3 ustawy z dnia 29 listopada 2000 r. – Prawo atomowe (Dz. U. z 2024 r. poz. 1277, 1897 i 1907) – w przypadku operatora składowiska odpadów promieniotwórczych;
- 2) uzyskania zezwolenia na eksploatację, o której mowa w art. 4 ust. 1 pkt 2 ustawy z dnia 29 listopada 2000 r. – Prawo atomowe, lub uzyskania koncesji na wytwarzanie energii elektrycznej lub ciepła, o których mowa w art. 32 ust. 1 pkt 1 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne (Dz. U. z 2024 r. poz. 266,

- z późn. zm.⁹⁾), w zależności od tego, które zostanie uzyskane pierwsze – w przypadku operatora elektrowni jądrowej;
- 3) uzyskania zezwolenia na eksploatację, o której mowa w art. 4 ust. 1 pkt 2 ustawy z dnia 29 listopada 2000 r. – Prawo atomowe, lub uzyskania koncesji na wydobywanie kopalin, o której mowa w art. 22 ust. 1 pkt 2 ustawy z dnia 9 czerwca 2011 r. – Prawo geologiczne i górnicze (Dz. U. z 2024 r. poz. 1290 oraz z 2025 r. poz. 769 i 1023), w zależności od tego, które zostanie uzyskane pierwsze – w przypadku operatora zakładu do wydobywania rud uranu i toru ze złóż i do ich wstępnego przetwarzania;
- 4) uzyskania zezwolenia na eksploatację, o której mowa w art. 4 ust. 1 pkt 2 ustawy z dnia 29 listopada 2000 r. – Prawo atomowe – w przypadku operatorów pozostałych obiektów energetyki jądrowej.

10. Do podmiotów kluczowych lub podmiotów ważnych nie zalicza się służb specjalnych w rozumieniu art. 11 ustawy z dnia 24 maja 2022 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2025 r. poz. 902), a także podmiotów podległych lub nadzorowanych przez Ministra Obrony Narodowej.

11. Minister Obrony Narodowej wskaże, w drodze decyzji niepodlegającej ogłoszeniu, jednostki jemu podległe lub przez niego nadzorowane, które uznaje się za podmioty kluczowe lub podmioty ważne, oraz określi sektor lub sektory, a także w razie potrzeby podsektor, do jakiego przypisuje dany podmiot.”;

- 11) po art. 5 dodaje się art. 5a w brzmieniu:

„Art. 5a. 1. Podmiot kluczowy lub podmiot ważny podlegają obowiązkom wynikającym z ustawy, jeżeli mają miejsce zamieszkania na terytorium Rzeczypospolitej Polskiej lub prowadzą działalność na terytorium Rzeczypospolitej Polskiej przez swoje siedziby, oddziały lub w ramach działalności transgranicznej.

2. Przedsiębiorca komunikacji elektronicznej podlega obowiązkom wynikającym z ustawy, jeżeli świadczy usługi na terytorium Rzeczypospolitej Polskiej.

3. Dostawca usług DNS, rejestr nazw domen najwyższego poziomu (TLD), podmiot świadczący usługi rejestracji nazw domen, dostawca chmury obliczeniowej, dostawca usługi centrum przetwarzania danych, dostawca sieci dostarczania treści, dostawca usług zarządzanych, dostawca usług zarządzanych w zakresie cyberbezpieczeństwa, dostawca

⁹⁾ Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2024 r. poz. 834, 859, 1847 i 1881 oraz z 2025 r. poz. 303, 759, 1218 i 1303.

internetowej platformy handlowej, dostawca wyszukiwarki internetowej oraz dostawca platformy usług sieci społecznościowych świadczący usługi na terytorium Rzeczypospolitej Polskiej podlega obowiązkom wynikającym z ustawy, jeżeli Rzeczpospolita Polska jest głównym miejscem prowadzenia działalności przez ten podmiot.

4. Głównym miejscem prowadzenia działalności jest państwo członkowskie Unii Europejskiej, w którym ma siedzibę kierownik podmiotu podejmujący decyzje w sprawie systemu zarządzania bezpieczeństwem informacji, o którym mowa w art. 8 ust. 1.

5. W przypadku gdy nie można ustalić, czy kierownik podmiotu podejmujący decyzje w sprawie systemu zarządzania bezpieczeństwem informacji ma siedzibę w państwie członkowskim Unii Europejskiej, to głównym miejscem prowadzenia działalności jest państwo członkowskie Unii Europejskiej, w którym są realizowane zadania związane z systemem zarządzania bezpieczeństwem informacji, o których mowa w art. 8 ust. 1.

6. W przypadku gdy informacji, o której mowa w ust. 5, również nie można ustalić, to głównym miejscem prowadzenia działalności jest państwo członkowskie Unii Europejskiej, w którym podmiot, o którym mowa w ust. 3, ma największą liczbę osób zatrudnionych w odniesieniu do innych państw członkowskich Unii Europejskiej.

7. Podmiot, o którym mowa w ust. 3, który nie posiada jednostki organizacyjnej w jednym z państw członkowskich Unii Europejskiej, ale oferuje swoje usługi na terytorium Rzeczypospolitej Polskiej, wyznacza przedstawiciela posiadającego jednostkę organizacyjną na terytorium Rzeczypospolitej Polskiej, o ile nie wyznaczył przedstawiciela posiadającego jednostkę organizacyjną w innym państwie członkowskim Unii Europejskiej.

8. Przedstawicielem, o którym mowa w ust. 7, może być osoba fizyczna, osoba prawna albo jednostka organizacyjna nieposiadająca osobowości prawnej, ustanowiona na terytorium Rzeczypospolitej Polskiej lub w innym państwie członkowskim Unii Europejskiej, wyznaczona do występowania w imieniu podmiotu wskazanego w ust. 1, który nie posiada jednostki organizacyjnej w jednym z państw członkowskich Unii Europejskiej, do którego organ właściwy do spraw cyberbezpieczeństwa, CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT sektorowy może się zwrócić w związku z obowiązkami podmiotu wynikającymi z ustawy.

9. Podmiot, o którym mowa w ust. 3, który nie posiada jednostki organizacyjnej w jednym z państw członkowskich Unii Europejskiej, ale oferuje swoje usługi na terytorium Rzeczypospolitej Polskiej, podlega właściwości polskiego organu właściwego do spraw cyberbezpieczeństwa, jeżeli wyznaczył przedstawiciela posiadającego jednostkę organizacyjną na terytorium Rzeczypospolitej Polskiej.

10. Ustawę stosuje się do podmiotów publicznych niezależnie od miejsca ich siedziby.”;

12) uchyla się art. 6;

13) art. 7 otrzymuje brzmienie:

„Art. 7. 1. Wykaz podmiotów kluczowych i podmiotów ważnych, zwany dalej „wykazem”, jest prowadzony w celu:

- 1) identyfikacji podmiotów kluczowych i podmiotów ważnych;
- 2) zapewnienia wymiany informacji w zakresie cyberbezpieczeństwa, w tym o incydentach, podatnościach i cyberzagrożeniach między podmiotami kluczowymi i podmiotami ważnymi a CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT sektorowymi i organami właściwymi do spraw cyberbezpieczeństwa;
- 3) umożliwienia prowadzenia czynności nadzorczych nad podmiotami kluczowymi i podmiotami ważnymi.

2. Wykaz zawiera:

- 1) nazwę (firmę) podmiotu kluczowego lub podmiotu ważnego;
- 2) sektor, podsektor i rodzaj lub rodzaje podmiotu, zgodnie z załącznikiem nr 1 lub 2 do ustawy;
- 3) adres siedziby i adres do korespondencji;
- 4) adres do doręczeń elektronicznych, jeżeli został wpisany do bazy adresów elektronicznych;
- 5) adres poczty elektronicznej;
- 6) numer identyfikacji podatkowej (NIP), jeżeli został nadany;
- 7) numer identyfikacyjny podmiotu publicznego w krajowym rejestrze urzędowym podmiotów gospodarki narodowej (REGON), jeżeli został nadany;
- 8) numer we właściwym rejestrze działalności regulowanej, jeżeli został nadany;
- 9) zakres publicznych adresów IP wykorzystywanych przez podmiot kluczowy lub podmiot ważny w sposób ciągły;

- 10) domeny internetowe wykorzystywane przez podmiot kluczowy lub podmiot ważny w sposób ciągły;
- 11) dane osób do kontaktu z podmiotami z krajowego systemu cyberbezpieczeństwa zawierające: imię i nazwisko, numer telefonu służbowego oraz adres służbowej poczty elektronicznej, a w przypadku osoby, która będzie pełnić rolę administratora konta podmiotu w systemie teleinformatycznym, o którym mowa w art. 46 ust. 1, dodatkowo numer PESEL lub niepowtarzalny identyfikator środka identyfikacji elektronicznej, o którym mowa w aktach wykonawczych Komisji Europejskiej, wydanych na podstawie art. 12 ust. 8 rozporządzenia 910/2014;
- 12) numer telefonu przyporządkowany do wykonywanej działalności;
- 13) deklarację podmiotu kluczowego lub podmiotu ważnego, czy spełnia kryteria mikro-przedsiębiorcy, małego przedsiębiorcy, średniego przedsiębiorcy, o którym mowa w art. 2 ust. 1 załącznika I do rozporządzenia 651/2014/UE, albo przekracza te kryteria, a w przypadku podmiotu leczniczego, który nie jest przedsiębiorcą, oraz urzędu gminy – deklarację wskazującą liczbę osób zatrudnionych według stanu na dzień sporządzenia sprawozdania finansowego;
- 14) informację określającą, w których państwach członkowskich Unii Europejskiej podmiot kluczowy lub podmiot ważny wykonuje działalność, wraz z określeniem rodzaju wykonywanej działalności;
- 15) w przypadku dostawcy usług DNS, rejestru nazw domen najwyższego poziomu (TLD), podmiotu świadczącego usługi rejestracji nazw domen, dostawcy chmury obliczeniowej, dostawcy usługi centrum przetwarzania danych, dostawcy sieci dostarczania treści, dostawcy usług zarządzanych, dostawcy usług zarządzanych w zakresie cyberbezpieczeństwa, dostawcy internetowej platformy handlowej, dostawcy wyszukiwarki internetowej oraz dostawcy platformy usług sieci społecznościowych – główne miejsce prowadzenia działalności ustalone zgodnie z art. 5a ust. 3–6;
- 16) informację o zawarciu umowy z dostawcą usług zarządzanych w zakresie cyberbezpieczeństwa na realizację zadań, o których mowa w art. 8 i art. 11, wraz z danymi tego dostawcy zawierającymi nazwę (firmę) dostawcy, adres siedziby, adres do korespondencji, numer telefonu, adres poczty elektronicznej;

- 17) informację o ustanowieniu przedstawiciela podmiotu kluczowego lub podmiotu ważnego, o którym mowa w art. 5a ust. 7, wraz z danymi kontaktowymi do tego przedstawiciela obejmujące:
 - a) w przypadku osób fizycznych: imię i nazwisko, adres do korespondencji, numer telefonu służbowego oraz adres służbowej poczty elektronicznej,
 - b) w przypadku osób prawnych i jednostek organizacyjnych nieposiadających osobowości prawnej: nazwę (firmę) przedstawiciela, adres siedziby, adres do korespondencji, numer telefonu oraz adres poczty elektronicznej;
- 18) informację o zawarciu przez podmiot kluczowy lub podmiot ważny porozumienia, o którym mowa w art. 8h ust. 6;
- 19) informację o uznaniu podmiotu kluczowego lub podmiotu ważnego za podmiot krytyczny;
- 20) wskazanie organu właściwego do spraw cyberbezpieczeństwa dla podmiotu kluczowego lub podmiotu ważnego;
- 21) wskazanie CSIRT sektorowego właściwego dla podmiotu kluczowego lub podmiotu ważnego;
- 22) wskazanie CSIRT MON, CSIRT NASK lub CSIRT GOV właściwego dla podmiotu kluczowego lub podmiotu ważnego;
- 23) numer w wykazie;
- 24) datę wpisu do wykazu;
- 25) podstawę prawną wpisania do wykazu;
- 26) datę wykreślenia z wykazu.

3. Do danych, o których mowa w ust. 2, nie stosuje się przepisów ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2022 r. poz. 902) oraz ustawy z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego (Dz. U. z 2023 r. poz. 1524).

4. Organ właściwy do spraw cyberbezpieczeństwa prowadzi wykaz podmiotów kluczowych i podmiotów ważnych w zakresie nadzorowanego sektora i w tym zakresie jest administratorem danych zawartych w wykazie.

5. Organ właściwy do spraw cyberbezpieczeństwa:

- 1) może wpisać podmiot do wykazu zgodnie z art. 7j i art. 7l ust. 6;
- 2) wykreśla podmiot z wykazu zgodnie z art. 7f ust. 2;
- 3) może dokonać czynności sprawdzających, o których mowa w art. 7k.

6. Minister właściwy do spraw informatyzacji zapewnia utrzymanie i rozwój systemu teleinformatycznego, o którym mowa w art. 46 ust. 1, za pomocą którego wykaz jest prowadzony.

7. Minister właściwy do spraw informatyzacji jest współadministratorem danych, w tym danych osobowych, gromadzonych w wykazie.

8. Minister właściwy do spraw informatyzacji podejmuje czynności, o których mowa w art. 7a, art. 7b ust. 1 i 2, art. 7d ust. 6, art. 7e, art. 7f ust. 1, art. 7g ust. 1 i 2, art. 7i oraz art. 7m.”;

14) po art. 7 dodaje się art. 7a–7m w brzmieniu:

„Art. 7a. 1. Dane, o których mowa w art. 7 ust. 2 pkt 19–26, uzupełnia minister właściwy do spraw informatyzacji.

2. W przypadku:

- 1) przedsiębiorców telekomunikacyjnych,
- 2) dostawców usług zaufania,
- 3) podmiotów publicznych,
- 4) podmiotów krytycznych

– minister właściwy do spraw informatyzacji wpisuje do wykazu dane, o których mowa w art. 7 ust. 2 pkt 1–8 oraz pkt 19–26, dotyczące tych podmiotów – na podstawie danych zawartych w rejestrach publicznych, bazie adresów elektronicznych lub przekazanych przez właściwe organy nadzorcze.

Art. 7b. 1. Zawiadomienie o wpisie do wykazu z urzędu minister właściwy do spraw informatyzacji doręcza podmiotom kluczowym lub podmiotom ważnym.

2. Minister właściwy do spraw informatyzacji wzywa podmioty kluczowe lub podmioty ważne, o których mowa w art. 7a ust. 2, do uzupełnienia brakujących danych w wykazie, w terminie 2 miesięcy od dnia doręczenia wezwania, pod rygorem nałożenia kary pieniężnej.

3. Wezwanie, o którym mowa w ust. 2, zawiera:

- 1) podstawę prawną wpisu do wykazu;
- 2) numer podmiotu w wykazie;
- 3) dane podmiotu wpisane do wykazu oraz wskazanie źródła ich pochodzenia;
- 4) wskazanie brakujących danych, które podmiot musi uzupełnić.

4. Podmioty kluczowe lub podmioty ważne, o których mowa w art. 7a ust. 2, uzupełniają dane w wykazie, składając wniosek o zmianę wpisu w tym wykazie, w tym

również uzupełniają dane w wykazie w zakresie ich działalności, która nie została objęta wpisem z urzędu.

5. Zawiadomienie o wpisie do wykazu z urzędu oraz wezwanie, o którym mowa w ust. 2, doręcza się w sposób określony w dziale I rozdziale 8 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (Dz. U. z 2024 r. poz. 572 oraz z 2025 r. poz. 769).

6. W przypadku przedsiębiorców telekomunikacyjnych zawiadomienie o wpisie do wykazu z urzędu oraz wezwanie, o którym mowa w ust. 2, może być doręczone za pomocą Platformy Usług Elektronicznych Urzędu Komunikacji Elektronicznej w ramach współpracy ministra właściwego do spraw informatyzacji z Prezesem Urzędu Komunikacji Elektronicznej.

7. Sprawy, o których mowa w ust. 1 i 2, mogą być załatwiane w sposób, o którym mowa w art. 14 § 1b ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego.

Art. 7c. 1. Podmiot kluczowy lub podmiot ważny składają wniosek o wpis do wykazu, w terminie 3 miesięcy od dnia spełnienia przesłanek uznania za podmiot kluczowy lub podmiot ważny.

2. Wniosek o wpis do wykazu zawiera dane, o których mowa w art. 7 ust. 2 pkt 1–18.

3. Podmiot kluczowy lub podmiot ważny składają wniosek o zmianę wpisu w wykazie w zakresie danych, o których mowa w art. 7 ust. 2 pkt 1–18, w terminie 14 dni od dnia ich zmiany.

4. Wniosek o zmianę wpisu w wykazie zawiera wskazanie zmienianych danych oraz numer podmiotu w tym wykazie.

5. Wniosek o wpis, zmianę wpisu albo o wykreślenie z wykazu zawiera oświadczenie kierownika podmiotu kluczowego lub podmiotu ważnego o następującej treści: „Świadomy odpowiedzialności karnej za złożenie fałszywego oświadczenia wynikającej z art. 233 § 6 Kodeksu karnego oświadczam, że dane zawarte we wniosku są zgodne z prawdą.”. Klauzula ta zastępuje pouczenie o odpowiedzialności karnej za złożenie fałszywego oświadczenia. Odpowiedzialność za złożenie fałszywego oświadczenia nie obejmuje podania zakresów adresów IP oraz zakresów nazw domenowych.

6. Wniosek o wpis, zmianę wpisu albo o wykreślenie z wykazu sporządza się w postaci elektronicznej i opatruje kwalifikowanym podpisem elektronicznym, podpisem zaufanym, podpisem osobistym kierownika podmiotu kluczowego lub podmiotu ważnego lub osoby przez niego upoważnionej albo kwalifikowaną pieczęcią elektroniczną ze wskazaniem w treści pisma osoby opatrującej pismo pieczęcią. Wniosek składa się w systemie teleinformatycznym, o którym mowa w art. 46 ust. 1.

7. W przypadku działania przez pełnomocnika do wniosku dołącza się pełnomocnictwo w postaci elektronicznej podpisane kwalifikowanym podpisem elektronicznym, podpisem zaufanym, podpisem osobistym albo kwalifikowaną pieczęcią elektroniczną. W przypadku pełnomocnika podmiotu ujawnionego w Centralnej Ewidencji i Informacji o Działalności Gospodarczej lub prokurenta ujawnionego w Krajowym Rejestrze Sądowym nie dołącza się pełnomocnictwa.

Art. 7d. 1. Wpis podmiotu do wykazu dokonuje się z chwilą złożenia wniosku w systemie teleinformatycznym, o którym mowa w art. 46 ust. 1.

2. Podmiot kluczowy lub podmiot ważny prowadzący kilka rodzajów działalności wykazują odrębnie te działalności we wniosku.

3. Wpisu do wykazu nie dokonuje się, jeżeli wniosek:

- 1) nie zawiera danych podlegających wpisowi zgodnie z art. 7 ust. 2 pkt 1–18;
- 2) dotyczy podmiotu kluczowego lub podmiotu ważnego już wpisanego do wykazu;
- 3) nie zawiera oświadczenia, o którym mowa w art. 7c ust. 5;
- 4) nie został podpisany.

4. Zmiany wpisu do wykazu nie dokonuje się, jeżeli wniosek o zmianę wpisu:

- 1) nie zawiera nazwy podmiotu oraz numeru podmiotu w wykazie;
- 2) nie zawiera wskazania danych zmienianych;
- 3) nie zawiera oświadczenia, o którym mowa w art. 7c ust. 5;
- 4) nie został podpisany.

5. Wpis, zmiana wpisu oraz wykreślenie wpisu z wykazu jest czynnością materialno-techniczną i ma charakter deklaratoryjny.

6. Minister właściwy do spraw informatyzacji wydaje, na żądanie podmiotu wpisanego do wykazu, zaświadczenie o wpisie podmiotu do wykazu albo o zmianie tego wpisu wraz ze wskazaniem aktualnych danych zawartych w wykazie dotyczących podmiotu.

7. Zaświadczenie, o którym mowa w ust. 6, jest wydawane w postaci dokumentu elektronicznego, opatrzonego kwalifikowaną pieczęcią elektroniczną, za pomocą systemu teleinformatycznego, o którym mowa w art. 46 ust. 1.

Art. 7e. Minister właściwy do spraw informatyzacji co najmniej raz w roku aktualizuje dane zawarte we wpisach w wykazie w zakresie nazwy podmiotu na podstawie danych pozyskanych z publicznie dostępnych rejestrów publicznych.

Art. 7f. 1. Minister właściwy do spraw informatyzacji wykreśla podmiot z wykazu, po uzyskaniu informacji o wykreśleniu podmiotu z krajowego rejestru urzędowego podmiotów gospodarki narodowej (REGON), Krajowego Rejestru Sądowego lub Centralnej Ewidencji i Informacji o Działalności Gospodarczej.

2. Organ właściwy do spraw cyberbezpieczeństwa wykreśla podmiot z wykazu, w zakresie nadzorowanego sektora, podsektora lub rodzaju działalności, jeżeli:

- 1) podmiot wpisany do wykazu nie jest podmiotem kluczowym albo podmiotem ważnym;
- 2) podmiot wpisany do wykazu utracił status podmiotu kluczowego albo podmiotu ważnego po wpisie do wykazu.

3. Podmiot kluczowy lub podmiot ważny składają za pomocą systemu teleinformatycznego, o którym mowa w art. 46 ust. 1, wniosek o wykreślenie z wykazu w zakresie sektora, podsektora lub rodzaju działalności, jeżeli przestały spełniać przesłanki uznania za podmiot kluczowy lub podmiot ważny w tym sektorze, podsektorze lub dla określonego rodzaju działalności. Wniosek o wykreślenie z wykazu zawiera uzasadnienie.

4. Organ właściwy do spraw cyberbezpieczeństwa rozpatruje wniosek w terminie miesiąca od dnia złożenia wniosku i informuje o wykreśleniu albo odmowie wykreślenia z wykazu.

5. Organ właściwy do spraw cyberbezpieczeństwa odmawia wykreślenia podmiotu z wykazu, jeżeli podmiot nadal spełnia przesłanki uznania za podmiot kluczowy lub podmiot ważny.

6. Odmowa wykreślenia jest inną czynnością z zakresu administracji publicznej, na którą przysługuje skarga do sądu administracyjnego i wymaga uzasadnienia.

7. Brak odmowy wykreślenia podmiotu z wykazu w terminie, o którym mowa w ust. 4, skutkuje wykreśleniem podmiotu z wykazu.

8. Wykreślenie podmiotu z wykazu jest inną czynnością z zakresu administracji publicznej, na którą przysługuje skarga do sądu administracyjnego.

Art. 7g. 1. Minister właściwy do spraw informatyzacji udostępnia dane, o których mowa w art. 7 ust. 2, CSIRT MON, CSIRT NASK i CSIRT GOV oraz CSIRT sektorowemu w zakresie sektora lub podsektora, dla którego został ustanowiony, organowi właściwemu do spraw cyberbezpieczeństwa w zakresie nadzorowanego sektora lub podsektora, a także podmiotowi kluczowemu lub podmiotowi ważnemu w zakresie go dotyczącym.

2. Minister właściwy do spraw informatyzacji udostępnia dane, o których mowa w art. 7 ust. 2, na wniosek, następującym podmiotom:

- 1) Agencji Bezpieczeństwa Wewnętrznego,
- 2) Agencji Wywiadu,
- 3) dyrektorowi Rządowego Centrum Bezpieczeństwa,
- 4) organom Krajowej Administracji Skarbowej,
- 5) Najwyższej Izbie Kontroli,
- 6) Policji,
- 7) Prezesowi Urzędu Lotnictwa Cywilnego,
- 8) Prezesowi Urzędu Ochrony Danych Osobowych,
- 9) Prezesowi Urzędu Transportu Kolejowego,
- 10) Prokuraturii Generalnej Rzeczypospolitej Polskiej,
- 11) prokuratorowi,
- 12) sądom,
- 13) Służbie Kontrwywiadu Wojskowego,
- 14) Służbie Ochrony Państwa,
- 15) Służbie Wywiadu Wojskowego,
- 16) Straży Granicznej,
- 17) Żandarmerii Wojskowej

– w zakresie niezbędnym do realizacji ich ustawowych zadań.

3. Udostępnianie danych, o których mowa w art. 7 ust. 2, odbywa się za pomocą systemu teleinformatycznego, o którym mowa w art. 46 ust. 1.

4. Informacja o zmianie wpisu w wykazie lub o wykreśleniu podmiotu z wykazu jest przechowywana w systemie teleinformatycznym, o którym mowa w art. 46 ust. 1, przez

5 lat od dokonania tej zmiany lub wykreślenia. W informacji wskazuje się datę i czas dokonania zmiany lub wykreślenia.

5. Dane administratora konta podmiotu w systemie teleinformatycznym, o którym mowa w art. 46 ust. 1, w tym numer PESEL lub niepowtarzalny identyfikator środka identyfikacji elektronicznej, o którym mowa w aktach wykonawczych Komisji Europejskiej, wydanych na podstawie art. 12 ust. 8 rozporządzenia 910/2014, są dostępne wyłącznie dla ministra właściwego do spraw informatyzacji lub jednostki podległej temu ministrowi albo przez niego nadzorowanej, której powierzył realizację zadania rozwoju lub utrzymania systemu. Przepis ten nie narusza uprawnień sądu i prokuratora w postępowaniu karnym.

Art. 7h. Informację o uznaniu podmiotu kluczowego lub podmiotu ważnego za podmiot krytyczny przekazuje ministrowi właściwemu do spraw informatyzacji dyrektor Rządowego Centrum Bezpieczeństwa.

Art. 7i. Minister właściwy do spraw informatyzacji udostępnia w portalu danych, o którym mowa w ustawie z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego, liczbę podmiotów kluczowych lub podmiotów ważnych w podziale na sektory, podsektory i rodzaj działalności. Dane te są aktualizowane nie rzadziej niż raz na kwartał.

Art. 7j. 1. Organ właściwy do spraw cyberbezpieczeństwa może wpisać podmiot do wykazu, jeżeli podmiot ten spełnia przesłanki uznania go za podmiot kluczowy albo podmiot ważny, oraz podmiot ten nie złożył wniosku w terminie, o którym mowa w art. 7c ust. 1.

2. Dokonując wpisu podmiotu do wykazu, organ właściwy do spraw cyberbezpieczeństwa korzysta z danych zawartych w publicznie dostępnych rejestrach publicznych, danych dostępnych organowi na podstawie przepisów odrębnych oraz informacji uzyskanych od podmiotu na podstawie art. 43 ust. 1.

3. Organ właściwy do spraw cyberbezpieczeństwa zawiadamia podmiot o wpisie do wykazu na podstawie ust. 1 oraz wzywa ten podmiot do uzupełnienia brakujących danych w wykazie, w terminie 2 miesięcy od dnia otrzymania zawiadomienia, pod rygorem nałożenia kary pieniężnej.

4. Zawiadomienie o wpisie do wykazu na podstawie ust. 1 oraz wezwanie, o którym mowa w ust. 3, doręcza się w sposób określony w dziale I rozdziale 8 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego.

5. Wpis do wykazu na podstawie ust. 1 jest inną czynnością z zakresu administracji publicznej, na którą przysługuje skarga do sądu administracyjnego, i wymaga uzasadnienia.

Art. 7k. 1. Organ właściwy do spraw cyberbezpieczeństwa może dokonywać czynności sprawdzających mających na celu weryfikację zgodności ze stanem faktycznym danych zawartych w wykazie.

2. W przypadku stwierdzenia, że dane w wykazie są niezgodne ze stanem faktycznym, organ właściwy do spraw cyberbezpieczeństwa wzywa podmiot do zmiany wpisu, w terminie 7 dni od dnia doręczenia wezwania, pod rygorem nałożenia kary pieniężnej. Do doręczenia wezwania stosuje się przepisy działu I rozdziału 8 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego.

3. Organ właściwy do spraw cyberbezpieczeństwa poprawia, z urzędu, oczywiste omyłki i błędy zawarte w wykazie.

Art. 7l. 1. Organ właściwy do spraw cyberbezpieczeństwa, w drodze decyzji, może uznać osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej za podmiot kluczowy lub podmiot ważny, która nie spełnia przesłanek określonych w art. 5 ust. 1 pkt 1–3, pkt 4 lit. a–d oraz g–j, ust. 2 pkt 1–5 oraz 7 i 8, ust. 3–11, jeżeli:

- 1) jest podmiotem określonym w załączniku nr 1 lub 2 do ustawy;
- 2) spełnia co najmniej jedną z poniższych przesłanek:
 - a) jako jedyna świadczy usługę, za pomocą systemu informacyjnego, która ma kluczowe znaczenie dla krytycznej działalności społecznej lub gospodarczej,
 - b) zakłócenie usługi świadczonej przez nią za pomocą systemu informacyjnego spowoduje poważne zagrożenie dla bezpieczeństwa państwa, bezpieczeństwa i porządku publicznego, obronności lub zdrowia publicznego,
 - c) zakłócenie usługi świadczonej przez nią za pomocą systemu informacyjnego spowoduje ryzyko systemowe zaprzestania świadczenia usług przez podmioty kluczowe lub podmioty ważne lub
 - d) świadczenie przez nią, za pomocą systemu informacyjnego, usługi ma istotne znaczenie na poziomie wojewódzkim lub krajowym lub ma znaczenie dla dwóch lub więcej sektorów określonych w załączniku nr 1 lub 2 do ustawy.

2. Podmiot uznaje się za:

- 1) podmiot kluczowy, jeżeli prowadzi działalność określoną w załączniku nr 1 do ustawy;
- 2) podmiot ważny, jeżeli prowadzi działalność określoną w załączniku nr 2 do ustawy.

3. W decyzji, o której mowa w ust. 1, organ właściwy do spraw cyberbezpieczeństwa:

- 1) określa sektor i podsektor, do którego został przypisany podmiot;
- 2) wzywa podmiot do uzupełnienia brakujących danych w wykazie, w terminie 2 miesięcy od dnia doręczenia decyzji, pod rygorem nałożenia kary pieniężnej.

4. Do wezwania do uzupełnienia brakujących danych w wykazie stosuje się przepis art. 7b ust. 3.

5. Decyzja, o której mowa w ust. 1, podlega natychmiastowemu wykonaniu.

6. Organ właściwy do spraw cyberbezpieczeństwa niezwłocznie wpisuje do wykazu podmiot, wobec którego wydano decyzję, o której mowa w ust. 1.

7. Podmiot, wobec którego wydano decyzję, o której mowa w ust. 1:

- 1) realizuje obowiązki, o których mowa w rozdziale 3, w terminie 12 miesięcy,
- 2) zapewnia przeprowadzenie po raz pierwszy audytu, o którym mowa w art. 15 ust. 1, w terminie 24 miesięcy

– od dnia doręczenia tej decyzji.

Art. 7m. 1. Minister właściwy do spraw informatyzacji może uznać, w drodze decyzji, państwową osobę prawną, o której mowa w art. 3 ust. 1 ustawy z dnia 16 grudnia 2016 r. o zasadach zarządzania mieniem państwowym (Dz. U. z 2024 r. poz. 125, 834, 1823, 1897 i 1940), za podmiot kluczowy w sektorze podmiotów publicznych, jeżeli realizuje, za pomocą systemu informacyjnego, zadanie publiczne:

- 1) którego zakłócenie spowoduje poważne zagrożenie dla bezpieczeństwa państwa, bezpieczeństwa i porządku publicznego, obronności lub zdrowia publicznego lub
- 2) które ma istotne znaczenie na poziomie krajowym.

2. Decyzja, o której mowa w ust. 1, podlega natychmiastowemu wykonaniu.

3. Minister właściwy do spraw informatyzacji wzywa państwową osobę prawną, wobec której wydano decyzję, o której mowa w ust. 1, do uzupełnienia brakujących danych w wykazie, w terminie 2 miesięcy od dnia doręczenia decyzji, o której mowa w ust. 1, pod rygorem nałożenia kary pieniężnej.

4. Do wezwania do uzupełnienia brakujących danych w wykazie, o którym mowa w ust. 3, stosuje się przepis art. 7b ust. 3.

5. Minister właściwy do spraw informatyzacji niezwłocznie wpisuje do wykazu państwową osobę prawną, wobec której wydano decyzję, o której mowa w ust. 1.

6. Państwowa osoba prawna, wobec której wydano decyzję, o której mowa w ust. 1:

- 1) realizuje obowiązki, o których mowa w rozdziale 3, w terminie 6 miesięcy,
- 2) zapewnia przeprowadzenie po raz pierwszy audytu, o którym mowa w art. 15 ust. 1, w terminie 24 miesięcy

– od dnia doręczenia tej decyzji.”;

15) tytuł rozdziału 3 otrzymuje brzmienie:

„Obowiązki podmiotów kluczowych lub podmiotów ważnych”;

16) art. 8 otrzymuje brzmienie:

„Art. 8. 1. Podmiot kluczowy lub podmiot ważny wdraża system zarządzania bezpieczeństwem informacji w systemie informacyjnym wykorzystywanym w procesach wpływających na świadczenie usługi przez ten podmiot, zapewniający:

- 1) prowadzenie systematycznego szacowania ryzyka wystąpienia incydentu oraz zarządzanie tym ryzykiem;
- 2) wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, uwzględniających najnowszy stan wiedzy, koszty wdrożenia, wielkość podmiotu, prawdopodobieństwo wystąpienia incydentów, narażenie podmiotu na ryzyka, skutki społeczne i gospodarcze, w szczególności:
 - a) polityki szacowania ryzyka oraz bezpieczeństwa systemu informacyjnego, w tym polityki tematyczne,
 - b) bezpieczeństwo w procesie nabywania, rozwoju, utrzymania i eksploatacji systemu informacyjnego, w tym testowanie systemu informacyjnego,
 - c) bezpieczeństwo fizyczne i środowiskowe uwzględniające kontrole dostępu,
 - d) bezpieczeństwo zasobów ludzkich,
 - e) bezpieczeństwo i ciągłość łańcucha dostaw produktów ICT, usług ICT i procesów ICT, od których zależy świadczenie usługi, z uwzględnieniem związków pomiędzy bezpośrednim dostawcą sprzętu lub oprogramowania a podmiotem kluczowym lub podmiotem ważnym,
 - f) wdrażanie, dokumentowanie, testowanie i utrzymywanie planów ciągłości działania umożliwiających ciągłe i niezakłócone świadczenie usługi oraz

zapewniających poufność, integralność, dostępność i autentyczność informacji, planów awaryjnych oraz planów odtworzenia działalności umożliwiających odtworzenie systemu informacyjnego po zdarzeniu, które spowodowało straty przekraczające zdolności podmiotu do odbudowy za pomocą własnych środków,

- g) objęcie systemu informacyjnego wykorzystywanego do świadczenia usługi systemem monitorowania w trybie ciągłym,
 - h) polityki i procedury oceny skuteczności środków technicznych i organizacyjnych,
 - i) edukację z zakresu cyberbezpieczeństwa dla personelu podmiotu,
 - j) podstawowe zasady cyberhigieny,
 - k) polityki i procedury stosowania kryptografii, w tym w stosownych przypadkach szyfrowania,
 - l) stosowanie bezpiecznych środków komunikacji elektronicznej w ramach krajowego systemu cyberbezpieczeństwa oraz wewnątrz podmiotu, uwzględniających uwierzytelnianie wieloskładnikowe w stosownych przypadkach,
 - m) zarządzanie aktywami,
 - n) polityki kontroli dostępu;
- 3) zbieranie informacji o cyberzagrożeniach i podatnościach na incydenty systemu informacyjnego wykorzystywanego do świadczenia usługi;
- 4) zarządzanie incydentami;
- 5) stosowanie środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego wykorzystywanego do świadczenia usługi, w tym:
- a) stosowanie mechanizmów zapewniających poufność, integralność, dostępność i autentyczność danych przetwarzanych w systemie informacyjnym,
 - b) regularne przeprowadzanie aktualizacji oprogramowania, stosownie do zaleceń producenta, z uwzględnieniem analizy wpływu aktualizacji na bezpieczeństwo świadczonej usługi oraz poziomu krytyczności poszczególnych aktualizacji,
 - c) ochronę przed nieuprawnioną modyfikacją w systemie informacyjnym,
 - d) niezwłoczne podejmowanie działań po dostrzeżeniu podatności lub cyberzagrożeń, w tym również czasowe ograniczenie ruchu sieciowego

przychodzącego do infrastruktury podmiotu kluczowego lub podmiotu ważnego, które może skutkować zakłóceniem usług świadczonych przez ten podmiot, z uwzględnieniem konieczności minimalizacji skutków ograniczenia dostępności tych usług, z uwagi na podjęte działania.

2. Wdrażając środki, o których mowa w ust. 1 pkt 2 lit. e, podmiot kluczowy lub podmiot ważny uwzględnia:

- 1) podatności związane z dostawcą sprzętu lub oprogramowania;
- 2) ogólną jakość produktów ICT, usług ICT i procesów ICT pochodzących od dostawcy sprzętu lub oprogramowania;
- 3) wyniki skoordynowanej oceny bezpieczeństwa przeprowadzonej przez Grupę Współpracy, o której mowa w art. 22 ust. 1 dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniającej rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającą dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz. Urz. UE L 333 z 27.12.2022, str. 80), zwanej dalej „dyrektywą 2022/2555”;
- 4) wyniki postępowania, o którym mowa w art. 67b.

3. Podmiot ważny będący podmiotem publicznym nie stosuje przepisu ust. 1. Podmiot ważny będący podmiotem publicznym opracowuje, wdraża, realizuje, monitoruje i utrzymuje w systemach informacyjnych kontrolowanych przez ten podmiot system zarządzania bezpieczeństwem informacji spełniający wymogi określone w załączniku nr 4 do ustawy.

4. Podmiot publiczny uwzględnia w systemie zarządzania bezpieczeństwem informacji system informacyjny dostarczany przez inny podmiot publiczny, w tym na podstawie przepisów ustawy, w szczególności system informacyjny zapewniający działanie rejestru publicznego w zakresie odpowiadającym zakresowi kompetencji tego podmiotu, wynikającym z polityki bezpieczeństwa danego systemu informacyjnego lub przepisów prawa regulujących sposób działania tego systemu.”;

- 17) po art. 8 dodaje się art. 8a–8j w brzmieniu:

„Art. 8a. Rada Ministrów może określić, w drodze rozporządzenia, odrębnie dla danego rodzaju działalności wykonywanej przez podmioty kluczowe lub podmioty ważne, szczegółowe wymagania dla systemu zarządzania bezpieczeństwem informacji, o którym mowa w art. 8 ust. 1, biorąc pod uwagę rekomendacje międzynarodowe

o charakterze specjalistycznym, w tym rekomendacje Agencji Unii Europejskiej do spraw Cyberbezpieczeństwa, zwanej dalej „ENISA”, wielkość podmiotu, skalę działalności wykonywanej przez te podmioty oraz potrzebę podejmowania przez te podmioty działań zapewniających cyberbezpieczeństwo.

Art. 8b. 1. Dostawcy usług DNS, rejestry nazw domen najwyższego poziomu (TLD), dostawcy usług chmurowych, dostawcy usługi centrum przetwarzania danych, dostawcy sieci dostarczania treści, dostawcy usług zarządzanych, dostawcy usług zarządzanych w zakresie cyberbezpieczeństwa, dostawcy internetowych platform handlowych, dostawcy wyszukiwarek internetowych oraz dostawcy platform usług sieci społecznościowych stosują, w ramach systemu, o którym mowa w art. 8 ust. 1, środki zarządzania ryzykiem określone w rozporządzeniu wykonawczym Komisji (UE) 2024/2690 z dnia 17 października 2024 r. ustanawiającym zasady stosowania dyrektywy (UE) 2022/2555 w odniesieniu do wymogów technicznych i metodycznych dotyczących środków zarządzania ryzykiem w cyberbezpieczeństwie oraz doprecyzowujące przypadki, w których incydent uznaje się za poważny w odniesieniu do dostawców usług DNS, rejestrów nazw TLD, dostawców usług chmurowych, dostawców usług ośrodka przetwarzania danych, dostawców sieci dostarczania treści, dostawców usług zarządzanych, dostawców usług zarządzanych w zakresie bezpieczeństwa, dostawców internetowych platform handlowych, wyszukiwarek internetowych i platform usług sieci społecznościowych oraz dostawców usług zaufania (Dz. Urz. UE L 2024/2690 z 18.10.2024, z późn. zm.¹⁰⁾).

2. W ramach systemu, o którym mowa w art. 8 ust. 1, podmioty kluczowe lub podmioty ważne, inne niż określone w ust. 1, stosują środki zarządzania ryzykiem dla danego rodzaju podmiotu określone w aktach wykonawczych Komisji Europejskiej, wydanych na podstawie art. 21 ust. 5 dyrektywy 2022/2555.

3. Podmioty kluczowe lub podmioty ważne z podsektora energii elektrycznej, uznane za podmiot o dużym wpływie lub podmiot o krytycznym wpływie, o którym mowa w art. 52a ust. 2, dodatkowo stosują środki określone w rozporządzeniu delegowanym Komisji (UE) 2024/1366 z dnia 11 marca 2024 r. uzupełniającym rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/943 poprzez ustanowienie kodeksu sieci dotyczącego zasad sektorowych w zakresie aspektów cyberbezpieczeństwa

¹⁰⁾ Zmiana wymienionego rozporządzenia została ogłoszona w Dz. Urz. UE L 2024/90225 z 12.03.2025.

w transgranicznych przepływach energii elektrycznej (Dz. Urz. UE L 2024/1366 z 24.05.2024, z późn. zm.¹¹⁾), zwanym dalej „rozporządzeniem 2024/1366”.

Art. 8c. 1. Kierownik podmiotu kluczowego lub podmiotu ważnego ponosi odpowiedzialność za wykonywanie obowiązków w zakresie cyberbezpieczeństwa przez podmiot kluczowy lub podmiot ważny, o których mowa w art. 7b ust. 4, art. 7c, art. 7f ust. 3, art. 8, art. 8d, art. 8e, art. 8f ust. 1 i 2, art. 9–12b, art. 14 i art. 15.

2. W przypadku gdy kierownikiem podmiotu kluczowego lub podmiotu ważnego jest organ wieloosobowy i nie została wskazana osoba odpowiedzialna, odpowiedzialność ponoszą wszyscy członkowie tego organu.

3. Kierownik podmiotu kluczowego lub podmiotu ważnego ponosi odpowiedzialność także wtedy, gdy niektóre z obowiązków albo wszystkie obowiązki zostały powierzone innej osobie za jej zgodą.

Art. 8d. Kierownik podmiotu kluczowego lub podmiotu ważnego:

- 1) podejmuje decyzje w zakresie przygotowania, wdrażania, stosowania, przeglądu i nadzoru systemu zarządzania bezpieczeństwem informacji w podmiocie;
- 2) planuje adekwatne środki finansowe na realizację obowiązków z zakresu cyberbezpieczeństwa;
- 3) przydziela zadania z zakresu cyberbezpieczeństwa w tym podmiocie i nadzoruje ich wykonanie;
- 4) zapewnia, że personel podmiotu jest świadomy obowiązków z zakresu cyberbezpieczeństwa i zna wewnętrzne regulacje podmiotu w tym zakresie;
- 5) zapewnia zgodność działania tego podmiotu z przepisami prawa oraz z wewnętrznymi regulacjami podmiotu.

Art. 8e. 1. Kierownik podmiotu kluczowego lub podmiotu ważnego oraz osoba, której powierzono obowiązki kierownika w zakresie cyberbezpieczeństwa, raz w roku kalendarzowym przechodzi szkolenie.

2. Zakres szkolenia obejmuje wykonywania obowiązków, o których mowa w art. 7b ust. 4, art. 7c, art. 7f ust. 3, art. 8, art. 8d, art. 8f ust. 1 i 2, art. 9–12b, art. 14 i art. 15.

3. Udział w szkoleniu jest udokumentowany.

Art. 8f. 1. Przed rozpoczęciem realizacji zadań, o których mowa w art. 8 lub art. 11, osoba przedstawia podmiotowi kluczowemu lub podmiotowi ważnemu informację

¹¹⁾ Zmiana wymienionego rozporządzenia została ogłoszona w Dz. Urz. UE L 2024/90558 z 16.09.2024.

o osobie z Krajowego Rejestru Karnego stwierdzającą niekaralność za przestępstwa przeciwko ochronie informacji. Kierownik podmiotu kluczowego lub podmiotu ważnego dopuszcza osobę do realizacji zadań, o których mowa w art. 8 lub art. 11, po otrzymaniu informacji, o której mowa w zdaniu pierwszym.

2. Podmiot kluczowy lub podmiot ważny wzywa osobę realizującą zadania, o których mowa w art. 8 lub art. 11, do ponownego przedstawienia informacji o osobie z Krajowego Rejestru Karnego, jeżeli poweźmie uzasadnione podejrzenie, że osoba ta została skazana za przestępstwo przeciwko ochronie informacji.

3. Wymagania, o których mowa w ust. 1 i 2, uznaje się za spełnione, jeżeli osoba realizująca zadania, o których mowa w art. 8 i art. 11, posiada ważne poświadczenie bezpieczeństwa upoważniające do dostępu do informacji niejawnych o klauzuli „poufne” lub wyższej.

4. Osoba skazana prawomocnym wyrokiem sądu za przestępstwa przeciwko ochronie informacji nie może realizować zadań, o których mowa w art. 8 lub art. 11.

Art. 8g. Podmiot kluczowy będący dostawcą usług zarządzanych w zakresie cyberbezpieczeństwa świadczącym usługę obsługi incydentów udostępnia na swojej stronie internetowej co najmniej następujące informacje na temat swojej działalności:

- 1) nazwę (firmę);
- 2) zakres działania, w tym:
 - a) oferowany rodzaj wsparcia,
 - b) zasady współpracy i wymiany informacji,
 - c) politykę komunikacji;
- 3) oferowane usługi oraz politykę obsługi incydentów i koordynacji incydentów;
- 4) dane kontaktowe, w tym:
 - a) adres ze wskazaniem strefy czasowej,
 - b) numer telefonu, adres poczty elektronicznej oraz wskazanie innych dostępnych środków komunikacji elektronicznej z dostawcą,
 - c) dane o wykorzystywanych kluczach publicznych i sposobach szyfrowania komunikacji z dostawcą,
 - d) sposoby kontaktu z dostawcą, w tym sposób zgłaszania incydentów.

Art. 8h. 1. Podmioty kluczowe, podmioty ważne, CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT sektorowy, dostawcy sprzętu lub oprogramowania dla tych podmiotów lub organizacje społeczne zrzeszające podmioty kluczowe lub podmioty

ważne mogą wymieniać między sobą informacje dotyczące cyberbezpieczeństwa, w tym informacje o cyberzagrożeniach, potencjalnych zdarzeniach dla cyberbezpieczeństwa, podatnościach, technikach i procedurach, oznakach naruszenia integralności systemu informacyjnego, wrogich taktykach, a także informacje o grupach przestępczych, ostrzeżenia dotyczące cyberbezpieczeństwa i zalecenia dotyczące konfiguracji narzędzi bezpieczeństwa mających wykrywać cyberataki.

2. Wymiana informacji, ostrzeżeń i zaleceń, o których mowa w ust. 1, jest dopuszczalna, jeżeli:

- 1) ma na celu zapobieganie incyidentom, ich wykrywanie, reagowanie na nie, przywracanie normalnego działania po incyidentach lub łagodzenie ich skutków lub
- 2) zwiększa poziom cyberbezpieczeństwa, w szczególności przez podnoszenie świadomości na temat cyberzagrożeń, ograniczanie lub utrudnianie ich rozprzestrzeniania się, eliminowanie i ujawnianie podatności, techniki wykrywania cyberzagrożeń, ograniczania ich zasięgu i zapobiegania im, strategie ograniczania ryzyka, etapy reagowania i przywracania normalnego działania lub sprzyjanie współpracy między podmiotami publicznymi i prywatnymi w badaniach nad cyberzagrożeniami.

3. Wymiana informacji, ostrzeżeń i zaleceń, o których mowa w ust. 1, odbywa się za pomocą systemu teleinformatycznego, o którym mowa w art. 46 ust. 1, systemów teleinformatycznych zapewnianych przez organy właściwe do spraw cyberbezpieczeństwa lub w drodze porozumień, o których mowa w ust. 6.

4. Wymieniając informacje, o których mowa w ust. 1, podmioty kluczowe lub podmioty ważne oznaczają zakres odbiorców tych informacji. Odbiorca informacji może ją udostępniać w zakresie określonym przez wytwórcę informacji.

5. Wymieniając informacje, o których mowa w ust. 1, za pomocą systemu teleinformatycznego, o którym mowa w art. 46 w ust. 1, nie przekazuje się danych osobowych.

6. Podmioty kluczowe, podmioty ważne, CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT sektorowy, dostawcy sprzętu lub oprogramowania dla tych podmiotów lub organizacje społeczne zrzeszające podmioty kluczowe lub podmioty ważne mogą zawierać porozumienia w sprawie wymiany informacji, o których mowa w ust. 1, w szczególności określając sposób wymiany informacji i zachowania informacji w poufności pomiędzy stronami porozumienia.

7. Koszty wykonania porozumień, o których mowa w ust. 6, są ponoszone w równych częściach przez wszystkie strony, chyba że w danym porozumieniu postanowiono inaczej.

Art. 8i. 1. Do podmiotów kluczowych lub podmiotów ważnych z sektora bankowości i infrastruktury rynków finansowych nie stosuje się przepisów ustawy dotyczących systemu zarządzania bezpieczeństwem informacji lub zgłaszania poważnych incydentów, z wyjątkiem art. 3a, art. 5 ust. 1–3, art. 7–7m, art. 8 ust. 1 pkt 1 i pkt 2 lit. j, art. 8h, art. 9, art. 11 ust. 1 pkt 5 i 6, art. 13, art. 16, art. 26a ust. 2–4, art. 32, art. 33 ust. 5, 7 i 8, art. 36a, art. 36b, art. 37, art. 43, art. 45 ust. 3, art. 46 ust. 1 pkt 1, 2, 4–7 i ust. 4–6, art. 67a, art. 67c, art. 67d oraz art. 67g–67i.

2. Do podmiotów kluczowych lub podmiotów ważnych z sektora bankowości i infrastruktury rynków finansowych stosuje się odpowiednio przepisy art. 8c–8f, art. 12 ust. 7 oraz art. 31 ust. 1.

3. Do podmiotów kluczowych lub podmiotów ważnych z sektora bankowości i infrastruktury rynków finansowych stosuje się przepisy rozdziałów 11 i 14 ustawy w zakresie art. 3a, art. 5 ust. 1–3, art. 7–7m, art. 8 ust. 1 pkt 1 i pkt 2 lit. j, art. 8h, art. 9, art. 11 ust. 1 pkt 5 i 6, art. 13, art. 15, art. 16, art. 26a ust. 2–4, art. 32, art. 33 ust. 5, 7 i 8, art. 36a, art. 36b, art. 37, art. 43, art. 45 ust. 3, art. 46 ust. 1 pkt 1, 2, 4–7 i ust. 4–6, art. 67a, art. 67c, art. 67d, art. 67g–67i oraz stosowanych odpowiednio przepisów art. 8c–8f, art. 12 ust. 7 oraz art. 31 ust. 1.

Art. 8j. Służby specjalne mogą stosować środki zapobiegające i ograniczające wpływ incydentów na bezpieczeństwo systemu informacyjnego wykorzystywanego do realizacji zadań w tym niezwłocznie podejmować działania po dostrzeżeniu podatności lub cyberzagrożeń, w tym również dokonywać czasowego ograniczenia ruchu sieciowego przychodzącego do infrastruktury służb specjalnych, który może skutkować zakłóceniem realizacji zadań służb specjalnych, mając na uwadze konieczność minimalizacji skutków ograniczenia możliwości realizacji tych działań.”;

18) art. 9 i art. 10 otrzymują brzmienie:

„Art. 9. 1. Podmiot kluczowy lub podmiot ważny:

- 1) wyznacza co najmniej dwie osoby odpowiedzialne za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa;
- 2) zapewnia użytkownikowi usługi dostępu do wiedzy pozwalającej na zrozumienie cyberzagrożeń i stosowanie skutecznych sposobów zabezpieczania się przed tymi

- zagrożeniami w zakresie związanym ze świadczonymi usługami, w szczególności przez udostępnianie informacji na ten temat na swojej stronie internetowej;
- 3) zapewnia użytkownikowi usługi możliwość zgłoszenia cyberzagrożenia, incydentu lub podatności związanych ze świadczoną usługą;
 - 4) po uzyskaniu wpisu podmiotu do wykazu rozpoczyna korzystanie z systemu teleinformatycznego, o którym mowa w art. 46 ust. 1.

2. Podmiot kluczowy lub podmiot ważny będący mikro- lub małym przedsiębiorcą, o którym mowa w art. 2 ust. 1 załącznika I do rozporządzenia 651/2014/UE, wyznacza co najmniej jedną osobę odpowiedzialną za utrzymywanie kontaktów z innymi podmiotami kluczowymi lub podmiotami ważnymi.

3. Podmiot ważny będący podmiotem publicznym wyznacza co najmniej jedną osobę odpowiedzialną za utrzymywanie kontaktów z innymi podmiotami kluczowymi lub podmiotami ważnymi.

4. Obowiązek, o którym mowa w ust. 1 pkt 2, może być zrealizowany przez zamieszczenie na stronie internetowej podmiotu hiperłącza do stron internetowych organu właściwego do spraw cyberbezpieczeństwa, CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT sektorowego.

Art. 10. 1. Podmiot kluczowy lub podmiot ważny opracowuje, stosuje i aktualizuje dokumentację dotyczącą bezpieczeństwa systemu informacyjnego wykorzystywanego w procesie świadczenia usługi.

2. Do dokumentacji dotyczącej bezpieczeństwa systemu informacyjnego wykorzystywanego w procesie świadczenia usługi, o której mowa w ust. 1, zalicza się:

- 1) dokumentację normatywną;
- 2) dokumentację operacyjną.

3. Dokumentację normatywną stanowią:

- 1) dokumentacja systemu zarządzania bezpieczeństwem informacji;
- 2) dokumentacja ochrony infrastruktury, z wykorzystaniem której jest świadczona usługa, obejmująca:
 - a) charakterystykę usługi oraz infrastruktury, w której świadczona jest usługa,
 - b) ocenę aktualnego stanu ochrony infrastruktury,
 - c) szacowanie ryzyka dla obiektów infrastruktury,
 - d) plan postępowania z ryzykiem,
 - e) opis zabezpieczeń technicznych obiektów infrastruktury,

- f) zasady organizacji i wykonywania ochrony fizycznej infrastruktury,
 - g) dane o specjalistycznej uzbrojonej formacji ochronnej, o której mowa w art. 2 pkt 7 ustawy z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz. U. z 2025 r. poz. 532), chroniącej infrastrukturę – jeżeli występuje;
- 3) dokumentacja systemu zarządzania ciągłością działania;
 - 4) dokumentacja techniczna systemu informacyjnego wykorzystywanego w procesie świadczenia usługi;
 - 5) dokumentacja wynikająca ze specyfiki świadczonej usługi w danym sektorze lub podsektorze.

4. Dokumentację operacyjną stanowią zapisy poświadczające wykonywanie czynności wymaganych przez postanowienia zawarte w dokumentacji normatywnej, w tym automatycznie generowane zapisy w dziennikach systemów informacyjnych.

5. Dokumentacja dotycząca bezpieczeństwa systemu informacyjnego wykorzystywanego w procesie świadczenia usługi może być prowadzona w postaci papierowej lub w postaci elektronicznej.

6. Podmiot kluczowy lub podmiot ważny jest obowiązany do ustanowienia nadzoru nad dokumentacją dotyczącą bezpieczeństwa systemu informacyjnego wykorzystywanego w procesie świadczenia usługi, zapewniającego:

- 1) dostępność dokumentów wyłącznie dla osób upoważnionych, zgodnie z realizowanymi przez nie zadaniami;
- 2) ochronę dokumentów przed uszkodzeniem, zniszczeniem, utratą, nieuprawnionym dostępem, niewłaściwym użyciem lub utratą integralności;
- 3) oznaczanie kolejnych wersji dokumentów umożliwiające określenie zmian dokonanych w tych dokumentach.

7. Podmiot kluczowy lub podmiot ważny przechowuje dokumentację dotyczącą bezpieczeństwa systemu informacyjnego wykorzystywanego w procesie świadczenia usługi przez okres co najmniej 2 lat od dnia jej wycofania z użytkowania lub zakończenia świadczenia usługi, liczony od dnia 1 stycznia roku następującego po roku, w którym wygasa okres jej przechowywania. Przepisu nie stosuje się do podmiotów podlegających ustawie z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz. U. z 2020 r. poz. 164 oraz z 2025 r. poz. 1173).

8. Zniszczenie wycofanej z użytkowania dokumentacji dotyczącej bezpieczeństwa systemu informacyjnego wykorzystywanego w procesie świadczenia usługi potwierdza

się protokołem brakowania zawierającym w szczególności: datę protokołu, oznaczenie niszczonej dokumentacji, opis sposobu zniszczenia, dane osoby zatwierdzającej protokół. Protokoły brakowania dokumentacji dotyczącej bezpieczeństwa systemu informacyjnego wykorzystywanego w procesie świadczenia usługi są przechowywane w sposób trwały.”;

19) w art. 11:

a) w ust. 1:

- wprowadzenie do wyliczenia otrzymuje brzmienie:
„Podmiot kluczowy lub podmiot ważny:”,
- pkt 2 otrzymuje brzmienie:
„2) zapewnia dostęp do informacji o rejestrowanych incydentach właściwemu CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT sektorowemu w zakresie niezbędnym do realizacji jego zadań;”,
- pkt 4 otrzymuje brzmienie:
„4) zgłasza wczesne ostrzeżenie o incydencie poważnym niezwłocznie, nie później niż w ciągu 24 godzin od momentu jego wykrycia, do właściwego CSIRT sektorowego;”,
- po pkt 4 dodaje się pkt 4a–4c w brzmieniu:
„4a) zgłasza incydent poważny niezwłocznie, nie później niż w ciągu 72 godzin od momentu jego wykrycia, do właściwego CSIRT sektorowego;
4b) przekazuje, na wniosek właściwego CSIRT sektorowego, sprawozdanie okresowe z obsługi incydentu poważnego;
4c) przekazuje właściwemu CSIRT sektorowemu sprawozdanie końcowe z obsługi incydentu poważnego, nie później niż w ciągu miesiąca od dnia zgłoszenia, o którym mowa w pkt 4a;”,
- pkt 5 otrzymuje brzmienie:
„5) współdziała podczas obsługi incydentu poważnego i incydentu krytycznego z właściwym CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT sektorowym, przekazując niezbędne dane, w tym dane osobowe;”,

b) po ust. 1 dodaje się ust. 1a w brzmieniu:

„1a. Dostawca usług zaufania zgłasza incydent poważny niezwłocznie, nie później niż w ciągu 24 godzin od momentu jego wykrycia do właściwego CSIRT sektorowego.”,

- c) ust. 2 otrzymuje brzmienie:

„2. Wczesne ostrzeżenie, o którym mowa w ust. 1 pkt 4, zgłoszenie, o którym mowa w ust. 1 pkt 4a, sprawozdanie okresowe, o którym mowa w ust. 1 pkt 4b, sprawozdanie końcowe, o którym mowa w ust. 1 pkt 4c, oraz sprawozdanie z postępu obsługi incydentu poważnego, o którym mowa w art. 12b ust. 1, są przekazywane za pomocą systemu teleinformatycznego, o którym mowa w art. 46 ust. 1.”,

- d) po ust. 2 dodaje się ust. 2a i 2b w brzmieniu:

„2a. W przypadku zaistnienia poważnego cyberzagrożenia podmiot kluczowy lub podmiot ważny informuje użytkowników swoich usług, na których takie cyberzagrożenie może mieć wpływ, o możliwych środkach zapobiegawczych, które użytkownicy ci mogą podjąć. Podmiot kluczowy lub podmiot ważny informuje tych użytkowników o samym poważnym cyberzagrożeniu, jeżeli nie spowoduje to zwiększenia poziomu ryzyka dla bezpieczeństwa systemów informacyjnych.

2b. Podmiot kluczowy lub podmiot ważny informuje użytkowników swoich usług o incydencie poważnym, jeżeli ma on niekorzystny wpływ na świadczenie tych usług.”,

- e) uchyla się ust. 3,

- f) ust. 4 otrzymuje brzmienie:

„4. Rada Ministrów określi, w drodze rozporządzenia, progi uznania incydentu za poważny według rodzaju zdarzenia w poszczególnych sektorach i podsektorach określonych w załącznikach nr 1 i 2 do ustawy, z wyłączeniem progów uznania incydentu za poważny, dla podmiotów, dla których progi te określiła Komisja Europejska w akcie wykonawczym wydanym na podstawie art. 23 ust. 11 dyrektywy 2022/2555, wskazując w zależności od rodzaju zdarzenia czy odnosi się ono do:

- 1) liczby użytkowników, których dotyczy zakłócenie świadczenia usługi,
- 2) czasu oddziaływania incydentu na świadczoną usługę,
- 3) zasięgu geograficznego obszaru, którego dotyczy incydent,
- 4) innych czynników charakterystycznych dla danego sektora lub podsektora, jeżeli występują

– kierując się potrzebą zapewnienia ochrony przed zagrożeniem życia lub zdrowia ludzi, znacznymi stratami majątkowymi oraz obniżeniem jakości świadczonej usługi.”;

20) art. 12 otrzymuje brzmienie:

„Art. 12. 1. Wczesne ostrzeżenie, o którym mowa w art. 11 ust. 1 pkt 4, zawiera:

- 1) dane podmiotu zgłaszającego, w tym firmę przedsiębiorcy, numer z właściwego rejestru, siedzibę i adres;
- 2) imię i nazwisko, numer telefonu służbowego oraz adres służbowej poczty elektronicznej osoby dokonującej zgłoszenia;
- 3) imię i nazwisko, numer telefonu służbowego oraz adres służbowej poczty elektronicznej osoby uprawnionej do składania wyjaśnień dotyczących zgłaszanych informacji;
- 4) wskazanie momentu wystąpienia i wykrycia incydentu poważnego oraz czas jego trwania;
- 5) wskazanie, czy incydent poważny został wywołany działaniem bezprawnym lub działaniem w złej wierze, jeżeli możliwe jest dokonanie takiej oceny;
- 6) określenie, czy incydent dotyczy innych państw członkowskich Unii Europejskiej.

2. Wczesne ostrzeżenie, o którym mowa w art. 11 ust. 1 pkt 4, może zawierać wnioski o wskazanie wytycznych dotyczących możliwych do wdrożenia środków ograniczających skutki incydentu poważnego lub o dodatkowe wsparcie techniczne przy obsłudze incydentu. CSIRT sektorowy nie później niż w ciągu 24 godzin przekazuje podmiotowi zgłaszającemu wytyczne dotyczące wdrożenia środków lub udziela dodatkowego wsparcia technicznego, a w przypadku incydentu poważnego wyczerpującego znamiona przestępstwa również informacje o sposobie zgłoszenia organom ścigania.

3. Zgłoszenie, o którym mowa w art. 11 ust. 1 pkt 4a, zawiera:

- 1) opis wpływu incydentu poważnego na świadczenie usługi, w tym:
 - a) wskazanie usługi zgłaszającego, na którą incydent poważny miał wpływ,
 - b) liczbę użytkowników usługi, na których incydent poważny miał wpływ,
 - c) zasięg geograficzny obszaru, którego dotyczy incydent poważny,
 - d) wpływ incydentu poważnego na świadczenie usługi przez inne podmioty;
- 2) opis przyczyn tego incydentu, sposób jego przebiegu oraz prawdopodobne skutki oddziaływania na systemy informacyjne lub świadczone usługi;
- 3) informacje o podjętych działaniach zapobiegawczych;
- 4) informacje o podjętych działaniach naprawczych;
- 5) aktualizację informacji, o których mowa w ust. 1, jeżeli nastąpiła ich zmiana.

4. Zgłoszenie, o którym mowa w art. 11 ust. 1 pkt 4a, może zawierać także inne istotne informacje związane z przebiegiem incydentu poważnego lub podjętymi działaniami.

5. Podmiot kluczowy lub podmiot ważny przekazuje informacje znane mu w chwili dokonywania zgłoszenia, o którym mowa w art. 11 ust. 1 pkt 4a, które uzupełnia w trakcie obsługi incydentu poważnego.

6. Podmiot kluczowy lub podmiot ważny przekazuje, w niezbędnym zakresie, we wczesnym ostrzeżeniu, o którym mowa w art. 11 ust. 1 pkt 4, lub zgłoszeniu, o którym mowa w art. 11 ust. 1 pkt 4a, informacje stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa, gdy jest to konieczne do realizacji zadań właściwego CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT sektorowego.

7. Właściwy CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT sektorowy może zwrócić się do podmiotu kluczowego lub podmiotu ważnego o uzupełnienie wczesnego ostrzeżenia, o którym mowa w art. 11 ust. 1 pkt 4, lub zgłoszenia, o którym mowa w art. 11 ust. 1 pkt 4a, o informacje, w tym informacje stanowiące tajemnice prawnie chronione, w zakresie niezbędnym do realizacji zadań, o których mowa w ustawie.

8. We wczesnym ostrzeżeniu, o którym mowa w art. 11 ust. 1 pkt 4, lub w zgłoszeniu, o którym mowa w art. 11 ust. 1 pkt 4a, podmiot kluczowy lub podmiot ważny oznacza informacje stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa.”;

21) po art. 12 dodaje się art. 12a–12c w brzmieniu:

„Art. 12a. Sprawozdanie końcowe, o którym mowa w art. 11 ust. 1 pkt 4c, zawiera:

- 1) szczegółowy opis incydentu poważnego, w tym spowodowane zakłócenia i szkody;
- 2) rodzaj zagrożenia lub przyczynę, która prawdopodobnie była źródłem incydentu;
- 3) zastosowane i wdrażane środki ograniczające ryzyko;
- 4) w odpowiednich przypadkach transgraniczne skutki incydentu.

Art. 12b. 1. W przypadku gdy obsługa incydentu poważnego nie zakończyła się w terminie składania sprawozdania końcowego, o którym mowa w art. 11 ust. 1 pkt 4c, podmiot kluczowy lub podmiot ważny przekazuje właściwemu CSIRT sektorowemu sprawozdanie z postępu obsługi tego incydentu.

2. W przypadku gdy obsługa incydentu poważnego nie zakończyła się w terminie składania sprawozdania końcowego, o którym mowa w art. 11 ust. 1 pkt 4c, podmiot

kluczowy lub podmiot ważny przekazuje właściwemu CSIRT sektorowemu sprawozdanie końcowe nie później niż w ciągu miesiąca od zakończenia obsługi incydentu poważnego.

Art. 12c. Do podmiotu ważnego będącego podmiotem publicznym stosuje się przepisy art. 11–12, z wyjątkiem przepisów o przekazywaniu wczesnego ostrzeżenia, sprawozdania okresowego, sprawozdania z postępu obsługi incydentu i sprawozdania końcowego.”;

22) art. 13 i art. 14 otrzymują brzmienie:

„Art. 13. 1. Podmiot kluczowy lub podmiot ważny mogą przekazywać do właściwego CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT sektorowego informacje o:

- 1) innych incydentach;
- 2) cyberzagrożeniach;
- 3) wynikach szacowania ryzyka;
- 4) podatnościach;
- 5) potencjalnych zdarzeniach dla cyberbezpieczeństwa;
- 6) wykorzystywanych technologiach.

2. Informacje, o których mowa w ust. 1, są przekazywane w postaci elektronicznej za pomocą systemu teleinformatycznego, o którym mowa w art. 46 ust. 1, a w przypadku braku możliwości przekazania w postaci elektronicznej przy użyciu innych dostępnych środków komunikacji.

3. Podmiot kluczowy lub podmiot ważny oznacza informacje, o których mowa w ust. 1, stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa.

Art. 14. Podmiot kluczowy lub podmiot ważny w celu realizacji zadań, o których mowa w art. 8 oraz w art. 9–13, powołuje wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo lub zawiera umowę z dostawcą usług zarządzanych w zakresie cyberbezpieczeństwa.”;

23) w art. 15:

a) ust. 1 otrzymuje brzmienie:

„1. Podmiot kluczowy przeprowadza, na własny koszt, co najmniej raz na 3 lata, audyt bezpieczeństwa systemu informacyjnego wykorzystywanego w procesie świadczenia usługi, zwanego dalej „audytem”, licząc od dnia sporządzenia

i podpisania przez audytorów przeprowadzających audyt raportu z ostatniego audytu.”,

b) po ust. 1 dodaje się ust. 1a–1c w brzmieniu:

„1a. Podmiot kluczowy przedstawia w postaci elektronicznej kopię raportu z przeprowadzonego audytu, o którym mowa w ust. 1, organowi właściwemu do spraw cyberbezpieczeństwa, w terminie trzech dni roboczych od dnia jego otrzymania przez podmiot kluczowy lub podmiot ważny.

1b. Organ właściwy do spraw cyberbezpieczeństwa może nakazać podmiotowi kluczowemu w każdym czasie lub podmiotowi ważnemu w przypadku wystąpienia incydentu poważnego lub innego naruszenia przepisów ustawy przez ten podmiot, w drodze decyzji, przeprowadzenie zewnętrznego audytu bezpieczeństwa systemu informacyjnego wykorzystywanego w procesie świadczenia usługi, wraz z określeniem terminu przekazania kopii raportu z przeprowadzonego audytu i wskazaniem rodzaju podmiotów uprawnionych do przeprowadzenia audytu. Organ właściwy do spraw cyberbezpieczeństwa może również określić zakres audytu.

1c. Decyzja, o której mowa w ust. 1b, podlega natychmiastowemu wykonaniu.”,

c) w ust. 2 w pkt 3 wyrazy „sektorowy zespół cyberbezpieczeństwa” zastępuje się wyrazami „CSIRT sektorowy”,

d) po ust. 2 dodaje się ust. 2a w brzmieniu:

„2a. Audyt nie może być przeprowadzony przez osobę realizującą w podmiocie audytowanym zadania, o których mowa w art. 8 oraz art. 9–13, lub która realizowała te zadania w podmiocie audytowanym w przeciągu roku przed rozpoczęciem audytu.”,

e) w ust. 3 uchyla się pkt 3,

f) w ust. 5 wyrazy „operatorowi usługi kluczowej” zastępuje się wyrazami „podmiotowi kluczowemu lub podmiotowi ważnemu”,

g) uchyla się ust. 6,

h) w ust. 7:

– wprowadzenie do wyliczenia otrzymuje brzmienie:

„Podmiot kluczowy lub podmiot ważny przekazuje kopię raportu z przeprowadzonego audytu na wniosek:”,

– uchyla się pkt 1,

- w pkt 2 wyrazy „operator usługi kluczowej” zastępuje się wyrazami „podmiot kluczowy lub podmiot ważny”;

24) art. 16 otrzymuje brzmienie:

„Art. 16. Podmiot:

- 1) kluczowy lub ważny realizuje obowiązki, o których mowa w niniejszym rozdziale, w terminie 6 miesięcy,
- 2) kluczowy zapewnia przeprowadzenie audytu, o którym mowa w art. 15 ust. 1, po raz pierwszy w terminie 24 miesięcy

– od dnia spełnienia przesłanek uznania za podmiot kluczowy lub podmiot ważny.”;

25) uchyla się art. 16a;

26) po rozdziale 3 dodaje się rozdział 3a i 3b w brzmieniu:

„Rozdział 3a

Obowiązki rejestrów nazw domen najwyższego poziomu oraz zadania i obowiązki podmiotów świadczących usługi rejestracji nazw domen

Art. 16b. 1. Rejestr nazw domen najwyższego poziomu (TLD) i podmioty świadczące usługi rejestracji nazw domen z należytą starannością zbierają i zachowują dokładne i kompletne dane dotyczące rejestracji nazw domen.

2. Podmioty świadczące usługi rejestracji nazw w konkretnej domenie najwyższego poziomu współpracują z rejestrem nazw tej domeny. Baza danych dotycząca rejestracji nazw domen może funkcjonować w szczególności przez umożliwianie podmiotom świadczącym usługi rejestracji nazw domen przez rejestr nazw domen najwyższego poziomu (TLD) na podstawie umów, zautomatyzowanego wprowadzania i aktualizowania danych oraz inicjowanie związanych z tym czynności administracyjnych i technicznych. W takim przypadku przetwarzanie danych przez podmioty świadczące usługi rejestracji nazw domen nie jest uznawane za powielanie zadań rejestru nazw domen najwyższego poziomu (TLD).

3. W odniesieniu do danych będących danymi osobowymi przetwarzanie w zakresie, o którym mowa w ust. 1 i 2, następuje zgodnie z przepisami dotyczącymi ochrony danych osobowych.

4. Baza danych dotyczących rejestracji nazw domen zawiera:

- 1) nazwę domeny;
- 2) datę rejestracji;

- 3) imię i nazwisko lub nazwę abonenta nazwy domeny oraz adres poczty elektronicznej i numer telefonu;
- 4) adres poczty elektronicznej i numer telefonu, pod którymi można skontaktować się z punktem kontaktowym zarządzającym nazwą domeny, w przypadku gdy różnią się od adresu poczty elektronicznej i numeru telefonu abonenta nazwy domeny, a w przypadku gdy usługi punktu kontaktowego zarządzającego nazwą domeny nie są dopuszczone dla konkretnej domeny najwyższego poziomu (TLD), należy podać co najmniej dane identyfikujące podmiot świadczący usługi rejestracji nazw domen.

5. Rejestry nazw domen najwyższego poziomu (TLD) i podmioty świadczące usługi rejestracji nazw domen opracowują i wdrażają polityki i procedury, w tym procedury weryfikacji, służące zapewnieniu, aby bazy danych, o których mowa w ust. 1, zawierały dokładne i kompletne dane. Procedury weryfikacji danych:

- 1) obejmują działania weryfikacyjne na etapie rejestracji nazwy domeny lub po takiej rejestracji;
- 2) są wyważone i proporcjonalne;
- 3) prowadzą do zweryfikowania co najmniej jednego ze sposobów kontaktu, o których mowa w ust. 4 pkt 3 i 4;
- 4) obejmują uprawnienie rejestru nazw domen najwyższego poziomu (TLD) lub podmiotów świadczących usługi rejestracji nazw domen do żądania, w uzasadnionych przypadkach, udokumentowania danych identyfikacyjnych innych niż wymienione w ust. 3 i 4, w szczególności numeru lub innego oznaczenia identyfikacyjnego abonenta nazwy domeny zawartego w rejestrach publicznych, o ile obowiązek jego posiadania wynika z przepisów prawa krajowego obowiązującego takiego abonenta.

6. Polityki i procedury, o których mowa w ust. 5, rejestr nazw domen najwyższego poziomu (TLD) i podmioty świadczące usługi rejestracji nazw domen publikują na swoich stronach internetowych. Polityki i procedury podmiotów świadczących usługi rejestracji nazw w konkretnej domenie najwyższego poziomu (TLD) są zgodne z politykami i procedurami opublikowanymi przez rejestr nazw tej domeny najwyższego poziomu (TLD).

7. Po rejestracji nazwy domeny rejestr nazw domen najwyższego poziomu (TLD) i podmioty świadczące usługi rejestracji nazw domen niezwłocznie publikują na stronie

internetowej dane dotyczące rejestracji nazwy domeny, z wyłączeniem danych osobowych.

8. Obowiązek, o którym mowa w ust. 7, może zostać zrealizowany w szczególności przez zamieszczenie danych w ogólnodostępnej bazie abonentów upublicznianej przez rejestr nazw domen najwyższego poziomu (TLD).

9. W przypadku gdy podanie danych, w tym adresu poczty elektronicznej abonenta nazwy domeny, wymaga uzyskania zgody, obowiązek jej uzyskania obciąża podmiot przetwarzający te dane jako pierwszy.

Art. 16c. 1. Rejestry nazw domen najwyższego poziomu (TLD) oraz podmioty świadczące usługi rejestracji nazw domen na żądanie:

- 1) sądu – w celu przeprowadzenia dowodu w postępowaniu karnym, postępowaniu w sprawach o wykroczenia lub w postępowaniu cywilnym,
- 2) prokuratora – w celu przeprowadzenia dowodu w postępowaniu karnym lub postępowaniu w sprawach o wykroczenia,
- 3) Policji oraz innych upoważnionych organów w postępowaniu karnym lub czynnościach wyjaśniających w sprawie o wykroczenie i postępowaniu w sprawach o wykroczenia, w celu przeprowadzenia dowodu w postępowaniu karnym lub czynnościach wyjaśniających w sprawie o wykroczenie i postępowaniu w sprawach o wykroczenia,
- 4) CSIRT sektorowego – w celu przeprowadzenia obsługi incydentu poważnego przez CSIRT sektorowy związanego z daną domeną,
- 5) CSIRT GOV, CSIRT MON lub CSIRT NASK – w celu przeprowadzenia obsługi incydentu poważnego lub incydentu krytycznego związanego z daną domeną,
- 6) podmiotu wykonującego postanowienie sądu w przedmiocie zabezpieczenia środka dowodowego, o którym mowa w art. 479¹⁰⁰ § 1 ustawy z dnia 17 listopada 1964 r. – Kodeks postępowania cywilnego (Dz. U. z 2024 r. poz. 1568 i 1841 oraz z 2025 r. poz. 620, 1172 i 1302),
- 7) Prezesa Urzędu Komunikacji Elektronicznej – w celu weryfikacji czy podmiot składający sprzeciw wobec wpisania domeny na listę ostrzeżeń, o którym mowa w art. 21 ust. 1 ustawy z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji

elektronicznej (Dz. U. z 2024 r. poz. 1803), dysponuje do tej domeny tytułem prawnym

– udzielają dostępu do konkretnych danych dotyczących rejestracji nazw domen, które mają znaczenie dla prowadzonego postępowania lub czynności wyjaśniających w sprawie o wykroczenie, z zachowaniem przepisów dotyczących ochrony danych osobowych.

2. Żądanie udostępnienia danych, o których mowa w ust. 1, składa się w postaci elektronicznej i opatruje kwalifikowanym podpisem elektronicznym, podpisem zaufanym, podpisem osobistym albo kwalifikowaną pieczęcią elektroniczną. Żądanie zawiera uzasadnienie.

3. Rejestry nazw domen najwyższego poziomu (TLD) oraz podmioty świadczące usługi rejestracji nazw domen udzielają odpowiedzi nie później niż w terminie 72 godzin od dnia otrzymania żądania udostępnienia danych, o którym mowa w ust. 1, w sposób określony w opracowanej przez siebie i podanej do publicznej wiadomości polityce i procedurze ujawniania takich danych.

Rozdział 3b

Wspólne wykonywanie obowiązków z zakresu cyberbezpieczeństwa przez podmioty publiczne

Art. 16d. Podmiot publiczny realizuje obowiązki, o których mowa w art. 7b ust. 4, art. 7c, art. 7f ust. 3, art. 8, art. 8c–8f, art. 9–12b i art. 15, jeżeli wykorzystuje system informacyjny w celu realizacji zadania publicznego.

Art. 16e. 1. Minister kierujący działem administracji rządowej może wyznaczyć, obsługujący go urząd, jednostkę jemu podległą albo przez niego nadzorowaną jako jednostkę odpowiedzialną za realizację obowiązków, o których mowa w art. 7b ust. 4, art. 7c, art. 7f ust. 3, art. 8, art. 8c–8f, art. 9–12b lub art. 15, w pozostałych jednostkach organizacyjnych lub organach podległych oraz nadzorowanych przez tego ministra, a także w obsługującym go urzędzie.

2. Centralny organ administracji rządowej, niebędący ministrem, może wyznaczyć, obsługujący go urząd, jednostkę jemu podległą albo przez niego nadzorowaną jako jednostkę odpowiedzialną za realizację obowiązków, o których mowa w art. 7b ust. 4, art. 7c, art. 7f ust. 3, art. 8, art. 8c–8f, art. 9–12b lub art. 15, w pozostałych jednostkach organizacyjnych podległych oraz nadzorowanych przez ten organ, a także w obsługującym go urzędzie.

3. Wojewoda może wyznaczyć obsługujący go urząd, jednostkę jemu podległą albo przez niego nadzorowaną jako jednostkę odpowiedzialną za realizację obowiązków, o których mowa w art. 7b ust. 4, art. 7c, art. 7f ust. 3, art. 8, art. 8c–8f, art. 9–12b lub art. 15, w pozostałych jednostkach organizacyjnych podległych oraz nadzorowanych przez wojewodę, a także w obsługującym go urzędzie.

4. Prokurator Generalny może spośród powszechnych jednostek organizacyjnych prokuratury wyznaczyć jednostkę odpowiedzialną za realizację obowiązków, o których mowa w art. 7b ust. 4, art. 7c, art. 7f ust. 3, art. 8, art. 8c–8f, art. 9–12b lub art. 15, w pozostałych jednostkach prokuratury.

5. Jednostka samorządu terytorialnego może zapewnić wspólną obsługę realizacji obowiązków, o których mowa w art. 7b ust. 4, art. 7c, art. 7f ust. 3, art. 8, art. 8c–8f, art. 8h, art. 9–12b lub art. 15. Do wyznaczenia jednostki obsługującej i obsługiwanej stosuje się odpowiednio art. 10a–10d ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2025 r. poz. 1153), art. 6a–6d ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym (Dz. U. z 2024 r. poz. 107 i 1907) oraz art. 8c–8f ustawy z dnia 5 czerwca 1998 r. o samorządzie województwa (Dz. U. z 2025 r. poz. 581).

6. Jednostki samorządu terytorialnego mogą zawrzeć porozumienie w sprawie powierzenia jednej z nich realizacji obowiązków, o których mowa w art. 7b ust. 4, art. 7c, art. 7f ust. 3, art. 8, art. 8c–8f, art. 8h, art. 9–12b lub art. 15.

7. W porozumieniu, o którym mowa w ust. 6, wskazuje się jednostki organizacyjne, samorządowe osoby prawne lub spółki, o których mowa w art. 9 ust. 1 ustawy z dnia 20 grudnia 1996 r. o gospodarce komunalnej, jednostki samorządu terytorialnego powierzającej realizacji obowiązków, o których mowa w art. 7b ust. 4, art. 7c, art. 7f ust. 3, art. 8, art. 8c–8f, art. 8h, art. 9–12b lub art. 15, objęte porozumieniem.

8. Jednostka samorządu terytorialnego, której powierzono realizację obowiązków, o których mowa w art. 7b ust. 4, art. 7c, art. 7f ust. 3, art. 8, art. 8c–8f, art. 8h, art. 9–12b lub art. 15, wyznacza jednostkę organizacyjną, samorządową osobę prawną lub spółkę, o której mowa w art. 9 ust. 1 ustawy z dnia 20 grudnia 1996 r. o gospodarce komunalnej, do realizacji tych obowiązków.

9. Do porozumień, o których mowa w ust. 6, stosuje się odpowiednio art. 74 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym.

Art. 16f. Podmioty publiczne, dla których jednostka wyznaczona realizuje obowiązki z zakresu cyberbezpieczeństwa, współpracują z tą jednostką w szczególności przez:

- 1) przekazywanie informacji o incydentach;
- 2) wykonywanie decyzji kierownika tej jednostki w zakresie systemu zarządzania bezpieczeństwem informacji;
- 3) publikowanie na swojej stronie internetowej adresu strony internetowej jednostki wyznaczonej zawierającej informacje o cyberbezpieczeństwie, zgodnie z art. 9;
- 4) uczestnictwo kierownika jednostki w szkoleniach z zakresu cyberbezpieczeństwa, jeżeli są prowadzone przez jednostkę wyznaczoną.

Art. 16g. W celu prawidłowego wykonania obowiązków, o których mowa w art. 11 i art. 12, kierownik jednostki wyznaczonej, o której mowa w art. 16e, może wskazać podmiotom publicznym terminy na przekazanie informacji o incydentach.

Art. 16h. Jednostka wyznaczona, o której mowa w art. 16e:

- 1) zgłasza w imieniu podmiotu publicznego wczesne ostrzeżenie, zgłoszenie incyduentu poważnego, sprawozdanie okresowe i sprawozdanie końcowe, o których mowa w art. 11 ust. 1 pkt 4–4c, do CSIRT sektorowego;
 - 2) wskazuje osobę kontaktową do podmiotów publicznych, którym realizuje zadania z zakresu cyberbezpieczeństwa;
 - 3) korzysta z systemu teleinformatycznego, o którym mowa w art. 46 ust. 1, w celu realizacji obowiązków, o których mowa w rozdziale 3.”;
- 27) uchyla się rozdział 4 i 5;
- 28) w art. 26:
- a) w ust. 1:
 - po wyrazie „informatyzacji” dodaje się wyrazy „,CSIRT sektorowymi”;
 - wyrazy „zagrożeniom cyberbezpieczeństwa” zastępuje się wyrazem „cyberzagrożeniom”;
 - b) po ust. 1 dodaje się ust. 1a w brzmieniu:

„1a. W czasie stanu wojennego lub w czasie wojny CSIRT MON, w imieniu Ministra Obrony Narodowej, koordynuje działania CSIRT NASK i CSIRT GOV.”,

c) ust. 2 otrzymuje brzmienie:

„2. CSIRT MON, CSIRT NASK i CSIRT GOV na wniosek podmiotów krajowego systemu cyberbezpieczeństwa mogą zapewnić wsparcie tym podmiotom w obsłudze incydentów, w przypadku gdy:

- 1) incydent może wpłynąć na inne podmioty krajowego systemu cyberbezpieczeństwa;
- 2) podmiot obsługujący incydent nie dysponuje środkami pozwalającymi mu na jego skuteczną obsługę, a incydent powoduje przerwanie ciągłości świadczenia usługi.”,

d) po ust. 2 dodaje się ust. 2a–2c w brzmieniu:

„2a. Pełnomocnik może zlecić zapewnienie wsparcia w obsłudze incydentów, o których mowa w ust. 2:

- 1) CSIRT MON, za zgodą Ministra Obrony Narodowej lub
- 2) CSIRT NASK, lub
- 3) CSIRT GOV, za zgodą Szefa Agencji Bezpieczeństwa Wewnętrznego.

2b. Zgoda może być wyrażona w formie ustnej lub dokumentowej, w szczególności z wykorzystaniem środków komunikacji elektronicznej. Zgoda wyrażona w formie ustnej wymaga udokumentowania w ciągu 14 dni od dnia jej wydania.

2c. O zapewnieniu wsparcia w obsłudze incydentów, o którym mowa w ust. 2 lub 2a, jest informowany właściwy CSIRT sektorowy.”,

e) w ust. 3:

- w pkt 1 wyrazy „zagrożeń cyberbezpieczeństwa” zastępuje się wyrazem „cyberzagrożeń”,
- pkt 2–4 otrzymują brzmienie:
 - „2) szacowanie ryzyka związanego z ujawnionym cyberzagrożeniem oraz zaistniałymi incydentami, w tym zapewnianie dynamicznej analizy ryzyka;
 - 3) przekazywanie informacji dotyczących cyberzagrożeń, podatności, incydentów i ryzyk, wczesne ostrzeganie i alarmowanie podmiotów krajowego systemu cyberbezpieczeństwa;
 - 4) wydawanie komunikatów o zidentyfikowanych cyberzagrożeniach;”,
- pkt 6 i 7 otrzymują brzmienie:

- „6) klasyfikowanie incydentów, w tym incydentów poważnych, jako incydenty krytyczne oraz koordynowanie obsługi incydentów krytycznych;
- 7) zmiana klasyfikacji incydentów;”,
- w pkt 10:
 - wyrazy „sektorowymi zespołami cyberbezpieczeństwa” zastępuje się wyrazami „CSIRT sektorowymi”,
 - wyrazy „zagrożeniom cyberbezpieczeństwa” zastępuje się wyrazem „cyberzagrożeniom”,
- pkt 11 i 12 otrzymują brzmienie:
 - „11) przekazywanie do innych państw, w tym państw członkowskich Unii Europejskiej, i przyjmowanie z tych państw informacji o incydentach poważnych dotyczących dwóch lub większej liczby państw, a także przekazywanie do Pojedynczego Punktu Kontaktowego zgłoszenia incydentu poważnego dotyczącego dwóch lub większej liczby państw członkowskich Unii Europejskiej;
 - 12) przekazywanie, w terminie 14 dni od zakończenia danego kwartału, do Pojedynczego Punktu Kontaktowego zestawienia zgłoszonych w poprzednich 3 miesiącach:
 - a) poważnych incydentów,
 - b) incydentów,
 - c) cyberzagrożeń,
 - d) potencjalnych zdarzeń dla cyberbezpieczeństwa;”,
- w pkt 14 w lit. b i c wyrazy „zagrożeń cyberbezpieczeństwa” zastępuje się wyrazem „cyberzagrożeń”,
- uchyla się pkt 15,
- pkt 16 otrzymuje brzmienie:
 - „16) udział w Sieci CSIRT składającej się z przedstawicieli CSIRT państw członkowskich Unii Europejskiej, CSIRT właściwego dla instytucji Unii Europejskiej oraz Komisji Europejskiej;”,
- dodaje się pkt 17–23 w brzmieniu:
 - „17) w odpowiednich przypadkach gromadzenie i zabezpieczanie danych na potrzeby postępowań karnych;

- 18) współpraca z sektorowymi i międzysektorowymi społecznościami podmiotów kluczowych lub podmiotów ważnych oraz wymiana informacji dotyczących cyberbezpieczeństwa, jeżeli wymiana informacji zapewnia zwiększenie poziomu cyberbezpieczeństwa lub służy przeciwdziałaniu incyidentom;
 - 19) współpraca z krajowymi zespołami reagowania na incydeny bezpieczeństwa komputerowego z państw trzecich;
 - 20) udział we wdrażaniu bezpiecznych narzędzi wymiany informacji z podmiotami kluczowymi i podmiotami ważnymi oraz innymi podmiotami;
 - 21) prowadzenie działań na rzecz podnoszenia poziomu bezpieczeństwa systemów informacyjnych podmiotów krajowego systemu cyberbezpieczeństwa przez:
 - a) wykonywanie oceny bezpieczeństwa,
 - b) identyfikowanie podatności systemów dostępnych w otwartych sieciach teleinformatycznych, a także powiadamianie właścicieli tych systemów o wykrytych podatnościach oraz cyberzagrożeniach;
 - 22) promowanie, przyjmowanie i stosowanie wspólnych lub znormalizowanych praktyk, systemów klasyfikacji i systematyki związanych z:
 - a) procedurami obsługi incydentu,
 - b) zarządzaniem kryzysowym w obszarze cyberbezpieczeństwa,
 - c) ujawnianiem podatności;
 - 23) przekazywanie Pełnomocnikowi sprawozdania z wykonywania swoich zadań ustawowych zawierającego w szczególności informacje o zgłoszonych do CSIRT incydentach krytycznych, incydentach poważnych, incydentach, cyberzagrożeniach oraz potencjalnych zdarzeniach dla cyberbezpieczeństwa.”,
- f) po ust. 3 dodaje się ust. 3a w brzmieniu:
- „3a. Przy realizacji zadania, o którym mowa w ust. 3 pkt 19, CSIRT MON, CSIRT NASK i CSIRT GOV mogą wymieniać informacje, w tym dane osobowe w celu informowania o potencjalnych cyberzagrożeniach oraz zastosowanych sposobach ich zwalczania, w celu przeciwdziałania cyberzagrożeniom o charakterze

transgranicznym. Informacje, w tym dane osobowe, o których mowa w zdaniu pierwszym, przekazuje się w postaci elektronicznej.”,

- g) w ust. 5 w pkt 2 kropkę zastępuje się średnikiem i dodaje się pkt 3 w brzmieniu:
„3) Ministra Obrony Narodowej.”,
- h) w ust. 6:
 - w pkt 1:
 - – lit. a i b otrzymują brzmienie
 - „a) jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 2a–6 i 10–13 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych, z wyjątkiem podmiotów, o których mowa w ust. 5,
 - b) jednostki podległe organom administracji rządowej lub przez nie nadzorowane, z wyjątkiem podmiotów, o których mowa w ust. 5, oraz jednostek, o których mowa w ust. 7 pkt 2,”
 - – po lit. a dodaje się lit. aa w brzmieniu:
„aa) urzędy obsługujące jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 2 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych,”
 - – lit. c otrzymuje brzmienie:
„c) instytuty badawcze, z wyjątkiem podmiotów, o których mowa w ust. 5,”
 - – po lit. c dodaje się lit. ca–cc w brzmieniu:
 - „ca) międzynarodowe instytuty badawcze, z wyjątkiem podmiotów, o których mowa w ust. 5 pkt 2,
 - cb) Centrum Łukasiewicz,
 - cc) instytuty działające w ramach Sieci Badawczej Łukasiewicz, z wyjątkiem podmiotów, o których mowa w ust. 5 pkt 2,”
 - – uchyla się lit. e,
 - – uchyla się lit. i,
 - – lit. j otrzymuje brzmienie:
„j) podmioty kluczowe lub podmioty ważne, z wyjątkiem wymienionych w ust. 5 i 7,”
 - w pkt 2 wyrazy „zagrożeniach cyberbezpieczeństwa” zastępuje się wyrazem „cyberzagrożeniach”,

- i) w ust. 7:
 - pkt 1 otrzymuje brzmienie:
 - „1) jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 1, 8 i 9 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych, i urzędy je obsługujące, z wyjątkiem wymienionych w ust. 5 i 6;”,
 - po pkt 4 dodaje się pkt 4a–4e w brzmieniu:
 - „4a) Polską Agencję Żeglugi Powietrznej;
 - 4b) Polską Agencję Prasową;
 - 4c) Państwowe Gospodarstwo Wodne Wody Polskie;
 - 4d) Polski Fundusz Rozwoju i inne instytucje rozwoju, o których mowa w art. 2 ust. 1 pkt 3–6 ustawy z dnia 4 lipca 2019 r. o systemie instytucji rozwoju (Dz. U. z 2024 r. poz. 923 oraz z 2025 r. poz. 352, 769 i 1216);
 - 4e) Urząd Komisji Nadzoru Finansowego;”,
- j) po ust. 8 dodaje się ust. 8a w brzmieniu:
 - „8a. Minister właściwy do spraw informatyzacji może udzielić CSIRT NASK dotacji celowej na zakup, utrzymanie i rozbudowę infrastruktury teleinformatycznej niezbędnej do wykonywania zadań CSIRT NASK.”,
- k) dodaje się ust. 12–16 w brzmieniu:
 - „12. CSIRT MON, CSIRT NASK i CSIRT GOV mogą uczestniczyć w procesie wzajemnej oceny, o którym mowa w art. 40a.
 - 13. Przepisy ust. 2 i 3 stosuje się odpowiednio do zadań realizowanych przez CSIRT NASK lub CSIRT GOV w sektorze bankowości i infrastruktury rynków finansowych, w szczególności w zakresie poważnych incydentów związanych z ICT zgłaszanych przez podmioty kluczowe lub podmioty ważne z tego sektora.
 - 14. CSIRT NASK lub CSIRT GOV może również realizować swoje zadania w odniesieniu do podmiotów finansowych niebędących podmiotami kluczowymi lub podmiotami ważnymi, gdy nie stanowi to dla tego zespołu nieproporcjonalnego czy nadmiernego obciążenia, z uwzględnieniem priorytetowego traktowania poważnych incydentów związanych z ICT zgłaszanych przez podmioty finansowe będące podmiotami kluczowymi lub podmiotami ważnymi, oraz z uwzględnieniem odpowiedniego stosowania ust. 2 i 3 do realizacji zadań przez CSIRT NASK lub CSIRT GOV.

15. CSIRT NASK lub CSIRT GOV współpracują i wymieniają informacje z właściwym organem w rozumieniu rozporządzenia 2022/2554, gdy jest to niezbędne dla realizacji zadań CSIRT NASK lub CSIRT GOV bądź realizacji zadań tego właściwego organu.

16. CSIRT MON, CSIRT NASK i CSIRT GOV informują organ właściwy do spraw podmiotów krytycznych o poważnych incydentach, cyberzagrożeniach i potencjalnych zdarzeniach dla cyberbezpieczeństwa zgłoszonych przez podmiot krytyczny.”;

29) po art. 26 dodaje się art. 26a–26d w brzmieniu:

„Art. 26a. 1. CSIRT NASK pełni funkcję koordynatora na potrzeby skoordynowanego ujawniania podatności.

2. Osoba fizyczna, osoba prawna albo jednostka organizacyjna nieposiadająca osobowości prawnej może zgłosić wykrytą podatność do CSIRT NASK.

3. Zgłoszenie podatności jest przekazywane w postaci elektronicznej, a w przypadku braku możliwości przekazania jej w postaci elektronicznej – przy użyciu innych dostępnych środków komunikacji.

4. CSIRT NASK zapewnia formularz do dokonywania zgłoszeń podatności, zapewniający możliwość zachowania anonimowości przez osobę fizyczną lub prawną zgłaszającą podatność. CSIRT NASK może przetwarzać przekazane dane osobowe w celu realizacji zadań, o których mowa w ust. 5.

5. W ramach zadania, o którym mowa w ust. 1, CSIRT NASK:

- 1) przyjmuje informacje o wykrytych podatnościach;
- 2) identyfikuje dostawców produktów ICT lub usług ICT, na które podatność może mieć wpływ i informuje ich o wykrytej podatności;
- 3) w razie konieczności koordynuje komunikację między osobą fizyczną lub prawną zgłaszającą podatność a producentem lub dostawcą potencjalnie podatnych produktów ICT lub usług ICT, w zakresie weryfikacji zgłoszenia i terminu ujawniania podatności;
- 4) udziela pomocy podmiotom zgłaszającym podatność;
- 5) identyfikuje oraz klasyfikuje podatności;
- 6) prowadzi działania służące likwidacji podatności oraz likwidacji jej skutków;
- 7) koordynuje proces ujawniania podatności;
- 8) może publikować informacje o podatnościach;

9) zarządza ujawnionymi informacjami o podatnościach.

6. CSIRT NASK współpracuje z CSIRT innych państw członkowskich Unii Europejskiej przy podatnościach, które mają wpływ na podmioty, w pozostałych państwach członkowskich Unii Europejskiej.

Art. 26b. Minister Obrony Narodowej udostępnia CSIRT NASK, na jego wniosek, w terminie 14 dni od doręczenia wniosku, listę przedsiębiorców, wobec których wydano decyzję administracyjną, o której mowa w art. 648 ust. 2 ustawy z dnia 11 marca 2022 r. o obronie Ojczyzny (Dz. U. z 2025 r. poz. 825, 1014 i 1080).

Art. 26c 1. CSIRT NASK, w celu minimalizacji ryzyka powstania szkód materialnych i niematerialnych związanych z nieuprawnionym upublicznieniem danych osobowych w sieci internet, tworzy i udostępnia usługę online umożliwiającą sprawdzenie przez osobę fizyczną, czy jej dane osobowe nie zostały ujawnione w sieci internet w sposób nieuprawniony, na skutek incydentu lub cyberzagrożenia.

2. Dla realizacji usługi online, o której mowa w ust. 1, CSIRT NASK może gromadzić i przetwarzać następujące dane osobowe:

- 1) imię i nazwisko;
- 2) datę urodzenia;
- 3) adres zamieszkania;
- 4) płeć;
- 5) imię i nazwisko nadane podczas urodzenia;
- 6) miejsce urodzenia;
- 7) identyfikator użytkownika w Węźle Krajowym nadawany tymczasowo podczas uwierzytelniania;
- 8) login, który uległ nieuprawnionemu upublicznieniu;
- 9) adres poczty elektronicznej;
- 10) numer telefonu;
- 11) numer PESEL.

Art. 26d. 1. Przed rozpoczęciem realizacji zadań CSIRT MON, CSIRT NASK lub CSIRT GOV osoba przedstawia właściwemu CSIRT informację o osobie z Krajowego Rejestru Karnego stwierdzającą niekaralność za przestępstwa przeciwko ochronie informacji. Kierownik właściwego CSIRT dopuszcza osobę do realizacji zadań, o których mowa w art. 26 ust. 3, po otrzymaniu informacji, o której mowa w zdaniu pierwszym.

2. CSIRT MON, CSIRT NASK lub CSIRT GOV wzywa osobę realizującą jego zadania, o których mowa w art. 26 ust. 3, do ponownego przedstawienia informacji o osobie z Krajowego Rejestru Karnego stwierdzającą niekaralność za przestępstwa przeciwko ochronie informacji, jeżeli poweźmie uzasadnione podejrzenie, że osoba ta została skazana za przestępstwo przeciwko ochronie informacji.

3. Wymagania, o których mowa w ust. 1 i 2, uznaje się za spełnione, jeśli osoba realizująca zadania CSIRT MON, CSIRT NASK lub CSIRT GOV posiada ważne poświadczenie bezpieczeństwa upoważniające do dostępu do informacji niejawnych o klauzuli „poufne” lub wyższej.

4. Osoba skazana prawomocnym wyrokiem sądu za przestępstwa przeciwko ochronie informacji nie może realizować zadań CSIRT MON, CSIRT NASK lub CSIRT GOV, o których mowa w art. 26 ust. 3.”;

30) w art. 28:

- a) w ust. 1 wyrazy „operatora usługi kluczowej” zastępuje się wyrazami „podmiot kluczowy lub podmiot ważny”,
- b) w ust. 2 wyrazy „operatorowi usługi kluczowej” zastępuje się wyrazami „podmiotowi kluczowemu lub podmiotowi ważnemu”;

31) uchyla się art. 29;

32) w art. 30:

- a) w ust. 1 we wprowadzeniu do wyliczenia wyrazy „operatorzy usług kluczowych i dostawcy usług cyfrowych” zastępuje się wyrazami „podmioty kluczowe lub podmioty ważne”,
- b) w ust. 2 wyrazy „operatorów usług kluczowych i dostawców usług cyfrowych” zastępuje się wyrazami „podmiotów kluczowych lub podmiotów ważnych”;

33) art. 31 i art. 32 otrzymują brzmienie:

„Art. 31. 1. CSIRT MON, CSIRT NASK, CSIRT GOV oraz CSIRT sektorowe określają sposób przekazywania informacji i zgłoszeń, o których mowa w art. 11 i w art. 13, w przypadku braku możliwości przekazania ich za pomocą systemu teleinformatycznego, o którym mowa w art. 46 ust. 1.

2. CSIRT NASK określi sposób dokonywania zgłoszeń, o których mowa w art. 30 ust. 1.

3. Komunikat zawierający informacje o sposobie dokonywania zgłoszeń, o których mowa odpowiednio w art. 11, art. 13 i art. 30 ust. 1, CSIRT MON, CSIRT NASK, CSIRT

GOV oraz CSIRT sektorowe publikują odpowiednio na stronie podmiotowej Biuletynu Informacji Publicznej Ministra Obrony Narodowej, Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego, Agencji Bezpieczeństwa Wewnętrznego lub organu właściwego do spraw cyberbezpieczeństwa.

Art. 32. 1. CSIRT MON, CSIRT NASK i CSIRT GOV mogą wykonywać niezbędne działania techniczne związane z analizą zagrożeń, koordynacją obsługi incydentu poważnego i incydentu krytycznego.

2. CSIRT MON, CSIRT NASK lub CSIRT GOV mogą wystąpić do organu właściwego do spraw cyberbezpieczeństwa z wnioskiem o wezwanie podmiotu kluczowego lub podmiotu ważnego, aby w wyznaczonym terminie usunął podatności, które doprowadziły lub mogłyby doprowadzić do incydentu poważnego lub krytycznego.

3. Podmiot kluczowy lub podmiot ważny na wniosek CSIRT MON, CSIRT NASK lub CSIRT GOV udostępnia informacje techniczne związane z incydem, które będą niezbędne do przeprowadzenia analizy lub koordynacji obsługi incydentu.

4. CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT sektorowe na podstawie informacji, o których mowa w art. 13 ust. 1 pkt 3 i 5, uzyskanych od podmiotu kluczowego lub podmiotu ważnego, mogą przekazywać im informacje o podatnościach i sposobie usunięcia podatności w wykorzystywanych technologiach.”;

34) w art. 33:

- a) w ust. 1 wyrazy „urządzenia informatycznego lub oprogramowania” zastępuje się wyrazami „produktu ICT lub usługi ICT”,
- b) po ust. 1 dodaje się ust. 1a–1f w brzmieniu:

„1a. Badanie, o którym mowa w ust. 1, przeprowadza się także na pisemny wniosek Pełnomocnika lub przewodniczącego Kolegium, skierowany do organu prowadzącego lub nadzorującego właściwy CSIRT.

1b. Badanie, o którym mowa w ust. 1, przeprowadza się w środowisku testowym i nie może ono wpłynąć na ciągłość świadczenia usług przez podmioty kluczowe lub podmioty ważne.

1c. CSIRT MON, CSIRT NASK i CSIRT GOV prowadząc badanie, o którym mowa w ust. 1, są uprawnieni do stosowania technik mających na celu:

- 1) obserwację i analizę pracy produktu ICT lub usługi ICT;
- 2) uzyskanie dostępu do przetwarzanych danych;
- 3) odtworzenie postaci źródłowej produktu ICT lub usługi ICT;

- 4) zwielokrotnienie (powielenie) kodu programowego oraz tłumaczenie (translacja) jego formy;
- 5) odtworzenie algorytmu przetwarzania danych;
- 6) identyfikację realizowanych funkcji;
- 7) usunięcie lub przełamanie zabezpieczeń przed badaniem;
- 8) identyfikację podatności lub identyfikację nieudokumentowanych funkcji realizowanych przez produkt ICT lub usługę ICT.

1d. CSIRT MON, CSIRT NASK i CSIRT GOV w czasie prowadzenia badania, o którym mowa w ust. 1, nie są związane postanowieniami umów, w szczególności umów licencyjnych, badanych produktów ICT lub usług ICT, które ograniczyłyby możliwość przeprowadzenia tego badania.

1e. Badanie, o którym mowa w ust. 1:

- 1) nie narusza autorskich praw osobistych oraz majątkowych, oraz
- 2) nie wymaga zgody licencjodawcy lub dysponenta produktu ICT lub usługi ICT.

1f. Postanowienia umów sprzeczne z ust. 1–1e są nieważne.”,

c) ust. 2 otrzymuje brzmienie:

„2. CSIRT MON, CSIRT NASK albo CSIRT GOV, podejmując badanie produktu ICT, usługi ICT lub procesu ICT, informuje pozostałe CSIRT poziomu krajowego o fakcie podjęcia badań oraz o produkcie ICT lub usłudze ICT, których badanie dotyczy.”,

d) w ust. 4 i 6–8 wyrazy „urządzeń informatycznych lub oprogramowania” zastępuje się wyrazami „produktów ICT lub usług ICT”,

e) w ust. 4a wyrazy „zagrożeniu cyberbezpieczeństwa” zastępuje się wyrazem „cyberzagrożeniu”,

f) po ust. 4b dodaje się ust. 4c w brzmieniu:

„4c. Rekomendacje, o których mowa w ust. 4, a także informację o ich zmianie lub odwołaniu, Pełnomocnik publikuje na swojej stronie podmiotowej Biuletynu Informacji Publicznej.”,

g) ust. 5 otrzymuje brzmienie:

„5. Podmiot krajowego systemu cyberbezpieczeństwa może wniesć do Pełnomocnika zastrzeżenia do rekomendacji dotyczących stosowania produktów ICT lub usług ICT, z uwagi na ich negatywny wpływ na świadczoną usługę lub realizowane zadanie publiczne, nie później niż w terminie 14 dni od dnia publikacji

rekomendacji na stronie podmiotowej Biuletynu Informacji Publicznej Pełnomocnika.”,

- h) dodaje się ust. 9 w brzmieniu:

„9. CSIRT MON, CSIRT NASK lub CSIRT GOV przeprowadzający badanie mogą zwrócić się do producenta badanego produktu ICT lub dostawcy badanej usługi ICT o przekazanie dokumentacji. Przepis art. 53c stosuje się odpowiednio. O zwróceniu się do producenta, jak również o nieprzekazaniu przez producenta dokumentacji w terminie, CSIRT przeprowadzający badanie informuje ministra właściwego do spraw informatyzacji.”;

- 35) w art. 34:

- a) ust. 1 otrzymuje brzmienie:

„1. CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT sektorowe oraz dostawcy usług zarządzanych w zakresie cyberbezpieczeństwa współpracują z organami ścigania i wymiaru sprawiedliwości oraz służbami specjalnymi przy realizacji ich ustawowych zadań.”,

- b) w ust. 2 wyrazy „i CSIRT GOV” zastępuje się wyrazami „CSIRT GOV i CSIRT sektorowe”,

- c) dodaje się ust. 3 i 4 w brzmieniu:

„3. CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT sektorowe oraz dostawcy usług zarządzanych z zakresu cyberbezpieczeństwa współpracują z Prezesem Urzędu Lotnictwa Cywilnego, Prezesem Urzędu Komunikacji Elektronicznej oraz Komisją Nadzoru Finansowego.

4. CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT sektorowe współpracują z Narodowym Bankiem Polskim w zakresie wymiany informacji o incydentach, podatnościach i cyberzagrożeniach, które mają wpływ na systemy płatności.”;

- 36) w art. 35:

- a) ust. 1 otrzymuje brzmienie:

„1. CSIRT MON, CSIRT NASK i CSIRT GOV przekazują sobie wzajemnie informacje o incydencie krytycznym lub incydencie w cyberbezpieczeństwie na dużą skalę oraz informują o nim Rządowe Centrum Bezpieczeństwa, właściwy CSIRT sektorowy oraz ministra właściwego do spraw zagranicznych.”,

- b) w ust. 2 w pkt 1 w lit. a skreśla się wyrazy „w szczególności jeśli zakłóca świadczenie usługi kluczowej”,

- c) po ust. 2 dodaje się ust. 2a w brzmieniu:

„2a. Informacja, o której mowa w ust. 1, może zawierać dane osobowe tylko wtedy, gdy jest to niezbędne dla ochrony podmiotów krajowego systemu cyberbezpieczeństwa przed incydentami.”,
 - d) w ust. 4 i 5 wyrazy „zagrożeniach cyberbezpieczeństwa” zastępuje się wyrazem „cyberzagrożeniach”,
 - e) w ust. 5 wyraz „cyberbezpieczeństwa” zastępuje się wyrazem „bezpieczeństwa”;
- 37) po art. 35 dodaje się art. 35a w brzmieniu:
- „Art. 35a. W przypadku wystąpienia incydentu krytycznego Prezes Rady Ministrów może, na podstawie propozycji Rządowego Zespołu Zarządzania Kryzysowego, o której mowa w art. 9 ust. 1 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2023 r. poz. 122, z późn. zm.¹²⁾), zobowiązać Ministra Obrony Narodowej do udzielenia wsparcia CSIRT koordynującemu obsługę tego incydentu przez właściwe jednostki organizacyjne podległe Ministrowi Obrony Narodowej lub przez niego nadzorowane.”;
- 38) w art. 36:
- a) ust. 2–4 otrzymują brzmienie:

„2. W skład Zespołu wchodzi przedstawiciele CSIRT MON, CSIRT NASK, Szefa Agencji Bezpieczeństwa Wewnętrznego realizującego zadania w ramach CSIRT GOV, Rządowego Centrum Bezpieczeństwa oraz ministra właściwego do spraw zagranicznych.

3. Pełnomocnik przewodniczy pracom Zespołu.

4. Obsługę prac Zespołu zapewnia urząd obsługujący Pełnomocnika.”,
 - b) w ust. 6 wyrazy „dyrektor Rządowego Centrum Bezpieczeństwa” zastępuje się wyrazem „Pełnomocnik”;
- 39) po rozdziale 6 dodaje się rozdział 6a w brzmieniu:

¹²⁾ Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2024 r. poz. 834, 1222, 1473, 1572 i 1907.

„Rozdział 6a

Ocena bezpieczeństwa

Art. 36a. 1. CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT sektorowy mogą przeprowadzić ocenę bezpieczeństwa systemów informacyjnych wykorzystywanych przez podmioty krajowego systemu cyberbezpieczeństwa.

2. Ocena bezpieczeństwa polega na przeprowadzeniu testów bezpieczeństwa systemu informacyjnego w celu identyfikacji podatności tego systemu. Wyboru rodzaju testów bezpieczeństwa dokonuje się adekwatnie do systemu informacyjnego i świadczonej usługi z uwzględnieniem specyfiki sektora lub podsektora.

3. Przepisów niniejszego rozdziału nie stosuje się do ocen bezpieczeństwa systemów teleinformatycznych:

- 1) podmiotów krajowego systemu cyberbezpieczeństwa, które znajdują się w zbiorze organów i podmiotów, o których mowa w art. 32a ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu;
- 2) akredytowanych na podstawie art. 48 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2025 r. poz. 1209).

4. Zespołem właściwym do przeprowadzenia oceny bezpieczeństwa jest:

- 1) w przypadku podmiotów, o których mowa w art. 26 ust. 5 – CSIRT MON;
- 2) w przypadku podmiotów, o których mowa w art. 26 ust. 6 pkt 1 lit. a–k – CSIRT NASK;
- 3) w przypadku podmiotów, o których mowa w art. 26 ust. 7 pkt 1–4d – CSIRT GOV.

5. CSIRT MON, CSIRT NASK albo CSIRT GOV przeprowadza ocenę bezpieczeństwa systemu informacyjnego podmiotu krajowego systemu cyberbezpieczeństwa, po poinformowaniu organu właściwego do spraw cyberbezpieczeństwa o zamiarze przeprowadzenia oceny bezpieczeństwa.

6. CSIRT sektorowy może przeprowadzić ocenę bezpieczeństwa systemu informacyjnego podmiotu kluczowego lub podmiotu ważnego po uzyskaniu zgody CSIRT MON, CSIRT NASK lub CSIRT GOV właściwego dla danego podmiotu kluczowego lub podmiotu ważnego. O zamiarze przeprowadzenia oceny bezpieczeństwa systemu informacyjnego podmiotu krajowego systemu cyberbezpieczeństwa CSIRT sektorowy informuje organ właściwy do spraw cyberbezpieczeństwa dla danego sektora.

7. Przepisów ust. 5 i 6 nie stosuje się, gdy ocena bezpieczeństwa systemu informacyjnego jest przeprowadzana na zlecenie organu właściwego do spraw cyberbezpieczeństwa.

Art. 36b. 1. Ocena bezpieczeństwa systemu informacyjnego może być przeprowadzona:

- 1) za zgodą podmiotu krajowego systemu cyberbezpieczeństwa, wyrażoną w formie pisemnej lub formie elektronicznej pod rygorem nieważności albo
- 2) na zlecenie organu właściwego do spraw cyberbezpieczeństwa.

2. Ocenę bezpieczeństwa systemów informacyjnych Kancelarii Sejmu, Kancelarii Senatu, Kancelarii Prezydenta Rzeczypospolitej Polskiej, Narodowego Banku Polskiego, Biura Rzecznika Praw Obywatelskich, Biura Rzecznika Praw Dziecka, Instytutu Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu, Państwowej Inspekcji Pracy, Trybunału Konstytucyjnego, Sądu Najwyższego, sądów administracyjnych, Najwyższej Izby Kontroli, Krajowej Rady Radiofonii i Telewizji, Krajowego Biura Wyborczego, Urzędu Ochrony Danych Osobowych przeprowadza się wyłącznie po uzyskaniu zgody tych podmiotów.

3. Organ właściwy do spraw cyberbezpieczeństwa przed zleceniem przeprowadzenia oceny bezpieczeństwa przeprowadza analizę ryzyka, o której mowa w art. 53b ust. 2, i na jej podstawie dokonuje wyboru podmiotu kluczowego lub podmiotu ważnego, którego system informacyjny będzie podlegał ocenie bezpieczeństwa.

4. Ocenę bezpieczeństwa systemu informacyjnego przeprowadza się z uwzględnieniem zasady minimalizacji zakłócenia pracy systemu informacyjnego lub ograniczenia jego dostępności i nie może prowadzić do nieodwracalnego zniszczenia danych przetwarzanych w systemie informacyjnym podlegającym tej ocenie.

5. Ocena bezpieczeństwa nie może być przeprowadzona, a rozpoczętą przerywa się, jeżeli:

- 1) podmiot krajowego systemu cyberbezpieczeństwa nie posiada kopii bezpieczeństwa badanego systemu;
- 2) istnieje zagrożenie nieodwracalnego zniszczenia danych przetwarzanych w systemie;
- 3) czas potrzebny na przywrócenie systemu z kopii bezpieczeństwa może w istotny sposób zakłócić pracę systemu lub ograniczyć jego dostępność;

- 4) czynności podejmowane podczas oceny bezpieczeństwa mogą doprowadzić do uszkodzenia produktów ICT wchodzących w skład tego systemu oraz innych systemów informacyjnych podmiotu kluczowego;
- 5) istnieje zagrożenie ograniczenia dostępności usług świadczonych przez podmiot krajowego systemu cyberbezpieczeństwa.

6. W celu minimalizacji negatywnych następstw oceny bezpieczeństwa systemu informacyjnego CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT sektorowy uzgadnia z podmiotem krajowego systemu cyberbezpieczeństwa, w drodze porozumienia, tryb i ramowe warunki przeprowadzania tej oceny, w szczególności datę rozpoczęcia, harmonogram oraz zakres i rodzaj przeprowadzanych w ramach oceny bezpieczeństwa testów bezpieczeństwa.

7. Podmiot krajowego systemu cyberbezpieczeństwa, którego system informacyjny podlega ocenie bezpieczeństwa, przekazuje CSIRT przeprowadzającemu ocenę niezbędne informacje techniczne i organizacyjne niezbędne do przeprowadzenia oceny bezpieczeństwa oraz wskazuje imię i nazwisko, adres służbowej poczty elektronicznej oraz numer telefonu służbowego osoby upoważnionej do reprezentacji podmiotu, a także osoby upoważnionej do udzielania wyjaśnień CSIRT w trakcie przeprowadzania oceny bezpieczeństwa.

8. CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT sektorowy mogą wytwarzać lub pozyskiwać urządzenia lub programy komputerowe, o których mowa w art. 269b ustawy z dnia 6 czerwca 1997 r. – Kodeks karny (Dz. U. z 2025 r. poz. 383), oraz ich używać w celu określenia podatności ocenianego systemu informacyjnego na możliwość popełnienia przestępstw, o których mowa w art. 165 § 1 pkt 4, art. 267 § 3, art. 268a § 1 albo § 2 w związku z § 1, art. 269 § 1 i 2 albo art. 269a ustawy z dnia 6 czerwca 1997 r. – Kodeks karny.

9. Używając urządzeń lub programów komputerowych, o których mowa w ust. 8, CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT sektorowy mogą uzyskać dostęp do informacji dla nich nieprzeznaczonej, przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne zabezpieczenie, lub mogą uzyskać dostęp do całości lub części tego systemu informacyjnego.

10. Informacje uzyskane przez CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT sektorowy w wyniku przeprowadzania oceny bezpieczeństwa systemu informacyjnego

stanowią tajemnicę prawnie chronioną i nie mogą być wykorzystane do realizacji innych zadań ustawowych CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT sektorowego.

11. Materiały zawierające informacje, o których mowa w ust. 10, podlegają niezwłocznemu, trwałemu i nieodwracalnemu, protokolarnemu zniszczeniu, którego dokonuje komisja. Zniszczeniu nie podlegają informacje o czynnościach przeprowadzanych w ramach oceny bezpieczeństwa oraz o wykrytych podatnościach systemu informacyjnego.

12. Komisja, o której mowa w ust. 11 zdanie pierwsze, składa się z trzech osób powołanych przez osobę kierującą zespołem CSIRT spośród pracowników, funkcjonariuszy lub żołnierzy realizujących zadania odpowiednio w CSIRT MON, CSIRT NASK, CSIRT GOV albo CSIRT sektorowym.

13. Po przeprowadzeniu oceny bezpieczeństwa systemu informacyjnego CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT sektorowy sporządzają i przekazują podmiotowi, którego system podlegał ocenie bezpieczeństwa, raport zawierający podsumowanie przeprowadzonych w ramach oceny bezpieczeństwa czynności oraz wskazanie wykrytych podatności systemu informacyjnego. Jeżeli ocenę bezpieczeństwa przeprowadza CSIRT sektorowy, to raport przekazywany jest do właściwego CSIRT MON, CSIRT NASK albo CSIRT GOV.

Art. 36c. Jeżeli wykryta podatność może wystąpić w innych systemach informacyjnych, CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT sektorowy informują niezwłocznie ministra właściwego do spraw informatyzacji oraz Pełnomocnika o wykrytej podatności oraz o możliwości jej wystąpienia w innych systemach informacyjnych.

Art. 36d. Rada Ministrów określi, w drodze rozporządzenia:

- 1) tryb przeprowadzania oceny bezpieczeństwa, o której mowa w art. 36a,
- 2) szczegółowe informacje przekazywane do CSIRT niezbędne do przeprowadzenia oceny bezpieczeństwa;
- 3) rodzaje przeprowadzanych testów bezpieczeństwa w ramach oceny bezpieczeństwa, o których mowa w art. 36a ust. 2,
- 4) sposób niszczenia materiałów zawierających informacje, o których mowa w art. 36b ust. 10,
- 5) tryb działania komisji, o której mowa w art. 36b ust. 11 zdanie pierwsze,

6) wzór protokołu zniszczenia materiałów zawierających informacje, o których mowa w art. 36b ust. 10

– mając na uwadze konieczność zapewnienia sprawnego przeprowadzenia oceny bezpieczeństwa, bezpieczeństwo systemów informacyjnych podlegających ocenie, rodzaj materiałów podlegających zniszczeniu i konieczność zapewnienia efektywności i przejrzystości prowadzonych działań komisji.”;

40) w art. 37:

a) ust. 1 i 2 otrzymują brzmienie:

„1. Do udostępniania informacji o podatnościach, incydentach i cyberzagrożeniach oraz o ryzyku wystąpienia incydentów nie stosuje się przepisów:

- 1) ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej;
- 2) ustawy z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego, z wyjątkiem informacji, których udostępnienie nie zagrażałoby bezpieczeństwu państwa lub bezpieczeństwu publicznemu.

2. Właściwy CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT sektorowy mogą, po konsultacji ze zgłaszającym podmiotem kluczowym lub podmiotem ważnym, opublikować na stronie podmiotowej Biuletynu Informacji Publicznej odpowiednio Ministra Obrony Narodowej, Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego, Agencji Bezpieczeństwa Wewnętrznego lub organu właściwego do spraw cyberbezpieczeństwa informacje o incydentach poważnych, gdy jest to niezbędne, aby zapobiec wystąpieniu incyduentu albo zapewnić obsługę incyduentu.”,

b) uchyla się ust. 3,

c) w ust. 4 skreśla się wyrazy „i 3”;

41) w art. 39:

a) ust. 1 otrzymuje brzmienie:

„1. W celu realizacji zadań, o których mowa w art. 26 ust. 3 pkt 1–11, 14 i 16–21 i ust. 5–8, art. 26a–26c oraz art. 44 ust. 1–1c i 3, CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT sektorowe przetwarzają dane pozyskane w związku z incydentami i cyberzagrożeniami, w tym dane osobowe, obejmujące także dane określone w art. 9 ust. 1 i art. 10 rozporządzenia Parlamentu Europejskiego i Rady

(UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.¹³⁾), zwanego dalej „rozporządzeniem 2016/679”, w zakresie i w celu niezbędnym do realizacji tych zadań.”,

b) w ust. 2:

- wyrazy „sektorowe zespoły cyberbezpieczeństwa” zastępuje się wyrazami „CSIRT sektorowe”,
- po wyrazach „art. 9 ust. 1” dodaje się wyrazy „i art. 10”,

c) w ust. 3:

- wprowadzenie do wyliczenia otrzymuje brzmienie:
„CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT sektorowe przetwarzają dane osobowe pozyskane w związku z incydentami i cyberzagrożeniami:”,
- pkt 3 i 4 otrzymują brzmienie:
„3) gromadzone przez podmioty kluczowe lub podmioty ważne w związku ze świadczeniem usług;
4) dotyczące podmiotów zgłaszających incydent zgodnie z art. 30 ust. 1.”,

d) w ust. 4:

- wprowadzenie do wyliczenia otrzymuje brzmienie:
„W celu realizacji zadań określonych w ustawie minister właściwy do spraw informatyzacji, dyrektor Rządowego Centrum Bezpieczeństwa, Pełnomocnik, minister właściwy do spraw zagranicznych oraz organy właściwe do spraw cyberbezpieczeństwa przetwarzają dane osobowe pozyskane w związku z incydentami i cyberzagrożeniami:”,
- pkt 1 otrzymuje brzmienie:
„1) gromadzone przez podmioty kluczowe lub podmioty ważne w związku ze świadczeniem usług;”,
- uchyla się pkt 2,

e) po ust. 4 dodaje się ust. 4a w brzmieniu:

¹³⁾ Zmiany wymienionego rozporządzenia zostały ogłoszone w Dz. Urz. UE L 127 z 23.05.2018, str. 1 oraz Dz. Urz. UE L 74 z 04.03.2021, str. 35.

„4a. Minister właściwy do spraw informatyzacji przetwarza dane osobowe zawierające imię i nazwisko oraz numer PESEL osób fizycznych lub niepowtarzalny identyfikator środka identyfikacji elektronicznej, o którym mowa w aktach wykonawczych Komisji Europejskiej, wydanych na podstawie art. 12 ust. 8 rozporządzenia 910/2014, które w imieniu podmiotu kluczowego lub podmiotu ważnego korzystają z systemu teleinformatycznego, o którym mowa w art. 46 ust. 1, w celu ich uwierzytelnienia w tym systemie.”,

f) ust. 5 i 6 otrzymują brzmienie:

„5. Dane, o których mowa w ust. 3 i 4, są anonimizowane przez CSIRT MON, CSIRT NASK i CSIRT sektorowy niezwłocznie po stwierdzeniu, że nie są niezbędne do realizacji zadań, o których mowa w art. 26 ust. 3 pkt 1–11, 14 i 16–21 i ust. 5–8, art. 26a–26c oraz art. 44 ust. 1–1c i 3.

6. Dane, o których mowa w ust. 3 i 4, niezbędne do realizacji zadań, o których mowa w art. 26 ust. 3 pkt 1–11, 14 i 16–21 i ust. 5–8, art. 26a–26c oraz art. 44 ust. 1–1c i 3, są anonimizowane przez CSIRT MON, CSIRT NASK i CSIRT sektorowy po upływie 5 lat od zakończenia obsługi incydentu, którego dotyczą, z uwzględnieniem ust. 6a.”,

g) po ust. 6 dodaje się ust. 6a i 6b w brzmieniu:

„6a. Dane, o których mowa w ust. 3 i 4, niezbędne do realizacji zadania, o którym mowa w art. 26a, są anonimizowane przez CSIRT NASK po upływie 5 lat od dnia ich pozyskania.

6b. Dane, o których mowa w art. 26c ust. 2, są anonimizowane przez CSIRT NASK po upływie 5 lat od dnia ich pozyskania.”,

h) w ust. 7 wyrazy „sektorowe zespoły cyberbezpieczeństwa” zastępuje się wyrazami „CSIRT sektorowe”,

i) ust. 8 otrzymuje brzmienie:

„8. Realizacja obowiązków wynikających z art. 15, art. 16, art. 18 ust. 1 lit. a i d oraz art. 19 zdanie drugie rozporządzenia 2016/679 przez CSIRT MON, CSIRT NASK i CSIRT sektorowe, w zakresie danych, o których mowa w ust. 3, jest możliwa dopiero po zakończeniu obsługi incydentu, w związku z którym dane zostały pozyskane, lub po zakończeniu obsługi incydentu, do którego obsługi te dane są niezbędne.”,

- j) w ust. 9 we wprowadzeniu do wyliczenia wyrazy „sektorowe zespoły cyberbezpieczeństwa” zastępuje się wyrazami „CSIRT sektorowe”,
- k) dodaje się ust. 10 i 11 w brzmieniu:

„10. Dane, o których mowa w ust. 4, są anonimizowane przez ministra właściwego do spraw informatyzacji, dyrektora Rządowego Centrum Bezpieczeństwa, Pełnomocnika, ministra właściwego do spraw zagranicznych oraz organy właściwe do spraw cyberbezpieczeństwa niezwłocznie po stwierdzeniu, że nie są niezbędne do realizacji zadań wynikających z ustawy, nie później niż po 5 latach po ich uzyskaniu.

11. Minister właściwy do spraw informatyzacji przetwarza dane osobowe, w tym dane, o których mowa w art. 9 ust. 1 rozporządzenia 2016/679, które zostały zawarte w stanowiskach zgłoszonych w ramach konsultacji publicznych projektu dokumentu, o którym mowa w art. 45 ust. 3.”;

- 42) użyte w art. 40, w art. 42 w ust. 1 w pkt 5, w art. 44 w ust. 3 w zdaniu pierwszym i drugim, w art. 49 w ust. 3 we wprowadzeniu do wyliczenia, w art. 64 oraz w art. 93 w ust. 11 w pkt 4, w różnej liczbie i różnym przypadku, wyrazy „sektorowy zespół cyberbezpieczeństwa” zastępuje się użytymi w odpowiedniej liczbie i odpowiednim przypadku wyrazami „CSIRT sektorowy”;
- 43) po art. 40 dodaje się art. 40a w brzmieniu:

„Art. 40a. 1. CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT sektorowy i organy właściwe do spraw cyberbezpieczeństwa mogą, w porozumieniu z Pełnomocnikiem, uczestniczyć w procesie oceny wzajemnej, w celu wymiany doświadczeń, zwiększania wzajemnego zaufania pomiędzy organami z różnych państw, osiągnięcia wysokiego, wspólnego poziomu cyberbezpieczeństwa, a także zwiększenia kluczowych zdolności państw członkowskich Unii Europejskiej w zakresie cyberbezpieczeństwa i doskonalenia ich polityki w tej dziedzinie.

2. Ocena wzajemna jest przeprowadzana przez ekspertów do spraw cyberbezpieczeństwa wyznaczonych na podstawie metodyki obejmującej obiektywne, niedyskryminacyjne, sprawiedliwe i przejrzyste kryteria jako uprawnionych do prowadzenia ocen wzajemnych.

3. Ocena wzajemna może obejmować:

- 1) stopień wdrożenia środków zarządzania ryzykiem w cyberbezpieczeństwie oraz obowiązków dotyczących zgłaszania incydentów;

- 2) poziom zdolności, w tym dostępne zasoby finansowe, techniczne i ludzkie, oraz skuteczność wykonywania zadań przez właściwe organy;
- 3) zdolność operacyjną CSIRT;
- 4) poziom wdrożenia wzajemnej pomocy;
- 5) poziom wdrożenia ustaleń dotyczących mechanizmów wymiany informacji na temat cyberbezpieczeństwa;
- 6) szczególne zagadnienia transgraniczne lub międzysektorowe.

4. W ramach procesu oceny wzajemnej podmioty, o których mowa w ust. 1, mogą przekazywać wyznaczonym przez inne państwa członkowskie Unii Europejskiej ekspertom do spraw cyberbezpieczeństwa informacje dotyczące funkcjonowania tych podmiotów, z uwzględnieniem przepisów o tajemnicach prawnie chronionych.

5. Pełnomocnik może wskazać innym państwom członkowskim Unii Europejskiej uczestniczącym w ocenie wzajemnej szczególne zagadnienia transgraniczne lub międzysektorowe, które należy uwzględnić w ocenie wzajemnej.

6. Pełnomocnik informuje inne państwa członkowskie Unii Europejskiej uczestniczące w ocenie wzajemnej o zakresie oceny wzajemnej przeprowadzanej w Rzeczypospolitej Polskiej.

7. W porozumieniu z Pełnomocnikiem podmioty, o których mowa w ust. 1, mogą przeprowadzić ocenę, o której mowa w ust. 3, dotyczącą krajowego systemu cyberbezpieczeństwa i przedstawić jej wyniki ekspertom z innych państw uczestniczących w ocenie wzajemnej. Ocenę tę przeprowadza się zgodnie z metodyką przyjętą przez Grupę Współpracy.

8. Oceny wzajemnej nie przeprowadza się w terminie 2 lat od sporządzenia sprawozdania z poprzedniej oceny wzajemnej, jeżeli dotyczy tego samego zakresu. Ocena wzajemna dotycząca tego samego zakresu może być przeprowadzona, jeżeli Pełnomocnik zwróci się o to do innego państwa członkowskiego Unii Europejskiej lub państwa członkowskie Unii Europejskiej uzgodnią to w ramach Grupy Współpracy.

9. Pełnomocnik może sprzeciwić się przeprowadzeniu oceny wzajemnej przez konkretnych ekspertów z innego państwa członkowskiego Unii Europejskiej, jeżeli występuje konflikt interesów.

10. Eksperci do spraw cyberbezpieczeństwa, wyznaczeni przez podmioty, o których mowa w ust. 1, uczestniczący w ocenie wzajemnej sporządzają sprawozdanie z oceny wzajemnej, które zatwierdza Pełnomocnik. Sprawozdanie zawiera podsumowanie

czynności podjętych w ramach oceny wzajemnej oraz zalecenia. Sprawozdanie udostępnia się innym państwom członkowskim Unii Europejskiej uczestniczącym w ocenie wzajemnej oraz organom właściwym do spraw cyberbezpieczeństwa, CSIRT MON, CSIRT NASK i CSIRT GOV.

11. Pełnomocnik może udostępnić sprawozdanie Grupie Współpracy lub Sieci CSIRT. Sprawozdanie to może zostać opublikowane w Biuletynie Informacji Publicznej Pełnomocnika w zakresie, w jakim nie zawiera informacji stanowiących tajemnice prawnie chronione.”;

44) w art. 41:

- a) po pkt 1 dodaje się pkt 1a w brzmieniu:
„1a) dla sektora inwestycji energii jądrowej – minister właściwy do spraw energii;”,
- b) pkt 8 otrzymuje brzmienie:
„8) dla sektora infrastruktury cyfrowej z wyłączeniem podmiotów, o których mowa w art. 26 ust. 5 pkt 1, oraz z wyłączeniem podsektora komunikacji elektronicznej – minister właściwy do spraw informatyzacji;”,
- c) po pkt 8 dodaje się pkt 8a w brzmieniu:
„8a) dla podsektora komunikacji elektronicznej, z wyłączeniem podmiotów, o których mowa w art. 26 ust. 5 pkt 1 – Prezes Urzędu Komunikacji Elektronicznej;”,
- d) w pkt 5, 6 i 9 wyrazy „o których mowa w art. 26 ust. 5” zastępuje się wyrazami „o których mowa w art. 26 ust. 5 pkt 1”,
- e) po pkt 9 dodaje się pkt 9a–9k w brzmieniu:
 - „9a) dla sektora zbiorowego odprowadzania ścieków – minister właściwy do spraw gospodarki wodnej;
 - 9b) dla sektora zarządzania usług ICT – minister właściwy do spraw informatyzacji;
 - 9c) dla sektora przestrzeni kosmicznej – minister właściwy do spraw gospodarki;
 - 9d) dla sektora produkcji, wytwarzania i dystrybucji chemikaliów – minister właściwy do spraw gospodarki;
 - 9e) dla sektora produkcji, przetwarzania i dystrybucji żywności – minister właściwy do spraw rolnictwa;

- 9f) dla sektora produkcji, z wyłączeniem podsektora produkcja wyrobów medycznych i wyrobów medycznych do diagnostyki in vitro – minister właściwy do spraw gospodarki;
 - 9g) dla podsektora produkcji wyrobów medycznych i wyrobów medycznych do diagnostyki in vitro – minister właściwy do spraw zdrowia;
 - 9h) dla sektora usług pocztowych – Prezes Urzędu Komunikacji Elektronicznej;
 - 9i) dla sektora gospodarowania odpadami – minister właściwy do spraw klimatu;
 - 9j) dla sektora dostawców usług cyfrowych – minister właściwy do spraw informatyzacji;
 - 9k) dla sektora badań naukowych – minister właściwy do spraw szkolnictwa wyższego i nauki.”,
- f) uchyla się pkt 10 i 11;
- 45) po art. 41 dodaje się art. 41a w brzmieniu:
- „Art. 41a. 1. Organem właściwym do spraw cyberbezpieczeństwa w sektorze podmiotów publicznych, z wyłączeniem podmiotów podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych oraz urzędu obsługującego tego ministra, jest minister właściwy do spraw informatyzacji.
2. Organem właściwym do spraw cyberbezpieczeństwa w sektorze podmiotów publicznych dla podmiotów podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych oraz dla urzędu obsługującego tego ministra jest Minister Obrony Narodowej.
3. Organem właściwym do spraw cyberbezpieczeństwa w sektorze podmiotów publicznych dla jednostek organizacyjnych podległych ministrowi właściwemu do spraw finansów publicznych lub przez niego nadzorowanych, urzędu obsługującego tego ministra oraz spółki, o której mowa w art. 2 ust. 1 ustawy z dnia 29 kwietnia 2016 r. o szczególnych zasadach wykonywania niektórych zadań dotyczących informatyzacji w zakresie działów administracji rządowej budżet i finanse publiczne (Dz. U. z 2021 r. poz. 186 oraz z 2025 r. poz. 1158), jest minister właściwy do spraw finansów publicznych.
4. Dla podmiotu publicznego, który jest wymieniony w innym sektorze niż sektor podmiotów publicznych, organem właściwym do spraw cyberbezpieczeństwa jest organ właściwy dla danego sektora. Przepis nie dotyczy samorządowych podmiotów publicznych.

5. Minister właściwy do spraw informatyzacji może powierzyć realizację zadań nadzorczych nad podmiotami kluczowymi w sektorze podmiotów publicznych CSIRT NASK, z wyjątkiem wydawania decyzji administracyjnych. Zadania te są finansowane w ramach dotacji, o której mowa w art. 26 ust. 9. Przepisów art. 42 ust. 3–6 nie stosuje się w tym zakresie.”;

46) w art. 42:

a) w ust. 1:

– pkt 1–3 otrzymują brzmienie:

- „1) prowadzi bieżącą analizę podmiotów w danym sektorze lub podsektorze pod kątem uznania ich za podmiot kluczowy lub podmiot ważny;
- 2) wpisuje z urzędu podmiot kluczowy lub podmiot ważny do wykazu podmiotów kluczowych i podmiotów ważnych, jeżeli podmiot ten nie zarejestrował się w tym wykazie;
- 3) wydaje decyzję o uznaniu podmiotu za podmiot kluczowy lub podmiot ważny, o której mowa w art. 71 ust. 1;”;

– uchyla się pkt 4,

– pkt 6–8 otrzymują brzmienie:

- „6) monitoruje stosowanie przepisów ustawy przez podmioty kluczowe lub podmioty ważne;
- 7) wzywa na wniosek CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT sektorowego podmioty kluczowe lub podmioty ważne do usunięcia w wyznaczonym terminie podatności, które doprowadziły lub mogły doprowadzić do incydentu poważnego lub krytycznego;
- 8) prowadzi kontrole podmiotów kluczowych lub podmiotów ważnych;”;

– pkt 10 otrzymuje brzmienie:

„10) przetwarza informacje, w tym dane osobowe, dotyczące podmiotów kluczowych lub podmiotów ważnych oraz świadczonych przez nich usług, w zakresie niezbędnym do:

- a) identyfikacji podmiotów kluczowych lub podmiotów ważnych,
- b) zapewnienia wymiany informacji w zakresie cyberbezpieczeństwa, w tym o incydentach, podatnościach i cyberzagrożeniach między podmiotami kluczowymi lub podmiotami ważnymi a CSIRT MON,

CSIRT NASK, CSIRT GOV, CSIRT sektorowymi i organami właściwymi do spraw cyberbezpieczeństwa,

c) prowadzenia czynności nadzorczych nad podmiotami kluczowymi lub podmiotami ważnymi;”,

- w pkt 11 kropkę zastępuje się średnikiem i dodaje się pkt 12 i 13 w brzmieniu:
- „12) współpracuje oraz wymienia informacje i dokumenty z właściwym organem w rozumieniu rozporządzenia 2022/2554, w zakresie niezbędnym do wykonywania przez ten organ obowiązków wynikających z rozporządzenia 2022/2554;
- 13) współpracuje oraz wymienia informacje i dokumenty z organem właściwym do spraw podmiotów krytycznych w zakresie nadzoru nad podmiotem kluczowym będącym podmiotem krytycznym.”,

b) uchyla się ust. 2;

c) dodaje się ust. 9–11 w brzmieniu:

„9. Organ właściwy do spraw cyberbezpieczeństwa dla sektora bankowości i infrastruktury rynków finansowych realizuje swoje zadania, z uwzględnieniem zakresu zastosowania ustawy do podmiotów finansowych.

10. W ramach współpracy, o której mowa w ust. 1 pkt 12, mającej związek z podmiotem kluczowym lub podmiotem ważnym, który zgodnie z rozporządzeniem 2022/2554 został wyznaczony jako kluczowy zewnętrzny dostawca usług ICT, organ właściwy do spraw cyberbezpieczeństwa w szczególności udziela informacji oraz istotnych zaleceń technicznych i pomocy technicznej, a także umożliwia skuteczną i szybką koordynację działań nadzorczych, w tym na potrzeby prowadzenia kontroli.

11. Organ właściwy do spraw cyberbezpieczeństwa prowadzi i regularnie aktualizuje wykaz osób, wobec których wydana została decyzja o zastosowaniu środka nadzorczego, o którym mowa w art. 53 ust. 9 pkt 6, obejmujący:

- 1) imię (imiona);
- 2) nazwisko;
- 3) numer PESEL, a w przypadku jego nieposiadania – datę urodzenia;
- 4) nazwę podmiotu kluczowego;
- 5) datę wydania decyzji;
- 6) znak sprawy;
- 7) okres obowiązywania zakazu;

8) podstawę prawną wydania decyzji.”;

47) w art. 43:

a) ust. 1 otrzymuje brzmienie

„1. Organ właściwy do spraw cyberbezpieczeństwa może, bez wszczynania postępowania, o którym mowa w art. 7j lub art. 7l, wystąpić do podmiotu, o którym mowa w załączniku nr 1 lub 2 do ustawy, o udzielenie informacji, które umożliwią wstępną ocenę, czy dany podmiot należy uznać za podmiot kluczowy lub podmiot ważny. Przepis art. 53c ust. 2 i 3 stosuje się odpowiednio.”,

b) uchyla się ust. 2–5,

c) ust. 6 otrzymuje brzmienie:

„6. Informacje udzielone przez podmiot, o którym mowa w ust. 1, mogą stanowić podstawę do wpisania podmiotu do wykazu na podstawie art. 7j albo wydania decyzji, o której mowa w art. 7l.”;

48) w art. 44:

a) ust. 1 otrzymuje brzmienie:

„1. Organ właściwy do spraw cyberbezpieczeństwa zapewnia funkcjonowanie CSIRT sektorowego dla podmiotów kluczowych lub podmiotów ważnych w danym sektorze lub podsektorze wymienionych w załączniku nr 1 i 2 do ustawy, do którego zadań należy:

- 1) przyjmowanie wczesnych ostrzeżeń, zgłoszeń o incydentach, sprawozdań okresowych i sprawozdań końcowych, o których mowa w art. 11 ust. 1 pkt 4–4c;
- 2) przyjmowanie zgłoszeń o potencjalnych zdarzeniach dla cyberbezpieczeństwa;
- 3) reagowanie na incydenty;
- 4) gromadzenie informacji o podatnościach i cyberzagrożeniach;
- 5) współpraca z podmiotem kluczowym lub podmiotem ważnym w zakresie wymiany dobrych praktyk oraz informacji o podatnościach i cyberzagrożeniach, organizacja i uczestniczenie w ćwiczeniach oraz wspieranie inicjatyw szkoleniowych;
- 6) współpraca z CSIRT MON, CSIRT NASK i CSIRT GOV w koordynowanym przez nie reagowaniu na incydenty, w szczególności w zakresie wymiany informacji o cyberzagrożeniach oraz stosowanych środkach zapobiegających i ograniczających wpływ incydentów;

- 7) współpraca z innymi CSIRT sektorowymi w zakresie wymiany informacji o podatnościach i cyberzagrożeniach.”,
- b) po ust. 1 dodaje się ust. 1a–1d w brzmieniu:
 - „1a. CSIRT sektorowy przekazuje, za pomocą systemu teleinformatycznego, o którym mowa w art. 46 ust. 1, wczesne ostrzeżenie, zgłoszenie incydentu, sprawozdanie okresowe i sprawozdanie końcowe, o których mowa w art. 11 ust. 1 pkt 4–4c, niezwłocznie, nie później niż 8 godzin od jego otrzymania, do właściwego CSIRT MON, CSIRT NASK albo CSIRT GOV.
 - 1b. CSIRT sektorowy może, w szczególności:
 - 1) zapewniać we współpracy z CSIRT MON, CSIRT NASK i CSIRT GOV dynamiczną analizę ryzyka i analizę incydentów oraz wspomagać w podnoszeniu świadomości cyberzagrożeń wśród podmiotów kluczowych lub podmiotów ważnych danego sektora lub podsektora;
 - 2) wykonywać niezbędne działania techniczne związane z analizą cyberzagrożeń oraz reagowaniem na incydent poważny;
 - 3) koordynować, w ramach sektora lub podsektora, w uzgodnieniu z podmiotami kluczowymi lub podmiotami ważnymi obsługę incydentów, które ich dotyczą;
 - 4) wspierać, w uzgodnieniu z podmiotem kluczowym lub podmiotem ważnym, wykonywanie przez niego obowiązków określonych w art. 11, art. 12–12b i art. 13;
 - 5) w ramach reagowania na incydent poważny wystąpić do organu właściwego do spraw cyberbezpieczeństwa z wnioskiem o wezwanie podmiotu kluczowego lub podmiotu ważnego, aby w wyznaczonym terminie usunął podatności, które doprowadziły lub mogłyby doprowadzić do incydentu poważnego;
 - 6) prowadzić działania na rzecz podnoszenia poziomu bezpieczeństwa systemów informacyjnych podmiotów kluczowych lub podmiotów ważnych w danym sektorze lub podsektorze, w szczególności przez:
 - a) wykonywanie oceny bezpieczeństwa,
 - b) identyfikowanie podatności systemów dostępnych w otwartych sieciach teleinformatycznych, a także powiadamianie właścicieli tych systemów o wykrytych podatnościach oraz cyberzagrożeniach;

- 7) na wniosek podmiotu kluczowego lub ważnego wspierać dany podmiot w zakresie monitorowania ich sieci i systemów informatycznych w czasie rzeczywistym lub zbliżonym do rzeczywistego.

1c. CSIRT sektorowy, który otrzymał zgłoszenie incydentu, a nie jest właściwy do jego przyjęcia, przekazuje niezwłocznie to zgłoszenie do właściwego CSIRT wraz z otrzymanymi informacjami.

1d. CSIRT sektorowy informuje o złożeniu wniosku, o którym mowa w ust. 1b pkt 5, właściwy CSIRT MON, CSIRT NASK albo CSIRT GOV;”,

- c) uchyla się ust. 2,

- d) ust. 4 otrzymuje brzmienie:

„4. Organ właściwy do spraw cyberbezpieczeństwa informuje podmioty kluczowe lub podmioty ważne w danym sektorze oraz CSIRT MON, CSIRT NASK i CSIRT GOV o ustanowieniu CSIRT sektorowego i zakresie realizowanych zadań.”,

- e) dodaje się ust. 5 i 6 w brzmieniu:

„5. Przepisy ust. 1–1d, 3 i 4 stosuje się odpowiednio do CSIRT sektorowego ustanowionego w sektorze bankowości i infrastruktury rynków finansowych, w szczególności w zakresie poważnych incydentów związanych z ICT zgłaszanych przez podmioty kluczowe lub podmioty ważne.

6. CSIRT sektorowy ustanowiony w sektorze bankowości i infrastruktury rynków finansowych może również realizować swoje zadania w odniesieniu do podmiotów finansowych niebędących podmiotami kluczowymi lub podmiotami ważnymi, w szczególności w zakresie wsparcia w obsłudze poważnych incydentów związanych z ICT, gdy nie stanowi to dla niego nieproporcjonalnego czy nadmiernego obciążenia, z uwzględnieniem priorytetowego traktowania poważnych incydentów związanych z ICT zgłaszanych przez podmioty finansowe będące podmiotami kluczowymi lub podmiotami ważnymi oraz odpowiedniego stosowania ust. 1–1d, 3 i 4 do realizacji zadań.”;

- 49) po art. 44 dodaje się art. 44a–44f w brzmieniu:

„Art. 44a. 1. Organ właściwy do spraw cyberbezpieczeństwa może powierzyć realizację zadania lub zadań CSIRT sektorowego:

- 1) jednostce jemu podległej lub przez niego nadzorowanej;
- 2) organowi przez niego nadzorowanemu;

3) urzędowi, który go obsługuje.

2. Organ właściwy do spraw cyberbezpieczeństwa może powierzyć realizację zadania albo zadań CSIRT sektorowego państwowej osobie prawnej, o której mowa w art. 3 ustawy z dnia 16 grudnia 2016 r. o zasadach zarządzania mieniem państwowym, jeżeli dysponuje ona zdolnościami technicznymi i organizacyjnymi niezbędnymi do wypełniania zadań CSIRT sektorowego w danym sektorze lub podsektorze.

3. Organy właściwe do spraw cyberbezpieczeństwa mogą, w drodze porozumienia, powierzyć realizację zadania lub zadań CSIRT sektorowego dla kilku sektorów lub podsektorów, dla których są właściwe, jednostce podległej jednemu z tych organów albo nadzorowanej przez jeden z tych organów. Stroną tego porozumienia jest również jednostka, której powierzono zadania.

4. Organy właściwe do spraw cyberbezpieczeństwa określają w porozumieniu, o którym mowa w ust. 3, w szczególności zakres powierzonych zadań, weryfikację prawidłowości ich wykonania oraz sposób finansowania powierzonych zadań.

Art. 44b. 1. Minister będący organem właściwym do spraw cyberbezpieczeństwa dla kilku sektorów lub podsektorów może powierzyć jednostce jemu podległej albo nadzorowanej przez niego zadanie lub zadania CSIRT sektorowego.

2. Powierzenie odbywa się w drodze decyzji, do której nie stosuje się przepisów ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego.

3. Komunikat o powierzeniu przez ministra będącego organem właściwym do spraw cyberbezpieczeństwa dla kilku sektorów lub podsektorów zadania lub zadań CSIRT sektorowego jednostce podległej albo nadzorowanej przez tego ministra ogłasza się w dzienniku urzędowym organu właściwego do spraw cyberbezpieczeństwa.

4. Ministrowie, którzy przejęli właściwość nadzorczą nad sektorami, dla których dotychczasowy minister wyznaczył wspólny CSIRT sektorowy, zawierają porozumienie, w którym wyznaczają jednostkę, która przejmie zadania CSIRT sektorowego dla poszczególnych sektorów lub podsektorów. Do czasu zawarcia porozumienia decyzja, o której mowa w ust. 2, zachowuje moc.

Art. 44c. 1. Organ właściwy do spraw cyberbezpieczeństwa może powierzyć CSIRT MON, CSIRT NASK albo CSIRT GOV realizację zadania albo zadań CSIRT sektorowego.

2. Powierzenie, o którym mowa w ust. 1, następuje na podstawie porozumienia organu właściwego do spraw cyberbezpieczeństwa:

- 1) w przypadku powierzenia zadań CSIRT NASK – za zgodą ministra właściwego do spraw informatyzacji – z Dyrektorem Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego;
- 2) w przypadku powierzenia zadań CSIRT GOV – z Szefem Agencji Bezpieczeństwa Wewnętrznego;
- 3) w przypadku powierzenia zadań CSIRT MON – z Ministrem Obrony Narodowej.

3. Do porozumienia, o którym mowa w ust. 2, stosuje się przepis art. 44a ust. 4.

4. Minister Obrony Narodowej, jako organ właściwy do spraw cyberbezpieczeństwa, może powierzyć CSIRT MON realizację zadań CSIRT sektorowego w drodze decyzji niepodlegającej ogłoszeniu.

Art. 44d. 1. Zadania CSIRT sektorowego:

- 1) są finansowane z części budżetu państwa, której dysponentem jest minister albo centralny organ administracji rządowej, będący organem właściwym do spraw cyberbezpieczeństwa;
- 2) mogą być dofinansowywane:
 - a) ze środków pochodzących z budżetu Unii Europejskiej,
 - b) ze środków przeznaczonych na realizację programów finansowanych z udziałem środków pochodzących z budżetu Unii Europejskiej.

2. Jednostka, której powierzono zadania CSIRT sektorowego dla danego sektora lub podsektora, może otrzymać na realizację tych zadań dotację celową, z części budżetowej, której dysponentem jest minister będący organem właściwym do spraw cyberbezpieczeństwa dla danego sektora lub podsektora.

3. W przypadku gdy jednostce budżetowej powierzono realizację zadania lub zadań CSIRT sektorowego dla kilku sektorów lub podsektorów, otrzymuje ona środki z części budżetowych, których dysponentami są organy właściwe do spraw cyberbezpieczeństwa dla danego sektora lub podsektora, które zawarły porozumienie, o którym mowa w art. 44a ust. 3.

Art. 44e. 1. Komunikat o zawarciu porozumienia, o którym mowa w art. 44a ust. 3, art. 44b ust. 3 lub art. 44c ust. 2, ogłasza się w dzienniku urzędowym organu właściwego do spraw cyberbezpieczeństwa i wskazuje się:

- 1) adres strony internetowej, na której zostanie zamieszczona treść porozumienia wraz ze stanowiącymi jego integralną treść załącznikami;
- 2) termin, od którego porozumienie będzie obowiązywało.

2. Organ właściwy do spraw cyberbezpieczeństwa informuje Pełnomocnika o zawarciu porozumienia, o którym mowa w art. 44a ust. 3, art. 44b ust. 3 lub art. 44c ust. 2. Pełnomocnik publikuje komunikat o zawarciu porozumienia na swojej stronie podmiotowej Biuletynu Informacji Publicznej.

Art. 44f. Organ właściwy do spraw cyberbezpieczeństwa raz w roku, w terminie do dnia 31 stycznia, przedkłada Pełnomocnikowi sprawozdanie z funkcjonowania CSIRT sektorowego za rok poprzedni.”;

50) w art. 45:

a) w ust. 1:

- po pkt 1 dodaje się pkt 1a i 1b w brzmieniu:
 - „1a) monitorowanie wdrażania Krajowego planu reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę, zwanego dalej „Krajowym planem”, oraz realizację działań na rzecz jego wdrożenia;
 - 1b) prowadzenie wykazu podmiotów kluczowych i podmiotów ważnych;”;
- pkt 3 otrzymuje brzmienie:
 - „3) opracowywanie rocznych sprawozdań dotyczących incydentów poważnych zgłaszanych przez podmioty kluczowe lub podmioty ważne mających wpływ na ciągłość świadczenia usług przez te podmioty w Rzeczypospolitej Polskiej oraz ciągłość świadczenia usług w państwach członkowskich Unii Europejskiej;”;
- pkt 6 otrzymuje brzmienie:
 - „6) udostępnianie informacji i dobrych praktyk uzyskanych z Grupy Współpracy podmiotom krajowego systemu cyberbezpieczeństwa w celu usprawnienia działań krajowego systemu cyberbezpieczeństwa;”;

– dodaje się pkt 7–15 w brzmieniu:

- „7) rekomendowanie i wspieranie przy wykorzystywaniu europejskich lub międzynarodowych standardów, a także specyfikacji technicznych mających znaczenie dla bezpieczeństwa systemów informacyjnych;
- 8) zachęcanie do korzystania z produktów ICT, usług ICT i procesów ICT certyfikowanych w ramach europejskich lub krajowych programów certyfikacji cyberbezpieczeństwa;
- 9) ustanowienie odpowiednich struktur komunikacyjnych na potrzeby wczesnego wykrywania kryzysów w cyberbezpieczeństwie, reagowania kryzysowego w cyberbezpieczeństwie i zarządzania kryzysowego w cyberbezpieczeństwie, a także koordynacji współpracy w celu ochrony bezpieczeństwa technologii informacyjnej aktywów o krytycznym znaczeniu we współpracy z sektorem prywatnym;
- 10) współpracę w obszarze cyberbezpieczeństwa z państwami trzecimi;
- 11) koordynację działań organów państwa w przypadku wystąpienia sytuacji kryzysowej w cyberbezpieczeństwie niedotyczącej wymiaru militarnego;
- 12) uczestniczenie w pracach Europejskiej sieci organizacji łącznikowych do spraw kryzysów cyberbezpieczeństwa;
- 13) przekazywanie Komisji Europejskiej aktualnych informacji o organach właściwych do spraw cyberbezpieczeństwa oraz Pojedynczym Punkcie Kontaktowym, ich danych identyfikacyjnych oraz zadaniach;
- 14) przekazywanie Komisji Europejskiej aktualnych informacji o CSIRT MON, CSIRT NASK i CSIRT GOV oraz CSIRT sektorowych, wraz z ich danymi kontaktowymi oraz zadaniami;
- 15) udzielanie wsparcia finansowego na działania służące rozwojowi cyberbezpieczeństwa.”,

b) ust. 2 otrzymuje brzmienie

„2. Przez Grupę Współpracy rozumie się grupę, o której mowa w art. 14 dyrektywy 2022/2555.”,

c) dodaje się ust. 3–5 w brzmieniu:

„3. Minister właściwy do spraw informatyzacji może opublikować na swojej stronie podmiotowej Biuletynu Informacji Publicznej zestawienie wymogów dokumentów normalizacyjnych, o których mowa w art. 2 pkt 3 ustawy z dnia 12

września 2002 r. o normalizacji (Dz. U. z 2015 r. poz. 1483), których wykonywanie realizuje obowiązki wynikające z przepisów ustawy oraz z przepisów wydanych na podstawie art. 8a.

4. Projekt zestawienia, o którym mowa w ust. 3, minister właściwy do spraw informatyzacji kieruje do 30-dniowych konsultacji publicznych, z których sporządza raport, w którym wskazuje główne tezy zawarte w stanowiskach zgłoszonych do projektu zestawienia oraz odniesienie się do nich.

5. Projekt zestawienia, o którym mowa w ust. 3, uwagi zgłoszone w ramach konsultacji publicznych oraz raport ministra właściwego do spraw informatyzacji publikuje się na stronie podmiotowej Biuletynu Informacji Publicznej ministra właściwego do spraw informatyzacji, z wyłączeniem danych osobowych osób fizycznych biorących udział w konsultacjach publicznych.”;

51) art. 45a otrzymuje brzmienie:

„Art. 45a. 1. Minister właściwy do spraw informatyzacji może udzielić wsparcia finansowego w ramach programów rządowych lub innych programów finansowanych w całości albo w części z udziałem środków, o których mowa w art. 5 ust. 3 pkt 6 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych, na realizację projektów, których celem jest:

- 1) tworzenie i rozwój produktów ICT, usług ICT oraz procesów ICT z zakresu cyberbezpieczeństwa;
- 2) rozwój kompetencji w obszarze cyberbezpieczeństwa;
- 3) zapewnianie cyberbezpieczeństwa w danej jednostce organizacyjnej;
- 4) promocja dobrych praktyk, programów edukacyjnych, kampanii i szkoleń na rzecz poszerzania wiedzy i budowania świadomości z zakresu cyberbezpieczeństwa;
- 5) wsparcie w obszarze standaryzacji i certyfikacji cyberbezpieczeństwa;
- 6) rozwój infrastruktury służącej zapewnianiu cyberbezpieczeństwa;
- 7) wsparcie badań naukowych, rozwoju technologicznego i projektów pilotażowych związanych z cyberbezpieczeństwem;
- 8) wsparcie w obsłudze incydentów;
- 9) identyfikacja i mitygacja podatności produktów ICT, usług ICT i procesów ICT;
- 10) zwiększenie rozpoznawalności produktów lub usług z zakresu cyberbezpieczeństwa;
- 11) inne działania służące rozwojowi cyberbezpieczeństwa.

2. Wsparcie finansowe, o którym mowa w ust. 1, może być udzielane podmiotom publicznym, jak i prywatnym, i może stanowić:

- 1) pomoc publiczną dla podmiotów prywatnych;
- 2) pomoc *de minimis* dla podmiotów prywatnych;
- 3) dofinansowanie dla podmiotów publicznych.

3. Wsparcie finansowe, o którym mowa w ust. 1, jest udzielane podmiotom, które mają zdolność do realizacji projektu, o którym mowa w ust. 1.

4. Wsparcie finansowe, o którym mowa w ust. 1, może mieć charakter zwrotny albo bezzwrotny.

5. Wybór projektów, na które jest udzielane wsparcie finansowe, o którym mowa w ust. 1, następuje w trybie konkursowym albo pozakonkursowym.

6. Minister właściwy do spraw informatyzacji określi, odrębnie dla danego programu, o którym mowa w ust. 1, w drodze rozporządzenia, szczegółowe warunki, formę oraz tryb udzielania wsparcia finansowego, o którym mowa w ust. 1, a także podmioty go udzielające, uwzględniając konieczność realizacji celów określonych w tych programach, efektywność i skuteczność wykorzystania tego wsparcia oraz przejrzystość jego udzielania, a także zapewnienie jego zgodności z rynkiem wewnętrznym.”;

52) po art. 45a dodaje się art. 45b i art. 45c w brzmieniu:

„Art. 45b. Wsparcie finansowe, o którym mowa w art. 45a ust. 1, może być udzielane w imieniu ministra właściwego do spraw informatyzacji przez podmiot mu podległy albo przez niego nadzorowany.

Art. 45c 1. Wyboru projektów dokonuje się w sposób przejrzysty, rzetelny i bezstronny na podstawie obiektywnych kryteriów oceny biorąc pod uwagę w szczególności wpływ projektu na realizację celów określonych w art. 45a ust. 1 oraz na krajowy system cyberbezpieczeństwa.

2. Podstawę dofinansowania projektu stanowi umowa o dofinansowanie projektu zawarta z beneficjentem przez podmiot udzielający wsparcia finansowego, o którym mowa w art. 45a ust. 1.

3. Beneficjent może wykorzystywać otrzymane wsparcie tylko na wydatki służące realizacji celów wskazanych w art. 45a ust. 1.

4. Beneficjent jest obowiązany zwrócić wsparcie wykorzystane niezgodnie z ust. 3, w terminie nie dłuższym niż 15 dni od określonego w umowie dnia wykonania zadania.

5. Beneficjent informuje podmiot udzielający wsparcie o postępach w realizacji projektu w terminach wskazanych w umowie, o której mowa w ust. 2.

6. Do umowy, o której mowa w ust. 2, stosuje się odpowiednio art. 150 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych.”;

53) w art. 46:

a) w ust. 1:

- w pkt 5 wyrazy „zagrożeniach cyberbezpieczeństwa” zastępuje się wyrazem „cyberzagrożeniach”,
- kropkę zastępuje się średnikiem i dodaje się pkt 6–8 w brzmieniu:
 - „6) czynności nadzorcze organów właściwych do spraw cyberbezpieczeństwa;
 - 7) dokonywanie zgłoszenia naruszenia ochrony danych osobowych, o którym mowa w art. 33 rozporządzenia 2016/679 i art. 44 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2023 r. poz. 1206) przez podmioty kluczowe lub podmioty ważne;
 - 8) wymianę informacji o aktach ministra właściwego do spraw informatyzacji, Pełnomocnika, organów właściwych do spraw cyberbezpieczeństwa oraz Prezesa Rady Ministrów, o których mowa w art. 33 ust. 4, art. 42 ust. 1 pkt 5, art. 45 ust. 3, art. 67, art. 67a, art. 67b ust. 15, art. 67g ust. 1 i art. 67l ust. 1.”,

b) po ust. 1 dodaje się ust. 1a w brzmieniu:

„1a. W systemie teleinformatycznym prowadzi się wykaz podmiotów kluczowych i podmiotów ważnych.”,

c) ust. 2 otrzymuje brzmienie:

„2. CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT sektorowe, organy właściwe do spraw cyberbezpieczeństwa oraz Prezes Urzędu Ochrony Danych Osobowych korzystają z systemu teleinformatycznego w celu realizacji swoich zadań ustawowych.”,

d) uchyla się ust. 3,

e) dodaje się ust. 4–9 w brzmieniu:

„4. Podmioty kluczowe lub podmioty ważne, korzystają z systemu teleinformatycznego w zakresie, o którym mowa w ust. 1, w terminie 6 miesięcy od spełnienia przesłanek uznania za podmiot kluczowy lub podmiot ważny.

5. Uwierzytelnienie w systemie teleinformatycznym następuje za pomocą środków określonych w art. 20a ust. 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne.

6. W celu zapewnienia bezpiecznego korzystania z systemu teleinformatycznego podmioty kluczowe lub podmioty ważne są obowiązane zapewnić bezpieczeństwo, ciągłość działania, aktualność i skuteczność zabezpieczeń oraz rozliczalność stosowanych systemów teleinformatycznych.

7. W celu wykonania obowiązku, o którym mowa w ust. 6, podmioty kluczowe lub podmioty ważne dostosowują swoje systemy informacyjne do minimalnych wymagań technicznych i funkcjonalnych korzystania z systemu teleinformatycznego, opublikowanych przez ministra właściwego do spraw informatyzacji na jego stronie podmiotowej Biuletynu Informacji Publicznej w terminie 6 miesięcy od dnia opublikowania tych wymagań.

8. Minister właściwy do spraw informatyzacji publikuje na swojej stronie podmiotowej Biuletynu Informacji Publicznej wykaz usług stosowany w systemie teleinformatycznym, w szczególności świadczonych przez podmioty kluczowe lub podmioty ważne.

9. CSIRT MON, CSIRT NASK, CSIRT GOV, po uzyskaniu zgody właściwego CSIRT poziomu krajowego, mogą uzyskać dostęp do wszelkich informacji przetwarzanych w systemie teleinformatycznym, w zakresie dotyczącym podmiotu będącego we właściwości innego CSIRT, w szczególności w celu szacowania ryzyka bezpieczeństwa łańcucha dostaw produktów ICT, usług ICT i procesów ICT, od których zależy świadczenie usługi przez podmiot pozostający we właściwości danego CSIRT.”;

54) po art. 46 dodaje się art. 46a i art. 46b w brzmieniu:

„Art. 46a. W celu realizacji zadań, o których mowa w art. 11 ust. 2 oraz w art. 46 ust. 1 pkt 3, 4 i 6, Minister Obrony Narodowej, urząd go obsługujący oraz podmioty podległe Ministrowi Obrony Narodowej i przez niego nadzorowane mogą korzystać z środków komunikacji elektronicznej, innych niż system, o którym mowa w art. 46 ust. 1, zapewniających poufność, integralność, dostępność i autentyczność przetwarzanych danych.

Art. 46b. 1. W przypadku doręczenia pisma w postaci elektronicznej za pośrednictwem systemu, o którym mowa w art. 46 ust. 1, przez organ administracji publicznej doręczenie jest skuteczne, jeżeli adresat potwierdzi odbiór pisma w systemie.

2. W przypadku nieodebrania pisma w postaci elektronicznej za pośrednictwem systemu, o którym mowa w art. 46 ust. 1, organ administracji publicznej po upływie 7 dni, licząc od dnia jego wysłania, przesyła zawiadomienie o możliwości odebrania tego pisma.

3. Zawiadomienie o możliwości odebrania pisma może być automatycznie tworzone i przesyłane za pośrednictwem systemu, o którym mowa w art. 46 ust. 1, a odbioru tego zawiadomienia nie potwierdza się.

4. W przypadku nieodebrania pisma w postaci elektronicznej za pośrednictwem systemu, o którym mowa w art. 46 ust. 1, doręczenie uważa się za dokonane po upływie 14 dni, licząc od dnia wysłania pisma.”;

55) w art. 47:

a) ust. 1 otrzymuje brzmienie:

„1. Minister właściwy do spraw informatyzacji może powierzyć realizację zadań, o których mowa w art. 45 ust. 1, art. 45a ust. 1 i art. 46 ust. 1 i 1a, jednostkom jemu podległym lub przez niego nadzorowanym.”,

b) dodaje się ust. 3 w brzmieniu:

„3. Minister właściwy do spraw informatyzacji może udostępniać jednostkom, o których mowa w ust. 1, dane z wykazu podmiotów kluczowych i podmiotów ważnych w zakresie i w celu realizacji zadań im powierzonych, z uwzględnieniem poufności, integralności, dostępności i autentyczności tych danych.”;

56) w art. 48 pkt 1 i 2 otrzymują brzmienie:

„1) odbieranie zgłoszeń incydentu dotyczącego więcej niż jednego sektora lub dotyczącego innych państw członkowskich Unii Europejskiej z Pojedynczych Punktów Kontaktowych w innych państwach członkowskich Unii Europejskiej, także przekazywanie tych zgłoszeń do CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT sektorowego;

2) przekazywanie, na wniosek właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV, zgłoszenia incydentu dotyczącego więcej niż jednego sektora lub innych państw członkowskich Unii Europejskiej do Pojedynczych Punktów Kontaktowych w innych państwach członkowskich Unii Europejskiej;”;

57) w art. 49:

a) w ust. 1 w pkt 5 wyrazy „operatorów usług kluczowych” zastępuje się wyrazami „podmiotów kluczowych lub podmiotów ważnych”,

b) w ust. 3:

– w pkt 2 wyrazy „Agencji Unii Europejskiej do spraw Bezpieczeństwa Sieci i Informacji (ENISA)” zastępuje się wyrazem „ENISA”,

– pkt 4 otrzymuje brzmienie:

„4) dobrych praktyk w zakresie wymiany informacji związanych ze zgłaszaniem w Unii Europejskiej incydentów poważnych przez podmioty kluczowe lub podmioty ważne;”,

– pkt 6 otrzymuje brzmienie:

„6) dobrych praktyk w zakresie identyfikowania podmiotów kluczowych lub podmiotów ważnych przez państwa członkowskie Unii Europejskiej, w tym w odniesieniu do transgranicznych zależności, dotyczących ryzyka i incydentów.”,

b) dodaje się ust. 4–8 w brzmieniu:

„4. Pojedynczy Punkt Kontaktowy przekazuje ENISA aktualne dane z wykazu podmiotów kluczowych i podmiotów ważnych dotyczące dostawców usług DNS, rejestrów nazw domen najwyższego poziomu (TLD), dostawców chmury obliczeniowej, dostawców usługi centrum przetwarzania danych, dostawców sieci dostarczania treści, dostawców usług zarządzanych, dostawców usług zarządzanych w zakresie cyberbezpieczeństwa, jak również dostawców internetowych platform handlowych, wyszukiwarek internetowych i platform usług sieci społecznościowych.

5. Dane, o których mowa w ust. 4, obejmują:

- 1) nazwę (firmę) podmiotu;
- 2) sektor, podsektor i rodzaj podmiotu;
- 3) siedzibę i adres;
- 4) adres poczty elektronicznej;
- 5) numer telefonu przyporządkowany do wykonywanej działalności;
- 6) informację o wyznaczeniu przedstawiciela wraz z danymi kontaktowymi, o których mowa w art. 7 ust. 2 pkt 17 lit. a lub b;
- 7) adresy innych miejsc prowadzenia działalności na terenie Unii Europejskiej;

- 8) adres wyznaczonego przedstawiciela, jeśli został wyznaczony;
- 9) wskazanie państw członkowskich Unii Europejskiej, w których podmiot świadczy usługi;
- 10) główne miejsce prowadzenia działalności ustalone zgodnie z art. 5a ust. 3–6.

6. Pojedynczy Punkt Kontaktowy, co trzy miesiące, przedkłada ENISA sprawozdanie podsumowujące, zawierające dane o:

- 1) incydentach poważnych;
- 2) incydentach;
- 3) cyberzagrożeniach;
- 4) potencjalnych zdarzeniach dla cyberbezpieczeństwa.

7. Organ właściwy do spraw cyberbezpieczeństwa dla sektora infrastruktury cyfrowej, CSIRT sektorowy dla tego sektora oraz CSIRT MON, CSIRT NASK, CSIRT GOV może, za pośrednictwem Pojedynczego Punktu Kontaktowego, złożyć wniosek do ENISA o udostępnienie danych z rejestru dostawców usług DNS, rejestrów nazw domen najwyższego poziomu (TLD), dostawców chmury obliczeniowej, dostawców usług ośrodka przetwarzania danych, dostawców sieci dostarczania treści, dostawców usług zarządzanych, dostawców usług zarządzanych w zakresie cyberbezpieczeństwa, jak również dostawców internetowych platform handlowych, wyszukiwarek internetowych i platform usług sieci społecznościowych. We wniosku wskazuje się zakres żądanych danych.

8. Organy właściwe do spraw cyberbezpieczeństwa, Szef Agencji Bezpieczeństwa Wewnętrznego, Minister Obrony Narodowej, minister właściwy do spraw informatyzacji mogą, za pomocą Pojedynczego Punktu Kontaktowego, zwrócić się do ENISA o udzielenie wsparcia przy rozwijaniu CSIRT sektorowych oraz CSIRT MON, CSIRT NASK lub CSIRT GOV.”;

58) w art. 50 dotychczasową treść oznacza się jako ust. 1 i:

a) w ust. 1 pkt 2 otrzymuje brzmienie:

„2) co 2 lata informacje dotyczące krajowego systemu cyberbezpieczeństwa w szczególności:

- a) liczbę podmiotów kluczowych w podziale na poszczególne sektory,
- b) liczbę podmiotów ważnych w podziale na poszczególne sektory,
- c) rodzaje usług świadczonych przez podmioty kluczowe lub podmioty ważne,

- d) przepisy, na podstawie których podmioty kluczowe lub podmioty ważne zostały wskazane.”,
- b) dodaje się ust. 2 w brzmieniu:
 - „2. Pojedynczy Punkt Kontaktowy przekazuje Grupie Współpracy:
 - 1) liczbę podmiotów kluczowych w podziale na poszczególne sektory;
 - 2) liczbę podmiotów ważnych w podziale na poszczególne sektory.”;
- 59) w art. 51:
 - a) w pkt 2 wyrazy „zagrożenia cyberbezpieczeństwa” zastępuje się wyrazem „cyberzagrożenia”,
 - b) pkt 5–8 otrzymują brzmienie:
 - „5) koordynację działań związanych z obsługą incydentów w czasie stanu wojennego lub w czasie wojny, z zastrzeżeniem kompetencji Naczelnego Dowódcy Sił Zbrojnych;
 - 6) ocenę wpływu incydentów poważnych i krytycznych na system obronny państwa;
 - 7) ocenę cyberzagrożeń, w zakresie ich wpływu na system obronny państwa oraz przedstawianie właściwym organom, w przypadku wprowadzenia stanu wojennego lub stanu wojny, propozycji dotyczących działań obronnych z zastrzeżeniem kompetencji Naczelnego Dowódcy Sił Zbrojnych;
 - 8) koordynację, we współpracy z ministrem właściwym do spraw wewnętrznych i ministrem właściwym do spraw informatyzacji, realizacji zadań organów administracji rządowej i jednostek samorządu terytorialnego w czasie stanu wojennego lub w czasie wojny dotyczących działań obronnych w przypadku cyberzagrożenia z zastrzeżeniem kompetencji Naczelnego Dowódcy Sił Zbrojnych.”;
- 60) w art. 52:
 - a) w pkt 2 wyrazy „zagrożenia cyberbezpieczeństwa” zastępuje się wyrazem „cyberzagrożenia”,
 - b) w pkt 4 wyrazy „zagrożeniach cyberbezpieczeństwa” zastępuje się wyrazem „cyberzagrożeniach”;
- 61) po rozdziale 10 dodaje się rozdział 10a–10c w brzmieniu:

„Rozdział 10a

Zadania ministra właściwego do spraw energii

Art. 52a. 1. Organem właściwym, o którym mowa w art. 4 ust. 1 rozporządzenia 2024/1366, jest minister właściwy do spraw energii.

2. Właściwy organ, określony w ust. 1, identyfikuje podmioty o dużym wpływie i podmioty o krytycznym wpływie zgodnie z art. 24 rozporządzenia 2024/1366. Identyfikacja podmiotu o dużym wpływie lub podmiotu o krytycznym wpływie jest inną czynnością z zakresu administracji publicznej, na którą przysługuje skarga do sądu administracyjnego, i wymaga uzasadnienia.

3. Minister właściwy do spraw energii może wystąpić do podmiotu kluczowego lub podmiotu ważnego z podsektora energii elektrycznej o udzielenie informacji, które umożliwią wstępną ocenę, czy dany podmiot należy uznać za podmiot o dużym wpływie lub podmiot o krytycznym wpływie zgodnie z art. 24 rozporządzenia 2024/1366. Przepis art. 53c ust. 1–3 stosuje się odpowiednio.

Art. 52b. 1. Minister właściwy do spraw energii prowadzi kontrole podmiotów zidentyfikowanych jako podmioty o krytycznym wpływie, o których mowa w rozporządzeniu 2024/1366.

2. W przypadku kontroli, o której mowa w ust. 1, przepisy art. 54 stosuje się.

Rozdział 10b

Zadania ministra właściwego do spraw zagranicznych

Art. 52c. Minister właściwy do spraw zagranicznych prowadzi i koordynuje działalność dyplomatyczną w zakresie cyberbezpieczeństwa w stosunkach z państwami trzecimi i organizacjami międzynarodowymi.

Art. 52d. Minister właściwy do spraw informatyzacji przekazuje ministrowi właściwemu do spraw zagranicznych, z wyłączeniem danych osobowych:

- 1) informacje, odebrane i wysyłane przez Pojedynczy Punkt Kontaktowy, o wystąpieniu incydentu dotyczącego innych państw wraz z krótkim opisem i wskazaniem wszystkich państw, których dotyczył incydent;
- 2) sprawozdanie, o którym mowa w art. 49 ust. 6;
- 3) informacje pochodzące z Grupy Współpracy, o których mowa w art. 49 ust. 3 pkt 4–6;
- 4) informacje, o których mowa w art. 49 ust. 1;

- 5) informacje, odebrane i wysyłane przez Pojedynczy Punkt Kontaktowy, dotyczące sytuacji kryzysowych w cyberprzestrzeni.

Rozdział 10c

Organy odpowiedzialne za zarządzanie incydentami i zarządzanie kryzysowe w cyberbezpieczeństwie na dużą skalę

Art. 52e. Minister właściwy do spraw informatyzacji pełni rolę organu odpowiedzialnego za zarządzanie incydentami i zarządzanie kryzysowe w cyberbezpieczeństwie na dużą skalę w wymiarze cywilnym, z wyłączeniem spraw dotyczących zagrożeń terrorystycznych oraz zagrożeń związanych ze szpiegostwem.

Art. 52f. Minister Obrony Narodowej pełni rolę organu odpowiedzialnego za zarządzanie incydentami i zarządzanie kryzysowe w cyberbezpieczeństwie na dużą skalę w wymiarze militarnym.

Art. 52g. Szef Agencji Bezpieczeństwa Wewnętrznego pełni rolę organu odpowiedzialnego za zarządzanie incydentami i zarządzanie kryzysowe w cyberbezpieczeństwie na dużą skalę w wymiarze cywilnym w sprawach dotyczących zagrożeń terrorystycznych oraz zagrożeń związanych ze szpiegostwem.

Art. 52h. Organ odpowiedzialny za zarządzanie incydentami i zarządzanie kryzysowe w cyberbezpieczeństwie na dużą skalę koordynuje działania organów państwa zgodnie z Krajowym Planem reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę.”;

- 62) tytuł rozdziału 11 otrzymuje brzmienie:

„Nadzór i kontrola podmiotów kluczowych lub podmiotów ważnych”;

- 63) art. 53 otrzymuje brzmienie:

„Art. 53. 1. Nadzór dotyczący stosowania przepisów ustawy sprawują organy właściwe do spraw cyberbezpieczeństwa w zakresie wykonywania przez podmioty kluczowe i podmioty ważne wynikających z ustawy obowiązków.

2. W ramach nadzoru, o którym mowa w ust. 1, organ właściwy do spraw cyberbezpieczeństwa w stosunku do podmiotów kluczowych może:

- 1) prowadzić kontrole, w tym doraźne, w siedzibie podmiotu, miejscu wykonywania działalności gospodarczej lub zdalnie;

- 2) zobowiązać podmiot, w drodze decyzji, do przeprowadzania audytu, o którym mowa w art. 15 ust. 1b, w szczególności w sytuacji wystąpienia poważnego incydentu lub naruszenia przepisów ustawy;
- 3) zlecić CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT sektorowemu, dokonanie oceny bezpieczeństwa systemu informacyjnego podmiotu kluczowego;
- 4) wystąpić z wnioskiem o udzielenie informacji niezbędnych do oceny środków, o których mowa w art. 8 ust. 1 pkt 2 i 5, a także zgodności z obowiązkiem przedkładania informacji właściwym organom zgodnie z art. 7;
- 5) wystąpić z wnioskiem o udzielenie dostępu do danych, dokumentów i informacji koniecznych do wykonywania nadzoru;
- 6) wystąpić z wnioskiem o przedstawienie dowodów realizacji wymogów, o których mowa w art. 8 ust. 1.

3. Organy właściwe do spraw cyberbezpieczeństwa za pomocą działań nadzorczych sprawują nadzór o charakterze:

- 1) prewencyjnym i następczym nad podmiotami kluczowymi;
- 2) następczym nad podmiotami ważnymi, w szczególności w przypadku uzasadnionego podejrzenia, że zachodzi możliwość naruszenia przepisów ustawy.

4. W przypadku uzasadnionego podejrzenia, że działania lub zaniechania podmiotu kluczowego mogą naruszać przepisy ustawy, organ właściwy do spraw cyberbezpieczeństwa kieruje do tego podmiotu pismo w formie elektronicznej z ostrzeżeniem, w którym wskazuje czynności, jakie należy podjąć w celu zapobieżenia lub zaprzestania naruszania przepisów ustawy oraz termin na ich wykonanie.

5. W celu egzekwowania przepisów ustawy organ właściwy do spraw cyberbezpieczeństwa w stosunku do podmiotów kluczowych, także wtedy gdy podmiot kluczowy nie zastosował się do pisma z ostrzeżeniem, o którym mowa w ust. 4, może:

- 1) nakazać podjęcie określonych czynności dotyczących obsługi incydentu;
- 2) nakazać, w drodze decyzji, zaniechanie naruszania przepisów ustawy;
- 3) nakazać, w drodze decyzji, zapewnienie zgodności systemu zarządzania bezpieczeństwem informacji zgodnie z art. 8 ust. 1 pkt 2 lub zgodnie z art. 8 ust. 3 lub realizacji obowiązku zgłaszania incydentu poważnego;
- 4) nakazać, w drodze decyzji, poinformowanie, w określony przez niego sposób, odbiorców swoich usług, których dotyczy poważne cyberzagrożenie, o charakterze

tego zagrożenia oraz o możliwych środkach ochronnych lub naprawczych, jakie należy podjąć w reakcji na to zagrożenie;

- 5) nakazać, w drodze decyzji, wdrożenie, w określonym terminie, zaleceń wydanych w wyniku audytu bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi;
- 6) wyznaczyć, w drodze decyzji, na określony czas, nie dłuższy niż miesiąc, spośród osób zatrudnionych w urzędzie obsługującym ten organ, urzędnika monitorującego do nadzorowania wykonywania obowiązków, o których mowa w rozdziale 3, wskazując ściśle określone zadania, które urzędnik monitorujący realizuje w tym czasie;
- 7) nakazać, w drodze decyzji, podanie do wiadomości publicznej informacji o naruszeniach przepisów ustawy;
- 8) nakazać, w drodze decyzji wydanej w postępowaniu uproszczonym, o którym mowa w rozdziale 14 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego, podanie do publicznej wiadomości informacji o incydencie poważnym.

6. Organ właściwy do spraw cyberbezpieczeństwa, podejmując działania, o których mowa w ust. 5, wyznacza podmiotowi kluczowemu termin, w którym zobowiązuje ten podmiot do podjęcia określonych czynności, usunięcia uchybień lub zapewnienia zgodności z wymogami określonymi przez organ.

7. Nakaz, o którym mowa w ust. 5 pkt 1, jest inną czynnością z zakresu administracji publicznej, na którą przysługuje skarga do sądu administracyjnego i wymaga uzasadnienia.

8. Postępowanie w sprawach, o którym mowa w ust. 5 pkt 2–8, jest jednoinstancyjne, a na decyzję organu właściwego do spraw cyberbezpieczeństwa przysługuje skarga do sądu administracyjnego.

9. Organ właściwy do spraw cyberbezpieczeństwa, w przypadku gdy podmiot kluczowy nie zastosował się do nakazu, o którym mowa w ust. 5 pkt 1, lub postanowień decyzji, o której mowa w ust. 5 pkt 2–8, może:

- 1) wstrzymać udzieloną temu podmiotowi koncesję albo ograniczyć jej zakres do czasu usunięcia uchybień lub zaprzestania naruszeń lub

- 2) wstrzymać w całości albo w części działalność podmiotu kluczowego wpisanego do rejestru działalności regulowanej, do czasu usunięcia uchybień lub zaprzestania naruszeń, lub
- 3) wstrzymać zezwolenie na prowadzenie działalności gospodarczej wydane podmiotowi kluczowemu albo ograniczyć zakres tego zezwolenia do czasu usunięcia uchybień lub zaprzestania naruszeń, lub
- 4) wstrzymać w całości albo w części działalność podmiotu kluczowego, wpisanego do Centralnej Ewidencji i Informacji o Działalności Gospodarczej, do czasu usunięcia uchybień lub zaprzestania naruszeń, lub
- 5) wstrzymać w całości albo w części działalność podmiotu kluczowego, wpisanego do rejestru przedsiębiorców Krajowego Rejestru Sądowego do czasu usunięcia uchybień lub zaprzestania naruszeń, lub
- 6) zakazać pełnienia w podmiocie kluczowym funkcji zarządczych przez kierownika podmiotu do czasu usunięcia uchybień lub zaprzestania naruszeń, o ile nie doprowadzi to do uniemożliwienia funkcjonowania podmiotu kluczowego w zakresie jaki jest niezbędny do usunięcia uchybień lub zaprzestania naruszeń.

10. Środków, o których mowa w ust. 9, nie stosuje się do podmiotów publicznych.

11. W przypadku wniesienia przez podmiot kluczowy skargi do sądu administracyjnego, o której mowa w ust. 7 lub 8, środków, o których mowa w ust. 9, nie stosuje się do czasu rozstrzygnięcia sprawy przez ten sąd. Sąd rozstrzyga sprawę w terminie miesiąca od dnia wniesienia skargi.

12. Organ właściwy do spraw cyberbezpieczeństwa, podejmując działania, o których mowa w ust. 5 i 9, uwzględnia:

- 1) wagę naruszenia i znaczenie naruszonych przepisów ustawy, przy czym za poważne naruszenie należy uznać:
 - a) powtarzające się naruszenie,
 - b) niezgłoszenie lub nieobsłużenie incydentów poważnych,
 - c) nieusunięcie uchybień zgodnie z wiążącymi nakazami organów właściwych do spraw cyberbezpieczeństwa,
 - d) utrudnianie prowadzenia audytów lub działań monitorujących nakazanych przez organ właściwy do spraw cyberbezpieczeństwa po stwierdzeniu naruszenia,

- e) dostarczanie nieprawdziwych lub rażąco niedokładnych informacji w odniesieniu do środków zarządzania ryzykiem w cyberbezpieczeństwie lub obowiązków zgłaszania incydentów poważnych;
- 2) czas trwania naruszenia;
- 3) wcześniejsze poważne naruszenia ze strony danego podmiotu;
- 4) spowodowane szkody majątkowe i niemajątkowe, w tym straty finansowe lub gospodarcze, wpływ na inne usługi i liczbę użytkowników, których dotyczy incydent;
- 5) umyślny lub nieumyślny charakter czynu ze strony sprawcy naruszenia;
- 6) środki zastosowane przez podmiot, aby zapobiec szkodom majątkowym i niemajątkowym lub je ograniczyć;
- 7) stopień współpracy podmiotu z organem właściwym do spraw cyberbezpieczeństwa.

13. Organ właściwy do spraw cyberbezpieczeństwa przed zastosowaniem środków, o których mowa w ust. 4, 5 i 9, oraz przed nałożeniem kary pieniężnej, informuje podmiot kluczowy o wstępnych ustaleniach, które mogą prowadzić do wydania decyzji lub podjęcia działań, o których mowa w ust. 4, 5 i 9, lub do nałożenia kary pieniężnej. Informacja o wstępnych ustaleniach zawiera szczegółowe uzasadnienie, potwierdzające zasadność zamiaru zastosowania środków lub nałożenia kary pieniężnej.

14. Podmiot kluczowy może przedstawić swoje stanowisko niezwłocznie, nie później niż w terminie 7 dni od dnia poinformowania o wstępnych ustaleniach, o których mowa w ust. 13.

15. Organ właściwy do spraw cyberbezpieczeństwa po przedstawieniu przez podmiot kluczowy swojego stanowiska:

- 1) uwzględnia stanowisko tego podmiotu i odstępuje od zastosowania środków, o których mowa w ust. 4, 5 lub 9, lub od nałożenia kary pieniężnej, oraz informuje podmiot o tym fakcie;
- 2) odrzuca stanowisko tego podmiotu i stosuje środki, o których mowa w ust. 4, 5 lub 9, lub nakłada karę pieniężną, oraz informuje podmiot o tym fakcie wraz ze szczegółowym uzasadnieniem przyczyn odrzucenia stanowiska podmiotu.

16. Organ właściwy do spraw cyberbezpieczeństwa może odstąpić od poinformowania o wstępnych ustaleniach w przypadku gdy utrudniłoby to natychmiastowe działanie w celu zapobieżenia incydentom, reakcji na nie lub mogłoby mieć niekorzystny wpływ na bezpieczeństwo państwa lub porządek publiczny.

17. Organ właściwy do spraw cyberbezpieczeństwa sprawując nadzór w stosunku do podmiotu ważnego stosuje ust. 2, 4, 5 pkt 1–5 i 7–8 oraz ust. 6–8 i ust. 12–16.”;

64) po art. 53 dodaje się art. 53a–53f w brzmieniu:

„Art. 53a. 1. Organy właściwe do spraw cyberbezpieczeństwa mogą tworzyć, samodzielnie lub wspólnie, metodyki nadzoru dotyczące prowadzenia nadzoru nad podmiotami kluczowymi lub podmiotami ważnymi w zakresie stosowania przepisów ustawy.

2. Metodyki nadzoru określają w szczególności:

- 1) zakres nadzoru;
- 2) sposób przeprowadzania nadzoru;
- 3) kryteria oceny.

3. W przypadku stworzenia metodyki nadzoru organy właściwe do spraw cyberbezpieczeństwa co dwa lata oceniają skuteczność stosowania tej metodyki nadzoru, w szczególności oceniając efektywność sprawowanego nadzoru.

4. Na podstawie oceny skuteczności organy właściwe do spraw cyberbezpieczeństwa dokonują zmian w metodykach nadzoru.

Art. 53b. 1. Organy właściwe do spraw cyberbezpieczeństwa mogą ustalać hierarchię priorytetów w sprawowaniu nadzoru w oparciu o metodykę nadzoru, o której mowa w art. 53a ust. 1, uwzględniając w szczególności wyniki analizy ryzyka dla konkretnego podmiotu kluczowego lub podmiotu ważnego.

2. Analiza ryzyka przeprowadzana jest przez organ właściwy do spraw cyberbezpieczeństwa i uwzględnia w szczególności:

- 1) znaczenie usługi dla bezpieczeństwa narodowego i porządku publicznego;
- 2) wpływ usługi na gospodarkę i społeczeństwo;
- 3) prawdopodobieństwo wystąpienia incydentu w podmiocie nadzorowanym oraz rodzaj tego incydentu;
- 4) potencjalne skutki incydentu takie jak straty finansowe, szkody wizerunkowe, utrata danych osobowych lub zakłócenia w funkcjonowaniu systemów i infrastruktury.

Art. 53c. 1. Podmiot kluczowy lub podmiot ważny przekazuje na żądanie organu właściwego do spraw cyberbezpieczeństwa dane, informacje i dokumenty niezbędne do wykonywania przez ten organ jego uprawnień i obowiązków z zakresu sprawowania nadzoru i kontroli określonych w ustawie.

2. Żądanie, o którym mowa w ust. 1, ma być proporcjonalne do celu, jakiemu ma służyć, oraz zawierać:

- 1) wskazanie podmiotu kluczowego lub podmiotu ważnego, do którego jest skierowane;
- 2) datę żądania;
- 3) wskazanie żądanych danych, informacji lub dokumentów oraz okresu, których dotyczą;
- 4) wskazanie celu, jakiemu dane, informacje lub dokumenty mają służyć;
- 5) wskazanie terminu przekazania danych, informacji lub dokumentów adekwatnego do zakresu tego żądania, nie krótszego niż 7 dni;
- 6) uzasadnienie żądania;
- 7) pouczenie o zagrożeniu karą w przypadku, o którym mowa w art. 73 ust. 1 pkt 15.

3. Żądanie, o którym mowa w ust. 1, sporządza się w postaci elektronicznej i doręcza się w sposób określony w dziale I rozdziale 8 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego albo przez system teleinformatyczny, o którym mowa w art. 46 ust. 1 pkt 6.

4. Przepisy ust. 1–3 stosuje się odpowiednio do żądania udzielenia dostępu do danych, dokumentów i informacji koniecznych do wykonania nadzoru oraz dowodów realizacji wymogów, o których mowa w art. 8 ust. 1.

Art. 53d. 1. Urzędnik monitorujący, o którym mowa w art. 53 ust. 5 pkt 6, w zakresie nadzorowania wykonywania przez podmiot kluczowy obowiązków, o których mowa w rozdziale 3, jest uprawniony do:

- 1) swobodnego wstępu i poruszania się po terenie podmiotu kluczowego po uzyskaniu przepustki, wydanej bezzwłocznie, której wydania nie można odmówić;
- 2) wglądu do dokumentów dotyczących działalności podmiotu kluczowego;
- 3) przetwarzania danych osobowych w zakresie niezbędnym do realizacji celu nadzoru;
- 4) żądania złożenia ustnych lub pisemnych wyjaśnień w sprawach dotyczących zakresu nadzoru;
- 5) przeprowadzania oględzin urządzeń, nośników oraz systemów informacyjnych, po wcześniejszym zawiadomieniu podmiotu kluczowego.

2. Urzędnik monitorujący, o którym mowa w art. 53 ust. 5 pkt 6, realizuje powierzone mu zadania z zachowaniem przepisów o tajemnicy prawnie chronionej.

3. Do nadzorowania przez urzędnika monitorującego, o którym mowa w art. 53 ust. 5 pkt 6, wykonywania przez podmiot kluczowy obowiązków, o których mowa w rozdziale 3, stosuje się art. 58.

4. Zawiadomienie, o którym mowa w ust. 1 pkt 5, przekazuje się na adres do doręczeń elektronicznych albo za pomocą systemu teleinformatycznego, o którym mowa w art. 46 ust. 1 w terminie 1 dnia przed przeprowadzeniem oględzin.

Art. 53e. 1. Realizując uprawnienie, o którym mowa w art. 53 ust. 9, organ właściwy do spraw cyberbezpieczeństwa wydaje decyzję, która zawiera:

- 1) dane podmiotu kluczowego lub kierownika podmiotu kluczowego;
- 2) rodzaj stwierdzonych uchybień lub naruszeń dokonanych przez podmiot kluczowy lub kierownika podmiotu kluczowego;
- 3) podjęte dotychczas środki nadzorcze nad podmiotem kluczowym;
- 4) podstawę prawną i rodzaj środka określonego w art. 53 ust. 9;
- 5) termin stosowania tego środka;
- 6) uzasadnienie.

2. Termin stosowania środków, o których mowa w art. 53 ust. 9, określa się przy uwzględnieniu kryteriów, o których mowa w art. 53 ust. 12. Środek nie może być stosowany dłużej niż 14 dni od daty doręczenia decyzji o jego zastosowaniu.

3. W zależności od zastosowanego środka, jeżeli podmiot kluczowy usunął uchybienia lub zaprzestał naruszania przepisów ustawy przed terminem określonym w decyzji, uchyla się decyzję o zastosowaniu tego środka.

4. W przypadku powzięcia informacji, w szczególności na skutek stosowania innych środków nadzorczych, określonych w art. 53 ust. 1, 4 i 5, że podmiot kluczowy nie usunął wcześniej stwierdzonych uchybień lub w dalszym ciągu narusza przepisy ustawy lub w przypadku gdy podmiot kluczowy nie wykazał w terminie, na jaki został zastosowany środek, że usunął uchybienia lub zaprzestał naruszania przepisów ustawy, organ właściwy do spraw cyberbezpieczeństwa ponownie wydaje decyzję o zastosowaniu środka określonego w art. 53 ust. 9 na kolejny okres, nie dłuższy niż 14 dni. Przepis ten stosuje się do czasu usunięcia uchybień lub zaprzestania naruszeń przez podmiot kluczowy. W stosunku do ponownej decyzji nie stosuje się art. 53 ust. 13–16.

5. Organ właściwy do spraw cyberbezpieczeństwa z urzędu lub na wniosek podmiotu kluczowego uchyla decyzję, o której mowa w ust. 1, po usunięciu uchybień lub zaprzestaniu naruszeń przez podmiot kluczowy.

6. Podmiot kluczowy może złożyć wniosek, o którym mowa w ust. 5, po usunięciu uchybień lub zaprzestaniu naruszeń, przedstawiając dowody potwierdzające zastosowanie się odpowiednio do nakazu, o którym mowa w art. 53 ust. 5 pkt 1, lub postanowień decyzji, o której mowa w art. 53 ust. 5 pkt 2–8.

7. Wniosek, o którym mowa w ust. 5, organ właściwy do spraw cyberbezpieczeństwa rozpatruje niezwłocznie, nie później niż w terminie 7 dni od dnia jego otrzymania.

8. Czynności, o których mowa w ust. 3 i 5, organ dokonuje w formie decyzji.

9. Decyzja, o której mowa w ust. 1, jest wykonalna z dniem jej doręczenia podmiotowi kluczowemu. Decyzje, o których mowa w ust. 3, 4 i 5, są natychmiast wykonalne.

10. Postępowanie w sprawie stosowania i uchylania środków, o których mowa w art. 53 ust. 9, jest jednoinstancyjne. Na decyzje, o których mowa w ust. 1 i 3–5, podmiot kluczowy może wnieść skargę do sądu administracyjnego.

11. Organ właściwy do spraw cyberbezpieczeństwa publikuje na swojej stronie podmiotowej Biuletynu Informacji Publicznej informację o zastosowaniu wobec podmiotu kluczowego lub kierownika podmiotu kluczowego środków, o których mowa w art. 53 ust. 9. Informacja zawiera:

- 1) dane podmiotu kluczowego lub imię i nazwisko kierownika tego podmiotu kluczowego;
- 2) podstawę prawną i rodzaj zastosowanego środka, o którym mowa w art. 53 ust. 9;
- 3) wskazanie daty początkowej i końcowej okresu na jaki zastosowano środek;
- 4) wskazanie, czy wobec podmiotu kluczowego lub kierownika podmiotu kluczowego ponownie zastosowano środek, a jeśli tak, to wskazanie nowej daty końcowej stosowania tego środka.

12. Publikacja, o której mowa w ust. 11, nie obejmuje tajemnicy przedsiębiorstwa, jak również innych informacji podlegających ochronie na podstawie odrębnych przepisów.

13. Organ właściwy do spraw cyberbezpieczeństwa publikuje na swojej stronie podmiotowej Biuletynu Informacji Publicznej informację o uchyleniu decyzji, o której mowa w ust. 1.

14. Podmiot kluczowy, w okresie stosowania wobec niego środka, o którym mowa w art. 53 ust. 9, nie może wykonywać działalności, której dotyczy ten środek.

15. W okresie stosowania środka, o którym mowa w art. 53 ust. 9, podmiot kluczowy ma obowiązek niezwłocznie podjąć działania zmierzające jedynie do usunięcia uchybień bądź zaprzestania naruszeń. W tym celu w szczególności może składać oświadczenia woli i wiedzy, podejmować czynności procesowe w postępowaniach, przedsięwziąć czynności faktyczne, jeżeli nie stoją one w sprzeczności z celem stosowanego środka lub nie zmierzają do jego obejścia.

16. W zakresie nieuregulowanym, a dotyczącym zawieszania, ograniczania i wznawiania koncesji, zezwolenia na prowadzenie działalności gospodarczej lub wstrzymania prowadzenia działalności gospodarczej zastosowanie mają przepisy odrębne.

Art. 53f. 1. Organy właściwe do spraw cyberbezpieczeństwa mogą wspólnie sprawować nadzór, w tym wspólnie prowadzić kontrolę, nad podmiotami kluczowymi lub podmiotami ważnymi.

2. Organy właściwe do spraw cyberbezpieczeństwa, sprawując wspólnie nadzór, w tym prowadząc kontrolę, mogą wyznaczyć wiodący organ właściwy do spraw cyberbezpieczeństwa.

3. Organy właściwe do spraw cyberbezpieczeństwa informują się wzajemnie o zamiarze wszczęcia kontroli w podmiocie, nad którym wspólnie sprawują nadzór.

4. Przepisy ust. 1–3 stosuje się odpowiednio do współpracy organów właściwych do spraw cyberbezpieczeństwa i organów właściwych do spraw podmiotów krytycznych w przypadku, gdy nadzór jest sprawowany nad podmiotem kluczowym będącym podmiotem krytycznym.”;

65) art. 54 otrzymuje brzmienie:

„Art. 54. Do kontroli realizowanej wobec podmiotów kluczowych lub podmiotów ważnych:

- 1) będących przedsiębiorcami stosuje się przepisy rozdziału 5 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców;
- 2) niebędących przedsiębiorcami stosuje się przepisy ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej;
- 3) będących jednostkami samorządu terytorialnego stosuje się przepisy ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej.”;

66) w art. 56 dodaje się ust. 3 i 4 w brzmieniu:

„3. Organ przeprowadzający kontrolę może żądać od podmiotu kontrolowanego przedstawienia tłumaczenia na język polski sporządzonej w języku obcym dokumentacji przedłożonej przez podmiot kontrolowany. Tłumaczenie dokumentacji podmiot kontrolowany jest obowiązany wykonać na własny koszt. Zlecenie tłumaczenia dokumentacji podmiotom trzecim odbywa się z poszanowaniem tajemnicy prawnie chronionej na podstawie odrębnych przepisów.

4. Organ przeprowadzający kontrolę, występując do podmiotu kontrolowanego z żądaniem, o którym mowa w ust. 3, wskazuje zakres dokumentów, które mają zostać przetłumaczone, ich związek z przeprowadzaną kontrolą oraz określa termin na przedstawienie tłumaczenia dokumentacji, uwzględniający zakres koniecznego tłumaczenia.”;

67) w art. 58:

a) ust. 4–8 otrzymują brzmienie:

„4. W przypadku zastrzeżeń dotyczących ustaleń zawartych w protokole kontroli, kontrolowany ma prawo odmówić podpisania protokołu kontroli oraz złożyć umotywowane pisemne zastrzeżenia do tego protokołu w terminie 7 dni od dnia przedstawienia mu go do podpisu.

5. Odmowę podpisania protokołu kontroli osoba prowadząca czynności kontrolne odnotowuje w protokole wraz ze wskazaniem daty tej odmowy.

6. W razie złożenia zastrzeżeń do protokołu kontroli kierownik komórki organizacyjnej do spraw kontroli dokonuje ich analizy.

7. Kierownik komórki organizacyjnej do spraw kontroli:

- 1) odrzuca zastrzeżenia do protokołu kontroli wniesione przez osobę nieuprawnioną lub wniesione po upływie terminu i informuje o tym na piśmie zgłaszającego zastrzeżenia, podając przyczyny, albo
- 2) uwzględnia zastrzeżenia do protokołu kontroli w całości albo w części lub je oddala.

8. W razie potrzeby, w związku ze zgłoszeniem zastrzeżeń do protokołu, osoba prowadząca czynności kontrolne podejmuje dodatkowe czynności kontrolne, a w przypadku stwierdzenia przez kierownika komórki organizacyjnej do spraw kontroli zasadności zastrzeżeń do protokołu kontroli zmienia lub uzupełnia odpowiednią część protokołu kontroli w formie aneksu do protokołu.”,

b) dodaje się ust. 9–11 w brzmieniu:

„9. Kierownik komórki organizacyjnej do spraw kontroli, po rozpatrzeniu zastrzeżeń do protokołu kontroli, sporządza stanowisko wobec tych zastrzeżeń.

10. O nieuwzględnieniu zastrzeżeń do protokołu kontroli w całości albo w części kierownik komórki organizacyjnej do spraw kontroli informuje podmiot kontrolowany na piśmie.

11. Protokół kontroli:

- 1) w postaci papierowej sporządza się w dwóch egzemplarzach, z których jeden pozostawia się podmiotowi kontrolowanemu;
- 2) w postaci elektronicznej doręcza się podmiotowi kontrolowanemu na adres do doręczeń elektronicznych.”;

68) w art. 59:

a) ust. 1 otrzymuje brzmienie:

„1. Jeżeli na podstawie informacji zgromadzonych w toku kontroli organ właściwy do spraw cyberbezpieczeństwa uzna, że mogło dojść do naruszenia przepisów ustawy przez podmiot kontrolowany, przekazuje zalecenia pokontrolne wzywające do usunięcia nieprawidłowości. Organ właściwy do spraw cyberbezpieczeństwa wskazuje termin usunięcia tych nieprawidłowości, uwzględniając zakres i rodzaj naruszeń.”,

b) w ust. 3 skreśla się wyrazy „lub ministra właściwego do spraw informatyzacji”;

69) po art. 59 dodaje się art. 59a–59c w brzmieniu:

„Art. 59a. 1. W przypadku stwierdzenia podczas sprawowania nadzoru podejrzenia naruszenia ochrony danych osobowych organ właściwy do spraw cyberbezpieczeństwa informuje o tym Prezesa Urzędu Ochrony Danych Osobowych w terminie 7 dni od dnia stwierdzenia podejrzenia tego naruszenia.

2. W przypadku stwierdzenia podejrzenia naruszenia ochrony danych osobowych podczas sprawowania nadzoru nad jednostką organizacyjną prokuratury organ właściwy do spraw cyberbezpieczeństwa informuje właściwy organ prokuratury, o którym mowa w art. 191a § 1 ustawy z dnia 28 stycznia 2016 r. – Prawo o prokuraturze (Dz. U. z 2024 r. poz. 390 oraz z 2025 r. poz. 304 i 1178).

3. W przypadku stwierdzenia podejrzenia naruszenia ochrony danych osobowych podczas sprawowania nadzoru nad sądem organ właściwy do spraw cyberbezpieczeństwa informuje właściwego prezesa sądu albo Krajową Radę Sądownictwa, o których mowa

w art. 175dd § 1 ustawy z dnia 27 lipca 2001 r. – Prawo o ustroju sądów powszechnych (Dz. U. z 2024 r. poz. 334 i 1907 oraz z 2025 r. poz. 526, 820, 1172 i 1178).

Art. 59b. 1. Organ właściwy do spraw cyberbezpieczeństwa udziela pomocy organom innych państw członkowskich Unii Europejskiej w sprawowaniu nadzoru nad podmiotami kluczowymi lub podmiotami ważnymi, których systemy informacyjne znajdują się na terytorium Rzeczypospolitej Polskiej.

2. Organ właściwy do spraw cyberbezpieczeństwa może, za pośrednictwem Pojedynczego Punktu Kontaktowego, zwracać się do organów innych państw członkowskich Unii Europejskiej o przeprowadzenie czynności nadzorczych nad podmiotami kluczowymi lub podmiotami ważnymi, świadczącymi usługi na terytorium Rzeczypospolitej Polskiej, których siedziba, zarząd lub systemy informacyjne znajdują się na terytorium innego państwa członkowskiego Unii Europejskiej.

3. Organ właściwy do spraw cyberbezpieczeństwa odmawia udzielenia pomocy, o której mowa w ust. 1, jeżeli:

- 1) nie jest właściwy w sprawie;
- 2) żądana pomoc jest nieproporcjonalna do realizowanych przez organ zadań z zakresu nadzoru;
- 3) organ innego państwa członkowskiego Unii Europejskiej żąda udostępnienia informacji lub dokumentów, których udostępnienie narusza podstawowy interes bezpieczeństwa państwa, bezpieczeństwa i porządku publicznego lub obronności.

4. Przed odmową udzielenia pomocy organ właściwy do spraw cyberbezpieczeństwa konsultuje się z wnioskującym o udzielenie pomocy organem innego państwa, a także z Komisją Europejską i ENISA, jeśli żąda tego państwo członkowskie Unii Europejskiej.

5. Organ właściwy do spraw cyberbezpieczeństwa może prowadzić wspólne czynności nadzorcze z organem innego państwa członkowskiego Unii Europejskiej.

6. Organy właściwe do spraw cyberbezpieczeństwa współpracują za pośrednictwem Pojedynczego Punktu Kontaktowego z organami innych państw członkowskich Unii Europejskiej właściwych do stosowania rozporządzenia 2022/2554.

7. Organy właściwe do spraw cyberbezpieczeństwa informują forum nadzoru, o którym mowa w art. 32 ust. 1 rozporządzenia 2022/2554, jeżeli podejmują czynności nadzorcze wobec podmiotu kluczowego, który został wyznaczony jako kluczowy dostawca usług ICT zgodnie z art. 31 rozporządzenia 2022/2554.

Art. 59c. 1. W przypadkach uzasadnionych charakterem sprawy lub pilnością przeprowadzenia czynności kontrolnych wynikających z ochrony bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego lub w przypadku potrzeby realizacji wzajemnej pomocy, o której mowa w art. 59b ust. 1, lub potrzeby sprawdzenia, czy podmiot kluczowy usunął uchybienia lub zaprzestał dokonywania naruszeń, można zarządzić przeprowadzenie kontroli doraźnej, o której mowa w art. 53 ust. 2 pkt 1.

2. Kontrola doraźna, o której mowa w art. 53 ust. 2 pkt 1, może być zarządzona w szczególności w razie potrzeby:

- 1) sprawdzenia informacji uzyskanej od urzędnika monitorującego, o którym mowa w art. 53 ust. 5 pkt 6, że podmiot kluczowy może naruszać przepisy ustawy;
- 2) sprawdzenia, w celu podjęcia działań na podstawie art. 53e ust. 4 i 5, czy podmiot kluczowy usunął uchybienia lub zaprzestał dokonywania naruszeń;
- 3) sprawdzenia wykonania zaleceń pokontrolnych, wykonania decyzji albo postanowień nakazujących usunięcie naruszeń prawa w związku z przeprowadzoną kontrolą.

3. Kontrolę doraźną, o której mowa w art. 53 ust. 2 pkt 1, prowadzi się zgodnie z przepisami dotyczącymi kontroli na zasadach ogólnych. Do podmiotów kontrolowanych niebędących przedsiębiorcami nie stosuje się przepisów dotyczących programu kontroli i sporządzania wystąpienia pokontrolnego.

4. Kontrola doraźna, o której mowa w art. 53 ust. 2 pkt 1, może być prowadzona także wtedy, gdy nie było możliwości wcześniejszego powiadomienia podmiotu kontrolowanego o terminie przeprowadzenia kontroli. Uzasadnienie przyczyny braku powiadomienia o zamiarze wszczęcia kontroli umieszcza się w sprawozdaniu z kontroli albo protokole kontroli.

5. Kontrola doraźna, o której mowa w art. 53 ust. 2 pkt 1, kończy się sporządzeniem:

- 1) sprawozdania z kontroli – w przypadku jednostek samorządu terytorialnego oraz podmiotów niebędących przedsiębiorcami,
 - 2) protokołu kontroli – w przypadku podmiotów będących przedsiębiorcami
- zawierającymi opis ustalonego stanu faktycznego oraz jego ocenę, a także, w razie potrzeby, zalecenia lub wnioski wzywające do usunięcia nieprawidłowości lub usprawnienia funkcjonowania podmiotu kontrolowanego. Sprawozdanie z kontroli albo protokół kontroli podpisuje kierownik komórki do spraw kontroli w organie właściwym do spraw cyberbezpieczeństwa.

6. Kierownik podmiotu kontrolowanego w terminie 3 dni roboczych od dnia otrzymania sprawozdania z kontroli albo protokołu kontroli, o których mowa w ust. 5, ma prawo przedstawić do niego stanowisko. Nie wstrzymuje to realizacji ustaleń kontroli doraźnej.

7. Jeżeli w toku kontroli doraźnej, o której mowa w art. 53 ust. 2 pkt 1, zostaną ujawnione okoliczności wskazujące na naruszenia przepisów ustawy, które wykraczają poza zakres tej kontroli, kontrolę w dalszej części przeprowadza się na zasadach ogólnych z zastosowaniem art. 54–59b.

8. Do kontroli doraźnej, o której mowa w art. 53 ust. 2 pkt 1, w zakresie nieuregulowanym niniejszą ustawą w stosunku do podmiotów będących przedsiębiorcami stosuje się odpowiednio przepisy ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców, a w przypadku jednostek samorządu terytorialnego oraz podmiotów niebędących przedsiębiorcami – przepisy ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej. Przepisów art. 47 ust. 1 i 2 oraz art. 54 ust. 1 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców nie stosuje się.”;

70) w art. 61 ust. 3 otrzymuje brzmienie:

„3. Pełnomocnikiem jest minister właściwy do spraw informatyzacji, sekretarz stanu albo podsekretarz stanu w urzędzie obsługującym ministra właściwego do spraw informatyzacji.”;

71) w art. 62:

- a) w ust. 1 w pkt 1 wyrazy „i CSIRT GOV” zastępuje się wyrazami „CSIRT GOV i CSIRT sektorowych”,
- b) w ust. 2 w pkt 3 wyrazy „zagrożeń cyberbezpieczeństwa” zastępuje się wyrazem „cyberzagrożeń”,
- c) dodaje się ust. 3–8 w brzmieniu:

„3. Pełnomocnik może dokonywać zakupów produktów ICT, usług ICT lub procesów ICT z zakresu cyberbezpieczeństwa na rzecz podmiotów, o których mowa w art. 62a ust. 2 pkt 3, na podstawie umowy, przekazując prawa do zakupionych produktów ICT, usług ICT lub procesów ICT z zakresu cyberbezpieczeństwa.

4. Pełnomocnik może, w zakresie realizacji jego zadań, zlecać przeprowadzanie badań lub ekspertyz.

5. Pełnomocnik może, w drodze zarządzenia, powoływać zespoły doradcze.

6. Pełnomocnik może upoważnić do realizacji swoich zadań pracownika ministerstwa lub urzędu administracji rządowej go obsługującego, który:

- 1) pełni funkcję dyrektora departamentu, zastępcy dyrektora departamentu lub naczelnika wydziału;
- 2) spełnia wymagania określone w przepisach o ochronie informacji niejawnych w zakresie dostępu do informacji niejawnych o klauzuli „tajne”.

7. Organy administracji rządowej oraz jednostki organizacyjne podległe tym organom lub przez nie nadzorowane są obowiązane do udzielania pomocy Pełnomocnikowi przy realizacji jego zadań, w szczególności przez udostępnianie mu informacji i dokumentów.

8. Zadania Pełnomocnika są finansowane z części budżetowej, której dysponentem jest minister właściwy do spraw informatyzacji.”;

72) po art. 62 dodaje się art. 62a w brzmieniu:

„Art. 62a 1. Przy Pełnomocniku działa PCOC, jako organ pomocniczy w sprawach koordynowania działań i realizowania polityki rządu w zakresie zapewnienia cyberbezpieczeństwa w Rzeczypospolitej Polskiej.

2. W skład PCOC wchodzi:

- 1) Pełnomocnik;
- 2) sekretarz PCOC;
- 3) przedstawiciele:
 - a) ministra – członka Rady Ministrów właściwego do spraw koordynowania działalności służb specjalnych, jeżeli został powołany,
 - b) ministra właściwego do spraw informatyzacji,
 - c) ministra właściwego do spraw wewnętrznych,
 - d) ministra właściwego do spraw zagranicznych,
 - e) Ministra Obrony Narodowej,
 - f) Ministra Sprawiedliwości,
 - g) Szefa Kancelarii Prezesa Rady Ministrów,
 - h) organów właściwych do spraw cyberbezpieczeństwa,
 - i) CSIRT GOV,
 - j) CSIRT MON,
 - k) CSIRT NASK,
 - l) CSIRT sektorowych,

- m) Dowódcy Komponentu Wojsk Obrony Cyberprzestrzeni,
- n) dyrektora Rządowego Centrum Bezpieczeństwa,
- o) Komendanta Centralnego Biura Zwalczania Cyberprzestępczości,
- p) Komendanta Głównego Policji,
- q) Komendanta Służby Ochrony Państwa,
- r) Komendanta Głównego Straży Granicznej,
- s) Prokuratora Krajowego,
- t) Szefa Agencji Bezpieczeństwa Wewnętrznego,
- u) Szefa Agencji Wywiadu,
- v) Szefa Służby Kontrwywiadu Wojskowego,
- w) Szefa Służby Wywiadu Wojskowego.

3. Prezydent Rzeczypospolitej Polskiej może skierować do udziału w pracach PCOC swojego przedstawiciela.

4. Na posiedzenia PCOC mogą być zapraszani przedstawiciele podmiotów kluczowych, podmiotów ważnych lub innych podmiotów, jeżeli wymaga tego temat spotkania.

5. Posiedzeniu PCOC przewodniczy Pełnomocnik.

6. Do zadań PCOC należy:

- 1) wymiana informacji na temat cyberzagrożeń, incydentów i podatności na poziomie krajowym;
- 2) wymiana informacji o wynikach szacowania ryzyka związanego z ujawnionymi cyberzagrożeniami oraz zaistniałymi incydentami;
- 3) wymiana informacji o przeprowadzanych badaniach, o których mowa w art. 33 ust. 1;
- 4) wymiana informacji dotyczących sytuacji kryzysowych w cyberprzestrzeni;
- 5) przygotowywanie bieżących informacji na temat sytuacji w cyberprzestrzeni dla Pełnomocnika;
- 6) wymiana informacji dotycząca procesów i współpracy międzynarodowej w zakresie bezpieczeństwa w cyberprzestrzeni.

7. Sekretarz PCOC organizuje pracę PCOC i w tym zakresie może występować do CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT sektorowych oraz organów administracji rządowej o przedstawienie informacji niezbędnych w sprawach rozpatrywanych przez PCOC.

8. Sekretarza PCOC powołuje Pełnomocnik spośród osób spełniających wymagania określone w przepisach o ochronie informacji niejawnych w zakresie dostępu do informacji niejawnych o klauzuli „tajne”. Sekretarza PCOC odwołuje Pełnomocnik.

9. Sekretarz PCOC może powołać swojego zastępcę spośród osób spełniających wymagania określone w ust. 8. Zastępcę sekretarza PCOC odwołuje sekretarz PCOC.

10. W przypadku nieobecności sekretarza PCOC jego obowiązki wykonuje zastępca sekretarza PCOC.

11. Obsługę PCOC zapewnia ministerstwo lub inny urząd administracji rządowej obsługujący Pełnomocnika.

12. Pełnomocnik określi, w drodze zarządzenia tryb pracy PCOC, mając na uwadze charakter zadań PCOC oraz konieczność zapewnienia jego sprawnej pracy.

13. Zarządzenie jest publikowane na stronie podmiotowej Biuletynu Informacji Publicznej Pełnomocnika.”;

73) w art. 65:

a) w ust. 1:

- w pkt 1 wyrazy „zagrożeniom cyberbezpieczeństwa” zastępuje się wyrazem „cyberzagrożeniom”,
- w pkt 2:
 - wyrazy „sektorowe zespoły cyberbezpieczeństwa” zastępuje się wyrazami „CSIRT sektorowe”,
 - wyrazy „zagrożeniom cyberbezpieczeństwa” zastępuje się wyrazem „cyberzagrożeniom”,
- w pkt 3 wyrazy „i CSIRT NASK” zastępuje się wyrazami „CSIRT NASK i CSIRT sektorowych”,
- w pkt 4 wyrazy „sektorowych zespołów cyberbezpieczeństwa” zastępuje się wyrazami „CSIRT sektorowych”,
- pkt 8 otrzymuje brzmienie:

„8) współdziałania zespołów CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT sektorowego w sektorze bankowości i infrastruktury rynków finansowych oraz właściwego organu w rozumieniu rozporządzenia 2022/2554, w zakresie działalności podmiotów finansowych będących podmiotami kluczowymi lub podmiotami ważnymi;”,
- dodaje się pkt 9 w brzmieniu:

„9) decyzji w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka.”;

b) w ust. 2 wyrazy „Rady Ministrów” zastępuje się wyrazami „Prezesa Rady Ministrów”;

74) po art. 65 dodaje się art. 65a w brzmieniu:

„Art. 65a. 1. Przewodniczący Kolegium, działając z urzędu lub na wniosek innego członka Kolegium, może zlecić CSIRT MON, CSIRT NASK lub CSIRT GOV przeprowadzenie analizy dotyczącej wpływu konkretnych produktów ICT, usług ICT lub procesów ICT na bezpieczeństwo usług świadczonych przez podmioty określone w art. 67b ust. 1, uwzględniającej informacje przekazane przez państwa członkowskie Unii Europejskiej lub organy Unii Europejskiej i Organizacji Traktatu Północnoatlantyckiego oraz przekazane przez sektor prywatny.

2. Przewodniczący Kolegium, działając z urzędu lub na wniosek członka Kolegium, może zlecić CSIRT MON, CSIRT NASK lub CSIRT GOV, przeprowadzenie analizy dotyczącej trybu i zakresu, w jakim dostawca sprzętu lub oprogramowania, o którym mowa w art. 67b ust. 1, sprawuje nadzór nad procesem wytwarzania i dostarczania produktów ICT, usług ICT lub procesów ICT.

3. Zadania, o których mowa w ust. 1 i 2, są wykonywane w ramach ustawowych zadań odpowiednio CSIRT MON, CSIRT NASK lub CSIRT GOV.”;

75) w art. 66:

a) w ust. 1 w pkt 4 w lit. g kropkę zastępuje się przecinkiem i dodaje się lit. h w brzmieniu:

„h) organy właściwe do spraw cyberbezpieczeństwa.”,

b) ust. 3 otrzymuje brzmienie:

„3. Członkowie Kolegium, o których mowa w ust. 1 pkt 4 lit. a–e oraz lit. h, mogą być zastępowani przez upoważnionych przedstawicieli w randze sekretarza stanu, podsekretarza stanu, wiceprezesa urzędu lub zastępcy przewodniczącego.”,

c) w ust. 4:

– pkt 1 otrzymuje brzmienie:

„1) dyrektor Rządowego Centrum Bezpieczeństwa albo jego zastępca;”,

– w pkt 5 kropkę zastępuje się średnikiem i dodaje się pkt 6–9 w brzmieniu:

„6) Dowódca Komponentu Wojsk Obrony Cyberprzestrzeni albo jego zastępca;

- 7) Prokurator Generalny albo jego zastępca;
 - 8) Szef Agencji Wywiadu albo jego zastępca;
 - 9) Szef Służby Wywiadu Wojskowego albo jego zastępca.”,
- d) w ust. 5 w pkt 2 kropkę zastępuje się średnikiem i dodaje się pkt 3–8 w brzmieniu:
- „3) może pisemnie wnioskować o przeprowadzenie badania, o którym mowa w art. 33 ust. 1;
 - 4) może zlecić CSIRT MON, CSIRT NASK lub CSIRT GOV, przeprowadzenie analizy dotyczącej wpływu konkretnych produktów ICT, usług ICT lub procesów ICT na bezpieczeństwo usług, o której mowa w art. 65a ust. 1;
 - 5) może zlecić CSIRT MON, CSIRT NASK lub CSIRT GOV, przeprowadzenie analizy dotyczącej trybu i zakresu, w jakim dostawca sprawuje nadzór nad procesem wytwarzania i dostarczania produktów ICT, usług ICT lub procesów ICT, o której mowa w art. 65a ust. 2;
 - 6) może wnioskować o wszczęcie postępowania w sprawie uznania dostawcy sprzętu i oprogramowania za dostawcę wysokiego ryzyka, o którym mowa w art. 67b ust. 1;
 - 7) powołuje zespół opiniujący, o którym mowa w art. 67b ust. 13 pkt 1, oraz wskazuje przedstawicieli członków Kolegium wchodzących w jego skład;
 - 8) rozstrzyga spór, o którym mowa w art. 67b ust. 13 pkt 2 zdanie drugie, wskazując właściwego członka zespołu opiniującego.”,
- e) po ust. 5 dodaje się ust. 5a w brzmieniu:
- „5a. Kolegium przyjmuje i rozpatruje sprawy na posiedzeniu albo w drodze korespondencyjnego uzgodnienia stanowisk (tryb obiegowy).”,
- f) w ust. 7 wyrazy „sektorowych zespołów cyberbezpieczeństwa” zastępuje się wyrazami „CSIRT sektorowych”,
- g) po ust. 7 dodaje się ust. 7a i 7b w brzmieniu:
- „7a. Sekretarz Kolegium może powołać swojego zastępcę spośród osób spełniających wymagania określone w ust. 6. Zastępcę sekretarza Kolegium odwołuje sekretarz Kolegium.
- 7b. W przypadku nieobecności sekretarza Kolegium jego obowiązki wykonuje zastępca sekretarza Kolegium, w tym zastępuje go na posiedzeniu Kolegium.”;

76) po rozdziale 12 dodaje się rozdział 12a w brzmieniu:

„Rozdział 12a

Szczególne działania na rzecz zapewnienia cyberbezpieczeństwa na poziomie krajowym

Art. 67a. 1. Pełnomocnik może wydać rekomendacje określające środki techniczne i organizacyjne stosowane w celu zwiększania poziomu bezpieczeństwa systemów informacyjnych podmiotów krajowego systemu cyberbezpieczeństwa.

2. Rekomendacje Pełnomocnika są publikowane na stronie podmiotowej Biuletynu Informacji Publicznej Pełnomocnika.

3. Pełnomocnik przed wydaniem rekomendacji może zasięgnąć opinii Kolegium.

4. W rekomendacjach Pełnomocnik może wskazać kategorie podmiotów, do których kierowane są rekomendacje.

5. Stosowanie rekomendacji jest dobrowolne.

Art. 67b. 1. Minister właściwy do spraw informatyzacji, w celu ochrony bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego, może wszcząć, z urzędu albo na wniosek przewodniczącego Kolegium, postępowanie w sprawie uznania dostawcy sprzętu lub oprogramowania, które są wykorzystywane przez:

- 1) podmioty kluczowe lub podmioty ważne, z wyłączeniem podsektora komunikacji elektronicznej,
- 2) przedsiębiorców komunikacji elektronicznej, których roczne przychody z tytułu wykonywania działalności telekomunikacyjnej w poprzednim roku obrotowym były wyższe od kwoty 10 milionów złotych,
- 3) podmioty finansowe, z wyłączeniem podmiotów określonych w art. 16 rozporządzenia 2022/2554

– za dostawcę wysokiego ryzyka.

2. Do postępowania w sprawie uznania za dostawcę wysokiego ryzyka, jeżeli ustawa nie stanowi inaczej, stosuje się przepisy ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego, z wyłączeniem art. 28, art. 31, art. 51, art. 66a i art. 79 tej ustawy.

3. Stroną postępowania w sprawie uznania za dostawcę wysokiego ryzyka jest każdy, wobec kogo zostało wszczęte postępowanie w sprawie uznania za dostawcę wysokiego ryzyka.

4. Do postępowania w sprawie uznania za dostawcę wysokiego ryzyka może przystąpić, na wniosek, na prawach strony, przedsiębiorca telekomunikacyjny mający

siedzibę na terytorium Rzeczypospolitej Polskiej wpisany do rejestru przedsiębiorców telekomunikacyjnych, który w poprzednim roku obrotowym uzyskał przychód z tytułu prowadzenia działalności telekomunikacyjnej w wysokości co najmniej dwudziestotysięcznej krotności przeciętnego wynagrodzenia w gospodarce narodowej wskazanego w ostatnim komunikacie Prezesa Głównego Urzędu Statystycznego, o którym mowa w art. 20 pkt 1 lit. a ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych (Dz. U. z 2024 r. poz. 1631 i 1674 oraz z 2025 r. poz. 718, 769 i 1159). Przepisy art. 31 § 2 i 3 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego stosuje się odpowiednio.

5. Za poprzedni rok obrotowy uznaje się rok, przed którym postępowanie zostało wszczęte. Za ostatni komunikat Prezesa Głównego Urzędu Statystycznego uznaje się ostatni komunikat Prezesa Głównego Urzędu Statystycznego ogłoszony przed wszczęciem postępowania.

6. Minister właściwy do spraw informatyzacji zawiadamia o wszczęciu postępowania w sprawie uznania za dostawcę wysokiego ryzyka. Zawiadomienie publikuje się także na stronie podmiotowej Biuletynu Informacji Publicznej ministra właściwego do spraw informatyzacji, niezwłocznie po doręczeniu tego zawiadomienia.

7. Minister właściwy do spraw informatyzacji zawiadamia Prokuratora Generalnego o wszczęciu postępowania w sprawie uznania za dostawcę wysokiego ryzyka.

8. Jeżeli dostawcą sprzętu lub oprogramowania jest strona niemająca siedziby na terytorium państwa członkowskiego Unii Europejskiej, Konfederacji Szwajcarskiej albo państwa członkowskiego Europejskiego Porozumienia o Wolnym Handlu (EFTA) – stronie umowy o Europejskim Obszarze Gospodarczym zawiadomienie, o którym mowa w ust. 6, publikuje się na stronie podmiotowej Biuletynu Informacji Publicznej ministra właściwego do spraw informatyzacji. Udostępnienie ma skutek doręczenia zawiadomienia stronie po upływie 14 dni od dnia jego dokonania.

9. W terminie 14 dni od dnia opublikowania na stronie podmiotowej Biuletynu Informacji Publicznej ministra właściwego do spraw informatyzacji zawiadomienia, o którym mowa w ust. 6 i 8, organizacja społeczna może przedstawić ministrowi właściwemu do spraw informatyzacji stanowisko co do dostawcy sprzętu lub oprogramowania, wobec którego wszczęto postępowanie, oraz dostarczanych przez niego produktów ICT, usług ICT oraz procesów ICT. Minister właściwy do spraw informatyzacji, przed wydaniem decyzji, publikuje na swojej stronie podmiotowej

Biuletynu Informacji Publicznej raport ze złożonych w terminie stanowisk, wskazując w szczególności główne uwagi zawarte w stanowiskach.

10. Przed wydaniem decyzji minister właściwy do spraw informatyzacji zasięga opinii Kolegium. Kolegium przekazuje opinię w terminie 3 miesięcy od dnia wystąpienia o opinię. Okresu od dnia wystąpienia o opinię do Kolegium do dnia jej otrzymania nie wlicza się do terminu załatwienia sprawy. Przepisu art. 106 § 5 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego nie stosuje się.

11. Opinia, o której mowa w ust. 10 zdanie pierwsze, zawiera analizę:

- 1) zagrożeń bezpieczeństwa narodowego o charakterze ekonomicznym, wywiadowczym i terrorystycznym oraz zagrożeń dla realizacji zobowiązań sojusznicznych i europejskich, jakie stanowi dostawca sprzętu i oprogramowania, z uwzględnieniem informacji o zagrożeniach uzyskanych od państw członkowskich Unii Europejskiej lub organów Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego;
- 2) prawdopodobieństwa z jakim dostawca sprzętu lub oprogramowania znajduje się pod kontrolą państwa spoza terytorium Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, z uwzględnieniem:
 - a) przepisów prawa regulujących stosunki między dostawcą sprzętu lub oprogramowania, a tym państwem oraz praktyki stosowania prawa w tym zakresie,
 - b) prawodawstwa oraz stosowania prawa w zakresie ochrony danych osobowych, w szczególności w przypadku, gdy nie ma porozumień w zakresie ochrony tych danych między Unią Europejską i tym państwem,
 - c) struktury własnościowej dostawcy sprzętu lub oprogramowania,
 - d) zdolności ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania;
- 3) powiązań dostawcy sprzętu lub oprogramowania z podmiotami określonymi w załączniku do rozporządzenia Rady (UE) 2019/796 z dnia 17 maja 2019 r. w sprawie środków ograniczających w celu zwalczania cyberataków zagrażających

Unii lub jej państwom członkowskim (Dz. Urz. UE L 129I z 17.05.2019, str. 1, z późn. zm.¹⁴⁾);

- 4) liczby i rodzajów wykrytych podatności i incydentów dotyczących typów produktów ICT lub rodzajów usług ICT lub konkretnych procesów ICT dostarczanych przez dostawcę sprzętu lub oprogramowania oraz sposobu i czasu ich eliminowania;
- 5) trybu i zakresu, w jakim dostawca sprzętu lub oprogramowania sprawuje nadzór nad procesem wytwarzania i dostarczania sprzętu lub oprogramowania dla podmiotów, o których mowa w ust. 1, oraz ryzyka dla procesu wytwarzania i dostarczania sprzętu lub oprogramowania;
- 6) treści wydanych rekomendacji, o których mowa w art. 33 ust. 4, dotyczących sprzętu lub oprogramowania danego dostawcy.

12. Sporządzając opinię, o której mowa w ust. 10 zdanie pierwsze, Kolegium uwzględnia:

- 1) certyfikaty wydane dla produktów ICT, usług ICT lub procesów ICT, wydane lub uznawane w państwach członkowskich Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, w szczególności certyfikaty wydane w ramach europejskich programów certyfikacji cyberbezpieczeństwa;
- 2) analizy, o których mowa w art. 65a ust. 1 i 2.

13. Procedura sporządzenia opinii, o której mowa w ust. 10 zdanie pierwsze, przebiega w następujący sposób:

- 1) przewodniczący Kolegium powołuje zespół w celu opracowania projektu opinii w sprawie uznania dostawcy za dostawcę wysokiego ryzyka, zwany dalej „zespołem opiniującym”, w skład którego wchodzi przedstawiciele członków Kolegium wskazani przez przewodniczącego Kolegium;
- 2) każdy członek zespołu opiniującego przygotowuje stanowisko, w zakresie swojej właściwości, które następnie przekazuje zespołowi opiniującemu. W przypadku wystąpienia negatywnego sporu co do zakresu właściwości spór rozstrzyga przewodniczący Kolegium, wskazując właściwego członka zespołu opiniującego;

¹⁴⁾ Zmiany wymienionego rozporządzenia zostały ogłoszone w Dz. Urz. UE L 230 z 17.07.2020, str. 37, Dz. Urz. UE L 246 z 30.07.2020, str. 4, Dz. Urz. UE L 351I z 22.10.2020, str. 1, Dz. Urz. UE L 393 z 23.11.2020, str. 1, Dz. Urz. UE L 114 z 12.04.2022, str. 60, Dz. Urz. UE L 2694 z 28.11.2023, str. 1, Dz. Urz. UE L 1390 z 17.05.2024, str. 1, Dz. Urz. UE L 1778 z 24.06.2024, str. 1, Dz. Urz. UE L 90397 z 09.07.2024, str. 1, Dz. Urz. UE L 2465 z 12.09.2024, str. 1, Dz. Urz. UE L 173 z 27.01.2025, str. 1 oraz Dz. Urz. UE L 886 z 13.05.2025, str. 1.

- 3) jeżeli nie zostały wykonane analizy, o których mowa w art. 65a ust. 1 i 2, przewodniczący Kolegium zleca ich wykonanie;
- 4) zespół opiniujący przedstawia przewodniczącemu Kolegium projekt opinii;
- 5) ustalenie opinii następuje na posiedzeniu Kolegium;
- 6) ustaloną opinię przewodniczący Kolegium przekazuje ministrowi właściwemu do spraw informatyzacji.

14. W zespole opiniującym może wziąć udział również przedstawiciel Prezesa Urzędu Ochrony Konkurencji i Konsumentów. W posiedzeniu Kolegium, na którym następuje ustalenie opinii, może wziąć udział Prezes lub Wiceprezes Urzędu Ochrony Konkurencji i Konsumentów.

15. Minister właściwy do spraw informatyzacji, w drodze decyzji, uznaje dostawcę sprzętu lub oprogramowania oraz podmioty wchodzące w skład grupy kapitałowej, w rozumieniu art. 3 ust. 1 pkt 44 ustawy z dnia 29 września 1994 r. o rachunkowości, w ramach której funkcjonuje dostawca, za dostawcę wysokiego ryzyka, jeżeli dostawca ten stanowi zagrożenie dla podstawowego interesu bezpieczeństwa państwa.

16. Decyzja, o której mowa w ust. 15, zawiera w szczególności wskazanie typów produktów ICT, rodzajów usług ICT lub konkretnych procesów ICT pochodzących od dostawcy sprzętu lub oprogramowania uwzględnionych w postępowaniu w sprawie uznania za dostawcę wysokiego ryzyka.

17. Minister właściwy do spraw informatyzacji ogłasza decyzję, o której mowa w ust. 15, w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski” oraz publikuje na stronie podmiotowej Biuletynu Informacji Publicznej ministra właściwego do spraw informatyzacji, a także na stronie internetowej urzędu obsługującego tego ministra.

18. Decyzja, o której mowa w ust. 15, podlega natychmiastowemu wykonaniu.

19. Od decyzji, o której mowa w ust. 15, nie przysługuje wniosek o ponowne rozpatrzenie sprawy.

Art. 67c. 1. W przypadku wydania decyzji, o której mowa w art. 67b ust. 15, podmioty, o których mowa w art. 67b ust. 1:

- 1) nie wprowadzają do użytkowania typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT w zakresie objętym decyzją, dostarczanych przez dostawcę wysokiego ryzyka;

2) wycofują z użytkowania typy produktów ICT, rodzaje usług ICT i konkretne procesy ICT w zakresie objętym decyzją dostarczanych przez dostawcę wysokiego ryzyka nie później niż w terminie 7 lat od dnia ogłoszenia decyzji, o której mowa w art. 67b ust. 15, w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski”.

2. Przedsiębiorcy telekomunikacyjni, o których mowa w art. 67b ust. 1 pkt 2, wycofują w ciągu 4 lat od dnia ogłoszenia decyzji, o której mowa w art. 67b ust. 15, typy produktów ICT, rodzaje usług ICT, konkretne procesy ICT wskazane w decyzji i określone w wykazie kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług w załączniku nr 3 do ustawy.

3. Do czasu wycofania sprzętu lub oprogramowania, o którym mowa w ust. 1 pkt 2 oraz w ust. 2, dopuszcza się użytkowanie dotychczas posiadanych typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT w zakresie objętym decyzją, dostarczanych przez dostawcę wysokiego ryzyka, w zakresie naprawy, modernizacji, wymiany elementu lub aktualizacji, jeżeli jest to niezbędne dla zapewnienia odpowiedniej jakości i ciągłości świadczonych usług, w szczególności dokonywania niezbędnych napraw awarii lub uszkodzeń.

4. Podmioty, o których mowa w art. 67b ust. 1, do których stosuje się ustawę z dnia 11 września 2019 r. – Prawo zamówień publicznych (Dz. U. z 2024 r. poz. 1320, z późn. zm.¹⁵⁾), nie mogą nabywać typów produktów ICT, rodzajów usług ICT lub konkretnych procesów ICT określonych w decyzji, o której mowa w art. 67b ust. 15.

5. W przypadku gdy podmioty, o których mowa w art. 67b ust. 1, do których stosuje się ustawę z dnia 11 września 2019 r. – Prawo zamówień publicznych, nabyły, w drodze zamówienia publicznego, przed dniem ogłoszenia decyzji, o której mowa w art. 67b ust. 15, produkt ICT, usługę ICT lub proces ICT określone w tej decyzji, mogą korzystać z tych produktów, usług lub procesów nie dłużej niż 7 lat od dnia ogłoszenia decyzji, o której mowa w art. 67b ust. 15, w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski”, a w przypadku produktów ICT, usług ICT lub procesów ICT wykorzystywanych do wykonywania funkcji krytycznych określonych w załączniku nr 3 do ustawy, nie dłużej niż 4 lat od dnia ogłoszenia decyzji, o której mowa w art. 67b ust. 15.

¹⁵⁾ Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2025 r. poz. 620, 769, 794, 1165, 1173 i 1235.

Art. 67d. 1. Podmioty kluczowe lub podmioty ważne są obowiązane przekazać informacje na wniosek uprawnionych organów, o których mowa w ust. 2, o wycofywanych typach produktów ICT, rodzajach usług ICT i konkretnych procesach ICT w zakresie objętym decyzją, o której mowa w art. 67b ust. 15.

2. Uprawnionymi organami do uzyskania informacji, o których mowa w ust. 1, są organy właściwe do spraw cyberbezpieczeństwa.

3. Wniosek, o którym mowa w ust. 1, zawiera:

- 1) wskazanie podmiotu obowiązującego do przekazania informacji;
- 2) datę wydania decyzji, o której mowa w art. 67b ust. 15;
- 3) wskazanie zakresu żądanych informacji;
- 4) wskazanie terminu przekazania informacji adekwatnego do zakresu tego żądania, nie krótszego niż 7 dni;
- 5) uzasadnienie;
- 6) pouczenie o zagrożeniu karą, o której mowa w art. 73.

4. Minister właściwy do spraw informatyzacji może zwrócić się do organów właściwych do spraw cyberbezpieczeństwa, aby uzyskały informacje, o których mowa w ust. 1.

5. Na wniosek ministra właściwego do spraw informatyzacji organ właściwy do spraw cyberbezpieczeństwa przekazuje uzyskane informacje, o których mowa w ust. 1, temu ministrowi.

Art. 67e. 1. Sąd administracyjny rozpatruje skargę na decyzję, o której mowa w art. 67b ust. 15, na posiedzeniu niejawnym w składzie trzech sędziów.

2. Odpis sentencji wyroku z uzasadnieniem doręcza się wyłącznie ministrowi właściwemu do spraw informatyzacji. Skarżącemu doręcza się odpis wyroku z tą częścią uzasadnienia, która nie zawiera informacji niejawnych w rozumieniu przepisów o ochronie informacji niejawnych.

Art. 67f. Minister właściwy do spraw informatyzacji publikuje na stronie podmiotowej Biuletynu Informacji Publicznej urzędu go obsługującego listę produktów ICT, usług ICT i konkretnych procesów ICT objętych decyzjami, o których mowa w art. 67b ust. 15.

Art. 67g. 1. Minister właściwy do spraw informatyzacji w przypadku wystąpienia incydentu krytycznego może, w drodze decyzji, wydać polecenie zabezpieczające.

2. Polecenie zabezpieczające dotyczy nieokreślonej liczby podmiotów kluczowych lub podmiotów ważnych oraz podmiotów finansowych, z wyłączeniem podmiotów określonych w art. 16 rozporządzenia 2022/2554.

3. Do postępowania w sprawie o wydanie polecenia zabezpieczającego nie stosuje się art. 10, art. 34, art. 79, art. 81, art. 81a, art. 107 § 1 pkt 3, art. 145 § 1 pkt 4 i art. 156 § 1 pkt 4 oraz rozdziału 8 działu I ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego, a pozostałe przepisy tej ustawy stosuje się odpowiednio.

4. Stronę zawiadamia się o czynnościach w sprawie przez publiczne opublikowanie informacji na stronie podmiotowej Biuletynu Informacji Publicznej ministra właściwego do spraw informatyzacji.

5. Przed wydaniem polecenia zabezpieczającego minister właściwy do spraw informatyzacji przeprowadza we współpracy z Zespołem, o którym mowa w art. 35 ust. 3, analizę obejmującą:

- 1) istotność cyberzagrożenia związanego z incydem krytycznym;
- 2) szacowanie ryzyka związane z zaistniałym incydem krytycznym;
- 3) przewidywane lub zaistniałe skutki incydentu krytycznego;
- 4) skuteczność obowiązku określonego zachowania zmniejszającego skutki incydentu krytycznego lub zapobiegającego jego rozprzestrzenianiu się;
- 5) ocenę stopnia dotkliwości wprowadzanych obowiązków dla podmiotów objętych poleceniem zabezpieczającym oraz proporcjonalności tych obowiązków do celu ich wprowadzania.

6. Do analizy, o której mowa w ust. 5, nie stosuje się art. 106 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego.

7. Pełnomocnik, dyrektor Rządowego Centrum Bezpieczeństwa, Szef Agencji Bezpieczeństwa Wewnętrznego oraz minister właściwy do spraw informatyzacji, może wzywać podmioty, o których mowa w ust. 2, lub organy administracji publicznej do udzielenia informacji niezbędnych do przeprowadzenia analizy. Organy administracji publicznej udzielają informacji, o których mowa w zdaniu pierwszym, niezwłocznie, nie później niż w ciągu 72 godzin od otrzymania wezwania.

8. Przedstawiciele podmiotów, o których mowa w ust. 2, organizacji społecznych zrzeszających podmioty, o których mowa w ust. 2, lub organów administracji publicznej mogą być zapraszani przez Pełnomocnika do udziału w pracach Zespołu, o którym mowa

w art. 35 ust. 3, lub w jego posiedzeniach w związku z przygotowywaniem analizy, o której mowa w ust. 5.

9. Polecenie zabezpieczające zawiera:

- 1) wskazanie rodzaju lub rodzajów podmiotów, których dotyczy;
- 2) obowiązek określonego zachowania zmniejszającego skutki incydentu krytycznego lub zapobiegającego jego rozprzestrzenianiu się;
- 3) termin jego wdrożenia.

10. Obowiązkiem określonego zachowania, o którym mowa w ust. 9 pkt 2, jest:

- 1) nakaz przeprowadzenia szacowania ryzyka związanego ze stosowaniem określonego produktu ICT, usługi ICT lub procesu ICT i wprowadzenie środków ochrony proporcjonalnych do zidentyfikowanych ryzyk;
- 2) nakaz przeglądu planów ciągłości działania, planów awaryjnych i planów odtworzenia działalności pod kątem ryzyka wystąpienia incydentu krytycznego związanego z daną podatnością;
- 3) nakaz zastosowania określonej poprawki bezpieczeństwa w produkcie ICT lub usłudze ICT posiadającym daną podatność;
- 4) nakaz szczególnej konfiguracji produktu ICT lub usługi ICT, zabezpieczającej przed wykorzystaniem określonej podatności;
- 5) nakaz wzmożonego monitorowania zachowania systemu informacyjnego;
- 6) zakaz korzystania z określonego produktu ICT lub usługi ICT, które posiada podatność, która przyczyniła się do zaistnienia incydentu krytycznego;
- 7) nakaz wprowadzenia ograniczenia ruchu sieciowego przychodzącego do infrastruktury podmiotu kluczowego lub podmiotu ważnego, który skutkując zakłóceniem usług świadczonych przez ten podmiot został sklasyfikowany przez CSIRT MON, CSIRT NASK lub CSIRT GOV jako przyczyna trwającego incydentu krytycznego;
- 8) nakaz wstrzymania dystrybucji lub zakaz instalacji określonej wersji oprogramowania;
- 9) nakaz zabezpieczenia określonych informacji, w tym dzienników systemowych;
- 10) nakaz wytworzenia obrazów stanu określonych urządzeń zainfekowanych złośliwym oprogramowaniem.

11. Wskazanie obowiązku określonego zachowania, o którym mowa w ust. 9 pkt 2, następuje z uwzględnieniem środków adekwatnych, w szczególności w świetle analizy, o której mowa w ust. 5.

12. Polecenie zabezpieczające wydaje się na czas koordynacji obsługi incydentu krytycznego lub na czas oznaczony, nie dłużej niż na dwa lata.

13. Polecenie zabezpieczające wygasa:

- 1) z dniem wskazanym w ogłoszeniu o zakończeniu koordynacji obsługi incydentu w dzienniku urzędowym ministra właściwego do spraw informatyzacji, lub
- 2) po upływie czasu, na który zostało wydane.

14. Polecenie zabezpieczające podlega natychmiastowej wykonalności.

15. Minister właściwy do spraw informatyzacji ogłasza komunikat o wydaniu polecenia zabezpieczającego, w swoim dzienniku urzędowym oraz na stronie internetowej urzędu obsługującego ministra. Załącznikiem do komunikatu jest wydane polecenie zabezpieczające.

16. Polecenie zabezpieczające uznaje się za doręczone z chwilą ogłoszenia komunikatu o wydaniu polecenia zabezpieczającego w dzienniku urzędowym ministra właściwego do spraw informatyzacji.

17. Od polecenia zabezpieczającego nie przysługuje wniosek o ponowne rozpatrzenie sprawy.

Art. 67h. Podmioty, których dotyczy polecenie zabezpieczające, są obowiązane przekazać informacje na wniosek organów właściwych do spraw cyberbezpieczeństwa, o wykonywaniu polecenia zabezpieczającego. Przepisy art. 67c ust. 2–5 stosuje się.

Art. 67i. 1. Skargę na polecenie zabezpieczające wnosi się w terminie 2 miesięcy od dnia, w którym komunikat o wydaniu polecenia zabezpieczającego został ogłoszony w dzienniku urzędowym ministra właściwego do spraw informatyzacji.

2. Sąd administracyjny zarządza połączenie wszystkich oddzielnych spraw toczących się przed nim w celu ich łącznego rozpoznania i rozstrzygnięcia, jeżeli dotyczą tej samej decyzji.

3. Wniosek o przywrócenie terminu na złożenie skargi jest niedopuszczalny.

Art. 67j. 1. Do Narodowego Banku Polskiego nie stosuje się przepisów art. 67b, art. 67f oraz art. 67g.

2. Minister właściwy do spraw informatyzacji przekazuje niezwłocznie Prezesowi Narodowego Banku Polskiego informacje o decyzjach wydanych na podstawie art. 67b ust. 15 oraz art. 67f ust. 1.

Art. 67k. 1. Do podmiotów finansowych niebędących podmiotami kluczowymi lub podmiotami ważnymi stosuje się przepisy art. 67c, art. 67d, art. 67g oraz art. 67h.

2. Obowiązków, o których mowa w ust. 1, nie stosuje się wobec podmiotów finansowych niebędących podmiotami kluczowymi lub podmiotami ważnymi, do których stosuje się art. 16 ust. 1 rozporządzenia 2022/2554.

3. Nadzór nad wykonywaniem obowiązków, o których mowa w ust. 1, sprawuje organ właściwy do spraw cyberbezpieczeństwa dla sektora bankowości i infrastruktury rynków finansowych.

4. Do nadzoru i kontroli wykonywania obowiązków wymienionych w ust. 1, oraz do kar pieniężnych nakładanych za naruszenia tych obowiązków, odpowiednio stosuje się przepisy rozdziałów 11 i 14.

Art. 67l. 1. Prezes Rady Ministrów, działając na podstawie rekomendacji Kolegium, w uzgodnieniu z Ministrem Obrony Narodowej, może czasowo powierzyć temu ministrowi realizację wybranych zadań, o których mowa w art. 26.

2. Powierzając realizację wybranych zadań, o których mowa w art. 26, określa się w szczególności:

- 1) zakres powierzonych zadań;
- 2) czas realizacji powierzonych zadań, nie dłuższy niż 1 rok, lub sposób ich odwołania;
- 3) w razie potrzeby – szczególne zasady współpracy z CSIRT MON, CSIRT NASK i CSIRT GOV;
- 4) zasady informowania Kolegium o stanie realizacji powierzonych zadań.

3. Realizacja zadań, o których mowa w ust. 1, jest dokonywana przez Ministra Obrony Narodowej z wykorzystaniem jednostek mu podległych lub przez niego nadzorowanych, z uwzględnieniem art. 12a ustawy z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (Dz. U. z 2025 r. poz. 504).

4. Prezes Rady Ministrów wydaje komunikat o powierzeniu realizacji zadań, o których mowa w ust. 1, i niezwłocznie ogłasza go w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski”. Informacja o komunikacie jest publikowana

również na stronach internetowych CSIRT MON, CSIRT NASK, CSIRT GOV lub na stronie podmiotowej Biuletynu Informacji Publicznej Pełnomocnika.”;

77) art. 69 otrzymuje brzmienie:

„Art. 69. 1. Strategia określa:

- 1) cele strategiczne i cele szczegółowe oraz środki organizacyjne i regulacyjne, służące ich realizacji;
- 2) mechanizm służący określeniu istotnych zasobów i szacowanie ryzyka związanego z cyberbezpieczeństwem;
- 3) zasady współpracy między sektorem publicznym i prywatnym;
- 4) podmioty zaangażowane we wdrażanie i realizację Strategii;
- 5) środki służące koordynacji i wymiany informacji pomiędzy organami właściwymi w sprawach cyberbezpieczeństwa a właściwymi organami na podstawie dyrektywy 2022/2557 na temat ryzyka, cyberzagrożeń i incydentów, a także ryzyka, zagrożeń i incydentów poza cyberprzestrzenią oraz wykonywania zadań nadzorczych;
- 6) działania w zakresie zwiększenia ogólnego poziomu wiedzy obywateli o cyberbezpieczeństwie;
- 7) cele i sposób realizacji interesów cyberbezpieczeństwa krajowego w wymiarze międzynarodowym.

2. Przy opracowaniu strategii uwzględnia się:

- 1) rozwiązania dotyczące cyberbezpieczeństwa w łańcuchu dostaw produktów ICT, usług ICT i procesów ICT wykorzystywanych przez podmioty do świadczenia usług;
- 2) rozwiązania dotyczące uwzględniania w zamówieniach publicznych wymogów związanych z cyberbezpieczeństwem w odniesieniu do produktów ICT, usług ICT i procesów ICT oraz specyfikacji tych wymogów na potrzeby takich zamówień, w tym w odniesieniu do certyfikacji cyberbezpieczeństwa, szyfrowania oraz wykorzystywania produktów z zakresu cyberbezpieczeństwa opartych na otwartym oprogramowaniu;
- 3) rozwiązania dotyczące zarządzania podatnościami, obejmujące promowanie i ułatwianie skoordynowanego ujawniania podatności na podstawie art. 12 ust. 1 dyrektywy 2022/2555;

- 4) utrzymanie ogólnej dostępności, integralności i poufności publicznego rdzenia otwartego internetu, w tym, w stosownych przypadkach, cyberbezpieczeństwa podmorskich kabli komunikacyjnych;
- 5) promowanie rozwoju i integracji odpowiednich zaawansowanych technologii służących wdrożeniu najnowocześniejszych środków zarządzania ryzykiem w cyberbezpieczeństwie;
- 6) kształcenie i szkolenia w dziedzinie cyberbezpieczeństwa, umiejętności z zakresu cyberbezpieczeństwa, rozwój i promocję kwalifikacji rynkowych w zakresie cyberbezpieczeństwa w przemyśle, podnoszenie świadomości oraz inicjatywy badawczo-rozwojowe, a także wytyczne dotyczące dobrych praktyk i kontroli w zakresie higieny cyfrowej;
- 7) wspieranie instytucji akademickich i naukowych, w opracowywaniu, usprawnianiu i propagowaniu wprowadzania narzędzi z zakresu cyberbezpieczeństwa oraz bezpiecznej infrastruktury sieciowej;
- 8) zapewnienia odpowiednich procedur oraz narzędzi służących wymianie informacji;
- 9) rozwiązania wzmacniające podstawowy poziom cyberodporności i higieny cyfrowej małych i średnich przedsiębiorstw;
- 10) rozwiązania wspierające aktywne działania w cyberprzestrzeni.

3. Strategia obejmuje sektory, o których mowa w załącznikach nr 1 i 2 do ustawy.

4. Strategia jest realizowana w oparciu o plan działań uwzględniający w szczególności koszty realizacji i źródła finansowania działań określonych w Strategii, a także podmioty odpowiedzialne i planowany termin realizacji poszczególnych działań. Plan działań stanowi załącznik do Strategii.

5. Strategia jest przyjmowana na okres pięcioletni z możliwością wprowadzania w niej zmian na podstawie wyników przeglądu i oceny, o których mowa w art. 71.”;

78) w art. 70:

a) ust. 1 otrzymuje brzmienie:

„1. Projekt Strategii opracowuje minister właściwy do spraw informatyzacji we współpracy z Pełnomocnikiem, innymi ministrami, właściwymi kierownikami urzędów centralnych, a także właściwym organem w rozumieniu rozporządzenia 2022/2554.”,

b) dodaje się ust. 3 w brzmieniu:

„3. Strategia jest ogłaszana w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski”.”;

79) po art. 70 dodaje się art. 70a w brzmieniu:

„Art. 70a. 1. Podmioty, o których mowa w art. 69 ust. 1 pkt 4, przekazują na żądanie ministra właściwego do spraw informatyzacji informację o bieżącym stanie realizacji celów szczegółowych Strategii i działań określonych w planie działań.

2. CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT sektorowy i organ właściwy do spraw cyberbezpieczeństwa przekazują ministrowi właściwemu do spraw informatyzacji, w terminie do dnia 30 marca, informacje o realizacji celów Strategii w poprzednim roku i działań określonych w planie działań.”;

80) art. 71 otrzymuje brzmienie:

„Art. 71. Minister właściwy do spraw informatyzacji we współpracy z Pełnomocnikiem, innymi ministrami i właściwymi kierownikami urzędów centralnych dokonuje przeglądu Strategii i oceny jej skuteczności, nie rzadziej niż co 2,5 roku.”;

81) po rozdziale 13 dodaje się rozdział 13a w brzmieniu:

„Rozdział 13a

Krajowy plan reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę

Art. 72a. Rada Ministrów przyjmuje, w drodze uchwały, Krajowy plan reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę, zwany dalej „Krajowym Planem”.

Art. 72b. 1. Krajowy Plan określa cele i tryb zarządzania incydentami i zarządzania kryzysowego w cyberbezpieczeństwie na dużą skalę.

2. Krajowy Plan zawiera w szczególności:

- 1) cele działań w zakresie zarządzania kryzysowego w cyberbezpieczeństwie na dużą skalę;
- 2) zadania organów zaangażowanych w zarządzanie kryzysowe w cyberbezpieczeństwie;
- 3) procedury zarządzania kryzysowego w cyberprzestrzeni oraz kanały wymiany informacji;
- 4) krajowe środki służące zapewnieniu gotowości na wypadek wystąpienia incydentów w cyberbezpieczeństwie na dużą skalę, w tym ćwiczenia i szkolenia;

- 5) zasady współpracy między sektorem publicznym i prywatnym w obszarze zarządzania kryzysowego;
- 6) kryteria oceny infrastruktury informatycznej pod kątem jej znaczenia dla zarządzania kryzysowego;
- 7) krajowe procedury i ustalenia między odpowiednimi organami i instytucjami krajowymi mające na celu zapewnienie efektywnego uczestnictwa danego państwa członkowskiego Unii Europejskiej w skoordynowanym zarządzaniu incydentami i zarządzaniu kryzysowym w cyberbezpieczeństwie na dużą skalę na poziomie Unii Europejskiej oraz efektywnego wsparcia ze strony danego państwa członkowskiego Unii Europejskiej dla tego rodzaju skoordynowanego zarządzania;
- 8) postanowienia dotyczące zarządzania kryzysami i reagowania na nie w odniesieniu do transgranicznych przepływów energii elektrycznej, w rozumieniu art. 41 ust. 2 i 3 rozporządzenia 2024/1366;
- 9) uporządkowaną listę działań na rzecz ograniczenia ryzyka wystąpienia incydentu krytycznego w zakresie organizacyjnym i technicznym, z uwzględnieniem:
 - a) hierarchii działań,
 - b) ram czasowych ich realizacji,
 - c) podmiotów wiodących oraz współpracujących przy ich wykonywaniu,
 - d) sposobów finansowania oraz wysokości nakładów finansowych,
 - e) oceny osiągniętych efektów oraz wniosków z wdrożonych działań.

Art. 72c. Podmioty realizujące zadania z zakresu zarządzania kryzysowego na żądanie ministra właściwego do spraw informatyzacji przekazują informację o bieżącym stanie realizacji zadań wynikających z Krajowego Planu.

Art. 72d. 1. Projekt Krajowego Planu opracowuje minister właściwy do spraw informatyzacji we współpracy z Pełnomocnikiem, Rządowym Centrum Bezpieczeństwa, oraz z innymi ministrami, właściwymi kierownikami urzędów centralnych oraz z właściwym organem określonym w art. 52a ust. 1.

2. W pracach nad projektem może uczestniczyć przedstawiciel Prezydenta Rzeczypospolitej Polskiej.

3. Krajowy Plan jest ogłaszany w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski”.

Art. 72e. Krajowy Plan podlega aktualizacji nie rzadziej niż raz na dwa lata.

Art. 72f. Minister właściwy do spraw informatyzacji przekazuje Komisji Europejskiej i europejskiej sieci organizacji łącznikowych do spraw kryzysów cyberbezpieczeństwa ważne informacje związane z Krajowym Planem, w szczególności procedury, o których mowa w art. 72b ust. 2 pkt 3, w terminie 3 miesięcy od dnia jego przyjęcia przez Radę Ministrów.”;

82) w art. 73:

a) ust. 1 otrzymuje brzmienie:

„1. Karze pieniężnej podlega podmiot kluczowy lub podmiot ważny, który:

- 1) nie uzupełnił w terminie brakujących danych w wykazie podmiotów kluczowych i podmiotów ważnych pomimo wezwania, o którym mowa w art. 7b ust. 2 albo art. 7j ust. 3, albo art. 7k ust. 2, albo art. 7l ust. 3 pkt 2;
- 2) nie przeprowadza systematycznego szacowania ryzyka lub nie zarządza ryzykiem wystąpienia incydentu, o których mowa w art. 8 ust. 1 pkt 1;
- 3) nie wdrożył systemu zarządzania bezpieczeństwem informacji w systemie informacyjnym wykorzystywanym w procesach wpływających na świadczenie usługi albo system ten nie zapewnia funkcjonalności, o których mowa w art. 8 ust. 1 albo art. 8 ust. 3;
- 4) nie wykonuje obowiązków, o których mowa w art. 10 ust. 1;
- 5) nie wykonuje obowiązku, o którym mowa w art. 11 ust. 1 pkt 1;
- 6) nie wykonuje obowiązku, o którym mowa w art. 11 ust. 1 pkt 4;
- 7) nie wykonuje obowiązku, o którym mowa w art. 11 ust. 1 pkt 4a;
- 8) nie wykonuje obowiązku, o którym mowa w art. 11 ust. 1 pkt 4b;
- 9) nie wykonuje obowiązku, o którym mowa w art. 11 ust. 1 pkt 4c;
- 10) nie wykonuje obowiązku, o którym mowa w art. 11 ust. 1 pkt 5;
- 11) nie przeprowadza audytu w terminie, o którym mowa w art. 15 ust. 1 lub art. 16 pkt 2;
- 12) nie usuwa podatności, o których mowa w art. 32 ust. 2;
- 13) nie korzysta z systemu teleinformatycznego, o którym mowa w art. 46 ust. 1, w celu realizacji obowiązków, o których mowa w art. 11;
- 14) uniemożliwia lub utrudnia wykonywanie kontroli, o których mowa w art. 53 ust. 2 pkt 1;
- 15) nie realizuje obowiązku, o którym mowa w art. 53c;

- 16) uniemożliwia lub utrudnia urzędnikowi monitorującemu, o którym mowa w art. 53 ust. 5 pkt 6, wykonywanie powierzonych mu zadań lub realizację uprawnień, o których mowa w art. 53d ust. 1;
 - 17) nie wykonał w wyznaczonym terminie zaleceń pokontrolnych, o których mowa w art. 59 ust. 1;
 - 18) nie wykonuje obowiązków, o których mowa w art. 67c ust. 1, 2, 4 i 5;
 - 19) nie wdrożył w terminie określonym w poleceniu zabezpieczającym, o którym mowa w art. 67g ust. 9 pkt 3, określonego zachowania, o którym mowa w art. 67g ust. 10;
 - 20) odstąpił od wykonywania zawartego w poleceniu zabezpieczającym, o którym mowa w art. 67g ust. 9, określonego zachowania, o którym mowa w art. 67g ust. 10, przed wygaśnięciem polecenia zabezpieczającego.”,
- b) po ust. 1 dodaje się ust. 1a–1d w brzmieniu:
- „1a. Organ właściwy do spraw cyberbezpieczeństwa, jeżeli przemawia za tym waga i znaczenie naruszonych przepisów, może nałożyć karę pieniężną na podmiot, który:
- 1) w terminie, o którym mowa w art. 7c ust. 1, nie złożył wniosku o wpis do wykazu podmiotów kluczowych i podmiotów ważnych, o którym mowa w art. 7 ust. 1;
 - 2) nie wykonuje obowiązków, o których mowa w art. 9.
- 1b. Karze pieniężnej podlega także podmiot kluczowy lub podmiot ważny, którego działanie lub zaniechanie, o którym mowa w ust. 1 pkt 2, 4–12, 14–16 i 18 oraz ust. 1a pkt 2, miało charakter jednorazowy.
- 1c. Podmiot ważny będący podmiotem publicznym podlega karze pieniężnej, jeżeli nie wykonuje obowiązku, o którym mowa w art. 8 ust. 3.
- 1d. Przepis ust. 1 pkt 13 nie stosuje się do Ministra Obrony Narodowej, urzędu go obsługującego oraz podmiotów podległych Ministrowi Obrony Narodowej i przez niego nadzorowanych.”,
- c) uchyla się ust. 2,
- d) ust. 3 otrzymuje brzmienie:
- „3. Wysokość kary pieniężnej nie może przekroczyć 10 000 000 euro, wyrażonej w złotych i ustalonej przy zastosowaniu kursu średniego ogłaszanego przez Narodowy Bank Polski obowiązującego w dniu 31 grudnia w roku

poprzedzającym rok wydania decyzji o wymierzeniu kary lub 2% przychodów osiągniętych przez podmiot kluczowy z działalności gospodarczej w roku obrotowym poprzedzającym wymierzenie kary, przy czym zastosowanie ma kwota wyższa. Kara ta nie może być jednak niższa niż 20 000 zł.”,

e) po ust. 3 dodaje się ust. 3a w brzmieniu:

„3a. W przypadku gdy okres wykonywania działalności gospodarczej jest krótszy niż 12 miesięcy albo podmiot nie osiągnął przychodu za podstawę wymiaru kary pieniężnej przyjmuje się równowartość kwoty 500 000 euro, wyrażonej w złotych i ustalonej przy zastosowaniu kursu średniego ogłaszanego przez Narodowy Bank Polski obowiązującego w dniu 31 grudnia w roku poprzedzającym rok wydania decyzji o wymierzeniu kary.”,

f) ust. 4 i 5 otrzymują brzmienie:

„4. Wysokość kary pieniężnej nie może przekroczyć 7 000 000 euro, wyrażonej w złotych i ustalonej przy zastosowaniu kursu średniego ogłaszanego przez Narodowy Bank Polski obowiązującego w dniu 31 grudnia w roku poprzedzającym rok wydania decyzji o wymierzeniu kary lub 1,4% przychodów osiągniętych przez podmiot ważny z działalności gospodarczej w roku obrotowym poprzedzającym wymierzenie kary. Kara ta nie może być jednak niższa niż 15 000 zł. Przepis ust. 3a stosuje się odpowiednio z zastrzeżeniem, że za podstawę wymiaru kary pieniężnej przyjmuje się równowartość kwoty 250 000 euro.

5. Jeżeli podmiot kluczowy albo podmiot ważny narusza przepisy ustawy, powodując:

- 1) bezpośrednie i poważne cyberzagrożenie dla obronności, bezpieczeństwa państwa, bezpieczeństwa i porządku publicznego lub życia i zdrowia ludzi,
- 2) zagrożenie wywołania poważnej szkody majątkowej lub poważnych utrudnień w świadczeniu usług

– organ właściwy do spraw cyberbezpieczeństwa nakłada karę w wysokości do 100 000 000 zł.”;

83) po art. 73 dodaje się art. 73a–73c w brzmieniu:

„Art. 73a. 1. Karze pieniężnej może podlegać kierownik podmiotu kluczowego lub podmiotu ważnego, który:

- 1) nie wykonuje co najmniej jednego z obowiązków, o których mowa w art. 7b ust. 4, art. 7c ust. 1, art. 7c ust. 3 lub art. 7f ust. 3,

- 2) nie wykonuje co najmniej jednego z obowiązków, o których mowa w art. 8,
 - 3) nie wykonuje co najmniej jednego z obowiązków, o których mowa w art. 8d,
 - 4) nie wykonuje obowiązku, o którym mowa w art. 8e,
 - 5) nie wykonał obowiązku, o którym mowa w art. 8f ust. 2 lub 3,
 - 6) nie wyznaczył co najmniej dwóch osób do kontaktu z podmiotami kluczowymi lub podmiotami ważnymi, albo w przypadku kierowania mikro- lub małym przedsiębiorcą, o którym mowa w art. 2 ust. 1 załącznika I do rozporządzenia 651/2014/UE, co najmniej jednej osoby do kontaktu z podmiotami krajowego systemu cyberbezpieczeństwa,
 - 7) nie zapewnił użytkownikowi możliwości zgłoszenia cyberzagrożenia, incydentu lub podatności związanych ze świadczoną usługą,
 - 8) nie wykonuje co najmniej jednego z obowiązków, o których mowa w art. 10 ust. 1 i 6–8,
 - 9) nie wykonuje co najmniej jednego z obowiązków, o których mowa w art. 11,
 - 10) nie wykonuje co najmniej jednego z obowiązków, o których mowa w art. 12 ust. 5–8,
 - 11) przekazał sprawozdanie końcowe, o którym mowa w art. 11 ust. 1 pkt 4c, niezawierające elementów określonych w art. 12a,
 - 12) nie wykonuje obowiązku, o którym mowa w art. 12b,
 - 13) nie wykonuje obowiązku, o którym mowa w art. 14,
 - 14) nie wykonuje co najmniej jednego z obowiązków, o których mowa w art. 15
- jeżeli przemawia za tym czas, zakres lub charakter naruszenia.

2. Karze pieniężnej może podlegać także kierownik podmiotu kluczowego lub podmiotu ważnego, którego zaniechanie w realizacji obowiązków, o których mowa w ust. 1, miało charakter jednorazowy.

3. Niezależnie od kary pieniężnej, o której mowa w art. 73 ust. 1, karę pieniężną można nałożyć również na kierownika podmiotu kluczowego lub podmiotu ważnego za niedokonanie obowiązków wskazanych w tym przepisie.

4. Kara pieniężna, o której mowa w ust. 1–3, może być wymierzona w kwocie nie większej niż 300% otrzymywanego przez ukaranego wynagrodzenia obliczanego według zasad obowiązujących przy ustalaniu ekwiwalentu pieniężnego za urlop.

5. Kara pieniężna, o której mowa w ust. 1–3, może być wymierzona kierownikowi podmiotu kluczowego lub podmiotu ważnego będącym podmiotem publicznym w kwocie

nie większej niż 100% otrzymywanego przez ukaranego wynagrodzenia obliczanego według zasad obowiązujących przy ustalaniu ekwiwalentu pieniężnego za urlop. W przypadku gdy podmiot kluczowy lub podmiot ważny będące podmiotem publicznym są zobowiązane do stosowania ustawy również na podstawie innego sektora wskazanego w załączniku nr 1 lub 2 do ustawy, do kar pieniężnych wymierzanych kierownikom tych podmiotów stosuje się ust. 4.

Art. 73b. 1. Karze pieniężnej podlega:

- 1) podmiot świadczący usługi rejestracji nazw domen, który nie wykonuje obowiązków, o których mowa w art. 16b i art. 16c;
- 2) rejestr domen najwyższego poziomu (TLD), który nie wykonuje obowiązków, o których mowa w art. 16b i art. 16c;
- 3) producent lub dostawca, który nie przekazał dokumentacji badanego produktu ICT lub usługi ICT na wezwanie CSIRT MON, CSIRT NASK lub CSIRT GOV;
- 4) podmiot, który nie przekazał informacji, o których mowa w art. 43 ust. 1;
- 5) dostawca usług DNS, rejestr nazw domen najwyższego poziomu (TLD), podmiot świadczący usługi rejestracji nazw domen, dostawca chmury obliczeniowej, dostawca usług centrum przetwarzania danych, dostawca sieci dostarczania treści, dostawca usług zarządzanych, dostawca usług zarządzanych w zakresie cyberbezpieczeństwa, dostawca internetowej platformy handlowej, dostawca wyszukiwarki internetowej oraz dostawca platformy usług sieci społecznościowych świadczący usługi na terytorium Rzeczypospolitej Polskiej, który nie wyznaczył przedstawiciela zgodnie z art. 5a ust. 7.

2. Do wysokości kary pieniężnej, o której mowa w ust. 1 pkt 1 i 5, jeżeli dostawca usług DNS, rejestr nazw domen najwyższego poziomu (TLD), podmiot świadczący usługi rejestracji nazw domen, dostawca chmury obliczeniowej, dostawca usług centrum przetwarzania danych, dostawca sieci dostarczania treści, dostawca usług zarządzanych, dostawca usług zarządzanych w zakresie cyberbezpieczeństwa, dostawca internetowej platformy handlowej, dostawca wyszukiwarki internetowej oraz dostawca platformy usług sieci społecznościowych jest:

- 1) podmiotem kluczowym – stosuje się art. 73 ust. 3;
- 2) podmiotem ważnym – stosuje się art. 73 ust. 4.

3. Do wysokości kary pieniężnej, o której mowa w ust. 1 pkt 2, stosuje się art. 73 ust. 3.

4. Kara pieniężna, o której mowa w ust. 1 pkt 3 i 4, wynosi 50 000 zł.

Art. 73c. 1. Podmiot finansowy, który nie jest podmiotem kluczowym lub podmiotem ważnym oraz nie jest podmiotem określonym w art. 16 ust. 1 rozporządzenia 2022/2554, podlega karze pieniężnej, jeżeli:

- 1) nie wykonuje co najmniej jednego z obowiązków, o których mowa w art. 67c ust. 1, 2, 4 i 5;
- 2) nie wdrożył w terminie określonym w poleceniu zabezpieczającym, o którym mowa w art. 67g ust. 9 pkt 3, określonego zachowania, o którym mowa w art. 67g ust. 10;
- 3) odstąpił od wykonywania zawartego w poleceniu zabezpieczającym, o którym mowa w art. 67g ust. 9, określonego zachowania, o którym mowa w art. 67g ust. 10, przed wygaśnięciem polecenia zabezpieczającego.

2. Do wysokości kary pieniężnej, o której mowa w ust. 1, stosuje się art. 73 ust. 3.”;

84) art. 74 otrzymuje brzmienie:

„Art. 74. 1. Karę pieniężną, o której mowa w art. 73, art. 73a i art. 73b ust. 1 pkt 4, nakłada, w drodze decyzji, organ właściwy do spraw cyberbezpieczeństwa.

2. Karę pieniężną, o której mowa w art. 73b ust. 1 pkt 1–3, nakłada, w drodze decyzji, minister właściwy do spraw informatyzacji.

3. Karę pieniężną, o której mowa w art. 73c ust. 1, nakłada, w drodze decyzji, właściwy organ w rozumieniu rozporządzenia 2022/2554.

4. Organ właściwy do spraw cyberbezpieczeństwa lub właściwy organ w rozumieniu rozporządzenia 2022/2554 może decyzji, o której mowa w ust. 1 lub ust. 3, nadać rygor natychmiastowej wykonalności w całości albo w części, jeżeli wymaga tego ochrona bezpieczeństwa lub porządku publicznego.

5. Wpływy z tytułu kar pieniężnych, o których mowa w art. 73–73c, stanowią przychód Funduszu Cyberbezpieczeństwa, o którym mowa w art. 2 ustawy z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa.

6. Minister właściwy do spraw informatyzacji przekazuje Komisji Wspólnej Rządu i Samorządu Terytorialnego, do końca pierwszego kwartału danego roku, informację za rok poprzedni o wysokości wpływów z tytułu kar pieniężnych, nałożonych na samorządowe podmioty publiczne, stanowiących przychód Funduszu Cyberbezpieczeństwa, o którym mowa w art. 2 ustawy z dnia 2 grudnia 2021 r.

o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa.”;

85) uchyla się art. 75 i art. 76;

86) po art. 76 dodaje się art. 76a–76e w brzmieniu:

„Art. 76a. 1. Organ właściwy do spraw cyberbezpieczeństwa, podejmując decyzję o nałożeniu kary pieniężnej i ustalając jej wysokość, uwzględnia odpowiednio kryteria określone w art. 53 ust. 12 oraz wysokość przychodu uzyskanego z działalności gospodarczej w roku obrotowym poprzedzającym wymierzenie kary pieniężnej, możliwości finansowe podmiotu kluczowego lub podmiotu ważnego będącego podmiotem publicznym albo możliwości finansowe kierownika podmiotu kluczowego lub podmiotu ważnego. Przepisu art. 189a § 2 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego nie stosuje się.

2. W przypadku gdy podmiot kluczowy lub podmiot ważny powstał w wyniku połączenia lub przekształcenia innych podmiotów, obliczając wysokość jego przychodu organ właściwy do spraw cyberbezpieczeństwa uwzględnia przychód osiągnięty przez te podmioty w roku obrotowym poprzedzającym rok nałożenia kary pieniężnej. Przepisy art. 73 ust. 3–4 stosuje się odpowiednio.

3. W związku z toczącym się postępowaniem w sprawie nałożenia kary pieniężnej, podmiot, wobec którego wszczęto to postępowanie lub podmiot zatrudniający kierownika podmiotu kluczowego lub podmiotu ważnego jest obowiązany do dostarczenia organowi uprawnionemu do nałożenia kary pieniężnej na każde jego żądanie, w terminie wskazanym w wezwaniu, nie dłuższym niż 1 miesiąc od dnia otrzymania żądania, danych niezbędnych do określenia podstawy wymiaru kary pieniężnej.

4. W przypadku niedostarczenia danych lub dostarczenia danych uniemożliwiających ustalenie podstawy wymiaru kary pieniężnej, organ właściwy do spraw cyberbezpieczeństwa ustala podstawę wymiaru kary pieniężnej w sposób szacunkowy, uwzględniając w szczególności wielkość danego podmiotu kluczowego lub podmiotu ważnego, specyfikę działalności tego podmiotu lub ogólnodostępne dane finansowe.

5. Karę pieniężną uiszcza się w terminie 14 dni od dnia, w którym decyzja o jej wymierzeniu stała się ostateczna, lub od dnia doręczenia decyzji z rygorem natychmiastowej wykonalności, na rachunek bankowy organu właściwego do spraw cyberbezpieczeństwa, wskazany w decyzji o wymierzeniu kary pieniężnej.

6. Kary pieniężne nieuiszczone w terminie wraz z odsetkami podlegają ściągnięciu przez organ właściwy do spraw cyberbezpieczeństwa, który wymierzył karę pieniężną, w trybie określonym w przepisach o postępowaniu egzekucyjnym w administracji.

7. Organ właściwy do spraw cyberbezpieczeństwa przekazuje na rachunek Funduszu Cyberbezpieczeństwa środki pochodzące z kar pieniężnych w terminie 14 dni od dnia ich uiszczenia albo pobrania. W tym samym terminie przekazuje ministrowi właściwemu do spraw informatyzacji kopię decyzji o wymierzeniu kary pieniężnej lub innego dokumentu stanowiącego podstawę naliczenia, pobrania i przekazania na rachunek Funduszu Cyberbezpieczeństwa kary pieniężnej lub odsetek od nieterminowej wpłaty.

8. Organ właściwy do spraw cyberbezpieczeństwa w terminie 14 dni od dnia wystąpienia zdarzenia mogącego skutkować zmianą lub uchyleniem decyzji lub dokumentu stanowiącego podstawę do naliczenia, pobrania i przekazania na rachunek Funduszu Cyberbezpieczeństwa środków pochodzących z kar pieniężnych, informuje ministra właściwego do spraw informatyzacji o tym zdarzeniu, a w szczególności o wniesieniu skargi do sądu administracyjnego, skargi kasacyjnej, wydaniu prawomocnego wyroku, wszczęciu lub zakończeniu postępowania administracyjnego w zakresie wznowienia postępowania, uchylenia, zmiany lub stwierdzenia nieważności decyzji.

9. Organ właściwy do spraw cyberbezpieczeństwa może odstąpić od nałożenia kary pieniężnej, jeżeli waga naruszenia i znaczenie naruszonych przepisów są znikome, a podmiot albo kierownik podmiotu kluczowego lub podmiotu ważnego zaprzestał naruszania prawa lub naprawił wyrządzoną szkodę.

10. Do postępowania w sprawie nałożenia kar pieniężnych, o których mowa w art. 73b ust. 1 i art. 73c ust. 1, stosuje się odpowiednio ust. 1–9.

Art. 76b. 1. Niezależnie od kary pieniężnej nałożonej na podstawie art. 73 ust. 1, organ właściwy do spraw cyberbezpieczeństwa, w celu przymuszenia podmiotu kluczowego albo podmiotu ważnego do wykonania nałożonych na niego obowiązków, może nałożyć na ten podmiot, w drodze decyzji, okresową karę pieniężną w wysokości od 500 zł do 100 000 złotych za każdy dzień opóźnienia, w wykonaniu decyzji wydanych na podstawie art. 53 ust. 5 pkt 2–8.

2. Okresową karę pieniężną nakłada się, licząc od daty wskazanej w decyzji o nałożeniu tej kary.

3. Do okresowej kary pieniężnej stosuje się przepisy art. 74 ust. 4 i 5.

Art. 76c. 1. Jeżeli za czyn zagrożony karą określoną w art. 73 lub art. 73a została nałożona prawomocnie kara pieniężna przez Prezesa Urzędu Ochrony Danych Osobowych w związku z naruszeniem ochrony danych osobowych, organ właściwy do spraw cyberbezpieczeństwa nie wszczyna postępowania w sprawie nałożenia kary i poprzestaje na pouczeniu. Jeżeli zostało wszczęte postępowanie w sprawie nałożenia kary pieniężnej, stosuje się odpowiednio art. 189f ust. 1 pkt 2 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego.

2. W przypadku, o którym mowa w ust. 1, organ właściwy do spraw cyberbezpieczeństwa może stosować środki nadzoru określone w art. 53 ust. 4, 5 i 9.

Art. 76d. 1. W przypadku, o którym mowa w art. 73 ust. 1 pkt 3, kara pieniężna może być nakładana w sposób określony w art. 14 § 1b ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego.

2. Do postępowania w sprawie nałożenia kary pieniężnej stosuje się przepisy działu II rozdziału 14 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego, z wyjątkiem przepisów o milczącym załatwieniu sprawy.

Art. 76e. W zakresie nieuregulowanym w niniejszym rozdziale stosuje się odpowiednio przepisy działu IVa ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego.”;

- 87) w art. 83 wyrazy „Zagrożenia cyberbezpieczeństwa” zastępuje się wyrazem „Cyberzagrożenia”;
- 88) w art. 93 uchyla się ust. 8 i 23;
- 89) załączniki nr 1 i 2 otrzymują brzmienie określone odpowiednio w załącznikach nr 1 i 2 do niniejszej ustawy;
- 90) dodaje się załączniki nr 3 i 4.

Art. 2. W ustawie z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2025 r. poz. 1153) wprowadza się następujące zmiany:

- 1) w art. 10a:
 - a) po pkt 2 dodaje się pkt 2a w brzmieniu:
„2a) spółkom, o których mowa w art. 9 ust. 1 ustawy z dnia 20 grudnia 1996 r. o gospodarce komunalnej (Dz. U. z 2021 r. poz. 679),”;
 - b) pkt 3 otrzymuje brzmienie:
„3) innym zaliczanym do sektora finansów publicznych gminnym osobom prawnym utworzonym na podstawie odrębnych ustaw w celu wykonywania

zadań publicznych, z wyłączeniem przedsiębiorstw, instytutów badawczych i banków”;

- 2) w art. 10b ust. 1 otrzymuje brzmienie:

„1. Wspólną obsługę mogą prowadzić urząd gminy, inna jednostka organizacyjna gminy, jednostka organizacyjna związku międzygminnego, jednostka organizacyjna związku powiatowo-gminnego albo spółka, o której mowa w art. 9 ust. 1 ustawy z dnia 20 grudnia 1996 r. o gospodarce komunalnej, w tym spółka prawa handlowego powołana w celu prowadzenia wspólnej obsługi, zwane dalej „jednostkami obsługującymi”.”.

Art. 3. W ustawie z dnia 21 marca 1991 r. o obszarach morskich Rzeczypospolitej Polskiej i administracji morskiej (Dz. U. z 2024 r. poz. 1125 oraz z 2025 r. poz. 409) w art. 27d w ust. 2a wyrazy „o której mowa w załączniku nr 2 do ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2023 r. poz. 913 i 1703 oraz z 2024 r. poz. 834)” zastępuje się wyrazami „umożliwiającej dostęp do skalowalnego i elastycznego zbioru zasobów obliczeniowych do wspólnego wykorzystywania przez wielu użytkowników”.

Art. 4. W ustawie z dnia 24 sierpnia 1991 r. o Państwowej Straży Pożarnej (Dz. U. z 2025 r. poz. 1312 i 1366) wprowadza się następujące zmiany:

- 1) w art. 93 w ust. 1 w pkt 7 kropkę zastępuje się średnikiem i dodaje się pkt 8 w brzmieniu:
„8) świadczenie teleinformatyczne, o którym mowa w art. 5 ustawy z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1662 oraz z 2025 r. poz. 1017), zwane dalej „świadczeniem teleinformatycznym”.”;
- 2) po art. 97f dodaje się art. 97g w brzmieniu:

„Art. 97g. 1. Strażakowi wykonującemu zadania z zakresu cyberbezpieczeństwa, o których mowa w art. 26, art. 42 ust. 1, art. 44 ust. 1, art. 62 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077 i 1222 oraz z 2025 r. poz. 1017, 1069 i ...), lub w zakresie zapewnienia cyberbezpieczeństwa w Państwowej Straży Pożarnej przyznaje się na okres ich wykonywania świadczenie teleinformatyczne.

2. Do ustalenia wysokości świadczenia teleinformatycznego stosuje się przepisy wydane na podstawie art. 8 ust. 1 ustawy z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa.

3. Decyzję o przyznaniu świadczenia teleinformatycznego wydaje przełożony uprawniony do mianowania lub powołania nie później niż w terminie 30 dni po rozpoczęciu przez strażaka wykonywania zadań, o których mowa w ust. 1.

4. Przed wydaniem decyzji, o której mowa w ust. 3, strażak podlega opiniowaniu służbowemu na zasadach, o których mowa w art. 36a, jeżeli od dnia wydania ostatniej opinii o tym strażaku upłynęły co najmniej 3 miesiące.

5. Świadczenia teleinformatycznego nie przyznaje się w przypadkach, o których mowa w art. 97e ust. 6. Przepisy art. 97e ust. 7 i 8 stosuje się.

6. Świadczenia teleinformatycznego nie wypłaca się w przypadkach, o których mowa w art. 97e ust. 9.

7. Do wypłaty świadczenia teleinformatycznego stosuje się przepisy art. 97e ust. 10–12.”.

Art. 5. W ustawie z dnia 20 sierpnia 1997 r. o Krajowym Rejestrze Sądowym (Dz. U. z 2025 r. poz. 869) wprowadza się następujące zmiany:

1) w art. 4d:

a) w ust. 2 w pkt 3 kropkę zastępuje się średnikiem i dodaje się pkt 4 w brzmieniu:

„4) w wykazach prowadzonych przez organy właściwe do spraw cyberbezpieczeństwa na podstawie art. 42 ust. 11 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077 i 1222 oraz z 2005 r. poz. 1017, 1069 i ...).”.

b) w ust. 5 w pkt 4 dodaje się przecinek i dodaje się pkt 5 w brzmieniu:

„5) w art. 53 ust. 9 pkt 6 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa”;

2) w art. 21 dodaje się ust. 4 w brzmieniu:

„4. Minister Sprawiedliwości, na podstawie wykazu, o którym mowa w art. 42 ust. 12 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, przekazuje sądowi rejestrowemu, za pośrednictwem systemu teleinformatycznego, po otrzymaniu żądania z tego systemu, informacje o osobach objętych zakazem pełnienia w podmiocie kluczowym funkcji zarządczych na podstawie decyzji organów właściwych do spraw cyberbezpieczeństwa.”.

Art. 6. W ustawie z dnia 29 sierpnia 1997 r. – Ordynacja podatkowa (Dz. U. z 2025 r. poz. 111, z późn. zm.¹⁶⁾) po art. 299h dodaje się art. 299i w brzmieniu:

„Art. 299i. § 1. Szef Krajowej Administracji Skarbowej udostępnia nieodpłatnie organom właściwym do spraw cyberbezpieczeństwa oraz Zespołowi Reagowania na Incydynty Bezpieczeństwa Komputerowego działającemu na poziomie krajowym, prowadzonemu przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy nieodpłatnie, w drodze teletransmisji, bez konieczności składania każdorazowo pisemnych wniosków o udostępnienie, dane w zakresie niezbędnym do dokonania przez te podmioty weryfikacji wielkości przedsiębiorstwa zgodnie z art. 5 ust. 1 i 2 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077 i 1222 oraz z 2025 r. poz. 1017, 1069 i ...).

§ 2. Dane, o których mowa w § 1, obejmują roczne zatrudnienie, a także roczny obrót netto ze sprzedaży towarów, wyrobów i usług oraz z operacji finansowych.

§ 3. Sposób udostępniania danych, o których mowa w § 1, określają porozumienia zawarte między Szefem Krajowej Administracji Skarbowej a podmiotami, o których mowa w § 1.”.

Art. 7. W ustawie z dnia 5 czerwca 1998 r. o samorządzie województwa (Dz. U. z 2025 r. poz. 581) wprowadza się następujące zmiany:

1) w art. 8c:

a) po pkt 2 dodaje się pkt 2a w brzmieniu:

„2a) spółkom, o których mowa w art. 9 ust. 1 ustawy z dnia 20 grudnia 1996 r. o gospodarce komunalnej (Dz. U. z 2021 r. poz. 679),”,

b) pkt 3 otrzymuje brzmienie:

„3) innym zaliczanym do sektora finansów publicznych wojewódzkim osobom prawnym utworzonym na podstawie odrębnych ustaw w celu wykonywania zadań publicznych, z wyłączeniem przedsiębiorstw, instytutów badawczych i banków”;

2) w art. 8d ust. 1 otrzymuje brzmienie:

„1. Wspólną obsługę mogą prowadzić urząd marszałkowski, inna wojewódzka samorządowa jednostka organizacyjna albo spółka, o której mowa w art. 9 ust. 1 ustawy z dnia 20 grudnia 1996 r. o gospodarce komunalnej, w tym spółka prawa handlowego

¹⁶⁾ Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2025 r. poz. 497, 621, 622, 769, 820, 1203 i 1235.

powołana w celu prowadzenia wspólnej obsługi, zwane dalej „jednostkami obsługującymi”.”.

Art. 8. W ustawie z dnia 5 czerwca 1998 r. o samorządzie powiatowym (Dz. U. z 2024 r. poz. 107 i 1907) wprowadza się następujące zmiany:

1) w art. 6a:

a) po pkt 2 dodaje się pkt 2a w brzmieniu:

„2a) spółkom, o których mowa w art. 9 ust. 1 ustawy z dnia 20 grudnia 1996 r. o gospodarce komunalnej (Dz. U. z 2021 r. poz. 679),”

b) pkt 3 otrzymuje brzmienie:

„3) innym zaliczanym do sektora finansów publicznych powiatowym osobom prawnym utworzonym na podstawie odrębnych ustaw w celu wykonywania zadań publicznych, z wyłączeniem przedsiębiorstw, instytutów badawczych i banków”;

2) w art. 6b ust. 1 otrzymuje brzmienie:

„1. Wspólną obsługę mogą prowadzić starostwo powiatowe, inna jednostka organizacyjna powiatu, jednostka organizacyjna związku powiatów, jednostka organizacyjna związku powiatowo-gminnego albo spółka, o której mowa w art. 9 ust. 1 ustawy o gospodarce komunalnej, w tym spółka prawa handlowego powołana w celu prowadzenia wspólnej obsługi, zwane dalej „jednostkami obsługującymi”.”.

Art. 9. W ustawie z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych (Dz. U. z 2025 r. poz. 350, z późn. zm.¹⁷⁾) w art. 50 dodaje się ust. 28 w brzmieniu:

„28. Zakład udostępnia organom właściwym do spraw cyberbezpieczeństwa i Zespołowi Reagowania na Incydenty Bezpieczeństwa Komputerowego działającemu na poziomie krajowym, prowadzonemu przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy, drogą elektroniczną, dane obejmujące roczną liczbę ubezpieczonych, którzy zostali zgłoszeni przez płatnika, w zakresie niezbędnym do realizacji ich ustawowych zadań. Dane, o których mowa w zdaniu pierwszym, obejmują ubezpieczonych zgłoszonych przez płatnika do Zakładu od dnia 1 stycznia do dnia 31 grudnia danego roku. Udostępnienie informacji następuje nieodpłatnie.”.

¹⁷⁾ Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2025 r. poz. 620, 622, 769, 820, 1083, 1160 i 1216.

Art. 10. W ustawie z dnia 24 maja 2000 r. o Krajowym Rejestrze Karnym (Dz. U. z 2024 r. poz. 276 oraz z 2025 r. poz. 1235) w art. 6 w ust. 1 po pkt 10a dodaje się pkt 10b w brzmieniu:

„10b) podmiotom kluczowym lub podmiotom ważnym w rozumieniu art. 5 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077, 1222 oraz z 2025 r. poz. 1017, 1069 i...) w zakresie niezbędnym do weryfikacji niekaralności osoby realizującej zadania, o których mowa w art. 8 i art. 11 tej ustawy;”.

Art. 11. W ustawie z dnia 21 grudnia 2000 r. o dozorze technicznym (Dz. U. z 2024 r. poz. 1194) w art. 37 w pkt 21 kropkę zastępuje się średnikiem i dodaje się pkt 22 w brzmieniu:

„22) wykonywanie zadań określonych w przepisach ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077 i 1222 oraz z 2025 r. poz. 1017, 1069 i ...), w szczególności w zakresie zadań powierzonych przez organ właściwy do spraw cyberbezpieczeństwa w ramach zadań CSIRT sektorowego.”.

Art. 12. W ustawie z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (Dz. U. z 2025 r. poz. 504) po art. 12 dodaje się art. 12a w brzmieniu:

„Art. 12a. W celu zabezpieczenia realizacji przewidzianych w art. 26 ust. 1a i ust. 3, art. 41 pkt 6 i 9, art. 41a ust. 2, art. 44, art. 51, art. 52, art. 52f ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077 i 1222 oraz z 2025 r. poz. 1017, 1069 i ...) zadań CSIRT MON oraz zadań Ministra Obrony Narodowej, Minister Obrony Narodowej, w drodze decyzji niepodlegającej ogłoszeniu, wydzieli z Dowództwa Komponentu Wojsk Obrony Cyberprzestrzeni oraz z jednostek podporządkowanych Dowódcy Komponentu Wojsk Obrony Cyberprzestrzeni zespoły specjalistów oraz zasoby materiałowe i sprzętowe, które będą podlegać Ministrowi Obrony Narodowej w przypadku mianowania Naczelnego Dowódcy Sił Zbrojnych i przejęcia przez niego dowodzenia Siłami Zbrojnymi.”.

Art. 13. W ustawie z dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym (Dz. U. z 2025 r. poz. 640 i 1069) wprowadza się następujące zmiany:

1) w art. 18zg:

a) w ust. 2 pkt 1 i 2 otrzymują brzmienie:

- „1) podmiotu finansowego będącego podmiotem kluczowym,
- 2) podmiotu finansowego będącego podmiotem ważnym
– w rozumieniu art. 5 ust. 1 i 2 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.”,
- b) w ust. 3 wyrazy „, o którym mowa w ust. 4 i 5” zastępuje się wyrazami „kluczowym lub podmiotem ważnym”,
- c) uchyla się ust. 4 i 5;
- 2) w art. 19 ust. 6 otrzymuje brzmienie:
„6. Z przychodów, o których mowa w ust. 2, pokrywa się koszty funkcjonowania Urzędu Komisji i jego organów oraz koszty realizacji zadań Komisji wynikających z ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.”.

Art. 14. W ustawie z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz. U. z 2025 r. poz. 302 i 779) w art. 19 ust. 16 otrzymuje brzmienie:

„16. Podmiot prowadzący rejestr medyczny określony w przepisach wydanych na podstawie art. 20 ust. 1 opracowuje, wdraża, nadzoruje, utrzymuje oraz w uzasadnionych przypadkach modyfikuje system zarządzania bezpieczeństwem informacji, zgodnie z wymogami określonymi w art. 8 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077 i 1222 oraz z 2025 r. poz. 1017, 1069 i ...).”.

Art. 15. W ustawie z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. z 2024 r. poz. 1725) wprowadza się następujące zmiany:

- 1) w art. 4 po ust. 5 dodaje się ust. 5a i 5b w brzmieniu:
„5a. Do wniosku o wpis, o którym mowa w ust. 1, dołącza się dane i informacje, o których mowa w art. 7 ust. 3 pkt 1–17 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077 i 1222 oraz z 2025 r. poz. 1017, 1069 i ...).
5b. Po wpisie do rejestru, minister właściwy do spraw informatyzacji dane i informacje, o których mowa w art. 7 ust. 3 pkt 1–17 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, wpisuje do wykazu podmiotów kluczowych i podmiotów ważnych, o którym mowa w art. 7 ust. 1 tej ustawy. Danych tych nie zamieszcza się w rejestrze.”;
- 2) w art. 15 w ust. 2 skreśla się wyrazy „oraz informacje o zdarzeniach powodujących naruszenia bezpieczeństwa lub utratę integralności, o których mowa w art. 20a ust. 2”;

- 3) uchyla się art. 20a;
- 4) w art. 21b w ust. 1 pkt 3 otrzymuje brzmienie:
„3) zapewnieniu przez podmiot odpowiedzialny za ten system wdrożenia systemu zarządzania bezpieczeństwem informacji zgodnego z wymogami określonymi w art. 8 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;”;
- 5) w art. 21t w ust. 1 pkt 1 otrzymuje brzmienie:
„1) zapewnieniu przez podmiot odpowiedzialny za ten system wdrożenia systemu zarządzania bezpieczeństwem informacji zgodnego z wymogami określonymi w art. 8 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;”;
- 6) w art. 21u w ust. 3 pkt 1 otrzymuje brzmienie:
„1) oświadczenie o zapewnieniu przez podmiot odpowiedzialny za ten system wdrożenia systemu zarządzania bezpieczeństwem informacji zgodnego z wymogami określonymi w art. 8 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;”;
- 7) uchyla się art. 30a;
- 8) uchyla się art. 39;
- 9) w art. 46 uchyla się pkt 8.

Art. 16. W ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781) art. 104 otrzymuje brzmienie:

„Art. 104. 1. Środki z administracyjnej kary pieniężnej stanowią dochód budżetu państwa, z uwzględnieniem ust. 2.

2. Środki z administracyjnej kary pieniężnej nałożonej za naruszenie art. 5 ust. 1 lit. f, art. 25 ust. 1 i 2, art. 28 ust. 3 lit. c oraz art. 32 ust. 1 i 2 rozporządzenia 2016/679 stanowią w 50% dochód budżetu państwa, a w 50% dochód Funduszu Cyberbezpieczeństwa, o którym mowa w art. 2 ustawy z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1662 oraz z 2025 r. poz. 1017).”.

Art. 17. W ustawie z dnia 11 września 2019 r. – Prawo zamówień publicznych (Dz. U. z 2024 r. poz. 1320, z późn. zm.¹⁸⁾) w art. 226 w ust. 1:

1) pkt 17 otrzymuje brzmienie:

„17) obejmuje ona produkt ICT, usługę ICT lub proces ICT wskazane w rekomendacji, o której mowa w art. 33 ust. 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077 i 1222 oraz z 2025 r. poz. 1017, 1069 i ...), stwierdzającej ich negatywny wpływ na podstawowy interes bezpieczeństwa państwa;”;

2) w pkt 18 kropkę zastępuje się średnikiem i dodaje się pkt 19 w brzmieniu:

„19) obejmuje ona produkt ICT, którego typ został określony w decyzji w sprawie uznania dostawcy za dostawcę wysokiego ryzyka, o której mowa w art. 67b ust. 15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, lub usługę ICT, lub proces ICT, określone w tej decyzji.”.

Art. 18. W ustawie z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1662 oraz z 2025 r. poz. 1017) wprowadza się następujące zmiany:

1) w art. 2:

a) w ust. 4:

– pkt 1 otrzymuje brzmienie:

„1) wpływy z kar pieniężnych, o których mowa w art. 73–73c ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077 i 1222 oraz z 2025 r. poz. 1017, 1069 i ...);”;

– po pkt 1a dodaje się pkt 1b w brzmieniu:

„1b) wpływy z kar pieniężnych, o których mowa w art. 101 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781 oraz z 2025 r. poz. ...);”;

b) w ust. 9 po wyrazie „Funduszu” dodaje się wyrazy „na wypłatę świadczenia teleinformatycznego”;

2) w art. 3 w ust. 1 wprowadzenie do wyliczenia otrzymuje brzmienie:

¹⁸⁾ Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2025 r. poz. 620, 769, 794, 1165, 1173 i 1235.

„Warunkiem ubiegania się o wsparcie ze środków Funduszu na wypłatę świadczenia teleinformatycznego jest złożenie przez podmiot, o którym mowa w art. 5, wniosku do ministra właściwego do spraw informatyzacji, zawierającego:”;

- 3) w art. 4 w ust. 1 po wyrazie „wniosek” dodaje się wyrazy „, o którym mowa w art. 3 ust. 1,”;
- 4) w art. 5:
 - a) pkt 1 otrzymuje brzmienie:

„1) w CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT sektorowych, organach właściwych do spraw cyberbezpieczeństwa lub w urzędzie obsługującym Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa, o których mowa odpowiednio w art. 26, art. 41, art. 44 lub art. 60 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;”;
 - b) w pkt 2 w lit. n dodaje się przecinek i dodaje się lit. o–zg w brzmieniu:

„o) Generalnej Dyrekcji Dróg Krajowych i Autostrad,
p) Głównym Inspektoracie Transportu Drogowego,
q) Instytucie Badawczym Dróg i Mostów w Warszawie,
r) Instytucie Kolejnictwa w Warszawie,
s) Instytucie Meteorologii i Gospodarki Wodnej – Państwowego Instytutu Badawczego,
t) Instytucie Transportu Samochodowego w Warszawie,
u) jednostkach organizacyjnych Krajowej Administracji Skarbowej, o których mowa w art. 36 ust. 1 pkt 3 i 5 ustawy z dnia 16 listopada 2016 r. o Krajowej Administracji Skarbowej (Dz. U. z 2025 r. poz. 1131),
v) Państwowej Straży Pożarnej,
w) Państwowym Gospodarstwie Wodnym Wody Polskie,
x) sądach powszechnych,
y) Transportowym Dozorze Technicznym,
z) Urzędzie do spraw Cudzoziemców,
za) Urzędzie Lotnictwa Cywilnego,
zb) Urzędzie Morskim w Gdyni,
zc) Urzędzie Morskim w Szczecinie,
zd) Urzędzie Ochrony Danych Osobowych,
ze) Urzędzie Żeglugi Śródlądowej w Bydgoszczy,

- zf) Urzędzie Żeglugi Śródlądowej w Szczecinie,
- zg) Urzędzie Żeglugi Śródlądowej we Wrocławiu.”;

5) po art. 26a dodaje się art. 26b w brzmieniu:

„Art. 26b. Świadczenie teleinformatyczne żołnierzom zawodowym realizującym zadania z zakresu cyberbezpieczeństwa w urzędzie obsługującym Ministra Obrony Narodowej przyznaje i cofa Minister Obrony Narodowej.”;

6) w art. 27 w ust. 1 pkt 5–10 otrzymują brzmienie:

- „5) w 2026 r. – 351,922 mln zł;
- 6) w 2027 r. – 351,935 mln zł;
- 7) w 2028 r. – 351,964 mln zł;
- 8) w 2029 r. – 351,996 mln zł;
- 9) w 2030 r. – 352,030 mln zł;
- 10) w 2031 r. – 352,067 mln zł.”.

Art. 19. W ustawie z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej (Dz. U. z 2024 r. poz. 1803) w art. 2 pkt 11 otrzymuje brzmienie:

„11) podmiot publiczny – podmiot wskazany w sektorze podmiotów publicznych w załącznikach nr 1 i 2 do ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;”.

Art. 20. W ustawie z dnia 12 lipca 2024 r. – Prawo komunikacji elektronicznej (Dz. U. poz. 1221 oraz z 2025 r. poz. 637 i 820) w art. 40 w ust. 1 w pkt 2 w lit. b wyrazy „operatorów usług” zastępuje się wyrazem „podmiotów”.

Art. 21. W ustawie z dnia 12 lipca 2024 r. – Przepisy wprowadzające ustawę – Prawo komunikacji elektronicznej (Dz. U. poz. 1222) w art. 68 uchyla się ust. 3.

Art. 22. 1. Operatorzy usług kluczowych, o których mowa w ustawie zmienianej w art. 1, stają się podmiotami kluczowymi, z dniem wejścia w życie niniejszej ustawy.

2. Do operatorów usług kluczowych, o których mowa w ust. 1, będących podmiotami podległymi lub nadzorowanymi przez Ministra Obrony Narodowej nie stosuje się art. 5 ust. 10 i 11 ustawy zmienianej w art. 1 w brzmieniu nadanym niniejszą ustawą.

Art. 23. Do obsługi incydentu, o której mowa w art. 11 pkt 1 ustawy zmienianej w art. 1, rozpoczętej i niezakończonej przed dniem wejścia w życie niniejszej ustawy, stosuje się przepisy dotychczasowe.

Art. 24. 1. Do audytu, o którym mowa w art. 15 ust. 1 ustawy zmienianej w art. 1, przeprowadzanego i niezakończonego przed dniem wejścia w życie niniejszej ustawy stosuje się przepisy dotychczasowe.

2. Do praktyki audytorów w zakresie audytu bezpieczeństwa systemów informacyjnych, o której mowa w art. 15 ust. 2 pkt 2 lit. b i c ustawy zmienianej w art. 1 w brzmieniu nadanym niniejszą ustawą, zalicza się:

- 1) udokumentowane wykonanie w ciągu ostatnich 3 lat przed dniem rozpoczęcia audytu 3 audytów w zakresie bezpieczeństwa systemów informacyjnych lub ciągłości działania albo
- 2) wykonywanie audytów bezpieczeństwa systemów informacyjnych lub ciągłości działania w wymiarze czasu pracy nie mniejszym niż 1/2 etatu, związanych z przeprowadzaniem audytu wewnętrznego w zakresie bezpieczeństwa informacji, o którym mowa w przepisach wydanych na podstawie art. 18 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2024 r. poz. 1557 i 1717 oraz z 2025 r. poz. 1006, 1019, 1158 i 1301) w brzmieniu przed dniem wejścia w życie niniejszej ustawy.

Art. 25. Do operatorów usług kluczowych, którzy wykonali audyt, o którym mowa w art. 15 ust. 1 ustawy zmienianej w art. 1, nie stosuje się art. 16 pkt 2 ustawy zmienianej w art. 1 w brzmieniu nadanym niniejszą ustawą.

Art. 26. Do badania urządzenia informatycznego lub oprogramowania, o którym mowa w art. 33 ust. 1 ustawy zmienianej w art. 1, przeprowadzanego i niezakończonego przed dniem wejścia w życie niniejszej ustawy, stosuje się przepisy art. 33 ustawy zmienianej w art. 1 w brzmieniu nadanym niniejszą ustawą.

Art. 27. 1. Rekomendacje Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa, o których mowa w art. 33 ust. 4 ustawy zmienianej w art. 1, wydane przed dniem wejścia w życie niniejszej ustawy zachowują moc.

2. Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa opublikuje dotychczas wydane rekomendacje na swojej stronie podmiotowej Biuletynu Informacji Publicznej w terminie miesiąca od dnia wejścia w życie niniejszej ustawy.

3. Do rekomendacji Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa, o których mowa w art. 33 ust. 4 ustawy zmienianej w art. 1, wydanych przed dniem wejścia w życie niniejszej ustawy stosuje się przepisy dotychczasowe.

Art. 28. Do kontroli operatorów usług kluczowych i dostawców usług cyfrowych prowadzonych na podstawie art. 42 ust. 1 pkt 8 ustawy zmienianej w art. 1 w brzmieniu dotychczasowym wszczętych i niezakończonych przed dniem wejścia w życie niniejszej ustawy stosuje się przepisy dotychczasowe.

Art. 29. Do postępowań administracyjnych w sprawie nałożenia kary pieniężnej, o której mowa w art. 73 ustawy zmienianej w art. 1, na operatora usługi kluczowej, dostawcę usługi cyfrowej albo kierownika operatora usługi kluczowej wszczętych i niezakończonych przed dniem wejścia w życie niniejszej ustawy stosuje się przepisy dotychczasowe.

Art. 30. Do postępowań o udzielenie zamówienia publicznego wszczętych i niezakończonych przed dniem wejścia w życie niniejszej ustawy stosuje się przepis art. 226 ust. 1 pkt 17 ustawy zmienianej w art. 17 w brzmieniu nadanym niniejszą ustawą.

Art. 31. Sprawy związane z przeprowadzeniem postępowania konkursowego dotyczącego udzielenia pomocy *de minimis* wszczęte i niezakończone na podstawie art. 45a ustawy zmienianej w art. 1 w brzmieniu dotychczasowym są kontynuowane na podstawie przepisów dotychczasowych do czasu rozliczenia udzielonej pomocy *de minimis*.

Art. 32. Dotychczasowe przepisy wykonawcze wydane na podstawie:

- 1) art. 11 ust. 4 ustawy zmienianej w art. 1, zachowują moc do dnia wejścia w życie przepisów wykonawczych wydanych na podstawie art. 11 ust. 4 ustawy zmienianej w art. 1,
- 2) art. 66 ust. 9 ustawy zmienianej w art. 1, zachowują moc do dnia wejścia w życie przepisów wykonawczych wydanych na podstawie art. 66 ust. 9 ustawy zmienianej w art. 1

– jednak nie dłużej niż przez 12 miesięcy od dnia wejścia w życie niniejszej ustawy oraz mogą być zmieniane na podstawie tych przepisów.

Art. 33. 1. Podmioty, które z dniem wejścia w życie niniejszej ustawy spełniają przesłanki uznania ich za podmiot kluczowy albo za podmiot ważny, realizują obowiązki określone w rozdziale 3 ustawy zmienianej w art. 1, w brzmieniu nadanym niniejszą ustawą, w terminie 6 miesięcy od dnia wejścia w życie niniejszej ustawy.

2. Podmioty, które z dniem wejścia w życie niniejszej ustawy spełniają przesłanki uznania ich za podmiot kluczowy przeprowadzają pierwszy audyt, o którym mowa w art. 15 ust. 1 ustawy zmienianej w art. 1, w brzmieniu nadanym niniejszą ustawą, w terminie 24 miesięcy od dnia wejścia w życie niniejszej ustawy.

3. Podmioty, które z dniem wejścia w życie niniejszej ustawy spełniają przesłanki uznania ich za podmiot kluczowy albo za podmiot ważny, są obowiązane zarejestrować się w wykazie podmiotów kluczowych i podmiotów ważnych zgodnie z harmonogramem określonym w art. 34 ust. 3 pkt 1 niniejszej ustawy.

4. Podmioty kluczowe lub podmioty ważne, które przed dniem wejścia w życie ustawy były operatorami usług kluczowych zgłaszają incydenty poważne zgodnie z art. 11–12b ustawy zmienianej w art. 1 w brzmieniu nadanym niniejszą ustawą w terminie 6 miesięcy od dnia wejścia w życie niniejszej ustawy.

5. Przedsiębiorcy telekomunikacyjni, którzy przed dniem wejścia w życie niniejszej ustawy realizowali obowiązki określone w dziale VIIa ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2024 r. poz. 34, 731 i 834), realizują te obowiązki na podstawie dotychczasowych przepisów do czasu rozpoczęcia realizacji obowiązków określonych w rozdziale 3 ustawy zmienianej w art. 1 w brzmieniu nadanym niniejszą ustawą.

6. Podmioty kluczowe lub podmioty ważne, które przed dniem wejścia w życie niniejszej ustawy były operatorami usług kluczowych do czasu wdrożenia systemu zarządzania bezpieczeństwem informacji zgodnego z art. 8 ustawy zmienianej w art. 1 w brzmieniu nadanym niniejszą ustawą, stosują system zarządzania bezpieczeństwem informacji zgodny z art. 8 ustawy zmienianej w art. 1 w brzmieniu dotychczasowym.

Art. 34. 1. Minister właściwy do spraw informatyzacji utworzy wykaz podmiotów kluczowych i podmiotów ważnych, w terminie miesiąca od dnia wejścia w życie niniejszej ustawy.

2. Minister właściwy do spraw informatyzacji wpisuje, z urzędu, do wykazu podmiotów kluczowych i podmiotów ważnych operatorów usług kluczowych wpisanych przed dniem wejścia w życie niniejszej ustawy do wykazu operatorów usług kluczowych. Przepis art. 7b ustawy zmienianej w art. 1 dodany niniejszą ustawą stosuje się odpowiednio.

3. Minister właściwy do spraw informatyzacji ogłasza w swoim dzienniku urzędowym komunikat określający harmonogram:

- 1) złożenia wniosków o wpis do wykazu podmiotów kluczowych i podmiotów ważnych przez podmioty kluczowe lub podmioty ważne, które w dniu wejścia w życie niniejszej ustawy spełniają przesłanki uznania ich za podmiot kluczowy albo podmiot ważny;
- 2) rozpoczęcia korzystania przez podmioty, o których mowa w pkt 1, z systemu teleinformatycznego, o którym mowa w art. 46 ust. 1 ustawy zmienianej w art. 1, w brzmieniu nadanym niniejszą ustawą.

4. W harmonogramie, o którym mowa w ust. 3, wskazuje się terminy dokonywania czynności przez poszczególne rodzaje podmiotów kluczowych lub podmiotów ważnych.

5. Komunikat, o którym mowa w ust. 3, może być zmieniany, jeżeli z powodów technicznych lub organizacyjnych niemożliwe jest dokonanie wpisów i rozpoczęcie korzystania z systemu teleinformatycznego, o którym mowa w art. 46 ust. 1, ustawy zmienianej w art. 1 przez podmioty kluczowe lub podmioty ważne w wyznaczonym harmonogramie.

Art. 35. Minister właściwy do spraw informatyzacji uruchomi funkcjonalności systemu teleinformatycznego, o których mowa w art. 46 ust. 1 pkt 6 i 7 ustawy zmienianej w art. 1, w brzmieniu nadanym niniejszą ustawą, w terminie roku od dnia wejścia w życie niniejszej ustawy.

Art. 36. Rejestr domen najwyższego poziomu (TLD) oraz podmiot świadczący usługi rejestracji nazw domen:

- 1) dostosowuje bazy danych dotyczących rejestracji nazw domen do wymagań określonych w art. 16b ustawy zmienianej w art. 1 dodany niniejszą ustawą, w terminie 6 miesięcy od dnia wejścia w życie niniejszej ustawy;
- 2) opracowuje i wdraża polityki i procedury, o których mowa w art. 16b ustawy zmienianej w art. 1 dodany niniejszą ustawą, w terminie 6 miesięcy od dnia wejścia w życie niniejszej ustawy.

Art. 37. Minister właściwy do spraw informatyzacji, w terminie 3 miesięcy od dnia wejścia w życie ustawy, przekaze:

- 1) Komisji Europejskiej informacje o:
 - a) liczbie podmiotów kluczowych, w podziale na poszczególne sektory,
 - b) liczbie podmiotów ważnych, w podziale na poszczególne sektory,
 - c) rodzajach usług świadczonych przez podmioty kluczowe lub podmioty ważne,
 - d) przepisach, na podstawie których podmioty kluczowe lub ważne zostały wskazane;
- 2) Grupie Współpracy informacje o:
 - a) liczbie podmiotów kluczowych, w podziale na poszczególne sektory,
 - b) liczbie podmiotów ważnych, w podziale na poszczególne sektory.

Art. 38. Minister właściwy do spraw informatyzacji, w terminie 3 miesięcy od dnia wejścia w życie ustawy, przekaze Komisji Europejskiej informacje o wyznaczeniu organu do spraw zarządzania kryzysowego w cyberbezpieczeństwie wraz z jego danymi identyfikacyjnymi.

Art. 39. 1. Postanowienia umów obowiązujących w dniu wejścia w życie niniejszej ustawy, uniemożliwiające przeprowadzenie badania, o którym mowa w art. 33 ust. 1b–1d ustawy zmienianej w art. 1 dodany niniejszą ustawą, są nieważne.

2. Porozumienia w sprawie korzystania z systemu teleinformatycznego, o którym mowa w art. 46 ust. 1 ustawy zmienianej w art. 1 w brzmieniu dotychczasowym, zawarte przed dniem wejścia w życie niniejszej ustawy, zachowują ważność do czasu ich wypowiedzenia.

3. Podmiot kluczowy lub podmiot ważny będący stroną porozumienia w sprawie korzystania z systemu teleinformatycznego, o którym mowa w art. 46 ust. 1 ustawy zmienianej w art. 1 w brzmieniu dotychczasowym, może uwierzytelnić się w tym systemie za pomocą:

- 1) czynnika uwierzytelniania, o którym mowa w pkt 1 ppkt 2 lit. a załącznika do rozporządzenia wykonawczego Komisji (UE) nr 2015/1502 z dnia 8 września 2015 r. w sprawie ustanowienia minimalnych specyfikacji technicznych i procedur dotyczących poziomów bezpieczeństwa w zakresie środków identyfikacji elektronicznej na podstawie art. 8 ust. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (Dz. Urz. UE L 235 z 09.09.2015, str. 7, z późn. zm.¹⁹⁾), zwanego dalej „rozporządzeniem 2015/1502”, którym jest urządzenie wydane podmiotowi kluczowemu lub podmiotowi ważnemu przez ministra właściwego do spraw informatyzacji przed wejściem w życie niniejszej ustawy, oraz
- 2) czynnika uwierzytelniania, o którym mowa w pkt 1 ppkt 2 lit. b załącznika do rozporządzenia 2015/1502, którym jest login oraz hasło.

Art. 40. CSIRT MON, CSIRT NASK lub CSIRT GOV dostosują w terminie 3 miesięcy od dnia wejścia w życie niniejszej ustawy porozumienia, o których mowa w art. 26 ust. 10 ustawy zmienianej w art. 1 w brzmieniu dotychczasowym, do przepisów art. 26 ustawy zmienianej w art. 1 w brzmieniu nadanym niniejszą ustawą.

Art. 41. 1. Organ właściwy do spraw cyberbezpieczeństwa ustanawia CSIRT sektorowy w terminie 18 miesięcy od dnia wejścia w życie niniejszej ustawy.

2. Organ właściwy do spraw cyberbezpieczeństwa ogłasza komunikat o osiągnięciu przez CSIRT sektorowy zdolności operacyjnej w swoim dzienniku urzędowym.

¹⁹⁾ Zmiany wymienionego rozporządzenia zostały ogłoszone w Dz. Urz. UE L 345 z 20.12.2016, str. 142 oraz Dz. Urz. UE L 165 z 21.06.2022, str. 40.

3. Informacja o osiągnięciu zdolności operacyjnej przez CSIRT sektorowy jest również publikowana na stronach internetowych:

- 1) ministerstwa albo innego urzędu administracji rządowej, obsługującego Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa,
- 2) CSIRT MON, CSIRT NASK, CSIRT GOV

– a także jest przekazywana za pomocą systemu teleinformatycznego, o którym mowa w art. 46 ust. 1 ustawy zmienianej w art. 1 w brzmieniu nadanym niniejszą ustawą.

Art. 42. 1. Do dnia wydania komunikatu, o którym mowa w art. 41 ust. 2 niniejszej ustawy, przez organ właściwy do spraw cyberbezpieczeństwa, o osiągnięciu przez właściwy CSIRT sektorowy zdolności operacyjnej, podmioty kluczowe lub podmioty ważne zgłaszają incydenty poważne zgodnie z art. 11–12b ustawy zmienianej w art. 1 w brzmieniu nadanym niniejszą ustawą do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV.

2. Podmiot kluczowy lub podmiot ważny zgłaszają incydenty poważne zgodnie z art. 11–12b ustawy zmienianej w art. 1 w brzmieniu nadanym niniejszą ustawą do CSIRT sektorowego od dnia następującego po dniu opublikowania komunikatu o osiągnięciu przez właściwy CSIRT sektorowy zdolności operacyjnej.

3. Przepisów ust. 1 i 2 nie stosuje się w przypadku, gdy sektorowy zespół cyberbezpieczeństwa dla danego sektora został powołany przed 2025 r.

Art. 43. W sprawozdaniu organu właściwego do spraw cyberbezpieczeństwa, o którym mowa w art. 44f ustawy zmienianej w art. 1 w brzmieniu nadanym niniejszą ustawą, które jest sporządzane za rok, w którym został utworzony CSIRT sektorowy, zawiera się informacje dotyczące utworzenia CSIRT sektorowego oraz jego funkcjonowania.

Art. 44. Sektorowy zespół cyberbezpieczeństwa powołany na podstawie art. 44 ustawy zmienianej w art. 1 staje się CSIRT sektorowym, z dniem wejścia w życie niniejszej ustawy.

Art. 45. W terminie 6 miesięcy od wejścia w życie niniejszej ustawy Rada Ministrów przyjmuje w drodze uchwały Krajowy plan reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę oraz Strategię Cyberbezpieczeństwa Rzeczypospolitej Polskiej.

Art. 46. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 20 – gospodarka, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

- 1) w 2025 r. – 0 tys. zł;
- 2) w 2026 r. – 5 662 tys. zł;

- 3) w 2027 r. – 5 353 tys. zł;
- 4) w 2028 r. – 5 587 tys. zł;
- 5) w 2029 r. – 5 836 tys. zł;
- 6) w 2030 r. – 6 101 tys. zł;
- 7) w 2031 r. – 6 384 tys. zł;
- 8) w 2032 r. – 6 682 tys. zł;
- 9) w 2033 r. – 7 000 tys. zł;
- 10) w 2034 r. – 7 338 tys. zł.

2. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 21 – gospodarka morska, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

- 1) w 2025 r. – 0 tys. zł;
- 2) w 2026 r. – 111 tys. zł;
- 3) w 2027 r. – 114 tys. zł;
- 4) w 2028 r. – 122 tys. zł;
- 5) w 2029 r. – 130 tys. zł;
- 6) w 2030 r. – 138 tys. zł;
- 7) w 2031 r. – 147 tys. zł;
- 8) w 2032 r. – 157 tys. zł;
- 9) w 2033 r. – 168 tys. zł;
- 10) w 2034 r. – 179 tys. zł.

3. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 22 – gospodarka wodna, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

- 1) w 2025 r. – 0 tys. zł;
- 2) w 2026 r. – 6 268 tys. zł;
- 3) w 2027 r. – 6 819 tys. zł;
- 4) w 2028 r. – 7 160 tys. zł;
- 5) w 2029 r. – 7 523 tys. zł;
- 6) w 2030 r. – 7 908 tys. zł;
- 7) w 2031 r. – 8 317 tys. zł;
- 8) w 2032 r. – 8 750 tys. zł;
- 9) w 2033 r. – 9 211 tys. zł;
- 10) w 2034 r. – 9 699 tys. zł.

4. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 27 – informatyzacja, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

- 1) w 2025 r. – 0 tys. zł;
- 2) w 2026 r. – 136 778 tys. zł;
- 3) w 2027 r. – 137 213 tys. zł;
- 4) w 2028 r. – 146 969 tys. zł;
- 5) w 2029 r. – 167 112 tys. zł;
- 6) w 2030 r. – 189 948 tys. zł;
- 7) w 2031 r. – 217 414 tys. zł;
- 8) w 2032 r. – 223 028 tys. zł;
- 9) w 2033 r. – 251 875 tys. zł;
- 10) w 2034 r. – 287 067 tys. zł.

5. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 28 – szkolnictwo wyższe i nauka, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

- 1) w 2025 r. – 0 tys. zł;
- 2) w 2026 r. – 5 754 tys. zł;
- 3) w 2027 r. – 6 289 tys. zł;
- 4) w 2028 r. – 6 594 tys. zł;
- 5) w 2029 r. – 6 917 tys. zł;
- 6) w 2030 r. – 7 259 tys. zł;
- 7) w 2031 r. – 7 622 tys. zł;
- 8) w 2032 r. – 8 007 tys. zł;
- 9) w 2033 r. – 8 415 tys. zł;
- 10) w 2034 r. – 8 848 tys. zł.

6. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 32 – rolnictwo, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

- 1) w 2025 r. – 0 tys. zł;
- 2) w 2026 r. – 7 295 tys. zł;
- 3) w 2027 r. – 7 878 tys. zł;
- 4) w 2028 r. – 8 294 tys. zł;
- 5) w 2029 r. – 8 736 tys. zł;
- 6) w 2030 r. – 9 207 tys. zł;

- 7) w 2031 r. – 9 706 tys. zł;
- 8) w 2032 r. – 10 237 tys. zł;
- 9) w 2033 r. – 10 801 tys. zł;
- 10) w 2034 r. – 11 401 tys. zł.

7. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 39 – transport, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

- 1) w 2025 r. – 0 tys. zł;
- 2) w 2026 r. – 6 473 tys. zł;
- 3) w 2027 r. – 7 030 tys. zł;
- 4) w 2028 r. – 7 387 tys. zł;
- 5) w 2029 r. – 7 766 tys. zł;
- 6) w 2030 r. – 8 168 tys. zł;
- 7) w 2031 r. – 8 595 tys. zł;
- 8) w 2032 r. – 9 048 tys. zł;
- 9) w 2033 r. – 9 529 tys. zł;
- 10) w 2034 r. – 10 040 tys. zł.

8. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 47 – energia, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

- 1) w 2025 r. – 0 tys. zł;
- 2) w 2026 r. – 6 268 tys. zł;
- 3) w 2027 r. – 6 819 tys. zł;
- 4) w 2028 r. – 7 160 tys. zł;
- 5) w 2029 r. – 7 523 tys. zł;
- 6) w 2030 r. – 7 908 tys. zł;
- 7) w 2031 r. – 8 317 tys. zł;
- 8) w 2032 r. – 8 750 tys. zł;
- 9) w 2033 r. – 9 211 tys. zł;
- 10) w 2034 r. – 9 699 tys. zł.

9. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 51 – klimat, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

- 1) w 2025 r. – 0 tys. zł;
- 2) w 2026 r. – 5 960 tys. zł;
- 3) w 2027 r. – 6 501 tys. zł;

- 4) w 2028 r. – 6 820 tys. zł;
- 5) w 2029 r. – 7 160 tys. zł;
- 6) w 2030 r. – 7 519 tys. zł;
- 7) w 2031 r. – 7 900 tys. zł;
- 8) w 2032 r. – 8 304 tys. zł;
- 9) w 2033 r. – 8 733 tys. zł;
- 10) w 2034 r. – 9 188 tys. zł.

10. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 57 – Agencja Bezpieczeństwa Wewnętrznego, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

- 1) w 2025 r. – 0 tys. zł;
- 2) w 2026 r. – 3 000 tys. zł;
- 3) w 2027 r. – 3 000 tys. zł;
- 4) w 2028 r. – 3 000 tys. zł;
- 5) w 2029 r. – 3 000 tys. zł;
- 6) w 2030 r. – 3 000 tys. zł;
- 7) w 2031 r. – 3 000 tys. zł;
- 8) w 2032 r. – 3 000 tys. zł;
- 9) w 2033 r. – 3 000 tys. zł;
- 10) w 2034 r. – 3 000 tys. zł.

11. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 76 – Urząd Komunikacji Elektronicznej, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

- 1) w 2025 r. – 0 tys. zł;
- 2) w 2026 r. – 8 014 tys. zł;
- 3) w 2027 r. – 8 619 tys. zł;
- 4) w 2028 r. – 9 087 tys. zł;
- 5) w 2029 r. – 9 586 tys. zł;
- 6) w 2030 r. – 10 115 tys. zł;
- 7) w 2031 r. – 10 678 tys. zł;
- 8) w 2032 r. – 11 277 tys. zł;
- 9) w 2033 r. – 11 915 tys. zł;
- 10) w 2034 r. – 12 593 tys. zł.

12. Minister właściwy do spraw gospodarki monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 1, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków minister właściwy do spraw gospodarki wdraża mechanizm korygujący polegający na ograniczeniu finansowania działalności:

- 1) organu właściwego do spraw cyberbezpieczeństwa dla sektorów produkcji i przestrzeni kosmicznej;
- 2) CSIRT sektorowego dla sektorów produkcji i przestrzeni kosmicznej.

13. Minister właściwy do spraw gospodarki morskiej monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 2, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków minister właściwy do spraw gospodarki morskiej wdraża mechanizm korygujący polegający na ograniczeniu finansowania działalności:

- 1) organu właściwego do spraw cyberbezpieczeństwa dla podsektora transportu wodnego;
- 2) CSIRT sektorowego dla podsektora transportu wodnego.

14. Minister właściwy do spraw gospodarki wodnej monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 3, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków minister właściwy do spraw gospodarki wodnej wdraża mechanizm korygujący polegający na ograniczeniu finansowania działalności:

- 1) organu właściwego do spraw cyberbezpieczeństwa dla sektorów zaopatrzenia w wodę pitną i jej dystrybucji oraz ścieków;
- 2) CSIRT sektorowego dla sektorów zaopatrzenia w wodę pitną i jej dystrybucji oraz ścieków.

15. Minister właściwy do spraw informatyzacji monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 4, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia

przyjętego na dany rok budżetowy limitu wydatków minister właściwy do spraw informatyzacji wdraża mechanizm korygujący polegający na ograniczeniu finansowania:

- 1) organu właściwego do spraw cyberbezpieczeństwa dla sektorów dostawców usług cyfrowych, infrastruktury cyfrowej oraz zarządzania usługami ICT;
- 2) CSIRT sektorowego dla sektorów dostawców usług cyfrowych, infrastruktury cyfrowej oraz zarządzania usługami ICT;
- 3) realizacji zadań ministra w obszarze zarządzania kryzysowego w cyberprzestrzeni;
- 4) dotacji podmiotowej dla CSIRT NASK;
- 5) dotacji celowych udzielanych jednostkom podległym ministrowi właściwemu do spraw informatyzacji albo przez niego nadzorowanym w związku z powierzeniem realizacji zadań ministra;
- 6) działalności edukacyjnej w zakresie cyberbezpieczeństwa;
- 7) realizacji zadań Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa.

16. Minister właściwy do spraw szkolnictwa wyższego i nauki monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 5, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków minister właściwy do spraw szkolnictwa wyższego i nauki wdraża mechanizm korygujący polegający na ograniczeniu finansowania działalności:

- 1) organu właściwego do spraw cyberbezpieczeństwa dla sektora badań naukowych;
- 2) CSIRT sektorowego dla sektora badań naukowych.

17. Minister właściwy do spraw rolnictwa monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 6, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków minister właściwy do spraw rolnictwa wdraża mechanizm korygujący polegający na ograniczeniu finansowania działalności:

- 1) organu właściwego do spraw cyberbezpieczeństwa dla sektora produkcji, przetwarzania i dystrybucji żywności;
- 2) CSIRT sektorowego dla sektora produkcji, przetwarzania i dystrybucji żywności.

18. Minister właściwy do spraw transportu monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 7, i dokonuje oceny wykorzystania tego limitu według stanu na koniec

każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków minister właściwy do spraw transportu wdraża mechanizm korygujący polegający na ograniczeniu finansowania działalności:

- 1) organu właściwego do spraw cyberbezpieczeństwa dla sektora transportu;
- 2) CSIRT sektorowego dla sektora transportu.

19. Minister właściwy do spraw energii monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 8, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków minister właściwy do spraw energii wdraża mechanizm korygujący polegający na ograniczeniu finansowania działalności CSIRT sektorowego:

- 1) organu właściwego do spraw cyberbezpieczeństwa dla sektora energii;
- 2) CSIRT sektorowego dla sektora energii.

20. Minister właściwy do spraw klimatu monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 9, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków minister właściwy do spraw klimatu wdraża mechanizm korygujący polegający na ograniczeniu finansowania:

- 1) organu właściwego do spraw cyberbezpieczeństwa dla sektora gospodarowania odpadami;
- 2) CSIRT sektorowego dla sektora gospodarowania odpadami.

21. Szef Agencji Bezpieczeństwa Wewnętrznego monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 10, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków Szef Agencji Bezpieczeństwa Wewnętrznego wdraża mechanizm korygujący polegający na ograniczeniu finansowania czynności nadzorczych wobec podmiotów publicznych w zakresie cyberbezpieczeństwa. Wdrożenie tego mechanizmu korygującego następuje w uzgodnieniu z ministrem – członkiem Rady Ministrów właściwym do spraw koordynowania działalności służb specjalnych albo

z Prezesem Rady Ministrów, jeżeli minister – członek Rady Ministrów właściwy do spraw koordynowania działalności służb specjalnych nie został powołany.

22. Prezes Urzędu Komunikacji Elektronicznej monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 11, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków Prezes Urzędu Komunikacji Elektronicznej wdraża mechanizm korygujący polegający na ograniczeniu finansowania działalności:

- 1) organu właściwego do spraw cyberbezpieczeństwa dla sektora poczty i podsektora komunikacji elektronicznej;
- 2) CSIRT sektorowego dla sektora poczty i podsektora komunikacji elektronicznej.

Art. 47. Ustawa wchodzi w życie po upływie miesiąca od dnia ogłoszenia.

Załączniki
do ustawy
z dnia
(Dz. U. poz.)

Załącznik nr 1

SEKTORY KLUCZOWE

I	II	III
Sektor	Podsektor	Rodzaj podmiotu
Energia	Wydobywanie kopalin	Podmioty prowadzące działalność gospodarczą w zakresie wydobywania gazu ziemnego na podstawie koncesji, o której mowa w art. 22 ust. 1 ustawy z dnia 9 czerwca 2011 r. – Prawo geologiczne i górnicze
		Podmioty prowadzące działalność gospodarczą w zakresie wydobywania ropy naftowej na podstawie koncesji, o której mowa w art. 22 ust. 1 ustawy z dnia 9 czerwca 2011 r. – Prawo geologiczne i górnicze
		Podmioty prowadzące działalność gospodarczą w zakresie wydobywania węgla brunatnego na podstawie koncesji, o której mowa w art. 22 ust. 1 ustawy z dnia 9 czerwca 2011 r. – Prawo geologiczne i górnicze
		Podmioty prowadzące działalność gospodarczą w zakresie wydobywania węgla kamiennego na podstawie koncesji, o której mowa w art. 22 ust. 1 ustawy z dnia 9 czerwca 2011 r. – Prawo geologiczne i górnicze
		Podmioty prowadzące działalność gospodarczą w zakresie wydobywania pozostałych kopalin na podstawie koncesji, o której mowa w art. 22 ust. 1 ustawy z dnia 9 czerwca 2011 r. – Prawo geologiczne i górnicze

	Energia elektryczna	Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie wytwarzania energii elektrycznej
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 24 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie przesyłania energii elektrycznej
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 25 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie dystrybucji energii elektrycznej
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie obrotu energią elektryczną
		Podmioty, o których mowa w art. 3 pkt 28b ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne
		Uczestnicy rynku świadczący usługę, o której mowa w art. 3 pkt 6e ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne
		Uczestnicy rynku świadczący usługę, o której mowa w art. 3 pkt 11j ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne
		Uczestnicy rynku świadczący usługę, o której mowa w art. 3 pkt 59 i art. 3 pkt 59a ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne

		Przedsiębiorcy odpowiedzialni za zarządzanie punktem ładowania i jego obsługę, świadczący usługę ładowania na rzecz użytkowników końcowych, w tym w imieniu i na rzecz dostawcy usług w zakresie mobilności
	Ciepło	Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie wytwarzania ciepła
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie obrotu ciepłem
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie przesyłania ciepła
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie dystrybucji ciepła
	Ropa i paliwa	Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie wytwarzania paliw ciekłych, o której mowa w art. 32 ust. 1 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne
		Podmioty prowadzące działalność gospodarczą w

		zakresie przesyłania ropy naftowej
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie przesyłania paliw ciekłych siecią rurociągów, o której mowa w art. 32 ust. 1 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne
		Podmiot prowadzący działalność gospodarczą w zakresie magazynowania ropy naftowej, w tym w zakresie bezzbiornikowego podziemnego magazynowania ropy naftowej, o którym mowa w art. 22 ust. 1 ustawy z dnia 9 czerwca 2011 r. – Prawo geologiczne i górnicze
		Podmioty prowadzące działalność gospodarczą w zakresie przeładunku ropy naftowej
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, wykonujące działalność gospodarczą w zakresie magazynowania paliw ciekłych, o którym mowa w art. 32 ust. 1 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, oraz podmiot prowadzący działalność w zakresie bezzbiornikowego podziemnego magazynowania paliw ciekłych, o którym mowa w art. 22 ust. 1 ustawy z dnia 9 czerwca 2011 r. – Prawo geologiczne i górnicze
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, wykonujące działalność gospodarczą w zakresie przeładunku paliw ciekłych, o którym mowa w art. 32 ust. 1 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne

		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, wykonujące działalność gospodarczą w zakresie obrotu paliwami ciekłymi lub w zakresie obrotu paliwami ciekłymi z zagranicą, o którym mowa w art. 32 ust. 1 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne
		Podmioty prowadzące działalność gospodarczą w zakresie wytwarzania paliw syntetycznych
		Agencja wykonawcza utworzona na podstawie ustawy z dnia 17 grudnia 2020 r. o rezerwach strategicznych (Dz. U. z 2024 r. poz. 1598 i 1907)
	Gaz	Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, prowadzące działalność w zakresie wytwarzania paliw gazowych, o którym mowa w art. 3 pkt 45 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie przesyłania paliw gazowych
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie obrotu gazem ziemnym z zagranicą lub na wykonywanie działalności gospodarczej w zakresie obrotu paliwami gazowymi
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 24 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, będące wyznaczonym

		przez Prezesa Urzędu Regulacji Energetyki operatorem systemu przesyłowego gazowego
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 25 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, będące wyznaczonym przez Prezesa Urzędu Regulacji Energetyki operatorem systemu dystrybucyjnego gazowego
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 26 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, będące wyznaczonym przez Prezesa Urzędu Regulacji Energetyki operatorem systemu magazynowania paliw gazowych
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 27 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, będące wyznaczonym przez Prezesa Urzędu Regulacji Energetyki operatorem systemu skraplania gazu ziemnego
		Przedsiębiorstwa energetyczne prowadzące działalność gospodarczą w zakresie rafinacji i przetwarzania gazu ziemnego
	Energetyka jądrowa	Podmiot będący operatorem obiektu energetyki jądrowej, określonego w art. 2 pkt 2 ustawy z dnia 29 czerwca 2011 r. o przygotowaniu i realizacji inwestycji w zakresie obiektów energetyki jądrowej oraz inwestycji towarzyszących
	Wodór	Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, prowadzące działalność w zakresie przesyłania wodoru
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r.

		– Prawo energetyczne, prowadzące działalność w zakresie magazynowania wodoru
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, prowadzące działalność w zakresie wytwarzania wodoru
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, prowadzące działalność w zakresie dystrybucji wodoru
Transport	Transport lotniczy	Przewoźnik lotniczy, o którym mowa w art. 3 pkt 4 rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 300/2008 z dnia 11 marca 2008 r. w sprawie wspólnych zasad w dziedzinie ochrony lotnictwa cywilnego i uchylającego rozporządzenie (WE) nr 2320/2002 (Dz. Urz. UE L 97 z 09.04.2008, str. 72)
		Zarządzający lotniskiem, o którym mowa w art. 2 pkt 7 ustawy z dnia 3 lipca 2002 r. – Prawo lotnicze (Dz. U. z 2025 r. poz. 1431)
		Przedsiębiorca, o którym mowa w art. 177 ust. 2 ustawy z dnia 3 lipca 2002 r. – Prawo lotnicze, wykonujący dla przewoźników lotniczych oraz innych użytkowników statków powietrznych jedną lub więcej kategorii usług, o których mowa w art. 176 tej ustawy, oraz przedsiębiorca, o którym mowa w art. 186b ust. 1 pkt 2 ustawy z dnia 3 lipca 2002 r. – Prawo lotnicze, wykonujący zadania związane z kontrolą bezpieczeństwa
		Instytucja zapewniająca służby żeglugi powietrznej, o której mowa w art. 127 ust. 1 ustawy z dnia 3 lipca 2002 r. – Prawo lotnicze

	Transport kolejowy	Zarządca infrastruktury kolejowej w rozumieniu art. 4 pkt 7 ustawy z dnia 28 marca 2003 r. o transporcie kolejowym (Dz. U. z 2025 r. poz. 1234), z wyłączeniem zarządców wyłącznie infrastruktury nieczynnej, o której mowa w art. 4 pkt 1b tej ustawy, infrastruktury prywatnej, o której mowa w art. 4 pkt 1c, oraz infrastruktury kolei wąskotorowej, o której mowa w art. 4 pkt 1d tej ustawy
		Przewoźnik kolejowy, o którym mowa w art. 4 pkt 9 ustawy z dnia 28 marca 2003 r. o transporcie kolejowym, którego działalność podlega licencjonowaniu, oraz operator obiektu infrastruktury usługowej, o którym mowa w art. 4 pkt 52 ustawy z dnia 28 marca 2003 r. o transporcie kolejowym, jeżeli przedsiębiorca wykonujący funkcję operatora jest jednocześnie przewoźnikiem kolejowym
	Transport wodny	Armator w transporcie morskim pasażerów i towarów zgodnie z definicją dla transportu morskiego w załączniku I do rozporządzenia (WE) nr 725/2004 Parlamentu Europejskiego i Rady z dnia 31 marca 2004 r. w sprawie podniesienia ochrony statków i obiektów portowych (Dz. Urz. UE L 129 z 29.04.2004, str. 6, z późn. zm. ¹⁾), z wyłączeniem poszczególnych statków, na których prowadzą działalność ci armatorzy
		Armator, o którym mowa w art. 5 ust. 1 pkt 2 ustawy z dnia 21 grudnia 2000 r. o żegludze śródlądowej (Dz. U. z 2025 r. poz. 18)

¹⁾ Sprostowanie rozporządzenia zostało ogłoszone w Dz. Urz. UE L 161 z 20.06.2008 r., zmiany rozporządzenia zostały ogłoszone w Dz. Urz. UE L 29 z 31.01.2009, str. 53 oraz Dz. Urz. UE L 87 z 31.03.2009, str. 109.

		Podmiot zarządzający portem morskim, o którym mowa w art. 3 ust. 1 pkt 2 ustawy z dnia 4 września 2008 r. o ochronie żeglugi i portów morskich (Dz. U. z 2024 r. poz. 597)
		Podmiot zarządzający obiektem portowym, o którym mowa w art. 2 pkt 11 rozporządzenia (WE) 725/2004 Parlamentu Europejskiego i Rady z dnia 31 marca 2004 r. w sprawie podniesienia ochrony statków i obiektów portowych
		Podmioty prowadzące na terenie portu działalność wspomagającą transport morski ujęte w klasie 52.22 klasyfikacji NACE Rev. 2, ujętej w załączniku I do rozporządzenia (WE) nr 1893/2006 Parlamentu Europejskiego i Rady z dnia 20 grudnia 2006 r. w sprawie statystycznej klasyfikacji działalności gospodarczej NACE Rev. 2 i zmieniającego rozporządzenie Rady (EWG) nr 3037/90 oraz niektóre rozporządzenia WE w sprawie określonych dziedzin statystycznych (Dz. Urz. UE L 393 z 30.12.2006, str. 1, z późn. zm. ²⁾)
		VTs (Służba Kontroli Ruchu Statków) – aparat pomocniczy dyrektora urzędu morskiego powołany w celu monitorowania ruchu statków i przekazywania informacji, stanowiący część składową Narodowego Systemu SafeSeaNet, o którym mowa w art. 91 ustawy z dnia 18 sierpnia 2011 r. o bezpieczeństwie morskim (Dz. U. z 2025 r. poz. 883)
	Transport drogowy	Zarządca drogi, o którym mowa w art. 19 ust. 2

²⁾ Sprostowanie rozporządzenia zostało ogłoszone w Dz. Urz. UE L 90785 z 6.12.2024, str. 1, zmiany rozporządzenia zostały ogłoszone w Dz. Urz. UE L 97 z 9.04.2008, str. 13, Dz. Urz. UE L 198 z 25.07.2019, str. 241 oraz Dz. Urz. UE L 19 z 20.01.2023, str. 5.

		pkt 1 ustawy z dnia 21 marca 1985 r. o drogach publicznych
		Podmioty świadczące usługę ITS, o której mowa w art. 4 pkt 36 ustawy z dnia 21 marca 1985 r. o drogach publicznych
Bankowość i infrastruktura rynków finansowych		Instytucja kredytowa, o której mowa w art. 4 ust. 1 pkt 17 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe (Dz. U. z 2024 r. poz. 1646, z późn. zm. ³⁾)
		Bank krajowy, o którym mowa w art. 4 ust. 1 pkt 1 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe
		Oddział banku zagranicznego, o którym mowa w art. 4 ust. 1 pkt 20 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe
		Spółdzielcze kasy oszczędnościowo-kredytowe w rozumieniu ustawy z dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych
		Podmiot prowadzący rynek regulowany, o którym mowa w art. 14 ust. 1 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi (Dz. U. z 2024 r. poz. 722, z późn. zm. ⁴⁾)
		Podmiot, o którym mowa w art. 3 pkt 49 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi
		Podmiot, o którym mowa w art. 48 ust. 7 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi

³⁾ Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2024 r. poz. 1685 i 1863 oraz z 2025 r. poz. 146, 222, 525, 769, 820, 1069, 1170, 1191 i 1216.

⁴⁾ Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2024 r. poz. 1863 oraz z 2025 r. 146, 820, 923, 1014, 1069 i 1216.

		Podmiot prowadzący ASO w rozumieniu art. 3 pkt 2 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi
		Podmiot prowadzący OTF w rozumieniu art. 3 pkt 10b ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi
		Administratorzy kluczowych wskaźników referencyjnych
		Podmiot utworzony na podstawie art. 67 ustawy – Prawo bankowe
		Podmiot, o którym mowa w art. 3 pkt 21a ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi mający siedzibę na terytorium Rzeczypospolitej Polskiej
Ochrona zdrowia	Udzielanie świadczeń zdrowotnych i zdrowie publiczne	Podmiot leczniczy, o którym mowa w art. 4 ust. 1 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej (Dz. U. z 2025 r. poz. 450, 620, 637 i 1211)
		Laboratoria referencyjne UE, o których mowa w art. 15 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2371 z dnia 23 listopada 2022 r. w sprawie poważnych transgranicznych zagrożeń zdrowia oraz uchylenia decyzji nr 1082/2013/UE (Dz. Urz. UE L 314 z 06.12.2022, str. 1)
		Jednostka podległa ministrowi właściwemu do spraw zdrowia albo przez niego nadzorowana, właściwa w zakresie systemów informacyjnych ochrony zdrowia
		Urzędy obsługujące organy Państwowej Inspekcji Sanitarnej
		Krajowe Centrum Monitorowania Ratownictwa

		Medycznego, o którym mowa w art. 27a ustawy z dnia 8 września 2006 r. o Państwowym Ratownictwie Medycznym (Dz. U. z 2025 r. poz. 91 i 637)
		Jednostki organizacyjne publicznej służby krwi, o których mowa w art. 4 ust. 3 pkt 2 ustawy z dnia 22 sierpnia 1997 r. o publicznej służbie krwi (Dz. U. z 2024 r. poz. 1782)
		Podmioty udzielające świadczeń opieki zdrowotnej będące podwykonawcą dla podmiotów kluczowych lub ważnych w sektorze ochrona zdrowia, w rozumieniu art. 133 ustawy z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (Dz. U. z 2025 r. poz. 1461)
		Świadczeniodawcy posiadający w swojej strukturze organizacyjnej Szpitalny Oddział Ratunkowy, Centrum Urazowe lub Centrum Urazowe dla Dzieci
	Produkcja i dystrybucja substancji czynnych, produktów leczniczych i wyrobów medycznych	Urząd Rejestracji Produktów Leczniczych, Wyrobów Medycznych i Produktów Biobójczych
		Urzędy obsługujące organy Inspekcji Farmaceutycznej
		Podmioty prowadzące działalność badawczo-rozwojową w zakresie produktów leczniczych zdefiniowanych w art. 1 pkt 2 dyrektywy 2001/83/WE Parlamentu Europejskiego i Rady z dnia 6 listopada 2001 r. w sprawie wspólnotowego kodeksu odnoszącego się do produktów leczniczych stosowanych u ludzi (Dz. Urz. UE L 311 z 28.11.2001, str. 67, z późn.

		zm. ⁵⁾)
		Podmioty produkujące podstawowe substancje farmaceutyczne oraz leki i pozostałe wyroby farmaceutyczne, o których mowa w sekcji C dział 21 klasyfikacji NACE Rev. 2
		Podmioty produkujące wyroby medyczne uznane za mające krytyczne znaczenie podczas danego stanu zagrożenia zdrowia publicznego („wykaz wyrobów medycznych o krytycznym znaczeniu w przypadku stanu zagrożenia zdrowia publicznego”) w rozumieniu art. 22 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/123 z dnia 25 stycznia 2022 r. w sprawie wzmocnienia roli Europejskiej Agencji Leków w zakresie gotowości na wypadek sytuacji kryzysowej i zarządzania kryzysowego w odniesieniu do produktów leczniczych i wyrobów medycznych (Dz. Urz. UE L 20 z 31.01.2022, str. 1, z późn. zm. ⁶⁾)
		Przedsiębiorca prowadzący działalność polegającą na prowadzeniu hurtowni farmaceutycznej w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne (Dz. U. z 2025 r. poz. 750, 905, 924 i 1416)
		Przedsiębiorca lub podmiot prowadzący działalność gospodarczą w państwie

⁵⁾ Sprostowanie dyrektywy zostało ogłoszone w Dz. Urz. UE L 230 z 24.08.2006, str. 12, Dz. Urz. UE L 87 z 31.03.2009, str. 174, Dz. Urz. UE L 276 z 21.10.2011, str. 63 oraz Dz. Urz. UE L 131 z 22.05.2012, str. 11, zmiany dyrektywy zostały ogłoszone w Dz. Urz. UE L 33 z 8.02.2003, str. 30, Dz. Urz. UE L 159 z 27.06.2003, str. 46, Dz. Urz. UE L 136 z 30.04.2004, str. 34 i 85, Dz. Urz. UE L 378 z 27.12.2006, str. 1, Dz. Urz. UE L 324 z 10.12.2007, str. 121, Dz. Urz. UE L 81 z 20.03.2008, str. 51, Dz. Urz. UE L 168 z 30.06.2009, str. 33, Dz. Urz. UE L 242 z 15.09.2009, str. 3, Dz. Urz. UE L 348 z 31.12.2010, str. 74, Dz. Urz. UE L 174 z 1.07.2011, str. 74, Dz. Urz. UE L 299 z 27.10.2012, str. 1, Dz. Urz. UE L 117 z 5.05.2017, str. 1, Dz. Urz. UE L 4 z 7.01.2019, str. 24, Dz. Urz. UE L 198 z 25.07.2019, str. 241, Dz. Urz. UE L 118 z 20.04.2022, str. 4 oraz Dz. Urz. UE L 157 z 20.06.2023, str. 1.

⁶⁾ Sprostowanie rozporządzenia zostało ogłoszone w Dz. Urz. UE L 71 z 9.03.2023, str. 37, zmiana rozporządzenia została ogłoszona w Dz. Urz. UE L 568 z 14.02.2024, str. 1.

		członkowskim Unii Europejskiej lub państwie członkowskim Europejskiego Porozumienia o Wolnym Handlu (EFTA) – stronie umowy o Europejskim Obszarze Gospodarczym, który uzyskał pozwolenie na dopuszczenie do obrotu produktu leczniczego
		Importer produktu leczniczego lub substancji czynnej w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne
		Wytwórca produktu leczniczego lub substancji czynnej w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne
		Importer równoległy w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne
		Dystrybutor substancji czynnej w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne
		Przedsiębiorca prowadzący działalność w formie apteki ogólnodostępnej w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne
Zaopatrzenie w wodę pitną i jej dystrybucja		Podmiot dostarczający wodę przeznaczoną do spożycia przez ludzi, w tym przedsiębiorstwo wodociągowo-kanalizacyjne, o którym mowa w art. 2 pkt 4 ustawy z dnia 7 czerwca 2001 r. o zbiorowym zaopatrzeniu w wodę i zbiorowym odprowadzaniu ścieków (Dz. U. z 2024 r. poz. 757), z wyłączeniem podmiotów, dla których dostarczanie wody przeznaczonej do spożycia przez ludzi jest inną niż istotną częścią ich ogólnej działalności
Zbiorowe odprowadzanie		Podmiot odprowadzający lub oczyszczający ścieki, w tym przedsiębiorstwo wodociągowo-

ścieków		kanalizacyjne, o którym mowa w art. 2 pkt 4 ustawy z dnia 7 czerwca 2001 r. o zbiorowym zaopatrzeniu w wodę i zbiorowym odprowadzaniu ścieków, z wyłączeniem podmiotów, dla których odprowadzanie lub oczyszczanie ścieków jest inną niż istotną częścią ich ogólnej działalności
Infrastruktura cyfrowa	Infrastruktura cyfrowa z wyłączeniem komunikacji elektronicznej	Dostawca punktu wymiany ruchu internetowego
		Dostawca usług DNS, z wyłączeniem operatorów głównych serwerów nazw
		Rejestr nazw domen najwyższego poziomu (TLD)
		Dostawca chmury obliczeniowej
		Dostawca usług centrum przetwarzania danych
		Dostawca sieci dostarczania treści
		Dostawca usług zaufania
		Podmiot świadczący usługę rejestracji nazw domen
	Komunikacja elektroniczna	Przedsiębiorca komunikacji elektronicznej
Zarządzanie usługami ICT		Dostawca usług zarządzanych
		Dostawca usług zarządzanych w zakresie cyberbezpieczeństwa
Przestrzeń kosmiczna		Operator infrastruktury naziemnej, który wspiera świadczenie usług kosmicznych, z wyjątkiem operatora, o którym mowa w art. 2 pkt 40 lit. b ustawy z dnia 12 lipca 2024 r. – Prawo komunikacji elektronicznej
		Polska Agencja Kosmiczna
Podmioty publiczne		1) Podmioty z uwzględnieniem pkt 2–4: a) jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 1 ustawy z dnia

		27 sierpnia 2009 r. o finansach publicznych oraz urzędy je obsługujące, b) jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 3, 5–6, 8 i 9 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych, c) państwowe instytucje kultury, d) instytuty badawcze, e) Narodowy Bank Polski, f) Bank Gospodarstwa Krajowego, g) Urząd Dozoru Technicznego, h) Polska Agencja Żeglugi Powietrznej, i) Polskie Centrum Akredytacji, j) Urząd Komisji Nadzoru Finansowego, k) Polska Agencja Prasowa, l) Państwowe Gospodarstwo Wodne Wody Polskie, o którym mowa w ustawie z dnia 20 lipca 2017 r. – Prawo wodne (Dz. U. z 2025 r. poz. 960), m) Polski Fundusz Rozwoju i inne instytucje rozwoju, o których mowa w art. 2 ust. 1 pkt 1 i 3–6 ustawy z dnia 4 lipca 2019 r. o systemie instytucji rozwoju. n) Narodowy Fundusz Ochrony Środowiska i Gospodarki Wodnej, o) wojewódzkie fundusze ochrony środowiska i gospodarki wodnej, p) Państwowy Fundusz Rehabilitacji Osób Niepełnosprawnych, q) Zakład Unieszkodliwiania Odpadów Promieniotwórczych z siedzibą w Otwocku-Świerku,

		r) państwowa osoba prawna, wobec której wydano decyzję, o której mowa w art. 7m s) spółka, o której mowa w art. 2 ust. 1 ustawy z dnia 29 kwietnia 2016 r. o szczególnych zasadach wykonywania niektórych zadań dotyczących informatyzacji w zakresie działań administracji rządowej budżet i finanse publiczne
		2) w odniesieniu do samorządu województwa: jednostki budżetowe oraz zakłady budżetowe z wyłączeniem: a) jednostek organizacyjnych, o których mowa w art. 2 ustawy z dnia 14 grudnia 2016 r. – Prawo oświatowe (Dz. U. z 2025 r. poz. 1043 i 1160) oraz ich zespołów, b) jednostek organizacyjnych wspierania rodziny i systemu pieczy zastępczej, o których mowa w art. 2 ust. 3 ustawy z dnia 9 czerwca 2011 r. o wspieraniu rodziny i systemie pieczy zastępczej (Dz. U. z 2025 r. poz. 49 i 1301), c) jednostek organizacyjnych, o których mowa w art. 6 pkt 5 ustawy z dnia 12 marca 2004 r. o pomocy społecznej, oprócz regionalnych ośrodków polityki społecznej, d) wojewódzkich urzędów pracy, e) parków krajobrazowych i ich zespołów, f) jednostek obsługujących, o których mowa w art. 8d ustawy z dnia 5 czerwca 1998 r. o samorządzie województwa, w zakresie

		w jakim prowadzą wspólną obsługę jednostek, o których mowa w lit. a–e
		3) w odniesieniu do samorządu powiatu: starostwo powiatowe
		4) w odniesieniu do samorządu gminy: urząd gminy, jeżeli zatrudnia na dzień 1 stycznia danego roku w przeliczeniu na pełny wymiar czasu pracy na podstawie umowy o pracę co najmniej 50 osób

SEKTORY WAŻNE

I	II	III
Sektor	Podsektor	Rodzaj podmiotu
Usługi pocztowe		Operator pocztowy, o którym mowa w art. 3 pkt 12 ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe (Dz. U. z 2025 r. poz. 366, 820 i 1456)
Inwestycje energetyki jądrowej		Podmiot będący inwestorem obiektu energetyki jądrowej określonego w art. 2 pkt 2 ustawy z dnia 29 czerwca 2011 r. o przygotowaniu i realizacji inwestycji w zakresie obiektów energetyki jądrowej oraz inwestycji towarzyszących, który uzyskał decyzję zasadniczą, o której mowa w art. 3a ust. 1 tej ustawy
Gospodarowanie odpadami	Zbieranie odpadów	Przedsiębiorstwa świadczące usługi w rozumieniu ustawy z dnia 14 grudnia 2012 r. o odpadach (Dz. U. z 2023 r. poz. 1587, z późn. zm. ⁷⁾), polegające na zbieraniu odpadów, zobowiązane do uzyskania wpisu w rejestrze, o którym mowa w art. 49 ust. 1 ustawy z dnia 14 grudnia 2012 r. o odpadach, z wyłączeniem przedsiębiorstw, dla których usługi te nie stanowią podstawowej działalności gospodarczej określonej zgodnie z przepisami wydanymi na podstawie art. 40 ust. 2

⁷⁾ Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2023 r. poz. 1597, 1688, 1852 i 2029 oraz z 2024 r. poz. 1834, 1911 i 1914.

		ustawy z dnia 29 czerwca 1995 r. o statystyce publicznej (Dz. U. z 2024 r. poz. 1799)
	Transport odpadów	Przedsiębiorstwa świadczące usługi w rozumieniu ustawy z dnia 14 grudnia 2012 r. o odpadach, polegające na transporcie odpadów, zobowiązane do uzyskania wpisu w rejestrze, o którym mowa w art. 49 ust. 1 ustawy z dnia 14 grudnia 2012 r. o odpadach, z wyłączeniem przedsiębiorstw, dla których usługi te nie stanowią podstawowej działalności gospodarczej określonej zgodnie z przepisami wydanymi na podstawie art. 40 ust. 2 ustawy z dnia 29 czerwca 1995 r. o statystyce publicznej
	Przetwarzanie odpadów, w tym sortowanie, wraz z nadzorem nad wymienionymi działaniami, a także późniejsze postępowanie z miejscami unieszkodliwiania odpadów	Przedsiębiorstwa świadczące usługi w rozumieniu ustawy z dnia 14 grudnia 2012 r. o odpadach, polegające na przetwarzaniu odpadów w tym sortowaniu, wraz z nadzorem nad wymienionymi działaniami, a także podmioty świadczące usługi z późniejszym postępowaniem z miejscami unieszkodliwiania odpadów, zobowiązane do uzyskania wpisu w rejestrze, o którym mowa w art. 49 ust. 1 ustawy z dnia 14 grudnia 2012 r. o odpadach, z wyłączeniem przedsiębiorstw, dla których usługi te nie stanowią podstawowej działalności gospodarczej

		określonej zgodnie z przepisami wydanymi na podstawie art. 40 ust. 2 ustawy z dnia 29 czerwca 1995 r. o statystyce publicznej
	Działania wykonywane w charakterze sprzedawcy odpadów lub pośrednika w obrocie odpadami	Przedsiębiorstwa świadczące usługi w rozumieniu ustawy z dnia 14 grudnia 2012 r. o odpadach, polegające na działaniach wykonywanych w charakterze sprzedawcy odpadów lub pośrednika w obrocie odpadami, zobowiązane do uzyskania wpisu w rejestrze, o którym mowa w art. 49 ust. 1 ustawy z dnia 14 grudnia 2012 r. o odpadach, z wyłączeniem przedsiębiorstw, dla których usługi te nie stanowią podstawowej działalności gospodarczej określonej zgodnie z przepisami wydanymi na podstawie art. 40 ust. 2 ustawy z dnia 29 czerwca 1995 r. o statystyce publicznej
Produkcja, wytwarzanie i dystrybucja chemikaliów		Przedsiębiorstwa zajmujące się produkcją substancji oraz dystrybucją substancji lub mieszanin, o których mowa w art. 3 pkt 9 i 14 rozporządzenia (WE) nr 1907/2006 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2006 r. w sprawie rejestracji, oceny, udzielania zezwoleń i stosowanych ograniczeń w zakresie chemikaliów (REACH) i utworzenia Europejskiej Agencji Chemikaliów, zmieniające dyrektywę 1999/45/WE oraz uchylające rozporządzenie Rady

		(EWG) nr 793/93 i rozporządzenie Komisji (WE) nr 1488/94, jak również dyrektywę Rady 76/769/EWG i dyrektywy Komisji 91/155/EWG, 93/67/EWG, 93/105/WE i 2000/21/WE (Dz. Urz. UE L 396 z 30.12.2006, str. 1, z późn. zm. ⁸⁾)
		Przedsiębiorstwa zajmujące się wytwarzaniem z substancji lub mieszanin wyrobów, o których mowa w art. 3 pkt 3 rozporządzenia (WE) nr 1907/2006 Parlamentu Europejskiego

⁸⁾ Sprostowanie rozporządzenia zostało ogłoszone w Dz. Urz. UE L 136 z 29.05.2007, str. 3, Dz. Urz. UE L 141 z 31.05.2008, str. 22, Dz. Urz. UE L 36 z 5.02.2009, str. 84, Dz. Urz. UE L 118 z 12.05.2010, str. 89, Dz. Urz. UE L 260 z 2.10.2010, str. 22, Dz. Urz. UE L 49 z 24.02.2011, str. 52, Dz. Urz. UE L 136 z 24.05.2011, str. 105, Dz. Urz. UE L 331 z 18.11.2014, str. 41, Dz. Urz. UE L 12 z 17.01.2017, str. 97, Dz. Urz. UE L 102 z 23.04.2018, str. 99, Dz. Urz. UE L 249 z 4.10.2018, str. 19 i 18, Dz. Urz. UE L 141 z 5.05.2020, str. 37, Dz. Urz. UE L 83 z 10.03.2022, str. 64 oraz Dz. Urz. UE L 90479 z 6.06.2025, str. 1, zmiany rozporządzenia zostały ogłoszone w Dz. Urz. UE L 304 z 22.11.2007, str. 1, Dz. Urz. UE L 268 z 9.10.2008, str. 14, Dz. Urz. UE L 353 z 31.12.2008, str. 1, Dz. Urz. UE L 46 z 17.02.2009, str. 3, Dz. Urz. UE L 164 z 26.06.2009, str. 7, Dz. Urz. UE L 86 z 1.04.2010, str. 7, Dz. Urz. UE L 133 z 31.05.2010, str. 1, Dz. Urz. UE L 44 z 18.02.2011, str. 2, Dz. Urz. UE L 58 z 3.03.2011, str. 27, Dz. Urz. UE L 69 z 16.03.2011, str. 3 i 7, Dz. Urz. UE L 101 z 15.04.2011, str. 12, Dz. Urz. UE L 134 z 21.05.2011, str. 2, Dz. Urz. UE L 37 z 10.02.2012, str. 1, Dz. Urz. UE L 41 z 15.02.2012, str. 1, Dz. Urz. UE L 128 z 16.05.2012, str. 1, Dz. Urz. UE L 252 z 19.09.2012, str. 1 i 4, Dz. Urz. UE L 253 z 20.09.2012, str. 1 i 5, Dz. Urz. UE L 43 z 14.02.2013, str. 24, Dz. Urz. UE L 108 z 18.04.2013, str. 1, Dz. Urz. UE L 158 z 10.06.2013, str. 1, Dz. Urz. UE L 328 z 7.12.2013, str. 69, Dz. Urz. UE L 90 z 26.03.2014, str. 1, Dz. Urz. UE L 93 z 28.03.2014, str. 24, Dz. Urz. UE L 136 z 9.05.2014, str. 19, Dz. Urz. UE L 244 z 19.08.2014, str. 6, Dz. Urz. UE L 50 z 21.02.2015, str. 1, Dz. Urz. UE L 58 z 3.03.2015, str. 43, Dz. Urz. UE L 104 z 23.04.2015, str. 2, Dz. Urz. UE L 132 z 29.05.2015, str. 8, Dz. Urz. UE L 233 z 5.09.2015, str. 2, Dz. Urz. UE L 9 z 14.01.2016, str. 1, Dz. Urz. UE L 40 z 17.02.2016, str. 5, Dz. Urz. UE L 144 z 1.06.2016, str. 27, Dz. Urz. UE L 165 z 23.06.2016, str. 4, Dz. Urz. UE L 166 z 24.06.2016, str. 1, Dz. Urz. UE L 255 z 21.09.2016, str. 14, Dz. Urz. UE L 337 z 13.12.2016, str. 3, Dz. Urz. UE L 35 z 10.02.2017, str. 6, Dz. Urz. UE L 104 z 20.04.2017, str. 8, Dz. Urz. UE L 150 z 14.06.2017, str. 7 i 14, Dz. Urz. UE L 224 z 31.08.2017, str. 110, Dz. Urz. UE L 6 z 11.01.2018, str. 45, Dz. Urz. UE L 99 z 19.04.2018, str. 3 i 7, Dz. Urz. UE L 114 z 4.05.2018, str. 4, Dz. Urz. UE L 256 z 12.10.2018, str. 1, Dz. Urz. UE L 308 z 4.12.2018, str. 1, Dz. Urz. UE L 322 z 18.12.2018, str. 14, Dz. Urz. UE L 154 z 12.06.2019, str. 37, Dz. Urz. UE L 186 z 11.07.2019, str. 1, Dz. Urz. UE L 259 z 10.10.2019, str. 9, Dz. Urz. UE L 35 z 7.02.2020, str. 1, Dz. Urz. UE L 110 z 8.04.2020, str. 1, Dz. Urz. UE L 203 z 26.06.2020, str. 28, Dz. Urz. UE L 252 z 4.08.2020, str. 24, Dz. Urz. UE L 423 z 15.12.2020, str. 6, Dz. Urz. UE L 425 z 16.12.2020, str. 3, Dz. Urz. UE L 431 z 21.12.2020, str. 38, Dz. Urz. UE L 24 z 26.01.2021, str. 19, Dz. Urz. UE L 216 z 18.06.2021, str. 121, Dz. Urz. UE L 259 z 21.07.2021, str. 1, Dz. Urz. UE L 282 z 5.08.2021, str. 29, Dz. Urz. UE L 415 z 22.11.2021, str. 16, Dz. Urz. UE L 418 z 24.11.2021, str. 6, Dz. Urz. UE L 446 z 14.12.2021, str. 34, Dz. Urz. UE L 98 z 25.03.2022, str. 38, Dz. Urz. UE L 112 z 11.04.2022, str. 6, Dz. Urz. UE L 123 z 8.05.2023, str. 1, Dz. Urz. UE L 149 z 9.06.2023, str. 49, Dz. Urz. UE L 180 z 17.07.2023, str. 12, Dz. Urz. UE L 238 z 27.09.2023, str. 67, Dz. Urz. UE L 2482 z 14.11.2023, str. 1, Dz. Urz. UE L 1328 z 17.05.2024, str. 1, Dz. Urz. UE L 2462 z 20.09.2024, str. 1, Dz. Urz. UE L 2929 z 28.11.2024, str. 1, Dz. Urz. UE L 660 z 2.04.2025, str. 1, Dz. Urz. UE L 1090 z 3.06.2025, str. 1 oraz Dz. Urz. UE L 1731 z 11.08.2025, str. 1.

		i Rady z dnia 18 grudnia 2006 r. w sprawie rejestracji, oceny, udzielania zezwoleń i stosowanych ograniczeń w zakresie chemikaliów (REACH) i utworzenia Europejskiej Agencji Chemikaliów, zmieniające dyrektywę 1999/45/WE oraz uchylające rozporządzenie Rady (EWG) nr 793/93 i rozporządzenie Komisji (WE) nr 1488/94, jak również dyrektywę Rady 76/769/EWG i dyrektywy Komisji 91/155/EWG, 93/67/EWG, 93/105/WE i 2000/21/WE
Produkcja, przetwarzanie i dystrybucja żywności		Przedsiębiorstwa spożywcze w rozumieniu art. 3 pkt 2 rozporządzenia (WE) nr 178/2002 Parlamentu Europejskiego i Rady z dnia 28 stycznia 2002 r. ustanawiające ogólne zasady i wymagania prawa żywnościowego, powołujące Europejski Urząd ds. Bezpieczeństwa Żywności oraz ustanawiające procedury w zakresie bezpieczeństwa żywności, zajmujące się dystrybucją hurtową oraz przemysłowymi produkcją i przetwarzaniem (Dz. Urz. UE L 31 z 01.02.2002, str. 1, z późn. zm. ⁹⁾)
Produkcja	Produkcja wyrobów	Podmioty produkujące wyroby

⁹⁾ Sprostowanie rozporządzenia zostało ogłoszone w Dz. Urz. UE L 179 z 7.07.2007, str. 59, Dz. Urz. UE L 327 z 12.11.2014, str. 9 oraz Dz. Urz. UE L 37 z 13.02.2015, str. 24, zmiany rozporządzenia zostały ogłoszone w Dz. Urz. UE L 245 z 29.09.2003, str. 4, Dz. Urz. UE L 100 z 8.04.2006, str. 3, Dz. Urz. UE L 60 z 5.03.2008, str. 17, L 188 z 18.07.2009, str. 14, Dz. Urz. UE L 189 z 27.06.2014, str. 1, Dz. Urz. UE L 35 z 10.02.2017, str. 10, Dz. Urz. UE L 117 z 5.05.2017, str. 1, Dz. Urz. UE L 198 z 25.07.2019, str. 241, Dz. Urz. UE L 231 z 6.09.2019, str. 1 oraz Dz. Urz. UE L 908 z 20.03.2024, str. 1.

	medycznych i wyrobów medycznych do diagnostyki <i>in vitro</i>	medyczne w rozumieniu art. 2 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2017/745 z dnia 5 kwietnia 2017 r. w sprawie wyrobów medycznych, zmiany dyrektywy 2001/83/WE, rozporządzenia (WE) nr 178/2002 i rozporządzenia (WE) nr 1223/2009 oraz uchylecia dyrektyw Rady 90/385/EWG i 93/42/EWG (Dz. Urz. UE L 117 z 05.05.2017, str. 1, z późn. zm.¹⁰⁾)
		Podmioty produkujące wyroby medyczne do diagnostyki <i>in vitro</i> w rozumieniu art. 2 ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2017/746 z dnia 5 kwietnia 2017 r. w sprawie wyrobów medycznych do diagnostyki <i>in vitro</i> oraz uchylecia dyrektywy 98/79/WE i decyzji Komisji 2010/227/UE (Dz. Urz. UE L 117 z 05.05.2017, str. 176, z późn. zm.¹¹⁾), z wyjątkiem podmiotów produkujących wyroby medyczne uznane za mające krytyczne znaczenie podczas danego stanu zagrożenia

¹⁰⁾ Sprostowanie rozporządzenia zostało ogłoszone w Dz. Urz. UE L 117 z 3.05.2019, str. 9, Dz. Urz. UE L 334 z 27.12.2019, str. 165 oraz Dz. Urz. UE L 241 z 8.07.2021, str. 7, zmiany rozporządzenia zostały ogłoszone w Dz. Urz. UE L 130 z 24.04.2020, str. 18, L 70 z 8.03.2023, str. 1, Dz. Urz. UE L 80 z 20.03.2023, str. 24, Dz. Urz. UE L 568 z 14.02.2024, str. 1 oraz Dz. Urz. UE L 1860 z 9.07.2024, str. 1.

¹¹⁾ Sprostowanie rozporządzenia zostało ogłoszone w Dz. Urz. UE L 117 z 3.05.2019, str. 11, Dz. Urz. UE L 334 z 27.12.2019, str. 167 oraz Dz. Urz. UE L 233 z 1.07.2021, str. 9, zmiany rozporządzenia zostały ogłoszone w Dz. Urz. UE L 19 z 28.01.2022, str. 3, Dz. Urz. UE L 70 z 8.03.2023, str. 3, Dz. Urz. UE L 80 z 20.03.2023, str. 24 oraz Dz. Urz. UE L 1860 z 9.07.2024, str. 1.

		zdrowia publicznego
	Produkcja komputerów, wyrobów elektronicznych i optycznych	Przedsiębiorca prowadzący którykolwiek z rodzajów działalności gospodarczej, o których mowa w sekcji C dział 26 klasyfikacji NACE Rev. 2, ujętej w załączniku I do rozporządzenia (WE) nr 1893/2006 Parlamentu Europejskiego i Rady z dnia 20 grudnia 2006 r. w sprawie statystycznej klasyfikacji działalności gospodarczej NACE Rev. 2 i zmieniającego rozporządzenie Rady (EWG) nr 3037/90 oraz niektóre rozporządzenia WE w sprawie określonych dziedzin statystycznych (Dz. Urz. UE L 393 z 30.12.2006, str. 1, z późn. zm. ¹²⁾)
	Produkcja urządzeń elektrycznych	Przedsiębiorca prowadzący którykolwiek z rodzajów działalności gospodarczej, o których mowa w sekcji C dział 27 klasyfikacji NACE Rev. 2
	Produkcja maszyn i urządzeń, gdzie indziej niesklasyfikowana	Przedsiębiorca prowadzący którykolwiek z rodzajów działalności gospodarczej, o których mowa w sekcji C dział 28 klasyfikacji NACE Rev. 2
	Produkcja pojazdów samochodowych, przyczep i naczep	Przedsiębiorca prowadzący którykolwiek z rodzajów działalności gospodarczej, o których mowa w sekcji C dział 29 klasyfikacji NACE Rev. 2
	Produkcja pozostałego	Przedsiębiorca prowadzący

¹²⁾ Sprostowanie rozporządzenia zostało ogłoszone w Dz. Urz. UE L 90785 z 6.12.2024, str. 1, zmiany rozporządzenia zostały ogłoszone w Dz. Urz. UE L 97 z 9.04.2008, str. 13, Dz. Urz. UE L 198 z 25.07.2019, str. 241 oraz Dz. Urz. UE L 19 z 20.01.2023, str. 5.

	sprzętu transportowego	którykolwiek z rodzajów działalności gospodarczej, o których mowa w sekcji C dział 30 klasyfikacji NACE Rev. 2
Dostawcy usług cyfrowych		Dostawca internetowej platformy handlowej
		Dostawca wyszukiwarki internetowej
		Dostawca platformy sieci usług społecznościowych
Badania naukowe		Organizacja badawcza
		Podmioty, o których mowa w art. 7 ust. 1 pkt 1–4, 6–7 ustawy z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce
Podmioty publiczne		samorządowe jednostki budżetowe; samorządowe zakłady budżetowe; samorządowe instytucje kultury; spółki wykonujące zadania o charakterze użyteczności publicznej w rozumieniu art. 1 ust. 2 ustawy z dnia 20 grudnia 1996 r. o gospodarce komunalnej (Dz. U. z 2021 r. poz. 679)

KATEGORIE FUNKCJI KRYTYCZNYCH DLA BEZPIECZEŃSTWA SIECI I USŁUG

LP.	OPIS FUNKCJI	IDENTYFIKACJA POWIĄZANEJ FUNKCJI SIECIOWEJ WG STANDARDÓW 3GPP
1.	Uwierzytelnianie urządzeń użytkowników i zarządzanie prawami dostępu.	AMF – Access & Mobility management Function AUSF – Authentication Server Function
2.	Przechowywanie danych kryptograficznych i identyfikacyjnych związanych z użytkownikami końcowymi.	UDM – Unified Data Management
3.	Zarządzanie łącznością z urządzeniami użytkowników i alokacja zasobów radiowych.	Radio Base Station Baseband Unit and other features such as Radio Units and antennas
4.	Ruting ruchu sieciowego pomiędzy urządzeniami użytkownika a sieciami i aplikacjami innych firm.	UPF – User Plane Function
5.	Zarządzanie połączeniami ze sprzętem użytkownika i sesjami.	SMF – Session Management Function
6.	Wdrażanie, zarządzanie i monitorowanie polityk dostępu do sieci.	PCF – Policy Control Function
7.	Przydzielanie elementu sieci dla połączeń z urządzeniami użytkowników.	NSSF – Network Slice Selection Function
8.	Rejestrowanie, autoryzacja i utrzymanie ciągłości usług sieciowych.	NRF – Network Repository Function
9.	Zabezpieczenia sieci przed oddziaływaniem aplikacji zewnętrznych.	NEF – Network Exposure Function
10.	Zabezpieczenia połączeń z innymi sieciami.	SEPP – Security Edge Protection Proxy

**WYMOGI DLA SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI DLA
PODMIOTU WAŻNEGO BĘDĄCEGO PODMIOTEM PUBLICZNYM**

- I. System zarządzania bezpieczeństwem informacji dla podmiotu ważnego będącego podmiotem publicznym obejmuje co najmniej:
- 1) inwentaryzację produktów ICT, usług ICT i procesów ICT służących do przetwarzania informacji;
 - 2) kontrolowanie podstawowych wersji używanego produktów ICT lub usług ICT, a jeżeli to możliwe, korzystanie z mechanizmów kontroli instalacji produktów ICT lub usług ICT na urządzeniach, w tym na urządzeniach mobilnych;
 - 3) zapewnienie ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, w zakresie:
 - a) ochrony fizycznej miejsc, w których jest przetwarzana informacja, w przypadku przetwarzania danych w urządzeniach znajdujących się pod kontrolą podmiotu,
 - b) ochrony wykorzystującej oprogramowanie zabezpieczające lub sprzętowe zabezpieczenia, w które są wyposażone urządzenia przetwarzające informacje, albo
 - c) udokumentowania mechanizmów zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami w przypadku korzystania z usług dostawcy chmury obliczeniowej lub dostawcy usługi centrum przetwarzania danych;
 - 4) dopuszczenie do informacji wyłącznie osób posiadających stosowne uprawnienia do systemów informacyjnych (w tym systemów operacyjnych, usług sieciowych i aplikacji) oraz zapewnienie środków uniemożliwiających nieautoryzowany dostęp do tych systemów;
 - 5) stosowanie zasad przyznania minimalnych uprawnień niezbędnych dla realizacji zadań;
 - 6) bezzwłoczne cofanie przyznanych uprawnień w przypadku stwierdzenia braku podstawy dostępu do informacji na stałe lub zawieszanie uprawnień w przypadku niewykonywania obowiązków co najmniej przez jeden miesiąc;
 - 7) modyfikację zakresu przyznanych uprawnień, jeżeli jest to zasadne z uwagi na zmianę charakteru wykonywanych zadań i zakresu dostępu do informacji;
 - 8) ustanowienie podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość;

- 9) kontrolę usług poczty elektronicznej wykorzystującej mechanizmy, o których mowa w art. 24 ust. 1 ustawy z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej;
- 10) wykonywanie zapasowych kopii danych odseparowanych logicznie i fizycznie od danych przetwarzanych w systemach informacyjnych dla realizacji zadania publicznego;
- 11) testowanie pod kątem kompletności i możliwości odtworzenia danych zawartych w zapasowych kopiach;
- 12) przygotowanie i testowanie procedury w przypadku wystąpienia awarii lub incydentu;
- 13) stosowanie oprogramowania antywirusowego;
- 14) stosowanie zasad cyberhigieny przez pracowników korzystających z systemów informacyjnych, w tym kierownika podmiotu;
- 15) monitorowanie częstotliwości wydawania kolejnych wersji produktów ICT, źródeł dystrybucji produktów ICT oraz cyklu życia produktów ICT w celu zapewnienia bezpieczeństwa systemu informacyjnego;
- 16) stosowanie stabilnych wersji produktów ICT lub usług ICT, w stosunku do których nie występują informacje o krytycznych podatnościach, a w przypadku ich wystąpienia dopuszczalne jest stosowanie tych wersji produktów ICT lub usług ICT, które nie stwarzają istotnego negatywnego wpływu na poziom bezpieczeństwa systemów informacyjnych;
- 17) stosowanie środków minimalizujących wystąpienie incydentów przez szkolenie osób zaangażowanych w proces przetwarzania informacji, ze szczególnym uwzględnieniem takich zagadnień, jak:
 - a) rodzaje cyberzagrożeń,
 - b) podstawowe zasady cyberhigieny,
 - c) reagowania na wystąpienie incydentu,
 - d) świadomość skutków naruszenia zasad bezpieczeństwa informacji.

II. System zarządzania bezpieczeństwem informacji dla podmiotu ważnego będącego podmiotem publicznym może dodatkowo obejmować:

- 1) stosowanie środków zapewniających bezpieczeństwo informacji, w tym produktów ICT, usług ICT lub procesów ICT minimalizujących ryzyko błędów ludzkich;
- 2) stosowanie dedykowanych usług poczty elektronicznej dla podmiotu na podstawie umowy lub w ramach wspólnego wykonywania obowiązków z zakresu cyberbezpieczeństwa przy pomocy jednostki wyznaczonej, o której mowa w art. 16d;

- 3) zapewnienie wysokiej dostępności systemów informacyjnych:
 - a) w zakresie określenia czasu dostępu do systemów informacyjnych,
 - b) przez zapewnianie zdolności działania systemu informacyjnego i jego dostępności niezależnie od wystąpienia awarii lub incydentu;
- 4) określanie i kontrolowanie zasad korzystania przez podmiotu publicznego będącego podmiotem ważnym z:
 - a) ogólnodostępnych usług dostawców chmury obliczeniowej,
 - b) usług ogólnodostępnych dużych generatywnych modeli sztucznej inteligencji;
- 5) monitorowanie dostępu do informacji oraz stanu działania systemów informacyjnych za pomocą dedykowanego oprogramowania wykorzystywanego przez pracowników albo korzystanie w tym zakresie z usług dostawcy usług zarządzanych w zakresie cyberbezpieczeństwa;
- 6) testowanie poziomów bezpieczeństwa systemów informacyjnych oraz zasad cyberhigieny przez pracowników;
- 7) zawieranie w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa systemów informacyjnych;
- 8) zapewnienie aktualności wykorzystywanych produktów ICT oraz usług ICT;
- 9) stosowanie dodatkowych środków technicznych i organizacyjnych, jeżeli jest to konieczne dla zapewnienia odpowiedniego poziomu bezpieczeństwa systemów informacyjnych.

III. Podmiot ważny będący podmiotem publicznym dokonuje przeglądu systemu zarządzania bezpieczeństwem informacji:

- 1) co najmniej raz w roku albo
- 2) bezzwłocznie w przypadku wydania przez Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa rekomendacji, w zakresie, w jakim dotyczy ona systemów informacyjnych, produktów ICT lub usług ICT podmiotu, albo
- 3) bezzwłocznie w przypadku wystąpienia okoliczności, które mogą wpłynąć na ryzyko wystąpienia incydentu poważnego i wymagających ponownego zrealizowania działań opisanych w przyjętym systemie zarządzania bezpieczeństwem informacji lub zmian w samym systemie.

IV. Podmiot ważny będący podmiotem publicznym dokumentuje realizację działań wskazanych do realizacji w systemie zarządzania cyberbezpieczeństwa.

UZASADNIENIE

1. Wstęp

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077 i 1222 oraz z 2025 r. poz. 1017 i 1069), zwana dalej „ustawą o KSC”, tworzy podstawy prawno-instytucjonalne dla cyberbezpieczeństwa na poziomie krajowym. Ustawa o KSC jest implementacją dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. Urz. UE. L 2016/1148 z 19.07.2016), zwanej dalej „dyrektywą NIS”.

Krajowy system cyberbezpieczeństwa tworzy wiele podmiotów, przede wszystkim operatorzy usług kluczowych, dostawcy usług cyfrowych oraz podmioty publiczne, na które nałożono obowiązki związane z zapewnieniem bezpieczeństwa informacji, a także obsługą incydentów. Operatorzy usług kluczowych zostali podzieleni według sektorów i podsektorów wskazanych w załączniku nr 1 do ustawy o KSC. Dla każdego sektora ustanowiono organ właściwy do spraw cyberbezpieczeństwa, zwany dalej „organem właściwym”, który odpowiada za identyfikację i wyznaczanie operatorów usług kluczowych oraz nadzór i kontrolę nad przestrzeganiem przepisów ustawy o KSC w danym sektorze.

Obecnie ani przedsiębiorcy telekomunikacyjni, ani dostawcy usług zaufania nie są podmiotami krajowego systemu cyberbezpieczeństwa.

Incydenty wpływające na działalność operatorów usług kluczowych (incydenty poważne) i dostawców usług cyfrowych (incydenty istotne), a także incydenty w podmiotach publicznych, są raportowane do jednego z trzech krajowych zespołów reagowania na incydenty bezpieczeństwa komputerowego, zwanych dalej „CSIRT”. Do zadań zespołów CSIRT należy m.in. klasyfikowanie incydentów jako krytyczne. Ustawa o KSC usankcjonowała istnienie trzech zespołów na poziomie krajowym – CSIRT GOV (działającego w Agencji Bezpieczeństwa Wewnętrznego), CSIRT NASK (działającego w Naukowej i Akademickiej Sieci Komputerowej – Państwowym Instytucie Badawczym, zwanym dalej „NASK-PIB”) oraz CSIRT MON (prowadzonego przez Ministra Obrony Narodowej). Zespoły CSIRT współpracują ze sobą w ramach Zespołu do spraw incydentów krytycznych.

1.1. Sektorowe zespoły cyberbezpieczeństwa

Organ właściwy może powołać sektorowy zespół cyberbezpieczeństwa. Zespół ten odpowiada za wsparcie obsługi incydentów u operatorów usług kluczowych w konkretnym sektorze lub podsektorze. Do tej pory powołano tylko dwa takie zespoły, tj. CSIRT KNF (zespół dla sektora finansowego), funkcjonujący przy Komisji Nadzoru Finansowego¹⁾, oraz Centrum e-Zdrowie²⁾ (w sektorze ochrony zdrowia).

1.2. Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa

Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa, zwany dalej „Pełnomocnikiem”, jest odpowiedzialny za koordynowanie działań i realizowanie polityki rządu w zakresie zapewnienia cyberbezpieczeństwa w Rzeczypospolitej Polskiej. Pełnomocnik, w randze ministra, sekretarza stanu albo podsekretarza stanu, jest powoływany i odwoływany przez Prezesa Rady Ministrów. Do jego zadań należy zarówno analiza i ocena funkcjonowania krajowego systemu cyberbezpieczeństwa (dokonywana na podstawie zagregowanych danych i wskaźników opracowanych przy udziale organów administracji państwowej, organów właściwych i zespołów CSIRT), jak i nadzór nad procesem zarządzania ryzykiem krajowego systemu cyberbezpieczeństwa z wykorzystaniem zagregowanych danych i wskaźników opracowanych przy udziale organów właściwych i zespołów CSIRT. Pełnomocnik jest ponadto odpowiedzialny za opiniowanie projektów aktów prawnych oraz innych dokumentów rządowych mających wpływ na realizację zadań z zakresu cyberbezpieczeństwa. Inicjuje także krajowe ćwiczenia z zakresu cyberbezpieczeństwa.

1.3. Kolegium do Spraw Cyberbezpieczeństwa

Kolegium do Spraw Cyberbezpieczeństwa, zwane dalej „Kolegium”, jest organem opiniodawczo-doradczym w sprawach planowania, nadzorowania i koordynowania działalności zespołów CSIRT, sektorowych zespołów cyberbezpieczeństwa oraz organów właściwych. Kolegium opiniuje sprawy planowane do ustalenia przez Prezesa Urzędu Komunikacji Elektronicznej w projekcie rozstrzygnięcia decyzji w sprawie rezerwacji częstotliwości, o którym mowa w art. 110 ust. 2 ustawy z dnia 12 lipca 2024 r. – Prawo komunikacji elektronicznej (Dz. U. poz. 1221 oraz z 2025 r. poz. 637 i 820). Przewodniczącym Kolegium jest Prezes Rady Ministrów, a w jego skład wchodzi: minister właściwy do spraw

¹⁾ https://www.knf.gov.pl/dla_ryнку/CSIRT_KNF.

²⁾ <https://cez.gov.pl/pl/page/o-nas-0>.

wewnętrznych, minister właściwy do spraw informatyzacji, Minister Obrony Narodowej, minister właściwy do spraw zagranicznych, Szef Kancelarii Prezesa Rady Ministrów, Szef Biura Bezpieczeństwa Narodowego (jeżeli został wyznaczony przez Prezydenta RP), minister – członek Rady Ministrów właściwy do spraw koordynowania działalności służb specjalnych, a jeżeli nie został wyznaczony – Szef Agencji Bezpieczeństwa Wewnętrznego oraz sekretarz Kolegium. W posiedzeniach Kolegium uczestniczą także: dyrektor Rządowego Centrum Bezpieczeństwa, Szef Agencji Bezpieczeństwa Wewnętrznego, Szef Służby Kontrwywiadu Wojskowego i Dyrektor NASK-PIB. Przewodniczący Kolegium może zapraszać do udziału w posiedzeniach Kolegium także inne osoby. Po otrzymaniu rekomendacji Kolegium, Prezes Rady Ministrów, w celu koordynacji działań administracji rządowej w zakresie cyberbezpieczeństwa, może wydawać wiążące wytyczne dotyczące zapewnienia cyberbezpieczeństwa na poziomie krajowym oraz funkcjonowania krajowego systemu cyberbezpieczeństwa.

1.4. Potrzeba i cele projektu ustawy

Dyrektywa NIS utworzyła nowe ramy systemu zapewnienia cyberbezpieczeństwa w Unii Europejskiej. Wprowadziła nowe zadania państw członkowskich Unii Europejskiej w tym obszarze, rozszerzyła zakres podmiotów objętych obowiązkami w zakresie cyberbezpieczeństwa oraz zredefiniowała zadania organów Unii Europejskiej w tym obszarze. Ponadto rozszerzeniu uległ katalog sektorów objętych dyrektywą NIS 2 – obok sektorów energii, transportu, zdrowia, bankowości, infrastruktury rynków finansowych, zaopatrzenia w wodę, infrastruktury cyfrowej, w dyrektywie NIS 2 dodano następujące sektory: ścieki, zarządzanie ICT, przestrzeń kosmiczną, pocztę, produkcję, produkcję i dystrybucję chemikaliów, produkcję i dystrybucję żywności. Dyrektywa NIS 2 zastąpiła dotychczasowy podział na operatorów usług kluczowych i dostawców usług cyfrowych określony w NIS, na podmioty kluczowe i podmioty ważne. Dyrektywa NIS 2 nakłada również szereg obowiązków na podmioty kluczowe i podmioty ważne. Jako podstawowy obowiązek należy wskazać stosowanie odpowiednich i proporcjonalnych środków technicznych, operacyjnych i organizacyjnych w celu zarządzania ryzykiem dla bezpieczeństwa sieci i systemów informatycznych wykorzystywanych przez te podmioty do prowadzenia działalności lub świadczenia usług oraz w celu zapobiegania wpływowi incydentów na odbiorców ich usług lub na inne usługi bądź minimalizowania takiego wpływu.

Zmiany te zostały wprowadzone w związku z szybko postępującą transformacją cyfrową i siecią wzajemnych połączeń w społeczeństwie, w tym w kontekście wymiany

transgranicznej, sieci i systemy informatyczne stały się zasadniczym elementem codziennego życia. Zmiana ta doprowadziła do ewolucji krajobrazu cyberzagrożeń, przynosząc nowe wyzwania, które wymagają dostosowanych, skoordynowanych i innowacyjnych reakcji we wszystkich państwach członkowskich. Liczba, skala, zaawansowanie, częstotliwość oraz wpływ incydentów stają się coraz większe i stanowią poważne zagrożenie dla funkcjonowania sieci i systemów informatycznych. W rezultacie incydenty mogą utrudniać prowadzenie działalności gospodarczej na rynku wewnętrznym, powodować straty finansowe, podważać zaufanie użytkowników oraz powodować poważne szkody dla gospodarki i społeczeństw.

Są one również efektem analizy funkcjonowania dyrektywy NIS, która dotychczas regulowała te zagadnienia. Uznano, że dotychczasowe środki w tym zakresie nie są adekwatne do obecnej skali wyzwań z jakimi można zetknąć się w cyberprzestrzeni. Projektowana ustawa określa mechanizmy skutecznej współpracy między odpowiedzialnymi organami w poszczególnych sektorach gospodarki, a także określa nowe obowiązki w zakresie cyberbezpieczeństwa, jak i środki ich egzekwowania.

Ustawa o KSC nie spełnia wymogów dyrektywy NIS 2, w związku z czym wymaga ona wdrożenia do porządku krajowego.

Pojawianie się nowych cyberzagrożeń, jak również szybki wzrost katalogu usług publicznych dostępnych online, powodują, że instytucje publiczne, jak i podmioty prywatne odpowiedzialne za cyberbezpieczeństwo będą zmuszone poświęcać coraz więcej środków na zapewnienie cyberbezpieczeństwa. Zmieniająca się sytuacja międzynarodowa oraz konieczność dostarczenia usług dużej grupie nowych klientów sprawia, że niezbędne jest dalsze wzmocnianie podmiotów krajowego systemu cyberbezpieczeństwa. Tą sytuację uwidaczniają statystyki zespołu CSIRT NASK. W 2022 r. do zespołu CSIRT NASK zgłoszono ponad 39 000 incydentów cyberbezpieczeństwa, w 2023 r. ponad 75 000 incydentów cyberbezpieczeństwa, a w 2024 r. 103048 incydentów. Dyrektywa NIS 2 i przepisy ją implementujące są odpowiedzią na dynamicznie zmieniającą się sytuację w cyberprzestrzeni.

Zauważono również, że uprawnienia Pełnomocnika są niewystarczające w stosunku do zadań, które organ ten musi wypełniać. Pełnomocnikowi brakuje skutecznych środków oddziaływania na podmioty krajowego systemu cyberbezpieczeństwa. W przeciwieństwie do innych Pełnomocników Rządu, nie ma on uprawnień do żądania niezbędnych informacji od organów administracji rządowej, możliwości powoływania zespołów problemowych, czy zlecania badań. Pełnomocnikowi brakuje również środka prawnego, który umożliwiłby wydawanie

rekomendacji o charakterze technicznym (w tym zakresie – Narodowych Standardów Cyberbezpieczeństwa, o których mowa w Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024, zwanej dalej „Strategią”) i jednocześnie obowiązku uwzględnienia tych rekomendacji przez podmioty krajowego systemu cyberbezpieczeństwa, w trakcie procesu zarządzania ryzykiem.

Jak wyżej wskazano, do tej pory zostały utworzone tylko dwa sektorowe zespoły cyberbezpieczeństwa – CSIRT KNF i CSIRT Centrum e-Zdrowie. W pozostałych sektorach gospodarki brakuje zespołów wspierających przedsiębiorców w reagowaniu na incydenty. Utworzenie tych zespołów przewiduje inwestycja C3.1.1 KPO Cyberbezpieczeństwo – CyberPL, infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo, planowana jest realizacja projektu pn. „Utworzenie lub rozwój przynajmniej 5 sektorowych Zespołów Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT)”. Celem nowelizacji ustawy o KSC jest wprowadzenie uwarunkowań prawnych skutecznego funkcjonowania CSIRT sektorowych.

Coraz większe znaczenie dla bezpieczeństwa usług kluczowych ma niezawodność usług telekomunikacyjnych. Stacjonarne sieci szerokopasmowe są uzupełniane przez sieci mobilne nowej generacji (sieci 5G i kolejnych generacji). Komisja Europejska wielokrotnie, m.in. w opublikowanych w marcu 2019 r. zaleceniach dot. cyberbezpieczeństwa sieci 5G, podkreślała, że kwestia zapewnienia bezpieczeństwa wdrażanej technologii 5G jest priorytetem. Potwierdzenie powyższego znajduje odzwierciedlenie w opublikowanym w styczniu 2020 r. zestawie środków dot. minimalnej harmonizacji i standaryzacji na poziomie Unii Europejskiej rozwiązań cyberbezpieczeństwa sieci 5G, określanym jako 5G Toolbox³⁾. Zestawienie to obejmuje zarówno rozwiązania o charakterze strategicznym, technicznym, jak i o charakterze wspierającym. Celami 5G Toolbox są po pierwsze bezpieczeństwo sieci 5G, a po drugie uspoźnienie polityk państw członkowskich Unii Europejskiej w obszarze bezpieczeństwa technologii 5G.

5G Toolbox definiuje zestaw środków zabezpieczających na poziomie strategicznym i technicznym oraz wskazuje działania wspierające stosowanie tych środków, niezbędne do ograniczenia ryzyk cyberbezpieczeństwa w sieciach 5G, które będą podstawą Jednolitego

³⁾ *Cybersecurity of 5G networks. EU Toolbox of risk mitigating measures*, <https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures>.

Rynku Cyfrowego Unii Europejskiej. Wśród opisanych w 5G Toolbox środków strategicznych, technicznych i wspierających są środki o charakterze:

- strategicznym – m.in. większe uprawnienia dla organów właściwych, w tym w zakresie oceny bezpieczeństwa łańcucha dostaw, większe wymagania dla przedsiębiorców telekomunikacyjnych oraz ocena ryzyka dostawców sprzętu lub oprogramowania,
- technicznym – m.in. badanie bezpieczeństwa oprogramowania i urządzeń – czego odzwierciedleniem są na gruncie prawa krajowego uprawnienia Pełnomocnika oraz zespołów CSIRT poziomu krajowego, CSIRT MON, CSIRT NASK, CSIRT GOV wynikające z art. 33 ustawy o KSC,
- wspierającym – m.in. dotyczące prac nad europejskim programem standaryzacji i certyfikacji cyberbezpieczeństwa.

Wprowadzenie zmian do ustawy o KSC jest elementem działań na rzecz wdrożenia zaleceń z 5G Toolbox w Polsce.

1.5. Skutki gospodarcze

Celem projektowanych zmian jest wzmocnienie krajowego systemu cyberbezpieczeństwa. Wprowadzane w projekcie ustawy rozwiązania zobowiązują m.in. przedsiębiorców w poszczególnych sektorach gospodarki do dbania o cyberbezpieczeństwo. Skutkiem projektowanych przepisów może być konieczność poniesienia dodatkowych kosztów związanych z dostosowaniem się poszczególnych podmiotów krajowego systemu cyberbezpieczeństwa do wymogów wynikających z ustawy o KSC. Należy zauważyć, że wielu przedsiębiorców już obecnie posiada systemy zarządzania bezpieczeństwem informacji. Dzięki dalszemu inwestowaniu przez podmiot we własne cyberbezpieczeństwo zyskuje on zaufanie podmiotów, którym świadczy usługi i potencjalnych kontrahentów.

Dostosowanie się do nowych wymogów pozwoli przedsiębiorcom zwiększyć skuteczność działań podejmowanych przez przedsiębiorców w zakresie cyberbezpieczeństwa w ich działalności, co przełoży się na bezpieczne prowadzenie biznesu i minimalizację ryzyka strat.

1.6. Skutki społeczne

Nałożenie nowych obowiązków z zakresu cyberbezpieczeństwa na większą liczbę podmiotów przyczyni się do zwiększenia bezpieczeństwa usług, z których korzystają wszyscy obywatele. Zwiększy to pewność ciągłości usług. Polepszy się ochrona danych osobowych

przetwarzanych przez podmioty ważne i podmioty kluczowe. Część kosztów wypełnienia obowiązków ustawowych, w przypadku niektórych sektorów, może przełożyć się na wyższy koszt usługi dla odbiorcy końcowego.

Powołanie CSIRT sektorowych pozwoli na utworzenie jednostek, dzięki którym usprawnione zostanie funkcjonowanie i zwiększona skuteczność systemu reagowania na incydenty. Ponadto, dzięki powołaniu CSIRT sektorowego, w każdym sektorze powstanie baza wiedzy o cyberzagrożeniach i podatnościach danego sektora. Funkcjonowanie CSIRT sektorowych wpłynie na skrócenie czasu obsługi incydentów w sektorze, które będą obsługiwane z uwzględnieniem szczególnych uwarunkowań danego sektora.

1.7. Skutki finansowe

Tworzenie nowych struktur w ramach krajowego systemu cyberbezpieczeństwa będzie wymagało dodatkowych nakładów finansowych. Jest to inwestycja w bezpieczeństwo państwa. Incydenty bezpieczeństwa komputerowego są coraz częstsze i bardziej zaawansowane.

Szkody powstałe wskutek tych działań (np. zaszyfrowanie danych, wykradzenie danych, uniemożliwienie lub utrudnienie świadczenia usług publicznych) są bardzo poważne i często mają również istotny wymiar finansowy. Inwestycja w dostosowanie krajowego systemu cyberbezpieczeństwa do wyzwań wynikających z postępującej gwałtownie cyfryzacji pozwoli ograniczyć prawdopodobieństwo powstania tych szkód, a w przypadku ataków – znacząco zmniejszyć ich negatywne skutki. Wobec powyższego poniesienie dodatkowych nakładów finansowych jest jak najbardziej zasadne.

Ze względu na odwołania w samej dyrektywie NIS 2 do dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE (Dz. Urz. UE L 2022/2557 z 27.12.2022), zwanej dalej „dyrektywą CER”, oraz rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (Dz. Urz. UE L 2022/2554 z 27.12.2022), zwanego dalej „rozporządzeniem DORA” – projekt ustawy będzie

ulegał zmianom, głównie w obszarze siatki pojęciowej, mającym na celu dostosowanie projektu do regulacji transponujących rozporządzenie DORA⁴⁾ oraz dyrektywę CER⁵⁾.

2. Uzasadnienie poszczególnych przepisów

2.1. Zmiany w odnośnikach

W obowiązującej ustawie o KSC konieczna była korekta odnośnika. Aktualny odnośnik odwołuje się do dyrektywy NIS, która już nie obowiązuje. Odnośnik ten został zastąpiony nowym odnośnikiem nr 1, wskazującym, że ustawa o KSC wdraża dyrektywę Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniającą rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającą dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz. Urz. UE L 333 z 27.12.2022, str. 80). Ponadto został dodany nowy odnośnik nr 2, zgodnie z którym ustawa o KSC służy częściowemu stosowaniu rozporządzenia delegowanego Komisji (UE) 2024/1366 z dnia 11 marca 2024 r. uzupełniającego rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/943 poprzez ustanowienie kodeksu sieci dotyczącego zasad sektorowych w zakresie aspektów cyberbezpieczeństwa w transgranicznych przepływach energii elektrycznej (Dz. Urz. UE L 2024/1366 z 24.05.2024).

2.2. Zmiany w przepisach ogólnych

2.2.1. Zakres przedmiotowy i podmiotowy ustawy

Aktualny przepis art. 1 ustawy o KSC jest napisany w sposób ogólny. Dlatego nie wymaga większych zmian. Do zakresu przedmiotowego dodano kolejny punkt wskazujący, że ustawa określa również zakres Krajowego planu reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę. Jest to nowy rodzaj dokumentu przewidziany przez dyrektywę NIS 2, stąd też należy uzupełnić zakres przedmiotowy ustawy. Usunięto przepis wyłączający stosowanie ustawy do przedsiębiorców telekomunikacyjnych oraz dostawców usług zaufania. Obydwa rodzaje podmiotów podlegają pod dyrektywę NIS 2 i należy je również uwzględnić w ustawie.

⁴⁾ Projekt ustawy o zmianie niektórych ustaw w związku z zapewnieniem operacyjnej odporności cyfrowej sektora finansowego (UC11) <https://legislacja.rcl.gov.pl/projekt/12384252>.

⁵⁾ Projekt ustawy o zmianie ustawy o zarządzaniu kryzysowym oraz niektórych innych ustaw <https://legislacja.rcl.gov.pl/projekt/12386961>.

2.2.2. Definicje

Zmiany w zakresie definicji ustawowych wynikają ze zmian w siatce pojęciowej jakie wprowadziła dyrektywa NIS 2. W związku z tym konieczna była zmiana części definiowanych pojęć, usunięcie przestarzałych terminów oraz dodanie nowych. Wprowadzone zmiany zapewnią spójność siatki pojęciowej wykorzystywanej we wszystkich krajach Unii Europejskiej.

1) *CSIRT sektorowy*

Wprowadzono definicję CSIRT sektorowego – jest to Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie sektora lub podsektora, ustanowiony przez organ właściwy do spraw cyberbezpieczeństwa dla danego sektora lub podsektora. Wprowadzenie definicji było konieczne, ponieważ istnieją już w ustawie o KSC definicje zespołów CSIRT. CSIRT sektorowy może być powołany również dla podsektora, ponieważ mamy podsektory, dla których są odrębne organy właściwe do spraw cyberbezpieczeństwa, np. podsektor transportu wodnego.

2) *Abonent nazwy domeny*

Z uwagi na uwzględnienie w projekcie ustawy kwestii obowiązków rejestrów nazw domen najwyższego poziomu oraz podmiotów świadczących usługi rejestracji nazw domen zaszła konieczność wprowadzenia definicji abonenta nazwy domeny. Tworząc tą definicję odwzorowano stosunki prawne, jakie zachodzą przy rejestracji domeny. Abonentem jest więc podmiot (osoba fizyczna, osoba prawna, ułomna osoba prawna), który jest stroną umowy o utrzymywanie nazwy domeny (por. https://www.dns.pl/regulamin_nazw_domeny_pl) zawartej z rejestrem nazw domen najwyższego poziomu (TLD) za pośrednictwem podmiotu świadczącego usługi rejestracji nazw domen.

3) *Adres do doręczeń elektronicznych*

Definicja adresu do doręczeń elektronicznych okazała się konieczna, ponieważ pojawia się w kilku przepisach projektu ustawy. Tworząc tą definicję wprowadzono odesłanie dynamiczne do ustawy z dnia 18 listopada 2020 r. o doręczeniach elektronicznych (Dz. U. z 2024 r. poz. 1045 i 1841).

4) *Bezpieczeństwo systemów informacyjnych*

Dyrektywa NIS 2 odwołuje się do dwóch pojęć – bezpieczeństwa sieci i systemów informatycznych oraz cyberbezpieczeństwa. Bezpieczeństwo sieci i systemów odnosi się do odporności – jest to: odporność sieci i systemów informatycznych, przy danym poziomie zaufania, na wszelkie zdarzenia, które mogą naruszyć dostępność, autentyczność, integralność

lub poufność przechowywanych, przekazywanych lub przetwarzanych danych lub usług oferowanych przez te sieci i systemy informatyczne lub dostępnych za ich pośrednictwem. Ten zakres pojęciowy w obecnej ustawie o KSC był odzwierciedlony w definicji „cyberbezpieczeństwa”. Jednakże dyrektywa NIS 2 odmiennie definiuje cyberbezpieczeństwo – odwołuje się przy tym do aktu o cyberbezpieczeństwie, który stanowi, że „cyberbezpieczeństwo” oznacza działania niezbędne do ochrony sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób przed cyberzagrożeniami. Jest to podejście od drugiej strony, aktywne podejście.

Z tych powodów dotychczasową definicję cyberbezpieczeństwa zachowuje się, ale pod nazwą „bezpieczeństwa systemów informacyjnych”, aby zapewnić zgodność z dyrektywą NIS 2.

5) Cyberbezpieczeństwo

Z uwagi na to, że dotychczasowe pojęcie „cyberbezpieczeństwa” zostaje zastąpione „bezpieczeństwem systemów informacyjnych”, to odpowiednio dostosowuje się definicję incydentu – jest to zdarzenie, które ma lub może mieć niekorzystny wpływ na bezpieczeństwo systemów informacyjnych.

Definicja cyberbezpieczeństwa odnosi się do definicji zawartej w unijnym akcie o cyberbezpieczeństwie.

6) Cyberzagrożenie

Definicja cyberzagrożenia odwołuje się do definicji zawartej w unijnym akcie o cyberbezpieczeństwie. Brzmi ona następująco: *oznacza wszelkie potencjalne okoliczności, zdarzenie lub działanie, które mogą wyrządzić szkodę, spowodować zakłócenia lub w inny sposób niekorzystnie wpłynąć w przypadku sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób*. Zauważyć należy, że jest to definicja szeroka, która obejmuje całe spektrum zagrożeń, w tym także zagrożenia o charakterze fizycznym i środowiskowym. Pokazując to na całkiem realnym przykładzie – zdarza się czasem, że serwerownia jest w pomieszczeniu, które nie jest zamknięte i dostęp fizyczny mają do niej wszyscy – pracownicy czy interesariusze podmiotu. Jest to niewątpliwe cyberzagrożenie – każdy może uzyskać dostęp i chociażby wyjąć okablowanie lub przeprowadzić atak man in the middle.

Zasłała potrzeba zdefiniowania szeregu rodzajów podmiotów, które funkcjonują w sektorze infrastruktury cyfrowej.

7) Dostawca sieci dostarczania treści

Dostawca sieci dostarczania treści jest potocznie znany jako CDN – content delivery network provider. Często użytkownik internetu chce skorzystać ze strony internetowej, której serwer znajduje się bardzo daleko od fizycznej lokalizacji tego użytkownika. Powoduje to opóźnienia w dostępie do stron internetowych. Aby temu zapobiec powstały serwery content delivery network. Serwery te są rozmieszczone w różnych lokalizacjach i zawierają kopię treści z oryginalnego serwera. Użytkownik internetu zamiast łączyć się z oryginalnym serwerem łączy się z serwerem CDN, dostając tą samą treść w krótszym czasie aniżeli gdyby łączył się z oryginalnym serwerem. Serwery CDN umożliwiają rozładowanie ruchu w internecie.

Nawiązując do dyrektywy NIS 2 wskazano, że dostawcą sieci dostarczania treści jest osoba fizyczna, osoba prawna albo jednostka organizacyjna nieposiadająca osobowości prawnej, która dostarcza treści i usługi cyfrowe do sieci rozproszonych geograficznie serwerów służących zapewnieniu wysokiej i łatwej dostępności tych treści i usług cyfrowych lub ich szybkiego dostarczania na rzecz użytkowników internetu w imieniu dostawców treści i usług, jednakże z wyłączeniem przedsiębiorców komunikacji elektronicznej. Wielu przedsiębiorców komunikacji elektronicznej tworzy własne CDN, stąd też uznano, że warto tutaj rozgraniczyć te definicje. Przedsiębiorcy komunikacji elektronicznej i świadczone przez nich usługi podlegają reżimowi ustawy – ich usługi CDN też będą podlegać pod reżim ustawy jako usługi komunikacji elektronicznej.

8) Dostawca sprzętu lub oprogramowania

Nowością jest definicja dostawcy sprzętu lub oprogramowania – tutaj projekt ustawy odwołuje się do art. 2 pkt 3–6 rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 765/2008 z dnia 9 lipca 2008 r. ustanawiającego wymagania w zakresie akredytacji i uchylającego rozporządzenie (EWG) nr 339/93 (Dz. Urz. UE L 218 z 13.08.2008, str. 30, z późn. zm.), zwanego dalej „rozporządzeniem 765/2008”. Zgodnie z rozporządzeniem 765/2008, dostawcą jest:

- producent – każda osoba fizyczna lub prawna, która wytwarza produkt lub która zleca zaprojektowanie lub wytworzenie produktu i oferuje ten produkt pod własną nazwą lub znakiem towarowym,
- upoważniony przedstawiciel – osoba fizyczna lub prawna mająca siedzibę w Unii Europejskiej, posiadająca pisemne pełnomocnictwo od producenta do występowania w jego imieniu w zakresie określonych zadań w odniesieniu do obowiązków producentów wynikających z odpowiedniego prawodawstwa wspólnotowego,

– importer – każda osoba fizyczna lub prawna, mająca siedzibę w Unii Europejskiej, wprowadzająca na rynek wspólnotowy produkt z kraju trzeciego

lub

– dystrybutor – każda osoba fizyczna lub prawna w łańcuchu dostaw, inna niż producent lub importer, która udostępnia produkt na rynku.

Definicja jest wprowadzana w związku z przepisami dotyczącymi systemu zarządzania bezpieczeństwem informacji, a także przepisami odnoszącymi się do postępowania w sprawie uznania za dostawcę wysokiego ryzyka.

9) Dostawca internetowej platformy handlowej

Dostawca internetowej platformy handlowej to osoba fizyczna, osoba prawna albo jednostka organizacyjna nieposiadająca osobowości prawnej, która dostarcza internetową platformę handlową w rozumieniu art. 2 pkt 8 ustawy z dnia 30 maja 2014 r. o prawach konsumenta (Dz. U. z 2024 r. poz. 1796 oraz z 2025 r. poz. 1172). Zgodnie z tą ustawą (i prawodawstwem unijnym) internetowa platforma handlowa to usługa korzystająca z oprogramowania, w tym ze strony internetowej, z części strony internetowej lub aplikacji, obsługiwanego przez przedsiębiorcę lub w jego imieniu, w ramach której umożliwia się:

- a) konsumentom zawieranie z innymi przedsiębiorcami umów na odległość lub
- b) osobom fizycznym niebędącym przedsiębiorcami zawieranie umów na odległość z innymi osobami fizycznymi niebędącymi przedsiębiorcami. Podsumowując, internetowa platforma handlowa to nie jest tylko „tablica z ogłoszeniami” tylko usługa, która pozwala za pomocą internetu zawierać umowy na odległość między osobami fizycznymi lub między konsumentami a przedsiębiorcami.

10) Dostawca chmury obliczeniowej

Definicja dostawcy usług chmurowych obejmuje m.in. usługi w modelu infrastruktura jako usługa (IaaS), platforma jako usługa (PaaS), oprogramowanie jako usługa (SaaS) oraz sieć jako usługa (NaaS) co jest zgodne z motywem 33 dyrektywy NIS 2. Definicja ta jest przy tym na tyle szeroka, aby w sposób adekwatny odpowiadać na rozwój technologii chmurowych. Usługi chmurowe mogą być świadczone w chmurze prywatnej, publicznej, hybrydowej, czy wspólnotowej. Chmura obliczeniowa charakteryzuje się m.in. podzieloną odpowiedzialnością pomiędzy dostawcę i odbiorcę usług, szybkim udostępnianiem zasobów, samoobsługą na żądanie, szerokim dostępem do sieci, dynamicznym gromadzeniem zasobów oraz ich szybkim oraz elastycznym przydzielaniem i zwalnianiem, pomiarem i optymalizacją usług.

11) Dostawca usług DNS

Dostawca usług DNS to podmiot, który świadczy dostępne publicznie: rekurencyjne usługi rozpoznawania nazw domen na rzecz ogółu użytkowników końcowych internetu lub autorytatywne usługi rozpoznawania nazw domen do użytku ogółu użytkowników końcowych internetu z wyjątkiem głównych serwerów nazw⁶⁾.

System DNS umożliwia zamianę adresów IP na nazwę domen, dzięki czemu użytkownicy Internetu mogą żądać dostępu do danej strony internetowej wpisując jej nazwę w przeglądarce zamiast adresu IP. System DNS jest niezbędny do zapewnienia funkcjonowania internetu. Autorytatywne serwery DNS przechowują informacje o danej domenie. Z kolei rekurencyjne serwery DNS obsługują zapytania użytkowników internetu – poszukują prawidłowego adresu IP dla danej domeny⁷⁾. Zakłócenie funkcjonowania serwerów DNS utrudnia lub uniemożliwia korzystanie z internetu przez jego użytkowników. Stąd też dyrektywa NIS 2 uznała wszystkie tego rodzaju podmioty jako podmioty kluczowe. Jednocześnie zauważyć należy, że część przedsiębiorców telekomunikacyjnych, jako dostawcy usługi dostępu do internetu, również świadczy usługi DNS ale tylko dla swoich klientów. Czyli nie świadczy tych usług generalnie, dla wszystkich. Dlatego też doprecyzowano w definicji, że dostawcą usług DNS jest podmiot, który świadczy te usługi do użytku ogółu użytkowników końcowych internetu, co lepiej oddaje sens dyrektywy NIS 2.

⁶⁾ Tych 13 serwerów i ich operatorzy są dostępni na stronie <https://www.iana.org/domains/root/servers>. Głównie są to podmioty amerykańskie ale też i RIPE NCC z siedzibą w Amsterdamie.

⁷⁾ Szerzej i dokładniej opisuje to *Domain names - concepts and facilities, Request for Comments, RFC 1034*, Internet Engineering Task Force, 1987, <https://datatracker.ietf.org/doc/html/rfc1034>, w pkt 2.4: The DNS has three major components:

- The DOMAIN NAME SPACE and RESOURCE RECORDS, which are specifications for a tree structured name space and data associated with the names. Conceptually, each node and leaf of the domain name space tree names a set of information, and query operations are attempts to extract specific types of information from a particular set. A query names the domain name of interest and describes the type of resource information that is desired. For example, the Internet uses some of its domain names to identify hosts; queries for address resources return Internet host addresses.

- NAME SERVERS are server programs which hold information about the domain tree's structure and set information. A name server may cache structure or set information about any part of the domain tree, but in general a particular name server has complete information about a subset of the domain space, and pointers to other name servers that can be used to lead to information from any part of the domain tree. Name servers know the parts of the domain tree for which they have complete information; a name server is said to be an AUTHORITY for these parts of the name space. Authoritative information is organized into units called ZONES, and these zones can be automatically distributed to the name servers which provide redundant service for the data in a zone.

- RESOLVERS are programs that extract information from name servers in response to client requests. Resolvers must be able to access at least one name server and use that name server's information to answer a query directly, or pursue the query using referrals to other name servers. A resolver will typically be a system routine that is directly accessible to user programs; hence no protocol is necessary between the resolver and the user program.”.

12) Dostawca usługi centrum przetwarzania danych

Dostawca usługi centrum przetwarzania danych obejmuje podmioty świadczące usługę data center. Przez strukturę lub grupę struktur przeznaczonych do scentralizowanego hostingu, zapewniania wzajemnego połączenia i eksploatacji produktów ICT, usług ICT lub procesów ICT służącego do świadczenia usług przechowywania, przetwarzania i transportu danych wraz ze wszystkimi obiektami i całą infrastrukturą, zapewniającymi dystrybucję energii elektrycznej i kontrolę środowiskową należy m.in. rozumieć ośrodki obliczeniowe będące obiektami budowlanymi składającymi się z budynków, budowli, obiektów małej architektury, urządzeń budowlanych, wyposażenia oraz infrastruktury, którego podstawowym przeznaczeniem jest zgrupowanie pomieszczeń, połączeń i obsługi urządzeń techniki informatycznej oraz sieci telekomunikacyjnych zapewniających usługi przechowywania, przetwarzania i dostarczania danych.

13) Dostawca usług zarządzanych oraz dostawca usług zarządzanych w zakresie cyberbezpieczeństwa

Dyrektywa NIS 2 nałożyła wymogi z zakresu cyberbezpieczeństwa na podmioty świadczące usługi zarządzane. Wyróżniamy tutaj dwie definicje: dostawca usług zarządzanych i dostawa usług w zakresie cyberbezpieczeństwa. Definicja dostawcy usług zarządzanych obejmuje podmioty, które wspierają inne podmioty w codziennym korzystaniu z produktów ICT, usług ICT, czy procesów ICT przez pomoc przy ich instalacji, eksploatacji czy konserwacji. Wsparcie to jest prowadzone na miejscu u klienta lub zdalnie. Często wiąże się z tym aktywna administracja tymi zasobami.

Definicja dostawcy usług zarządzanych w zakresie cyberbezpieczeństwa, to podmiot zajmujący się testami bezpieczeństwa, audytami, doradztwem w zakresie cyberbezpieczeństwa i obsługą incydentów. Odnośnie do doradztwa to nie należy tutaj obejmować usług prawnych jako takich, ponieważ usługi te z reguły nie obejmują pozostałych aspektów zarządzania ryzykiem.

Raport ENISA⁸⁾ identyfikuje następujące usługi świadczone przez dostawców usług zarządzanych w zakresie cyberbezpieczeństwa:

Rozwiązania bezpieczeństwa i usługi techniczne:

- zarządzanie tożsamością i dostępem, w tym zarządzanie uprawnieniami,

⁸⁾ European Union Agency for Cybersecurity, MSS market analysis: an analysis of managed security service market, Publications Office of the European Union, Publications Office of the European Union 2025. <https://op.europa.eu/en/publication-detail/-/publication/185b9736-5306-11f0-a9d0-01aa75ed71a1/language-en>

- zarządzane bezpieczeństwem danych, w tym zapobieganie utracie danych, zarządzanie tworzenie kopii zapasowych i zarządzanie ciągłością działania,
- zarządzanie bezpieczeństwem urządzeń końcowych (endpoint),
- bezpieczeństwo *network perimeter* i infrastruktury, w tym systemy wykrywania włamań, systemy zapobiegania włamaniom, zapory sieciowe i bezpieczne usługi dostępne,
- zarządzane wykrywanie i reagowanie, w tym zarządzane informacje dotyczące bezpieczeństwa i zdarzeń, wykrywanie zagrożeń i inżynieria odwrotna,
- usługi oceny technicznej, w tym skanowanie podatności i testy penetracyjne,
- usługi zarządzania zagrożeniami, w tym wymiana informacji o cyberzagrożeniach,
- zarządzanie bezpieczeństwem chmury.

Usługi doradcze i wdrożeniowe:

- ocena zgodności;
- audyt i raportowanie,
- zarządzanie ryzykiem,
- opracowywanie symulacji lub ćwiczeń, w tym tworzenie, testowanie i ulepszanie ćwiczeń w zakresie wykrywania incydentów i reagowania na nie,
- ocena dojrzałości i polityki,
- wdrożenie.

Usługi szkoleniowe:

- symulacje lub ćwiczenia, w tym poprzez udział personelu w ćwiczeniach,
- podnoszenie świadomości pracowników w zakresie bezpieczeństwa.

14) Dostawca usług zaufania

Definicja dostawcy usług zaufania odwołuje się do rozporządzenia EIDAS. Oznacza ona osobę fizyczną lub prawną, która świadczy przynajmniej jedną usługę zaufania, jako kwalifikowany lub niekwalifikowany dostawca usług zaufania. Rodzaje usług zaufania zostały wyszczególnione w rozporządzeniu EIDAS⁹⁾.

⁹⁾ Zgodnie z rozporządzeniem „usługa zaufania” oznacza usługę elektroniczną zazwyczaj świadczoną za wynagrodzeniem i obejmującą którąkolwiek z następujących czynności:

- wydawanie certyfikatów podpisów elektronicznych, certyfikatów pieczęci elektronicznych, certyfikatów uwierzytelniania witryn internetowych lub certyfikatów do celów świadczenia innych usług zaufania;
- walidację certyfikatów podpisów elektronicznych, certyfikatów pieczęci elektronicznych, certyfikatów uwierzytelniania witryn internetowych lub certyfikatów do celów świadczenia innych usług zaufania;
- tworzenie podpisów elektronicznych lub pieczęci elektronicznych;
- walidację podpisów elektronicznych lub pieczęci elektronicznych;
- konserwację podpisów elektronicznych, pieczęci elektronicznych, certyfikatów podpisów elektronicznych lub certyfikatów pieczęci elektronicznych;
- zarządzanie urządzeniami do składania podpisu elektronicznego na odległość lub urządzeniami do

15) Dostawca wyszukiwarki internetowej

Dostawca wyszukiwarki internetowej obejmuje podmiot, który świadczy usługę cyfrową, która umożliwia użytkownikom wprowadzanie zapytań w celu wyszukiwania – co do zasady – wszystkich stron internetowych lub wszystkich stron internetowych w danym języku za pomocą zapytania na jakikolwiek temat przez podanie słowa kluczowego, zapytania głosowego, wyrażenia lub innej wartości wejściowej i która podaje wyniki wyszukiwania w dowolnym formacie, w którym można znaleźć informacje związane z zadaniem zapytaniem.

16) Incydent

Aktualna definicja incydentu odwołuje się do pojęcia cyberbezpieczeństwa, które zmienia znaczenie w związku z wyodrębnieniem definicji „cyberbezpieczeństwa” i „bezpieczeństwa sieci i systemów informatycznych” na gruncie dyrektywy NIS 2. Dlatego też wprowadza się zmianę tej definicji w ten sposób, że jest to „zdarzenie, które ma lub może mieć niekorzystny wpływ na bezpieczeństwo systemów informacyjnych”. Poprzez odwołanie się do bezpieczeństwa systemów informacyjnych odwołujemy się do czterech atrybutów bezpieczeństwa informacji – poufności, integralności, dostępności oraz autentyczności – które są również obecne w definicji incydentu z dyrektywy NIS 2.

W ten sposób zapewniamy spójność z dyrektywą NIS 2 i jednocześnie zachowujemy ciągłość tej definicji od 2018 r. Porównanie w tym zakresie przedstawia poniższa tabela:

Definicje z projektu ustawy UC32	Definicja z dyrektywy NIS 2
incydent – zdarzenie, które ma lub może mieć niekorzystny wpływ na bezpieczeństwo systemów informacyjnych	„incydent” oznacza zdarzenie naruszające dostępność, autentyczność, integralność lub poufność przechowywanych, przekazywanych lub przetwarzanych danych lub usług oferowanych przez sieci i systemy informatyczne lub dostępnych za ich pośrednictwem.
bezpieczeństwo systemów informacyjnych – odporność systemów informacyjnych, przy danym poziomie pewności, na zdarzenia naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy	

składania pieczęci elektronicznej na odległość;

- wydawanie elektronicznych poświadczeń atrybutów;
- walidację elektronicznych poświadczeń atrybutów;
- tworzenie elektronicznych znaczników czasu;
- walidację elektronicznych znaczników czasu;
- świadczenie usług rejestrowanego doręczenia elektronicznego;
- walidację danych przekazywanych za pośrednictwem usług rejestrowanego doręczenia elektronicznego i związanych z nimi dowodów;
- archiwizację elektroniczną danych elektronicznych i dokumentów elektronicznych;
- rejestrowanie danych elektronicznych w rejestrze elektronicznym.

Wyjaśnienia wymaga wskazanie w definicji, że incydent to zdarzenie „które ma lub może mieć” – ta fakultatywność jest obecna od 2018 r. i jest związana z zapewnieniem, aby zespoły CSIRT albo osoby odpowiedzialne za obsługę incydentów w podmiocie otrzymywały informację o zdarzeniu, które wystąpiło i nie można było mu zapobiec, a zagraża bezpieczeństwu systemów. Dzięki temu można już rozpocząć proces zarządzania incydem i na końcu wyciągnąć wnioski, które zapobiegą poważniejszym zdarzeniom w przyszłości. Takie ukształtowanie przepisu jest zarazem zgodne z brzmieniem art. 3 rozporządzenia wykonawczego 2024/2690, w którym w kilku miejscach wskazano, że incydent uznaje się za incydent poważny (w przypadku podmiotów z sektora infrastruktury cyfrowej) jeśli „incydent spowodował lub może spowodować ...”.

17) Incydent poważny

Z uwagi na treść dyrektywy NIS 2 zaszła konieczność uzupełnienia definicji incydemu poważnego. Wskazano, że jest to incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi przez podmiot kluczowy lub podmiot ważny – a nie jak do tej pory świadczenia usługi kluczowej przez operatora usługi kluczowej. Ponadto incydemu poważnym będzie też taki, który powoduje straty finansowe dla podmiotu kluczowego i podmiotu ważnego albo wpływa na inne podmioty – osoby fizyczne, osoby prawne i ułomne osoby prawne – w taki sposób, że wywołuje szkodę materialną albo niematerialną.

18) Incydent w cyberbezpieczeństwie na dużą skalę

Zgodnie z dyrektywą NIS 2 dodano także definicję incydemu w cyberbezpieczeństwie na dużą skalę – jest to incydent, którego skutki przekraczają możliwości reagowania państwa lub ma poważny wpływ na inne państwo członkowskie. Zakres tego pojęcia może krzyżować się z definicją incydemu krytycznego, jednakże jest to celowe działanie.

19) Uchylenie definicji incydemu istotnego i incydemu w podmiocie publicznym

Uchyła się odrębne definicje incydemu istotnego i incydemu w podmiocie publicznym, ponieważ podmioty kluczowe i podmioty ważne będą zgłaszały incydenty klasyfikowane jako incydenty poważne.

20) Kierownik podmiotu kluczowego lub podmiotu ważnego

Dyrektywa NIS 2 wyraźnie wskazuje na odpowiedzialność zarządu podmiotu kluczowego i podmiotu ważnego w realizacji obowiązków z zakresu cyberbezpieczeństwa. Dlatego konieczne jest wyraźne zdefiniowanie kto jest kierownikiem podmiotu kluczowego lub podmiotu ważnego w rozumieniu ustawy o KSC. Definicja odsyła więc do pojęcia kierownika jednostki w rozumieniu art. 3 ust. 1 pkt 6 ustawy z dnia 29 września 1994 r. o rachunkowości

(Dz. U. z 2023 r. poz. 120, z późn. zm.) kierującego podmiotem kluczowym lub podmiotem ważnym. Takie odesłanie zapewni spójność w systemie prawa – pojęcie kierownika jednostki jest znane i ugruntowane w orzecznictwie i doktrynie. Ponadto na gruncie ustawy z dnia 29 września 1994 r. o rachunkowości, kierownik jednostki odpowiada za szereg obowiązków dotyczących rachunkowości – podobna sytuacja będzie miała miejsce w przypadku cyberbezpieczeństwa. W przypadku gdy podmiotem kluczowym lub podmiotem ważnym będzie jednostka sektora finansów publicznych, kierownikiem tego podmiotu jest kierownik, o którym mowa w art. 53 ust. 1 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2024 r. poz. 1530, z późn. zm.). Zmianę tę wprowadzono na prośbę wyartykułowaną w trakcie prac Komisji Wspólnej Rządu i Samorządu Terytorialnego.

21) Organizacja badawcza

Definicja organizacji badawczej odwołuje się do osoby prawnej albo ułamnej osoby prawnej prowadzącej działalność wskazaną w ustawie z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce (Dz. U. z 2024 r. poz. 1571, z późn. zm.), tj. badania aplikacyjne oraz prace rozwojowe. Nie włączono w zakres tej definicji badań podstawowych, ponieważ nie mają one celu komercyjnego, a definicja z dyrektywy NIS 2 odnosi się do działalności naukowej nastawionej na cele komercyjne. Zgodnie z definicją organizacji badawczej zawartej w dyrektywie NIS 2 spod zakresu tej definicji wyłączono podmioty systemu szkolnictwa wyższego i nauki jak uczelnie i instytuty badawcze.

22) Podatność

Konieczna jest zmiana definicji podatności, która obecnie odwołuje się do pojęcia systemu informacyjnego. W projekcie ustawy będzie to właściwość produktu ICT lub usług ICT, które mogą być wykorzystane przez cyberzagrożenie, co zapewni zgodność z dyrektywą NIS 2, zwłaszcza z jej angielską wersją „(15) ‘vulnerability’ means a weakness, susceptibility or flaw of ICT products or ICT services **that can be exploited by a cyber threat;**”.

23) Platforma sieci usług społecznościowych

W definicji platformy sieci usług społecznościowych wskazano, że jest to usługa świadczona drogą elektroniczną, która umożliwia użytkownikom końcowym łączenie się z innymi osobami oraz komunikowanie się i wymianę, udostępnianie i odkrywanie treści za pomocą wielu urządzeń, co oddaje sens i cel zawarty w dyrektywie NIS 2. Istotnym dodatkiem jest doprecyzowanie, że jest to usługa świadczona drogą elektroniczną – tego nie ma wprost wskazane w dyrektywie NIS 2, ale każdy portal tego rodzaju jest tego typu usługą.

24) Podmiot finansowy

Należało wprowadzić definicję podmiotu finansowego, ponieważ rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (Dz. Urz. UE L 333 z 27.12.2022, str. 1, z późn. zm.¹⁰⁾) wskazuje tutaj odrębne wymagania dla tej grupy podmiotów.

25) Podmiot publiczny

Wprowadza się definicję podmiotu publicznego – w tym zakresie odsyła się do załącznika 1 oraz 2 do ustawy o KSC do sektora podmiotów publicznych. Będą to podmioty, które do tej pory były traktowane przez ustawę o KSC jako podmioty publiczne. W toku prac nad projektem ustawy wyodrębniono kategorię podmiotów publicznych będących podmiotami ważnymi, stąd też definicja ta musi obejmować również załącznik nr 2 do ustawy.

26) Podmiot krytyczny

Dyrektywa NIS 2 powołuje się na pojęcie podmiotu krytycznego w rozumieniu dyrektywy CER, która definiuje to pojęcie w art. 2 pkt 1. W związku z tym należało zdefiniować to pojęcie również w projekcie ustawy. Dyrektywa CER wciąż nie została wdrożona do polskiego porządku prawnego. Toczy się proces legislacyjny projektu ustawy wdrażającej tę dyrektywę. Mając świadomość, że nie odwołuje się do przepisów aktów niedających się bezpośrednio stosować zrobiono to wyjątkowo. W sytuacji, gdy będzie możliwość odwołania się do przepisów transponujących dyrektywę CER to definicja ta zostanie niezwłocznie zmieniona.

27) Podmiot świadczący usługi rejestracji nazw domen

Aby zarejestrować domenę internetową każdy zainteresowany musi skorzystać z usług rejestratorów nazw domen, którzy współpracują z rejestrarami nazw domen. Nie można bezpośrednio udać się do rejestru nazw domen aby zarejestrować domenę. Rejestratorzy korzystają często z usług agentów.

Definicja obejmuje także dostawcę lub odsprzedawcę usług w zakresie:

- prywatności (privacy services) – chodzi o usługę, która umożliwia abonentowi domeny podać alternatywny adres do kontaktu,

¹⁰⁾ Zmiana wymienionego rozporządzenia została ogłoszona w Dz. Urz. UE L 2024/90177 z 12.03.2024.

- pośrednictwa w rejestracji (proxy service) – chodzi o usługę, w której niektóre informacje kontaktowe i identyfikacyjne nie są publikowane w bazie WHO.IS (bazie o domenach)¹¹⁾.

28) Potencjalne zdarzenie dla cyberbezpieczeństwa

Definicja potencjalnego zdarzenia dla cyberbezpieczeństwa jest konieczna, ponieważ pojęcie to występuje w dyrektywie NIS 2. Państwa członkowskie sprawozdają się z liczby zgłoszonych potencjalnych zdarzeń dla cyberbezpieczeństwa. Jest to więc zdarzenie, które może mieć niekorzystny wpływ na bezpieczeństwo systemów informacyjnych. Zgłaszanie takich zdarzeń do zespołów CSIRT jest nieobowiązkowe. W samej możliwości zgłoszeń tego rodzaju zdarzeń chodzi o to, aby móc wyciągnąć informacje z tego rodzaju sytuacji, które nie doprowadziły do strat, ale wyciągnięte z nich wnioski mogą pozwolić na zabezpieczenie się przed innymi incydentami.

29) Poważne cyberzagrożenie

Wprowadza się definicję poważnego cyberzagrożenia – jest to cyberzagrożenie, które może mieć poważny wpływ na bezpieczeństwo systemów informacyjnych poprzez wywołanie szkody materialnej lub niematerialnej. Jest to więc kwalifikowana postać cyberzagrożenia – jego zaistnienie będzie powodowało obowiązek poinformowania o środkach, które mogą podjąć użytkownicy podmiotów kluczowych i podmiotów ważnych celem zabezpieczenia się przed jego skutkami.

30) Projekt

Na potrzeby przepisów o możliwości udzielania przez ministra właściwego do spraw informatyzacji wsparcia finansowego wprowadza się definicję projektu.

31) Poważny incydent związany z ICT

W przepisach projektu przewidziano możliwość reagowania na poważne incydenty związane z ICT przez zespoły CSIRT poziomu krajowego. Jest to definicja wynikająca z art. 3 pkt 10 rozporządzenia DORA – rozporządzenia 2022/2554. Wprowadzono więc definicję w słowniczku.

32) Przedsiębiorca komunikacji elektronicznej i przedsiębiorca telekomunikacyjny

Prawo unijne przewiduje likwidację odrębnych obowiązków regulacyjnych z zakresu cyberbezpieczeństwa dla sektora telekomunikacji. Dostawcy podlegają takim samym wymogom z zakresu cyberbezpieczeństwa, jak inne podmioty kluczowe. Dlatego konieczne

¹¹⁾ About Privacy/Proxy Registration Service - ICANN, <https://www.icann.org/resources/pages/privacy-proxy-registration-2013-03-22-en> [4 wrzesień 2025 r.].

jest wprowadzenie definicji do ustawy o KSC. W projekcie ustawy wprowadza się pojęcie przedsiębiorcy komunikacji elektronicznej. Na ten zbiór składają się przedsiębiorcy telekomunikacyjni prowadzący działalność regulowaną oraz podmioty świadczące usługę komunikacji interpersonalnej niewykorzystującej numerów – będą to podmioty świadczące swoje usługi za pośrednictwem internetu, które mogą konkurować z usługami telekomunikacyjnymi. Przykładami takich usług, oznaczanych jako OTT-1, są usługi komunikatorów internetowych czy poczty elektronicznej.

Definicje przedsiębiorcy telekomunikacyjnego, przedsiębiorcy komunikacji elektronicznej oraz usług komunikacji interpersonalnej niewykorzystującej numerów znajdują się w ustawie z dnia 12 lipca 2024 r. – Prawo komunikacji elektronicznej.

33) Proces ICT, produkt ICT, usługa ICT

Wprowadzone zostały pojęcia produktu ICT, usługi ICT oraz procesu ICT. Projekt w tym zakresie wprowadza odwołanie dynamiczne do definicji tych pojęć zawartej w akcie o cyberbezpieczeństwie. Produkt oznacza „element lub grupę elementów systemów informacyjnych”. Będzie więc obejmował praktycznie wszystkie przypadki oprogramowania oraz urządzeń. Usługi ICT to wszelkie działania związane z przetwarzaniem informacji za pośrednictwem systemów informacyjnych. Proces ICT oznacza „zestaw czynności wykonywanych w celu projektowania, budowy, rozwijania, dostarczania lub utrzymywania produktów ICT lub usług ICT”. Są to więc wszelkiego rodzaju działania związane z tworzeniem systemów informacyjnych i ich bieżącym utrzymaniem.

34) Rejestr nazw domen najwyższego poziomu (TLD)

Domeny najwyższego poziomu, czyli takie nad którymi nie ma już wyższej domeny, są tworzone przez amerykańską organizację ICANN (Internet Corporation for Assigned Names and Numbers) oraz zależną od niej IANA. Domeną najwyższego poziomu jest np. domena .pl, czy .com. Domenami najwyższego poziomu (TLD – top level domain) zarządzają rejestry nazw domen najwyższego poziomu, które podpisały stosowne porozumienie z ICANN. Podkreślić należy, że rejestr nazw domen najwyższego poziomu jest jednostką organizacyjną, nie jest to rejestr publiczny w rozumieniu ustawy o informatyzacji. W Polsce rejestrem nazw domen najwyższego poziomu dla domeny .pl jest Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy.

35) System informacyjny

Dotychczasową definicję systemu informacyjnego uzupełnia się o wskazanie, że może to być również urządzenie lub grupa połączonych urządzeń elektrycznych lub elektronicznych

i oprogramowania zaprogramowanych w celu przetwarzania danych. W ten sposób projektodawca chce wyeliminować wątpliwości, co do tego czy systemy OT mieszczą się w ramach obecnej definicji systemu informacyjnego czy nie.

36) Właściwy organ w rozumieniu rozporządzenia 2022/2554

Projekt odnosi się do definicji właściwego organu w rozumieniu rozporządzenia DORA. Zgodnie z ustawą z dnia 25 czerwca 2025 r. o zmianie niektórych ustaw w związku z zapewnieniem operacyjnej odporności cyfrowej sektora finansowego oraz emitowaniem europejskich zielonych obligacji (Dz. U. poz. 1069), która znowelizowała ustawy dotyczące rynku finansowego tym właściwym organem będzie Komisja Nadzoru Finansowego.

37) Uchylenie definicji usługi kluczowej i zagrożenia cyberbezpieczeństwa

Uchyła się definicję usługi kluczowej, ponieważ na gruncie dyrektywy NIS 2 nie występuje to pojęcie. Zostało ono bowiem przeniesione do dyrektywy CER.

Definicja zagrożenia cyberbezpieczeństwa stała się zbędna w związku z dodaniem definicji cyberzagrożenia, stąd należy ją usunąć.

38) Usługi a zadania publiczne

Dyrektywa NIS 2 posługuje się pojęciem usług w szerokim znaczeniu – odnosi się ona także do podmiotów publicznych. W polskim systemie prawnym podmioty publiczne realizują zadania publiczne. Aby uniknąć wątpliwości w przepisach ogólnych wskazuje się wprost, że w przypadku podmiotu publicznego pod pojęciem usługi rozumie się także zadanie publiczne realizowane przez ten podmiot. Oczywiście zdarza się, że podmiot publiczny, np. instytucja gospodarki budżetowej, świadczy komercyjne usługi, które nie są zadaniami publicznymi. Jednakże dla celów ustawy o KSC to uogólnienie jest konieczne, w przeciwnym razie konieczne byłoby utrzymanie dotychczasowego pojęcia „incydentu w podmiocie publicznym” czy też wprowadzenia odrębnych progów dla incydentu związanego z zadaniami publicznymi.

System Inwentaryzacji Systemów Teleinformatycznych¹²⁾ wskazuje 651 systemów eksploatowanych obecnie przez administrację rządową do realizacji zadań publicznych. Należy przy tym uwzględnić systemy elektronicznego zarządzania dokumentacją obecne w podmiotach publicznych, sieci wewnętrzne składające się z urządzeń końcowych (komputerów, smartfonów, serwerów itd.). Zdaniem projektodawcy systemy te powinny być objęte obowiązkami wynikającymi z proponowanej ustawy. Podmioty publiczne świadczą

¹²⁾ Tabela danych - SYSTEMY - SIST 2025 - Otwarte Dane [na:] https://dane.gov.pl/pl/dataset/195/resource/73987/table?page=1&per_page=20&q=&sort=, dostęp 9 września 2025 r.

zadania publiczne w oparciu o systemy informacyjne. Incydent może doprowadzić do zaprzestania realizacji zadania publicznego – obywatele wtedy nie mogą realizować swoich publicznych praw podmiotowych. Incydenty źle wpływają także na wizerunek administracji – czy to administracji rządowej czy administracji samorządowej, co obniża zaufanie obywatela do państwa.

2.2.3. Przepis o celu funkcjonowania krajowego systemu cyberbezpieczeństwa

Dostosowuje się obecny przepis art. 3, który wskazuje na cel funkcjonowania krajowego systemu cyberbezpieczeństwa. Zmiana polega na odniesieniu się do usług świadczonych przez podmioty kluczowe lub podmioty ważne zamiast dotychczasowych usług kluczowych i usług cyfrowych.

2.2.4. Działania w ramach obsługi incydentów

Przepisy projektu ustawy przesądzają, że w ramach obsługi incydentu dotknięty nim podmiot może wykrywać źródło ataku oraz czasowo ograniczyć ruch sieciowy z adresów IP lub adresów URL. Uprawnienia te są niezbędne dla zapewnienia skutecznej reakcji na incydent, a w praktyce sprawiają one problemy praktyczne. Wykrycie źródła ataku często jest niezbędne do jego powstrzymania i przywrócenia normalnego funkcjonowania systemów. Równocześnie te działania mogą prowadzić do ewentualnego naruszenia uprawnień innych podmiotów. Do tej pory istniały wątpliwości na ile takie działania mogą być podejmowane. W związku z tym konieczne jest wprowadzenie wyraźnej podstawy prawnej do takich działań.

2.3. Podmioty kluczowe i podmioty ważne

Dyrektywa NIS 2 odeszła od pojęć operatorów usług kluczowych i dostawców usług cyfrowych, które były podstawą krajowego systemu cyberbezpieczeństwa. Obecnie obowiązki wynikające z dyrektywy NIS 2 kierowane są do podmiotów kluczowych oraz podmiotów ważnych.

W związku ze zmianą siatki pojęciowej wprowadzonej w dyrektywie NIS 2 konieczne było dostosowanie do niej przepisu określającego podmioty krajowego systemu cyberbezpieczeństwa. Uzupełniono ten przepis także o wskazanie nowych rodzajów podmiotów w krajowym systemie cyberbezpieczeństwa – CSIRT sektorowe oraz Połączone Centrum Operacyjne Cyberbezpieczeństwa.

Przepisy definiują też, które podmioty są podmiotami kluczowymi i podmiotami ważnymi oraz określają procedurę ich rejestracji.

Dyrektywa NIS 2 dotyczy przede wszystkim średnich przedsiębiorstw w rozumieniu zalecenia Komisji 2003/361/WE z dnia 6 maja 2003 r. dotyczące definicji mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw (Dz. Urz. UE L 124 z 20.05.2003, str. 36). Zalecenie Komisji (UE) jest aktem prawa miękkiego i zgodnie z zasadami techniki prawodawczej nie odwołuje się do tego rodzaju aktów. Dlatego ustawa o KSC odwołuje się do progów średniego przedsiębiorstwa określonych w załączniku I do rozporządzenia Komisji (UE) nr 651/2014 z dnia 17 czerwca 2014 r. uznającego niektóre rodzaje pomocy za zgodne z rynkiem wewnętrznym w zastosowaniu art. 107 i 108 Traktatu (Dz. Urz. UE L 651/2014 z 26.06.2014 r.), zwane dalej „rozporządzeniem 651/2014/UE”, które jest identyczne z zaleceniem Komisji (UE). W tym przypadku nie jest możliwe odwołanie do ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców (Dz. U. z 2024 r. poz. 236, z późn. zm.), ponieważ jego przepisy nie odpowiadają ww. zaleceniu. Przy ustalaniu wielkości przedsiębiorstwa warto skorzystać z aktualnej wersji poradnika ¹³⁾. Ustalając wielkość podmiotu należy wziąć pod uwagę wszystkie wymogi załącznika I do rozporządzenia Komisji (UE) nr 651/2014. Przede wszystkim należy odnieść się do pojęcia przedsiębiorstwa, które zostało zdefiniowane w art. 1 tego załącznika. Następnie należy wziąć pod uwagę progi mikro, małych i średnich przedsiębiorstw wskazane w art. 2. Przy obliczaniu wielkości przedsiębiorstwa uwzględnia się również przedsiębiorstwa powiązane oraz przedsiębiorstwa partnerskie, co wskazano w art. 3¹⁴⁾. Art. 4 określa jakie dane finansowe oraz które dane dotyczące zatrudnienia uwzględnia się przy określaniu wielkości przedsiębiorstwa. Jest tutaj szczególna reguła dotycząca ustalania wielkości przedsiębiorstwa – zmiana statusu jest uznawana jeżeli trwa ona przynajmniej 2 lata obrotowe. Art. 5 określa kogo rozumiemy jako pracowników przy obliczaniu wielkości przedsiębiorstwa. Dodatkowe reguły ustalania danych przedsiębiorstwa zawiera art. 6.

Podstawowa różnica między podmiotem kluczowym a podmiotem ważnym wyraża się w kwestiach nadzorczych. Wobec podmiotu kluczowego można prowadzić czynności

¹³⁾ Dyrekcja Generalna ds. Rynku Wewnętrznego, Przemysłu, Przedsiębiorczości i MŚP (Komisja Europejska), Poradnik dla użytkowników dotyczący definicji MŚP, Urząd Publikacji Unii Europejskiej, Urząd Publikacji Unii Europejskiej 2019. <https://data.europa.eu/doi/10.2873/82417>.

¹⁴⁾ Nie stosuje się przy tym art. 3 ust. 4 zgodnie z którym: 4. Poza przypadkami określonymi w ust. 2 akapit drugi przedsiębiorstwa nie można uznać za małe lub średnie przedsiębiorstwo, jeżeli 25 % lub więcej kapitału lub praw głosu kontroluje bezpośrednio lub pośrednio, wspólnie lub indywidualnie, co najmniej jeden organ publiczny. Wyłączenie wynika wprost z dyrektywy NIS 2.

nadzorcze *ex ante* i *ex post*. Wobec podmiotu ważnego czynności nadzorcze można prowadzić tylko *ex post*. Pozostałe obowiązki podmiotów kluczowych i podmiotów ważnych są identyczne z wyjątkiem kwestii obowiązkowych audytów.

Podmiotem kluczowym jest:

- 1) osoba fizyczna, osoba prawna albo jednostka organizacyjna nieposiadająca osobowości prawnej wskazana w załączniku nr 1 do ustawy o KSC, która przewyższa wymogi dla średniego przedsiębiorstwa określone w art. 2 ust. 1 załącznika I do rozporządzenia 651/2014/UE – chodzi o dużego przedsiębiorcę;
- 2) przedsiębiorca komunikacji elektronicznej, który co najmniej spełnia wymogi dla średniego przedsiębiorcy określone w art. 2 ust. 1 załącznika I do rozporządzenia 651/2014/UE;
- 3) dostawca usług zarządzanych w zakresie cyberbezpieczeństwa, który co najmniej spełnia wymogi dla małego albo średniego przedsiębiorcy określone w art. 2 ust. 1 załącznika I do rozporządzenia 651/2014/UE albo je przewyższa – intencją tutaj jest objęcie mniejszych zespołów typu CSIRT, SOC lub CERT wymaganiami z zakresu cyberbezpieczeństwa;
- 4) niezależnie od wielkości podmiotu:
 - a) dostawca usług DNS,
 - b) kwalifikowany dostawca usług zaufania w rozumieniu art. 3 pkt 20 rozporządzenia nr 910/2014,
 - c) podmiot krytyczny – w rozumieniu dyrektywy CER,
 - d) podmiot publiczny wskazany w załączniku nr 1 do ustawy o KSC w sektorze podmioty publiczne,
 - e) podmiot zidentyfikowany jako podmiot kluczowy przez organ właściwy do spraw cyberbezpieczeństwa,
 - f) państwowa osoba prawna zidentyfikowana jako podmiot kluczowy w sektorze podmiotów publicznych,
 - g) podmiot, który nie jest przedsiębiorcą, a jest wskazany w załączniku nr 1 do ustawy o KSC z nazwy albo poprzez określenie jego rodzaju – jest to konieczne doprecyzowanie ponieważ, nie wszystkie rodzaje podmiotów określonych w załączniku to przedsiębiorcy i wobec tego nie można do nich zastosować progów wielkościowych z rozporządzenia 651/2014,

- h) podmiot będący operatorem obiektu energetyki jądrowej, określonego w art. 2 pkt 2 ustawy z dnia 29 czerwca 2011 r. o przygotowaniu i realizacji inwestycji w zakresie obiektów energetyki jądrowej oraz inwestycji towarzyszących (Dz. U. z 2025 r. poz. 1156),
- i) rejestr nazw domen najwyższego poziomu (TLD),
- j) podmiot świadczący usługi rejestracji nazw domen.

Podmiotem ważnym jest:

- 1) osoba fizyczna, osoba prawna albo jednostka organizacyjna nieposiadająca osobowości prawnej wskazana w załączniku nr 1 do ustawy o KSC, która spełnia wymogi dla średniego przedsiębiorcy określone w art. 2 ust. 1 załącznika I do rozporządzenia 651/2014/UE oraz która nie jest podmiotem kluczowym;
- 2) osoba fizyczna, osoba prawna albo jednostka organizacyjna nieposiadająca osobowości prawnej wskazana w załączniku nr 2 do ustawy o KSC, która spełnia wymogi dla średniego przedsiębiorcy określone w art. 2 ust. 1 załącznika I do rozporządzenia 651/2014/UE albo przewyższa te wymogi oraz która nie jest podmiotem kluczowym;
- 3) niekwalifikowany dostawca usług zaufania będący mikro-, małym lub średnim przedsiębiorcą, o którym mowa w art. 2 ust. 1 załącznika I do rozporządzenia 651/2014/UE;
- 4) przedsiębiorca komunikacji elektronicznej będący mikro-, lub małym przedsiębiorcą, o którym mowa w art. 2 ust. 2 i 3 załącznika I do rozporządzenia 651/2014/UE;
- 5) podmiot, będący inwestorem obiektu energetyki jądrowej określonego w art. 2 pkt 2 ustawy z dnia 29 czerwca 2011 r. o przygotowaniu i realizacji inwestycji w zakresie obiektów energetyki jądrowej oraz inwestycji towarzyszących, który uzyskał decyzję zasadniczą, o której mowa w art. 3a ust. 1 tej ustawy – niezależnie od jego wielkości;
- 6) podmiot zidentyfikowany jako podmiot ważny przez organ właściwy do spraw cyberbezpieczeństwa;
- 7) podmiot określony w załączniku nr 2 do ustawy o KSC nazwą rodzajową, a który nie jest przedsiębiorcą;
- 8) podmiot publiczny, który nie jest podmiotem kluczowym oraz jest samorządową jednostką budżetową, samorządowym zakładem budżetowym, samorządową instytucją kultury albo spółką prawa handlowego wykonującą zadania o charakterze

użyteczności publicznej w rozumieniu art. 1 ust. 2 ustawy z dnia 20 grudnia 1996 r. o gospodarce komunalnej (Dz. U. z 2021 r. poz. 679) jeżeli realizuje zadanie publiczne z wykorzystaniem systemów informacyjnych.

Względem dyrektywy NIS 2 przesądzono już na poziomie ustawowym, że dostawcy usług zarządzanych w zakresie cyberbezpieczeństwa (podmioty typu Security Operations Center, Computer Security Incident Response Team, Computer Emergency Response Team itp.) są podmiotami kluczowymi. Podmioty te świadczą usługi obsługi incydentów na rzecz innych podmiotów i powinny mieć obowiązki w zakresie zapewnienia własnego cyberbezpieczeństwa, ponieważ od tego tak naprawdę będzie zależeć cyberbezpieczeństwo ich usługobiorców. Z tego zakresu wyłączono mikroprzedsiębiorców, dla których te wymagania mogłyby być zbyt uciążliwe.

W przypadku podmiotów publicznych wyłączono stosowanie progów małych i średnich przedsiębiorstw. Większość podmiotów publicznych będzie traktowanych jako podmioty kluczowe. Katalog samorządowych podmiotów publicznych będących podmiotami kluczowymi ukształtowano pod wpływem dyskusji na Zespole Społeczeństwa Informacyjnego Komisji Wspólnej Rządu i Samorządu Terytorialnego. Wprowadzono także kategorię podmiotów publicznych będących podmiotami ważnymi – będą miały one uproszczone wymagania z zakresu cyberbezpieczeństwa.

Z pewnością wystąpi zjawisko multisektorowości – podmioty prowadzą zróżnicowaną działalność, która obejmuje wiele sektorów, zarówno sektory ważne, jak i kluczowe. Aby uniknąć rozważań, czy podmiot jest podmiotem ważnym czy kluczowym uznano, że w przypadku gdy spełnia on kryteria podmiotu kluczowego i podmiotu ważnego powinno się wyrównać do góry i traktować go jako podmiot kluczowy. Ułatwi to określenie statusu podmiotu.

Aby ułatwić podmiotom samoidentyfikację – i uniknąć obowiązku ciągłego sprawdzania przesłanek uznania za podmiot kluczowy czy podmiot ważny w przypadkach, gdy zależy to od wielkości podmiotu – wskazano, że przesłanki uznania za podmiot kluczowy, czy podmiot ważny bada się według stanu na dzień sporządzenia sprawozdania finansowego. Czyli taki podmiot musi raz w roku zbadać, czy jest podmiotem ważnym lub podmiotem kluczowym. Oczywiście dotyczy to wyłącznie przedsiębiorców i to takich, których status podmiotu kluczowego, czy podmiotu ważnego zależy od ich wielkości.

W projektowanych przepisach wdrożono motyw 16 dyrektywy NIS 2. Zgodnie z unijnymi kryteriami przy badaniu statusu mikro-, małych i średnich przedsiębiorstw bierze się pod uwagę przedsiębiorstwa powiązane i przedsiębiorstwa partnerskie – ich przychody, sumę bilansową i liczbę pracowników dolicza się przy ustalaniu wielkości podmiotu. To mogłoby oznaczać, że dany podmiot staje się średnim przedsiębiorcą, wliczając jego przedsiębiorstwa powiązane i partnerskie – i jest wtedy podmiotem ważnym. Ale jego systemy informacyjne mogą mieć charakter niezależny od systemów podmiotów partnerskich i powiązanych. Nie ma więc powodów, aby uznawać ten podmiot za podmiot ważny. Niezależność systemu informacyjnego zachodzi m.in. wtedy, gdy do świadczenia usług przez podmiot nie jest konieczne działanie podmiotu powiązanego czy partnerskiego. Niezależność może przejawiać się również pod względem zastępowalności sieci i systemów informatycznych, tj. jeżeli w akceptowalnym przez podmiot czasie oraz po akceptowalnych kosztach można zastąpić posiadane rozwiązanie jednego podmiotu rozwiązaniami innych, o nie gorszych właściwościach funkcjonalno-technicznych.

Wśród podmiotów leczniczych mamy także podmioty niebędące przedsiębiorcami – np. jednostki budżetowe. Trudno wobec nich stosować kryteria wielkości przedsiębiorców. Jednocześnie należy tutaj wprowadzić kryterium wielkościowe i zwolnić z obowiązków małe podmioty lecznicze. Wprowadzono więc regułę, że podmiot leczniczy, który nie jest przedsiębiorcą:

- 1) jest podmiotem ważnym, jeżeli zatrudnia od 50 do 249 osób;
- 2) jest podmiotem kluczowym, jeżeli zatrudnia co najmniej 250 osób.

Wprowadzono uprawnienie dla Ministra Obrony Narodowej do ustalenia, które jednostki jemu podległe lub przez niego nadzorowane będą podmiotami kluczowymi lub podmiotami ważnymi.

W odniesieniu do podmiotów paliwowego cyklu jądrowego moment uzyskania statusu podmiotu kluczowego mógłby zostać powiązany z uzyskaniem określonego zezwolenia, o którym mowa w art. 4 ustawy z dnia 29 listopada 2000 r. – Prawo atomowe (Dz. U. z 2024 r. poz. 1277, 1897 i 1907), np. zezwolenia na eksploatację – art. 4 ust. 1 pkt odpowiednio 2 lub 3 ustawy z dnia 29 listopada 2000 r. – Prawo atomowe.

W odniesieniu do operatora elektrowni jądrowej moment uzyskania statusu podmiotu kluczowego mógłby stanowić połączenie art. 4 ustawy z dnia 29 listopada 2000 r. – Prawo atomowe (zezwolenie na eksploatację) z art. 32 ustawy z dnia 10 kwietnia 2017 r. – Prawo

energetyczne (Dz. U. z 2024 r. poz. 266, z późn. zm.) – koncesje, w zależności od tego, które zostałyby uzyskane jako pierwsze.

W przypadku zakładu do wydobywania rud uranu i toru ze złóż i ich wstępnego przetwarzania moment uzyskania statusu podmiotu kluczowego mógłby stanowić połączenie art. 4 ustawy z dnia 29 listopada 2000 r. – Prawo atomowe (zezwolenie na eksploatację) z art. 22 ustawy z dnia 9 czerwca 2011 r. – Prawa geologicznego i górniczego (Dz. U. z 2024 r. poz. 1290 oraz z 2025 r. poz. 769 i 1023) (koncesje na wydobywanie kopalin) – w zależności od tego, które zostałyby uzyskane jako pierwsze.

Dyrektywa NIS 2 wyłącza spod swojego zakresu podmioty zajmujące się bezpieczeństwem państwa. Z tego powodu wskazano, że do podmiotów kluczowych i ważnych nie zalicza się służb specjalnych w rozumieniu art. 11 ustawy z dnia 24 maja 2022 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2025 r. poz. 902), zwanej dalej „ustawą o ABW i AW”. Chodzi o Agencję Bezpieczeństwa Wewnętrznego, Agencję Wywiadu, Służbę Kontrwywiadu Wojskowego i Służbę Wywiadu Wojskowego.

Takie ujęcie tej kwestii gwarantuje pełną zgodność z postanowieniami dyrektywy NIS 2. Szczególnie istotne jest odniesienie do spełniania wymogów dla średniego przedsiębiorstwa, w przypadku najbardziej szerokich kategorii przedsiębiorców. Takie rozwiązanie gwarantuje, że nakładane obowiązki będą proporcjonalne do możliwości podmiotów, na które zostaną nałożone.

W przypadku podmiotów publicznych mamy pewną różnorodność statusów prawnych jednostek organizacyjnych. Przykładowo urzędy skarbowe i urzędy celno-skarbowe są jednostkami organizacyjnymi podległymi izbie administracji skarbowej. Stąd też to izba administracji skarbowej będzie podmiotem kluczowym. Dyrektor izby administracji skarbowej będzie więc odpowiadał za cyberbezpieczeństwo podległych izbie urzędów skarbowych i urzędów celno-skarbowych. Podobna sytuacja nastąpi w przypadku prokuratur rejonowych – to prokuratura okręgowa jest dysponentem środków budżetowych i to ona będzie podmiotem kluczowym, odpowiedzialnym za cyberbezpieczeństwo prokuratur rejonowych.

Podmioty świadczące usługi niezbędne dla funkcjonowania współczesnego społeczeństwa informacyjnego mają charakter transgraniczny. Należało więc przesądzić, zgodnie z dyrektywą NIS 2, jurysdykcję państwa nad podmiotami świadczącymi te usługi.

Co do zasady podmiot kluczowy i podmiot ważny podlega obowiązkom wynikającym z ustawy, jeżeli posiada swoją siedzibę, albo w przypadku przedsiębiorców zagranicznych

oddział na terytorium Rzeczypospolitej Polskiej. Dyrektywa NIS 2 posługuje się tutaj sformułowaniem „miejsce prowadzenia działalności” – zgodnie z zasadami unijnymi przedsiębiorca może także świadczyć transgranicznie usługi co uwzględniono w przepisie. Jest to też zgodne z motywem 113 dyrektywy NIS 2, zgodnie z którym „Jeżeli podmiot świadczy usługi lub ma miejsce prowadzenia działalności w więcej niż jednym państwie członkowskim, powinien podlegać odrębnej i równoczesnej jurysdykcji każdego z tych państw członkowskich Unii Europejskiej. Właściwe organy tych państw członkowskich Unii Europejskiej powinny ze sobą współpracować, zapewniać sobie wzajemną pomoc oraz, w stosownych przypadkach, prowadzić wspólne działania nadzorcze.”.

Przedsiębiorca komunikacji elektronicznej podlega obowiązkom wynikającym z ustawy, jeżeli świadczy usługi na terytorium Rzeczypospolitej Polskiej. Jest to spójne z ustawą z dnia 12 lipca 2024 r. – Prawo komunikacji elektronicznej.

Podmioty z sektora infrastruktury cyfrowej podlegają jurysdykcji polskiej, jeżeli na terytorium Rzeczypospolitej Polskiej ma siedzibę kierownik podmiotu podejmujący decyzje w sprawie systemu zarządzania bezpieczeństwem informacji w podmiocie albo realizowane są zadania związane z systemem zarządzania bezpieczeństwem informacji w podmiocie albo podmiot ma największą liczbę pracowników w odniesieniu do innych państw członkowskich Unii Europejskiej.

Przepisy ustawy o KSC nakładają na przedsiębiorców spoza Unii Europejskiej działających na jej terenie obowiązek wyznaczenia przedstawiciela. W sprawach dotyczących cyberbezpieczeństwa instytucje krajowego systemu cyberbezpieczeństwa, takie jak zespoły CSIRT, będą mogły kontaktować się z tymi przedstawicielami w sprawach obowiązków spoczywających na tych podmiotach. Gwarantuje to, że w systemie zostaną ujęte wszystkie podmioty operujące na terenie Unii Europejskiej. Kierując się wykładnią językową oraz celowościową wdrażanego przepisu dyrektywy NIS 2 należy uznać, że przedsiębiorca spoza Unii Europejskiej, który świadczy usługi na terytorium Unii Europejskiej w różnych państwach członkowskich i wyznaczył przedstawiciela w Polsce, podlegać będzie polskiej jurysdykcji, zastosowanie będą miały do niego przepisy polskiej ustawy wdrażającej, a tym samym zgłoszeń incydentów dotyczących infrastruktury tego przedsiębiorcy, choćby znajdowały się w innym państwie członkowskim Unii Europejskiej, będzie należało dokonywać do właściwego CSIRT w Polsce. CSIRT poziomu krajowego będą przy tym tworzyły Sieć CSIRT, do której zadań należy wymiana informacji na temat incydentów, czy pomaganie państwom członkowskich Unii Europejskiej w reagowaniu na incydenty transgraniczne.

Ponadto wskazano, że ustawę stosuje się do podmiotów publicznych niezależnie od miejsca ich siedziby. Takie sformułowanie obejmie również polskie placówki dyplomatyczne i polskie przedstawicielstwa przy organizacjach międzynarodowych.

2.4. Uchylenie wykazu usług kluczowych

Uchyła się podstawę prawną do wydania rozporządzenia Rady Ministrów w sprawie wykazu usług kluczowych. Dyrektywa NIS 2 nakazuje podmiotom kluczowym i podmiotom ważnym wdrożyć środki zarządzania ryzykiem dotyczące usług świadczonych przez te podmioty, a nie jednej konkretnej usługi.

Usługi kluczowe występują w przypadku dyrektywy CER – ich wykaz został ustalony w rozporządzeniu delegowanym Komisji (UE) 2023/2450 z dnia 25 lipca 2023 r. uzupełniającym dyrektywę Parlamentu Europejskiego i Rady (UE) 2022/2557 przez ustanowienie wykazu usług kluczowych (Dz. Urz. UE L 2023/2450 z 30.10.2023). Tym bardziej prawodawca krajowy nie może precyzować usług kluczowych w rozporządzeniu.

2.5. Wykaz podmiotów kluczowych i podmiotów ważnych

Bardzo duża liczba podmiotów podlegająca obowiązkom z dyrektywy NIS 2 stanowi wyzwanie dla organów nadzorujących wykonywanie obowiązków z zakresu cyberbezpieczeństwa – czyli organów właściwych do spraw cyberbezpieczeństwa. Podstawowa trudność to ich prawidłowe zidentyfikowanie. Do tej pory operatorzy usług kluczowych byli wyznaczani w drodze decyzji administracyjnej organu właściwego do spraw cyberbezpieczeństwa. Duży problem stanowiła natomiast identyfikacja dostawców usług cyfrowych w rozumieniu dyrektywy NIS – nie byli oni identyfikowani w drodze decyzji administracyjnej, a dotychczasowe kody Polskiej Klasyfikacji Działalności nie identyfikowały dokładnie działalności podmiotów świadczących usługi przetwarzania w chmurze, wyszukiwarek internetowych oraz internetowych platform handlowych. Ponadto zgodnie z dyrektywą NIS 2 państwa członkowskie Unii Europejskiej mają obowiązek przekazać liczbę podmiotów w poszczególnych sektorach zidentyfikowanych w danym państwie. Po raz pierwszy państwo członkowskie Unii Europejskiej musiało tego dokonać do dnia 17 kwietnia 2025 r. W przypadku zaś sektora infrastruktury cyfrowej państwa członkowskie mają obowiązek podać konkretne podmioty świadczące usługi. Niezbędny jest więc mechanizm umożliwiający sprawną identyfikację podmiotów kluczowych i podmiotów ważnych.

Aby ułatwić identyfikację podmiotów kluczowych i podmiotów ważnych wprowadzono obowiązek samorejestracji tych podmiotów. Rejestracja będzie dokonywała się w wykazie

podmiotów kluczowych i podmiotów ważnych. Regulacja ta zastąpi dotychczasowe przepisy o wykazie operatorów usług kluczowych.

Wykaz będzie zawierał wszystkie informacje niezbędne do skutecznego nadzoru nad tymi podmiotami. Przede wszystkim będą to dane identyfikujące podmiot – nazwa (firma) podmiotu, sektor, podsektor i rodzaj lub rodzaje podmiotu, zgodnie z załącznikiem nr 1 lub 2 do ustawy o KSC, siedzibę i adres do korespondencji, adres do doręczeń elektronicznych, jeżeli został nadany, adres poczty elektronicznej, numer identyfikacji podatkowej (NIP), numer w krajowym rejestrze urzędowym podmiotów gospodarki narodowej (REGON) oraz numer we właściwym rejestrze działalności regulowanej.

Oprócz samych danych identyfikujących będą w nim zawarte informacje takie jak:

- 1) zakres publicznych adresów IP wykorzystywanych przez podmiot wykorzystywanych w sposób ciągły¹⁵⁾;
- 2) zakres nazw domen wykorzystywane przez ten podmiot w sposób ciągły;
- 3) dane osób do kontaktu z podmiotami krajowego systemu cyberbezpieczeństwa zawierające imię i nazwisko, numer telefonu służbowego oraz adres służbowej poczty elektronicznej (w przypadku mikro i małych przedsiębiorców – jednej osoby);
- 4) numer telefonu przyporządkowany do wykonywanej działalności;
- 5) deklarację podmiotu, czy spełnia kryteria mikroprzedsiębiorcy, małego przedsiębiorcy, średniego przedsiębiorcy lub przewyższa te progi;
- 6) informację określającą, w których państwach członkowskich Unii Europejskiej podmiot wykonuje działalność, wraz z określeniem wykonywanej działalności;
- 7) w przypadku dostawcy usług DNS, rejestru nazw domen najwyższego poziomu (TLD), podmiotu świadczącego usługi rejestracji nazw domen, dostawcy chmury obliczeniowej, dostawcy usługi centrum przetwarzania danych, dostawcy sieci dostarczania treści, dostawcy usług zarządzanych, dostawcy usług zarządzanych w zakresie cyberbezpieczeństwa, dostawcy internetowej platformy handlowej, dostawcy wyszukiwarki internetowej oraz dostawcy platformy usług sieci społecznościowych –główne miejsce prowadzenia działalności ustalone zgodnie z art. 5a ust. 3–6;

¹⁵⁾ Dyrektywa NIS 2 wskazuje na obowiązek podania adresów IP – wskutek konsultacji publicznych doprecyzowano, że chodzi o publiczne adresy IP. Podawanie prywatnych adresów IP mija się z celem regulacji. Wskazano też, że chodzi adresy IP wykorzystywane w sposób ciągły – wyłączono w ten sposób adresy IP, które są używane przez podmiot jedynie tymczasowo np. na potrzeby konkretnego projektu czy zlecenia.

- 8) informację o zawarciu umowy z dostawcą usług zarządzanych w zakresie bezpieczeństwa na realizację zadań, o których mowa w art. 8 i art. 11 projektu ustawy wraz z danymi tego podmiotu.

Tego rodzaju informacje są niezbędne CSIRT poziomowi krajowemu, CSIRT sektorowym i innym organom krajowego systemu cyberbezpieczeństwa do prawidłowego wykonywania ich ustawowych zadań. Umieszczenie ich w jednym rejestrze zapewni łatwy dostęp do nich upoważnionym organom. Dane osób kontaktowych umożliwią szybką komunikację między zespołem CSIRT a danym podmiotem w przypadku incydentu poważnego lub w sytuacji poinformowania podmiotu o istotnej podatności czy też znaczącym cyberzagrożeniu. Jedną z tych osób kontaktowych powinien być administrator konta podmiotu w systemie teleinformatycznym S46. Z tego powodu należy przekazać również dodatkowo PESEL tej osoby lub niepowtarzalny identyfikator środka identyfikacji elektronicznej, o którym mowa w przepisach wydanych na podstawie art. 12 ust. 8 rozporządzenia 910/2014. Identyfikatory te są zawarte w podpisie osobistym, podpisie zaufanym lub w kwalifikowanym podpisie elektronicznym, dzięki temu pozwolą administratorowi na uwierzytelnienie się do systemu teleinformatycznego S46.

Deklaracja podmiotu o statusie mikro-, małego lub średniego przedsiębiorcy umożliwi ustalenie statusu podmiotu – czy jest podmiotem ważnym czy podmiotem kluczowym.

Informacja o wykonywaniu działalności w innych państwach członkowskich Unii Europejskiej pozwoli określić np. czy incydent zgłoszony przez podmiot może mieć charakter transgraniczny. Ponadto będzie to przydatna informacja, jeżeli konieczna będzie współpraca organów nadzorczych z innymi państwami członkowskimi Unii Europejskiej. Zasadne jest też, żeby podmioty wpisane do wykazu informowały o dostawcy usług zarządzanych w zakresie cyberbezpieczeństwa, z którym zawarły umowę na realizację zadań z zakresu cyberbezpieczeństwa. W przypadku trwającego incydentu poważnego istotne jest dla CSIRT sektorowych lub CSIRT poziomu krajowego kto faktycznie zajmuje się obsługą incydentu w danym podmiocie. Umożliwi to szybszą komunikację między zespołami. Warto podkreślić, że dostawcą usług zarządzanych w zakresie cyberbezpieczeństwa może być także jednostka utworzona przez np. ministra kierującego danym działem administracji rządowej i świadcząca usługi reagowania na incydenty dla podmiotów podległych ministrowi i nadzorowanych przez tego ministra.

Organ właściwy do spraw cyberbezpieczeństwa powinien także wiedzieć, czy podmiot kluczowy albo podmiot ważny zawarł porozumienie w sprawie wymiany informacji o zdarzeniach z zakresu cyberbezpieczeństwa (w praktyce to będą porozumienia w sprawie sektorowych inicjatyw ISAC). Obowiązek poinformowania o zawarciu takiego porozumienia wynika z dyrektywy NIS 2. Bardzo istotna jest informacja czy podmiot jest podmiotem krytycznym w rozumieniu dyrektywy CER i podlega obowiązkom z dyrektywy CER.

Konieczne jest także zawarcie w wykazie informacji o przedstawicielu podmiotów kluczowych lub podmiotów ważnych z innych państw członkowskich Unii Europejskiej z sektora infrastruktury cyfrowej, które świadczą usługi na terenie Polski. Zgodnie z dyrektywą NIS 2 państwo członkowskie Unii Europejskiej może podejmować wobec tego przedstawiciela kroki prawne w przypadku naruszenia obowiązków wynikających z dyrektywy NIS 2. Należy rozróżnić przypadek gdy przedstawicielem tym będzie osoba fizyczna oraz osoba prawna czy jednostka organizacyjna nieposiadająca osobowości prawnej. W przypadku przedstawiciela będącego osobą fizyczną, mając na uwadze zasadę minimalizacji przetwarzanych danych wynikającą z rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.), zwanego dalej „RODO”, wskazano na konieczność podania imienia i nazwiska, adresu do korespondencji, numeru telefonu oraz adresu poczty elektronicznej. Imię i nazwisko jest konieczne do zidentyfikowania przedstawiciela, adres do korespondencji jest niezbędny do przekazywania oficjalnych pism związanych z czynnościami nadzorczymi, adres poczty elektronicznej oraz numer telefonu są niezbędne do szybkiej komunikacji z przedstawicielem, jeżeli zajdzie taka potrzeba np. w związku z incydem. W przypadku osób prawnych wskazano na konieczność podania nazwy (firmy) przedstawiciela, siedziby, adresu do korespondencji, numeru telefonu oraz adresu poczty elektronicznej.

Z uwagi na to, że podmiot krytyczny w rozumieniu dyrektywy CER staje się automatycznie podmiotem kluczowym w rozumieniu dyrektywy NIS 2, to w wykazie musi być zawarta informacja o tym, że podmiot został uznany za podmiot krytyczny. Informację tę prześle ministrowi właściwemu do spraw cyberbezpieczeństwa dyrektor Rządowego Centrum Bezpieczeństwa.

Zdecydowana większość informacji w wykazie będzie pochodziła od samego podmiotu kluczowego, czy podmiotu ważnego – zostanie to zawarte we wniosku o wpis do wykazu.

Natomiast część informacji będzie uzupełniana z urzędu przez ministra właściwego do spraw informatyzacji. Dotyczy to wskazania organu właściwego do spraw cyberbezpieczeństwa, właściwych zespołów CSIRT sektorowych i CSIRT poziomu krajowego oraz tytułu prawnego wpisania do wykazu. Te dane są do ustalenia przez ministra w oparciu o przekazane dane z wniosku o wpis do wykazu.

Wskazano zakres danych, których dotyczy wnioski o wpis do wykazu – są to wszystkie dane z wyjątkiem tych, które minister właściwy do spraw informatyzacji jest w stanie ustalić z urzędu. Wniosek o zmianę wpisu w wykazie będzie zawierał wskazanie danych zmienianych.

Równocześnie wiele z tych danych będzie wrażliwych a ich podanie do publicznej wiadomości mogłoby negatywnie wpłynąć na bezpieczeństwo tych podmiotów i na ich chronione prawem interesy. Z tego względu do wykazu nie będą miały zastosowanie przepisy ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2022 r. poz. 902) i ustawy z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego (Dz. U. z 2023 r. poz. 1524). Jednocześnie minister właściwy do spraw informatyzacji będzie miał obowiązek publikowania w serwisie otwartych danych – dane.gov.pl – liczbę podmiotów kluczowych i podmiotów ważnych w podziale na sektory i rodzaj działalności. W niezbędnym zakresie pozwoli to na udostępnienie informacji publicznej społeczeństwu chroniąc zarazem inne informacje o podmiotach w wykazie.

W toku prac legislacyjnych rozdzielono role organów właściwy do spraw cyberbezpieczeństwa i ministra właściwego do spraw informatyzacji.

Administratorem danych w systemie, o którym mowa w art. 46 ust. 1, w którym prowadzony jest wykaz podmiotów kluczowych i podmiotów ważnych, jako gestor tego systemu, jest minister właściwy do spraw informatyzacji.

Minister ten, analogicznie jak wszystkie organy właściwe do spraw cyberbezpieczeństwa, jest również administratorem danych osobowych gromadzonych w wykazie podmiotów kluczowych i podmiotów ważnych w zakresie własnego sektora. Z uwagi na to, że powyższe zakresy administrowania mogą się krzyżować, a także z uwagi na obowiązki ministra właściwego do spraw informatyzacji, m.in. obowiązek udostępnienia danych z wykazu na żądanie organu uprawnionego, niezbędne jest przesądzenie w ustawie, że minister właściwy do spraw informatyzacji jest także współadministratorem danych osobowych, które znajdują się w wykazie podmiotów kluczowych i podmiotów ważnych. Minister właściwy do spraw

informatyzacji będzie zatem łącznie z innym organem właściwym do spraw informatyzacji współadministratorem danych osobowych podmiotów kluczowych i podmiotów ważnych spoza sektorów podlegających nadzorowi tego ministra.

Zjawisko współadministrowania zostało szczegółowo opisane w art. 26 RODO. Na tej podstawie minister właściwy do spraw informatyzacji i organy właściwe do spraw cyberbezpieczeństwa ustalą zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z tego rozporządzenia. RODO jest stosowane bezpośrednio, zatem nie ma potrzeby, aby przesądzać o zakresach odpowiedzialności współadministratorów w ustawie bądź zobowiązywać te podmioty do tego, aby zakres odpowiedzialności określali.

Organy właściwe do spraw cyberbezpieczeństwa będą miały uprawnienia do wpisania podmiotów do wykazu, wykreślenia błędnie wpisanych podmiotów a także do prowadzenia czynności sprawdzających. Czyli to one na bieżąco będą się zajmowały w zakresie nadzorowanego sektora, dbałością o jego aktualność.

W przypadkach, w których jest to możliwe, minister właściwy do spraw informatyzacji sam dokona rejestracji podmiotów z grup, które w całości znajdują się w wykazie, czyli przedsiębiorców telekomunikacyjnych, podmiotów krytycznych, dostawców usług zaufania, czy podmiotów publicznych wykorzystujących dane, które są już gromadzone w innych rejestrach publicznych. Celem projektodawcy jest wykorzystywanie informacji, które administracja publiczna już posiada oraz na unikaniu nakładania zbędnych obowiązków na podmioty prywatne. Nie wszystkie niezbędne dane są w dyspozycji administracji, z tego powodu niezbędne jest wprowadzenie podstawy do wezwania do uzupełnienia brakujących danych w wykazie. Podmioty te zostaną zawiadomione o wpisie do wykazu z urzędu przez ministra właściwego do spraw informatyzacji. Minister również wezwie te podmioty o uzupełnienie brakujących danych w wykazie w terminie 2 miesięcy od dnia doręczenia wezwania. Doprecyzowano przy tym, co będzie się znajdować w wezwaniu – podstawa prawna, numer podmiotu w wykazie, dane podmiotu wpisane do wykazu, oraz wskazanie źródła ich pochodzenia oraz wskazanie brakujących danych w wykazie. Dzięki temu podmioty dowiedzą się jakie czynności zostały wobec nich dokonane oraz skąd minister właściwy do spraw informatyzacji wziął dane. Po otrzymaniu wezwania do uzupełnienia braków formalnych podmioty, które minister wpisał z urzędu będą musiały uzupełnić brakujące dane w wykazie poprzez złożenie wniosku o zmianę wpisu w wykazie w terminie 2 miesięcy od dnia doręczenia wezwania. Dodatkowo też uzupełnią wykaz w zakresie działalności, która nie została objęta

wpisem z urzędu – pamiętać należy, że wiele z tych podmiotów świadczy różne rodzaje działalności.

Z uwagi na to, że nie wszyscy przedsiębiorcy telekomunikacyjni mają jeszcze adres do doręczeń elektronicznych, a z drugiej strony muszą korzystać z Platformy Usług Elektronicznych Urzędu Komunikacji Elektronicznej wprowadzono możliwość – ale nie obowiązek – przekazania zawiadomienia o wpisie w wykazie oraz wezwania do uzupełnienia braków formalnych przez tę właśnie Platformę.

Z uwagi na dużą liczbę podmiotów – zwłaszcza podmiotów publicznych jak i przedsiębiorców telekomunikacyjnych – wyraźnie wskazano, że sprawy dotyczące przekazania zawiadomienia o wpisie z urzędu oraz przekazywania wezwania o uzupełnienie braków formalnych mogą być załatwiane w drodze automatycznie generowanych pism, zgodnie z przepisem art. 14 § 1b ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego, zwanym dalej „Kpa”.

Podmioty spełniające wymogi dla podmiotów kluczowych i podmiotów ważnych będą obowiązane do zarejestrowania się w tym rejestrze w terminie 3 miesięcy od dnia spełnienia przesłanek uznania za podmiot kluczowy albo podmiot ważny. Nie dotyczy to oczywiście podmiotów publicznych, dostawców usług zaufania i przedsiębiorców telekomunikacyjnych, którzy będą wpisywani do wykazu z urzędu, zgodnie z procedurą opisaną powyżej. Wykaz będzie prowadzony w systemie teleinformatycznym S46, a wnioski do niego będą miały postać elektroniczną, co pozwoli na jego efektywną obsługę. Wnioski także będą składane w systemie teleinformatycznym S46. Wniosek będzie mógł być podpisany kwalifikowanym podpisem elektronicznym, podpisem zaufanym, podpisem osobistym kierownika podmiotu kluczowego lub podmiotu ważnego albo osoby upoważnionej albo kwalifikowaną pieczęcią elektroniczną. We wniosku powinny znaleźć się wszystkie informacje, które są wymagane w rejestrze. Wnioski mają zawierać również oświadczenia o świadomości odpowiedzialności karnej za złożenie fałszywego oświadczenia wynikającej z art. 233 § 6 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny (Dz. U. z 2025 r. poz. 383), zwanej dalej „Kodeks karny”. Powinno to zapewnić aktualność oraz prawdziwość danych w rejestrze. Spod tej odpowiedzialności zwolnione są punkty wniosku dotyczące wykorzystywanych adresów IP oraz domen. Adresy IP i domeny mogą ulegać bardzo szybkim zmianom, a także może ich być bardzo wiele. Z tego względu nie byłoby zasadne karanie za błędne podanie tych informacji. Przewidziano możliwość działania przez pełnomocnika – wniosek musi wtedy zawierać także

pełnomocnictwo w postaci elektronicznej podpisane kwalifikowanym podpisem elektronicznym, podpisem zaufanym albo podpisem osobistym.

Odstąpiono od wymogu podawania pełnomocnictwa w przypadku pełnomocnika lub prokurenta podmiotu, którzy są ujawnieni w Centralnej Ewidencji i Informacji o Działalności Gospodarczej lub w Krajowym Rejestrze Sądowym. Administracja już wie o pełnomocniku lub prokurencie i nie ma powodu, aby dodatkowo prosić podmiot o przedstawienie pełnomocnictwa.

Wpis do wykazu będzie dokonywał się automatycznie z chwilą złożenia podpisanego wniosku przez podmiot kluczowy i podmiot ważny. Organy właściwe do spraw cyberbezpieczeństwa będą mogły weryfikować czy podmioty wpisane do wykazu rzeczywiście spełniają odpowiednie kryteria podmiotów kluczowych lub podmiotów ważnych.

Może się zdarzyć, że podmiot kluczowy lub podmiot ważny prowadzi kilka działalności wskazanych w załącznikach nr 1 i 2 do ustawy. Dlatego we wniosku podmiot ma je odrębnie wykazać, co pozwoli na przypisanie właściwych sektorów.

Wskazano katalog sytuacji, w których wpisu do wykazu nie dokonuje się – przede wszystkim nie ma sensu wpisywać wniosku, który nie zawiera wszystkich niezbędnych danych. Nie powinno się wpisywać podmiotu, który już jest ujęty w wykazie. Wniosek, który nie zawiera oświadczenia oraz wniosek nie podpisany nie powinien być podstawą do wpisu. Podobnie wskazano podstawy do odmowy zmiany wpisu przy wniosku o zmianę wpisu.

Podmiot będzie mógł zwrócić się do ministra właściwego do spraw informatyzacji o wydanie zaświadczenia o wpisie podmiotu do wykazu albo o zmianie tego wpisu. Tutaj celem jest to aby sam podmiot uzyskał potwierdzenie wykonania obowiązku ustawowego. Przewiduje się, że zaświadczenie to będzie wydawane w systemie teleinformatycznym S46 automatycznie za pomocą kwalifikowanej pieczęci elektronicznej ministra właściwego do spraw informatyzacji.

Istotne jest to żeby wykaz był aktualny dlatego minister właściwy do spraw informatyzacji będzie mógł co najmniej raz w roku zaktualizować wykaz na podstawie danych pozyskanych z publicznie dostępnych rejestrów publicznych, czyli takich do których każdy ma dostęp. Przede wszystkim chodzi tutaj o dane zawarte w Krajowym Rejestrze Sądowym, Centralnej Ewidencji i Informacji o Działalności Gospodarczej, rejestrze REGON czy rejestrach działalności regulowanej. W razie uzyskania informacji o wykreśleniu podmiotu z krajowego rejestru urzędowego podmiotów gospodarki narodowej (REGON), Krajowego Rejestru Sądowego lub Centralnej Ewidencji i Informacji o Działalności Gospodarczej podmiot ten

Organ właściwy do spraw cyberbezpieczeństwa będzie mógł z urzędu wykreślić podmiot z wykazu podmiotów kluczowych i podmiotów ważnych jeżeli:

- Pozwoli to na utrzymanie aktualności tego wykazu.

Po dokonaniu wpisu podmioty będą musiały podłączyć się do systemu teleinformatycznego S46 w zakresie funkcjonalności umożliwiających szacowanie ryzyka i zgłaszanie incydentów. Jest to system już obecnie funkcjonujący, wspierający wymianę informacji między podmiotami krajowego systemu cyberbezpieczeństwa. Docelowo w ramach tego systemu będzie przechodziła cała komunikacja w sprawach cyberbezpieczeństwa. System ten będzie zawierał również narzędzia, które pomogą tym podmiotom m.in. w przygotowaniu oceny ryzyka. Te rozwiązania usprawnią komunikację w ramach krajowego systemu cyberbezpieczeństwa i pozwolą skutecznie wspierać jego podmioty w realizacji ich obowiązków.

39

elektronicznym, podpisem zaufanym, podpisem osobistym albo kwalifikowaną pieczęcią elektroniczną. Wnioski będą składane za pomocą systemu teleinformatycznego S46.

Dane z wykazu minister będzie udostępniał CSIRT MON, CSIRT NASK i CSIRT GOV oraz CSIRT sektorowemu w zakresie sektora lub podsektora, dla którego został ustanowiony, organowi właściwemu do spraw cyberbezpieczeństwa w zakresie nadzorowanego sektora lub podsektora, a także podmiotowi kluczowemu lub podmiotowi ważnemu w zakresie go dotyczącym. Ponadto o dostęp do tych danych będą mogły wnioskować inne organy państwa takie jak np. policja, służby specjalne, prokuratura i sądy, w zakresie niezbędnym do realizacji ich ustawowych zadań. Udostępnienie odbywa się za pomocą systemu teleinformatycznego S46 dzięki temu ograniczone zostanie przetwarzanie tych danych poza systemem.

Wprowadzono termin przechowywania informacji o zmianie wpisu w wykazie oraz o wykreśleniu podmiotu z wykazu – jest to termin 5 lat wraz z określeniem daty i czasu dokonania zmiany i wykreślenia. Konieczność przechowywania tych informacji wynika z tego, że mogą one być przydatne w postępowaniu w sprawie nałożenia administracyjnej kary pieniężnej – termin przedawnienia wynosi w tym przypadku 5 lat, zgodnie z art. 189g §1 Kodeksu postępowania administracyjnego. Ponadto informacje te mogą być przydatne przy postępowaniu karnym, jeśli dotyczy ono podania nieprawdziwych informacji we wpisie do wykazu. Stąd dla celów dowodowych zasadne jest zachowanie tych danych przez pewien okres.

W przypadku danych administratora konta podmiotu w systemie teleinformatycznym S46 to te dane będą dostępne jedynie ministrowi właściwemu do spraw informatyzacji oraz jednostce, której ten minister powierzył realizację zadania rozwoju lub utrzymania systemu. Celem jest ograniczenie liczby podmiotów, które mają dostęp do numeru PESEL tego administratora (czy niepowtarzalnego identyfikatora środka identyfikacji elektronicznej). Te dane są tak naprawdę potrzebne jedynie podmiotowi odpowiedzialnego za system teleinformatyczny S46. Przepis nie narusza jednak uprawnień sądu i prokuratora w postępowaniu karnym.

Organ właściwy do spraw cyberbezpieczeństwa będzie mógł również z urzędu wpisać dany podmiot do wykazu podmiotów kluczowych i podmiotów ważnych jeśli na podstawie danych zawartych w publicznie dostępnych rejestrach publicznych, danych dostępnych organowi na podstawie przepisów odrębnych oraz danych uzyskanych od samego podmiotu w drodze zapytania z art. 43 ust. 1 stwierdzi on, że dany podmiot spełnia kryteria podmiotu kluczowego

lub podmiotu ważnego, a podmiot ten nie wpisał się do wykazu w terminie 3 miesięcy od spełnienia przesłanek uznania za podmiot kluczowy lub podmiot ważny. To rozwiązanie gwarantuje, że nawet jeśli dany podmiot nie będzie chciał się wpisać do wykazu będzie możliwe włączenie go do rejestru. Czynność wpisania nie będzie miała charakteru decyzji administracyjnej, z uwagi na potencjalną liczbę podmiotów objętych obowiązkiem wpisu do wykazu – szacunkowo ponad 10 000. Jeżeli część z tych podmiotów nie wpisze się dobrowolnie do wykazu, to konieczne będzie wydawanie wielu decyzji administracyjnych, co będzie bardzo dużym obciążeniem dla organów właściwych do spraw cyberbezpieczeństwa. Z tego powodu lepsza jest formuła innej czynności z zakresu administracji publicznej. Podmiot będzie mógł zaskarżyć taką czynność do sądu administracyjnego, co gwarantuje mu skuteczną możliwość ochrony jego praw. Organ właściwy do spraw cyberbezpieczeństwa zawiadomi podmiot o wpisie do wykazu oraz wezwie ten podmiot do uzupełnienia brakujących danych w wykazie w terminie 2 miesięcy od dnia otrzymania zawiadomienia. Jest to konieczne, ponieważ należy podmiot poinformować o dokonanych wobec niego czynnościach.

Podmiot będzie mógł złożyć wniosek o wykreślenie z wykazu, jeżeli przestanie spełniać wymogi dla podmiotu kluczowego i podmiotu ważnego, ale będzie to weryfikowane przez organ właściwy do spraw cyberbezpieczeństwa.

Organ właściwy do spraw cyberbezpieczeństwa będzie mógł dokonywać czynności sprawdzających mających na celu weryfikację zgodności ze stanem faktycznym danych zawartych w wykazie i w razie potrzeby wzywać podmiot do ich zmiany pod rygorem nałożenia administracyjnej kary pieniężnej. Rozwiązanie to ma zapewnić aktualność danych w wykazie. Wprowadzono również podstawę prawną, aby organ właściwy do spraw cyberbezpieczeństwa mógł z urzędu poprawić oczywiste omyłki¹⁶⁾ i błędy zawarte w wykazach.

W szczególnie uzasadnionych przypadkach gdy dany podmiot nie spełnia wymogów uznania za podmiot kluczowy lub podmiot ważny, ale:

- 1) jako jedyny świadczy usługę, która ma kluczowe znaczenie dla krytycznej działalności społecznej lub gospodarczej¹⁷⁾,

¹⁶⁾ Omyłka to skutek niewłaściwego rozpoznania osób, rzeczy lub zjawisk i wzięcia jednych za drugie – por. wsjp.pl, Omyłka – Wielki słownik języka polskiego PAN [na:] „wsjp.pl”, <https://wsjp.pl/haslo/podglad/112164/omylka>, dostęp 29 września 2025 r.

¹⁷⁾ Krytyczna działalność społeczna lub gospodarcza (ang. *critical societal or economic activities*) jest pojęciem samoistnym na gruncie prawa unijnego, które nie zostało zdefiniowane. Poprzednio występowało na gruncie dyrektywy NIS. W przekonaniu wnioskodawcy pod tym pojęciem należy rozumieć działalności, które są

- 2) zakłócenie świadczenia usługi przez niego spowoduje poważne zagrożenie dla bezpieczeństwa państwa, bezpieczeństwa i porządku publicznego lub obronności,
- 3) zakłócenie świadczenia usługi przez niego spowoduje ryzyko systemowe¹⁸⁾ zaprzestania świadczenia usług przez podmioty kluczowe lub podmioty ważne lub
- 4) świadczenie przez niego usług ma istotne znaczenie na poziomie krajowym lub województwa lub ma znaczenie dla dwóch lub więcej sektorów określonych w załączniku nr 1 lub 2 do ustawy o KSC

– to w drodze decyzji administracyjnej organu właściwego będzie możliwe uznanie go za podmiot kluczowy lub podmiot ważny. Możliwość ta wynika z przepisów samej dyrektywy NIS 2. Przepis ten ma zagwarantować, że w krajowym systemie cyberbezpieczeństwa znajdą się wszystkie podmioty prowadzące szczególnie istotną dla państwa i społeczeństwa działalność. Jak wykazały doświadczenia pandemii w wielu przypadkach zaprzestanie działalności przez stosunkowo mały podmiot może mieć bardzo szerokie skutki dla innej działalności, np. w sektorze energetyki czy przemyśle. Tego rodzaju podmioty muszą znaleźć się w krajowym systemie cyberbezpieczeństwa.

O uznaniu takiego podmiotu za podmiot kluczowy lub podmiot ważny rozstrzyga decyzja administracyjna. W ramach tej procedury podmiot będzie miał możliwość ochrony swoich spraw, przedstawiania dowodów oraz podważania rozstrzygnięć organów.

Przewidziano także możliwość, aby można było uznać państwową osobę prawną za podmiot kluczowy. Procedura ta ma na celu nałożenie na państwowe osoby prawne, także te które powstaną w przyszłości, wymagań z zakresu cyberbezpieczeństwa. Dotyczyć to będzie państwowych osób prawnych, które realizują za pomocą systemu informacyjnego zadanie publiczne, którego zakłócenie spowoduje poważne zagrożenie dla bezpieczeństwa państwa, bezpieczeństwa i porządku publicznego, obronności lub zdrowia publicznego lub które ma istotne znaczenie na poziomie krajowym. Nie wszystkie państwowe osoby prawne w rozumieniu ustawy z 16 grudnia 2016 o zasadach zarządzania mieniem państwowym będą

niezbędne dla podtrzymania funkcjonowania państwa, społeczeństwa lub gospodarki. Organ właściwy do spraw cyberbezpieczeństwa przed wydaniem decyzji w tej sprawie powinien odpowiedzieć na pytanie, czy bez danej działalności społeczeństwo, gospodarka lub państwa może funkcjonować. Jeżeli odpowiedź jest negatywna, to taka działalność jest krytyczną działalnością społeczną lub gospodarczą. Jest to z pewnością klauzula generalna, która będzie się aktualizować w konkretnych okolicznościach.

¹⁸⁾ Ryzyko systemowe występuje na gruncie przepisów dotyczących nadzoru na rynku finansowym. Chodzi o taki rodzaj ryzyka, takie zakłócenia które zagrażają czy to całemu krajowemu systemowi cyberbezpieczeństwa czy też poszczególnym sektorom.

podlegać pod ustawę o KSC. Dlatego wprowadzono tą uznaniową procedurę, aby móc uzupełnić katalog podmiotów wchodzących w skład krajowego systemu cyberbezpieczeństwa.

2.6. Obowiązki podmiotów kluczowych i podmiotów ważnych

2.6.1. System zarządzania bezpieczeństwem informacji

Artykuł 21 dyrektywy NIS 2 nakazuje podmiotom kluczowym i podmiotom ważnym wprowadzenie odpowiednich i proporcjonalnych środków technicznych, operacyjnych i organizacyjnych w celu zarządzania ryzykiem dla bezpieczeństwa sieci i systemów informatycznych wykorzystywanych przez te podmioty do prowadzenia działalności lub świadczenia usług oraz w celu zapobiegania wpływowi incydentów na odbiorców ich usług lub na inne usługi bądź minimalizowania takiego wpływu.

Dyrektywa NIS 2 odeszła od wdrażania środków zapewniających bezpieczeństwo systemów informacyjnych tylko w zakresie świadczonych usług kluczowych. Podmiot ma dbać o bezpieczeństwo wszystkich swoich systemów wykorzystywanych do prowadzenia swojej działalności. Zauważyć bowiem należy, że podmioty gospodarcze choć działają dla zysku, to nie działają w próżni – ich działalność ma istotny wpływ na świadczenie usług przez inne podmioty, a także ma wpływ na funkcjonowanie konsumentów. Od zapewnienia odpowiedniego poziomu bezpieczeństwa systemów informacyjnych przedsiębiorstw energetycznych zależy funkcjonowanie przedsiębiorców telekomunikacyjnych, przewoźników kolejowych, dostawców usług chmurowych, serwerowni, czy wreszcie konsumentów. Podmioty dostarczające wodę pitną i odprowadzające ścieki używają systemów automatyki przemysłowej – tutaj incydent mógłby poważnie wpłynąć na zdrowie publiczne. Przykłady wzajemnego oddziaływania podmiotów współczesnej gospodarki można mnożyć. Wszystkie te podmioty używają systemów informacyjnych do świadczenia usług. Incydenty w jednym sektorze mogą spowodować poważne straty materialne oraz istotnie wpłynąć na funkcjonowanie społeczeństwa. Dlatego ważne jest nałożenie obowiązków z zakresu cyberbezpieczeństwa na podmioty kluczowe i podmioty ważne, aby przeciwdziałać negatywnemu wpływowi incydentów na funkcjonowanie społeczeństwa i gospodarki.

Dyrektywa NIS 2 mówi o wprowadzeniu środków zarządzania ryzykiem. Jednym z możliwych sposobów implementacji tych przepisów jest nałożenie obowiązków wdrożenia systemu zarządzania bezpieczeństwem informacji. Tak jest w chwili obecnej – operatorzy usług kluczowych mają obowiązek wdrożyć system zarządzania bezpieczeństwem informacji na podstawie aktualnego brzmienia art. 8 ustawy o KSC. Z kolei podmioty publiczne mają

także obowiązek wdrożyć system zarządzania bezpieczeństwem informacji na podstawie § 19 rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. poz. 773). Z tego powodu zdecydowano się wdrożyć art. 21 dyrektywy NIS 2 przez ewolucję obecnego art. 8 ustawy o KSC. Podmioty kluczowe i podmioty ważne będą więc obowiązane wdrożyć system zarządzania bezpieczeństwem informacji, obejmujący elementy wskazane w dyrektywie NIS 2. Takie podejście ułatwi dostosowanie się do regulacji podmiotom, które już obecnie są obowiązane na podstawie przepisów prawa posiadać wdrożony taki system – albo zrobiły to dobrowolnie. Podkreślić przy tym należy, że projekt nie wymaga uzyskania certyfikacji zgodności systemu zarządzania bezpieczeństwem informacji z jedną z norm technicznych. Wystarczające jest wdrożenie tego systemu zgodnie z ustawą o KSC oraz odpowiednie udokumentowanie tego faktu.

Zgodnie z nowym brzmieniem system zarządzania bezpieczeństwem informacji i ciągłości działania będzie wdrożony w systemach informacyjnych wykorzystywanych w procesach wpływających na świadczenie usług przez podmiot kluczowy lub podmiot ważny. Dzięki takiemu brzmieniu z jednej strony zachowamy brzmienie dyrektywy NIS 2, a z drugiej środki zarządzania ryzykiem będą wdrożone rzeczywiście w tych systemach, które służą świadczeniu usług.

Usługę należy rozumieć szeroko, jako *działalność gospodarczą służącą do zaspokajania potrzeb ludzi*¹⁹⁾. W tym znaczeniu usługą będzie również produkcja. Zresztą sama dyrektywa NIS 2 tak do tego podchodzi, przykładowo w art. 23 wskazuje na obowiązek zgłaszania incydentów, które mają poważny wpływ na świadczenie usług przez podmioty – jeśli założyć, że produkcja nie jest usługą w dyrektywie NIS 2, to wtedy nigdy żaden podmiot produkujący wyroby nie mógłby zgłosić incydentu poważnego, co prowadzi do absurdu. Zresztą przywołane wcześniej rozporządzenie delegowane Komisji (UE) 2023/2450 z dnia 25 lipca 2023 r. uzupełniające dyrektywę Parlamentu Europejskiego i Rady (UE) 2022/2557 przez ustanowienie wykazu usług kluczowych wskazuje, że usługą kluczową jest np. produkcja przemysłowa i przetwórstwo przemysłowe żywności na dużą skalę.

Aby zrealizować obowiązki wynikające ze znowelizowanego art. 8 podmiot kluczowy lub podmiot ważny musi zidentyfikować usługi jakie świadczy, zidentyfikować procesy jakie

¹⁹⁾ <https://sjp.pwn.pl/slowniki/us%C5%82uga.html>.

stosuje w celu świadczenia tych usług oraz zidentyfikować systemy informacyjne wykorzystywane w tych procesach.

Wdrażając art. 21 dyrektywy NIS 2 zachowano dotychczasową systematykę art. 8 ustawy o KSC.



Rysunek 1. System zarządzania bezpieczeństwem informacji w projekcie nowelizacji ustawy o KSC

Podstawowym obowiązkiem podmiotów kluczowych i podmiotów ważnych będzie wdrożenie systemu zarządzania bezpieczeństwem informacji obejmującego:

- 1) prowadzenie systematycznego szacowania ryzyka wystąpienia incydentu oraz zarządzanie tym ryzykiem – należy regularnie szacować ryzyko (identyfikować, analizować, oceniać), a następnie podejmować decyzję o podejściu do tego ryzyka;
- 2) wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, uwzględniających najnowszy stan wiedzy, koszty wdrożenia²⁰⁾, wielkość podmiotu²¹⁾, prawdopodobieństwo wystąpienia

²⁰⁾ Każda organizacja ma ograniczone zasoby, dlatego wybrane środki powinny być także adekwatne do jej możliwości finansowych.

²¹⁾ Inne są możliwości organizacyjne i finansowe dużych przedsiębiorstw, a inne średnich przedsiębiorstw i nie można tych możliwości porównywać.

incydentów, narażenie podmiotu na ryzyka, skutki społeczne i gospodarcze²²⁾, w szczególności:

- a) polityki szacowania ryzyka²³⁾ oraz bezpieczeństwa systemu informacyjnego²⁴⁾, w tym polityki tematyczne²⁵⁾,
- b) bezpieczeństwo w procesie nabywania, rozwoju, utrzymania i eksploatacji systemu informacyjnego, w tym testowanie systemu informacyjnego²⁶⁾,
- c) bezpieczeństwo fizyczne i środowiskowe, uwzględniające kontrolę dostępu²⁷⁾,
- d) bezpieczeństwo zasobów ludzkich²⁸⁾,
- e) bezpieczeństwo i ciągłość łańcucha dostaw produktów ICT, usług ICT i procesów ICT, od których zależy świadczenie usługi z uwzględnieniem związków pomiędzy bezpośrednim dostawcą sprzętu lub oprogramowania a podmiotem kluczowym lub podmiotem ważnym²⁹⁾,

²²⁾ Należy więc bardzo dobrze ustalić kontekst danej organizacji, jej charakterystykę, świadczone usługi, posiadane systemy, otoczenie regulacyjne, wymogi podmiotów trzecich.

²³⁾ Polityka szacowania ryzyka powinna opisać proces szacowania ryzyka w danej organizacji.

²⁴⁾ Należy ustanowić politykę bezpieczeństwa systemu informacyjnego wskazującą podejście podmiotu do zarządzania bezpieczeństwem informacji wraz z przypisaniem ról w tym procesie. Polityka ta powinna być adekwatna do danego podmiotu, wskazać cele bezpieczeństwa systemu informacyjnego, zobowiązanie do ciągłego rozwoju jak również przewidywać jej przegląd. Polityka powinna być zakomunikowana osobom zatrudnionym w podmiocie.

²⁵⁾ Polityki tematyczne – przykładowo są to *topic specific policies* o których mowa w normie ISO 27001. Założeniem tego przepisu jest to, aby tam gdzie to konieczne organizacja opracowała polityki tematyczne. Przykładowo, jeśli przyczyni się to do lepszej ochrony to organizacja może wprowadzić politykę bezpieczeństwa urządzeń mobilnych.

²⁶⁾ Należy opracować i wdrożyć procedury zarządzania konfiguracją, zmianami w systemie, testowanie systemu.

²⁷⁾ Podmiot kluczowy lub podmiot ważny powinien monitorować dostęp fizyczny do elementów systemu informacyjnego, zapobiegać cyberzagrożeniom mającym charakter fizyczny, zapobiegać utracie, uszkodzeniu urządzeń wspierających funkcjonowaniu systemu informacyjnego (np. urządzenia elektryczne).

²⁸⁾ Należy dbać o zrozumienie wymogów bezpieczeństwa wśród personelu. Personel o szczególnym dostępie do aktywów powinien w szczególności sposób wykonywać swoje zadania w. Pamiętać należy o personelu zewnętrznego dostawcy – należy wprowadzić odpowiednie postanowienia umowne dotyczące bezpieczeństwa oraz zachowaniu w poufności informacji. W procesie rekrutacji należy prowadzić weryfikację kandydatów (np. poprzez OSINT czy poprzez wymóg dostarczenia referencji czy zaświadczeń – przy czym należy pamiętać o wymogach RODO i poinformować kandydatów w ogłoszeniu, że takie czynności będą dokonywane i że wymagana jest ich zgoda); ponadto należy wprowadzić wewnętrzne reguły dyscyplinarne, jeśli nie wynikają z przepisów prawa powszechnie obowiązującego, dotyczące przypadków naruszenia obowiązków personelu w obszarze Cyberbezpieczeństwa, wraz z możliwością wypowiedzenia umowy; w postanowieniach umownych z personelem należy zawrzeć zapisy dotyczące zachowania w poufności informacji związanych z organizacją także po zakończeniu umowy.

²⁹⁾ Należy wprowadzić politykę łańcucha dostaw obejmującą relację z bezpośrednimi dostawcami. W polityce należy wskazać kryteria wyboru dostawców. W umowach z dostawcami należy zawierać postanowienia dotyczące Cyberbezpieczeństwa m. in. obowiązek zachowania informacji w poufności, obowiązek zgłaszania incydentów do podmiotu, informowanie o podatnościach, wymogi dotyczące personelu podmiotu (np. co do certyfikacji osób) itd. Pamiętać przy tym należy, że duzi dostawcy sprzętu lub oprogramowania często mają wdrożoną certyfikację własnych systemów, osób lub produktów/usług z zakresu cyberbezpieczeństwa, co z jednej strony ułatwia zarządzanie bezpieczeństwem łańcuchów dostaw, z drugiej może potencjalnie utrudnić dodatkowe wymogi, zwłaszcza, jeżeli zamawiający jest zdecydowanie mniejszym podmiotem. Tutaj wchodzi więc zasada proporcjonalnych środków technicznych i organizacyjnych. Organizacja powinna mieć

- f) wdrażanie, dokumentowanie, testowanie i utrzymywanie:
- planów ciągłości działania (*Business continuity plan – BCP*) umożliwiających ciągłe i niezakłócone świadczenie usług oraz zapewniających poufność, integralność, dostępność i autentyczność informacji,
 - planów awaryjnych (*Information System Contingency Plan – ISCP*), oraz
 - planów odtworzenia działalności umożliwiających odtworzenie systemu informacyjnego po zdarzeniu, które spowodowało straty przekraczające zdolności podmiotu do odbudowy za pomocą własnych środków – (*Disaster Recovery Plan – DRP*),
- g) objęcie systemu informacyjnego wykorzystywanego do świadczenia usługi systemem monitorowania w trybie ciągłym³⁰⁾,
- h) polityki i procedury oceny skuteczności środków technicznych i organizacyjnych³¹⁾,
- i) edukację z zakresu cyberbezpieczeństwa dla personelu podmiotu,
- j) podstawowe zasady cyberhigieny – jest to klauzula generalna, zmienna z uwagi na postęp technologiczny; podmiot kluczowy i podmiot ważny musi identyfikować te zasady w oparciu o aktualny poziom wiedzy technicznej,
- k) polityki i procedury stosowania kryptografii, w tym w stosownych przypadkach szyfrowania³²⁾,
- l) stosowanie bezpiecznych środków komunikacji elektronicznej w ramach krajowego systemu cyberbezpieczeństwa oraz wewnątrz podmiotu,

aktualny wykaz bezpośrednich dostawców z danymi kontaktowymi oraz wskazaniem jakie produkty ICT, usługi ICT czy procesy ICT dostarczają.

³⁰⁾ System informacyjny powinien być monitorowany ciągle – chodzi o to, aby zapewnić rozliczalność działań podejmowanych w systemie i analizować zaistniałe zdarzenia. Niekoniecznie trzeba w tym celu zatrudniać dodatkową osobę, można skorzystać z narzędzi open-source typu SIEM i ustawić adekwatne reguły. W szczególności należy monitorować zdarzenia, które mogą być przyczyną lub skutkiem incydentu. Monitorowanie dotyczy w szczególności ruchu z i do podmiotu, dostępu do systemu, kont z uprzywilejowanym dostępem, krytyczne pliki konfiguracyjne i kopii zapasowej, logi z narzędzi Cyberbezpieczeństwa (np. antywirusów, anti-spyware), zdarzenia środowiskowe, które mogą mieć wpływ na funkcjonowanie infrastruktury systemu (zalanie, pożar itd.).

³¹⁾ Należy ustalić, które aktywności w SZBI podmiotu będą monitorowane, jakie będą wskaźniki (KPI), kiedy, w jakich interwałach będą monitorowane, kto będzie to robił, czy nastąpi ich ewaluacja oraz kto za to będzie odpowiedzialny.

³²⁾ Polityki i procedury stosowania kryptografii obejmują m. in. jakie protokoły i algorytmy, rozwiązania i praktyki są zatwierdzone do używania w podmiocie oraz kwestie zarządzanie kluczami.

uwzględniających uwierzytelnianie wieloskładnikowe w stosownych przypadkach,

- m) zarządzanie aktywami³³⁾,
- n) polityki kontroli dostępu³⁴⁾;
- 3) zbieranie informacji o cyberzagrożeniach i podatnościach na incydenty systemu informacyjnego wykorzystywanego do świadczenia usługi³⁵⁾;
- 4) zarządzanie incydentami³⁶⁾;
- 5) stosowanie środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego wykorzystywanego do świadczenia usługi, w tym:
 - a) stosowanie mechanizmów zapewniających poufność, integralność, dostępność i autentyczność danych przetwarzanych w systemie informacyjnym,
 - b) regularne przeprowadzanie aktualizacji oprogramowania, stosownie do zaleceń producenta, z uwzględnieniem analizy wpływu aktualizacji na bezpieczeństwo świadczonej usługi oraz poziomu krytyczności poszczególnych aktualizacji,
 - c) ochronę przed nieuprawnioną modyfikacją w systemie informacyjnym,
 - d) niezwłoczne podejmowanie działań po dostrzeżeniu podatności lub cyberzagrożeń, w tym również czasowe ograniczenie ruchu sieciowego przychodzącego do infrastruktury podmiotu kluczowego lub podmiotu ważnego, które może skutkować zakłóceniem usług świadczonych przez ten podmiot, mając na uwadze konieczność minimalizacji skutków ograniczenia dostępności tych usług, z uwagi na podjęte działania.

Objęcie systemu informacyjnego wykorzystywanego do świadczenia usługi systemem monitorowania w trybie ciągłym należy rozumieć w ten sposób, że podmiot powinien monitorować wszelkie zdarzenia, które zaistniały w systemie informacyjnym. Celem jest nie tylko zapewnienie rozliczalności, ale także umożliwienie odtworzenia co się stało w systemie informacyjnym w danym momencie.

³³⁾ Należy ustalić klasyfikację aktywów, polityki/procedury właściwego zarządzania aktywami, prowadzić inwentaryzację aktywów oraz dbać o zwrot aktywów po zakończeniu umowy z personelem.

³⁴⁾ Należy ustalić politykę kontroli dostępu wskazującą kto może uzyskać dostęp fizyczny i logiczny do zasobów. Należy zarządzać prawami dostępu i anulować dostęp dla osób, które już nie potrzebują dostępu do aktywów, w tym także personelu zewnętrznego dostawcy. Należy prowadzić rejestr udzielonych dostępu.

³⁵⁾ Zbieranie informacji o cyberzagrożeniach i podatnościach pozwala na rozwój własnego personelu, zwiększa dojrzałość organizacji, umożliwia prewencyjne usunięcie podatności w systemie lub zabezpieczenie się przed cyberzagrożeniem.

³⁶⁾ Warto opracować politykę zarządzania incydentami, wprowadzić narzędzie do zgłaszania incydentów wewnątrz podmiotu, wprowadzić procedurę obsługi incydentów.

Podmioty kluczowe oraz podmioty ważne będą obowiązane uwzględnić wyniki skoordynowanych oszacowań ryzyka dla bezpieczeństwa krytycznych łańcuchów dostaw przeprowadzonych przez Grupę Współpracy, o której mowa art. 22 dyrektywy NIS 2.

W zakresie reagowania na incydenty należy również zwrócić uwagę na kwestię ograniczenia ruchu sieciowego. Jest to jeden ze środków reagowania na incydenty. Polega on na zaatakowaniu ofiary z wielu miejsc jednocześnie. Do przeprowadzenia ataku służą najczęściej komputery, nad którymi przejęto kontrolę przy użyciu specjalnego oprogramowania (różnego rodzaju tzw. boty i trojany). Na dany sygnał komputery zaczynają jednocześnie atakować system ofiary, zasypując go fałszywymi próbami skorzystania z usług jakie oferuje. Dla każdego takiego wywołania atakowany komputer musi przydzielić pewne zasoby (pamięć, czas procesora, pasmo sieciowe), co przy bardzo dużej liczbie żądań prowadzi do wyczerpania dostępnych zasobów, a w efekcie do przerwy w działaniu lub nawet zawieszenia systemu. Jest to jeden z najczęściej stosowanych typów ataku.

Ograniczenie ruchu sieciowego jest najskuteczniejszą metodą zablokowania takiego ataku. Równocześnie wiele podmiotów, w szczególności podmioty publiczne, wskazują, że zgodnie z przepisami muszą świadczyć usługi i nie powinny blokować do nich dostępu nikomu. W dotychczasowym stanie prawnym istniały wątpliwość czy obsługa incydentu i zapewnienia bezpieczeństwa swoim systemom upoważniają do zablokowania takiego ruchu.

W toku dyskusji z organizacjami zrzeszającymi jednostki samorządu terytorialnego prowadzonej w trakcie obrad Zespołu Społeczeństwa Informacyjnego Komisji Wspólnej Rządu i Samorządu Terytorialnego wskazano, że niektóre samorządowe podmioty publiczne – będące podmiotami ważnymi – powinny mieć wymagania z zakresu cyberbezpieczeństwa adekwatne do ich możliwości. Dlatego wprowadza się załącznik 4 w ustawie o KSC, który zawiera uproszczone wymagania cyberbezpieczeństwa dla tych podmiotów. Nadal będą to podmioty ważne – będą więc w krajowym systemie cyberbezpieczeństwa, będą podlegały obowiązkom nadzorczym jak dla podmiotów ważnych, będą podlegały administracyjnym karom pieniężnym, będą mogły być adresatami rekomendacji Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa.

Rada Ministrów będzie mogła ustalać, w drodze rozporządzenia, odrębnie dla danego rodzaju działalności wykonywanej przez podmioty kluczowe lub podmioty ważne szczegółowe wymagania dla systemu zarządzania bezpieczeństwem informacji. Przepis ten pozwoli

uwzględnić specyfikę poszczególnych sektorów i przedstawić rozwiązania dostosowane do tej specyfiki. Będzie to fakultatywne upoważnienie ustawowe.

Podkreślić należy, że zakłada się możliwość wydawania wielu rozporządzeń na podstawie dodawanego upoważnienia ustawowego. Projekt ustawy wdrażającej dyrektywę NIS 2 nakłada obowiązki na bardzo zróżnicowane podmioty w wielu sektorach gospodarki. W ramach poszczególnych rodzajów działalności występuje także wiele podrodzajów. Przygotowanie jednego rozporządzenia obejmującego wszystkie te sektory byłoby zadaniem karkołomnym – wprowadzone regulacje musiałyby pozostać na bardzo wysokim poziomie ogólności, co poddawałoby w wątpliwość celowość uregulowania tej materii w rozporządzeniu. Alternatywa w postaci wprowadzenia kilkunastu przepisów upoważniających dla określenia minimalnych wymagań dla systemu zarządzania bezpieczeństwem informacji w poszczególnych sektorach nie wydaje się słuszną. Trudno byłoby w takim przypadku określić organ wydający rozporządzenie – wszakże nie wszystkie organy właściwe do spraw cyberbezpieczeństwa mają prawo do wydawania rozporządzeń. Dlatego zdecydowano się na wprowadzenie upoważnienia ustawowego dla Rady Ministrów.

W ramach rządowego procesu legislacyjnego wnioskodawcą projektu rozporządzenia dotyczącego określonej działalności powinien być organ właściwy do spraw cyberbezpieczeństwa nadzorujący daną działalność. Jeśli organ właściwy do spraw cyberbezpieczeństwa nie ma uprawnień do procedowania projektu rozporządzenia, to wnioskodawcą projektu powinien być minister nadzorujący dany organ.

Przepisy aktów podustawowych muszą być zgodne nie tylko z ustawą, na podstawie której zostały wydane, ale także z innymi ustawami. Wynika to z hierarchii systemu źródeł prawa. Przepisy art. 8 ustawy o KSC w wersji znowelizowanej będą nakładały obowiązek wdrożenia systemu zarządzania bezpieczeństwem informacji na podmioty publiczne. Te podmioty już obecnie mają taki obowiązek – wynika on z § 19 rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych. Konieczna będzie nowelizacja tego rozporządzenia, aby uniknąć kolizji z przepisami art. 8 ustawy o KSC. Nie jest również wykluczone, że na podstawie art. 8a projektu ustawy zostanie wydane rozporządzenie precyzujące wymagania z zakresu cyberbezpieczeństwa dla podmiotów publicznych.

Komisja Europejska ma obowiązek wydania aktów wykonawczych do dyrektywy NIS 2 określających środki zarządzania ryzykiem dla części podmiotów z sektora infrastruktury cyfrowej. Dla pozostałych podmiotów Komisja może wydać takie akty. Dlatego w przepisie wskazano, że w ramach systemu zarządzania bezpieczeństwem informacji i ciągłości działania podmioty stosują środki określone w bezpośrednio stosowalnych aktach wykonawczych Komisji Europejskiej.

Wskazano również, że podmioty kluczowe z podsektora energii elektrycznej stosują, w ramach systemu zarządzania bezpieczeństwem informacji i ciągłości działania środki określone w rozporządzeniu delegowanym Komisji (UE) 2024/1366 z dnia 11 marca 2024 r. uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/943 poprzez ustanowienie kodeksu sieci dotyczącego zasad sektorowych w zakresie aspektów cyberbezpieczeństwa w transgranicznych przepływach energii elektrycznej.

2.6.2. Zadania kierownictwa

Dyrektywa NIS 2 wprowadziła obowiązek wskazania roli kierownictwa poszczególnych podmiotów w zakresie zapewnienia ich cyberbezpieczeństwa. Kierownik podmiotu kluczowego lub podmiotu ważnego z mocy ustawy ponosi odpowiedzialność za wykonywanie obowiązków podmiotu w zakresie cyberbezpieczeństwa. Jeżeli kierownikiem jest organ wieloosobowy to odpowiedzialność ponoszą wszyscy członkowie tego organu. Odpowiedzialność kierownika podmiotu następuje także wtedy gdy niektóre z obowiązków zostały powierzone innej osobie za jej zgodą. Celem tych rozwiązań jest to, aby kierownictwo podmiotu poważnie podchodziło do zapewnienia cyberbezpieczeństwa podmiotu, ponieważ obecnie bez bezpiecznych systemów informacyjnych nie jest możliwe sprawne świadczenie usług innym podmiotom i konsumentom.

Wskazano zadania kierownika podmiotu kluczowego lub podmiotu ważnego:

- 1) podejmuje decyzje w zakresie przygotowania, wdrażania, stosowania, przeglądu i nadzoru systemu zarządzania bezpieczeństwem informacji w podmiocie – co oznacza, że kierownik odpowiada za system zarządzania bezpieczeństwem informacji i jego rozwój zgodnie z cyklem Deminga;
- 2) planuje adekwatne środki finansowe na realizację obowiązków z zakresu cyberbezpieczeństwa – mając na uwadze, że cyberbezpieczeństwo wymaga nakładów i nie powinny one być pomijane w budżetach podmiotów kluczowych

- i podmiotów ważnych; z drugiej strony muszą być to adekwatne środki, czyli takie, które są też dostosowane do możliwości podmiotu;
- 3) przydziela zadania z zakresu cyberbezpieczeństwa w tym podmiocie i nadzoruje ich wykonanie;
 - 4) zapewnia, że personel podmiotu jest świadomy obowiązków z zakresu cyberbezpieczeństwa i zna wewnętrzne regulacje podmiotu w tym zakresie. System zarządzania bezpieczeństwem informacji wymaga, aby każdy pracownik organizacji miał przypisaną rolę i zadania do wykonania celem zachowania bezpieczeństwa informacji;
 - 5) zapewnia zgodność działania tego podmiotu z przepisami prawa oraz z wewnętrznymi regulacjami podmiotu – tu chodzi o zapewnienie stosowalności w podmiocie nie tylko przepisów prawa powszechnie obowiązującego, ale również własnych regulacji, aby nie były pomijane w codziennej pracy.

Osoby kierujące podmiotami kluczowymi lub podmiotami ważnymi muszą również raz na rok przejść szkolenie z zakresu wykonywania zadań z zakresu cyberbezpieczeństwa. Dotyczy to zadań związanych z opracowaniem systemu zarządzania bezpieczeństwem informacji, zgłaszania incydentów, dokumentowania SZBI. Gwarantuje to, że będą posiadać aktualną wiedzę merytoryczną potrzebną do podejmowania decyzji w tym obszarze.

2.6.3. Niekaralność personelu

Ważną gwarancją prawidłowego wykonywania zadań z zakresu cyberbezpieczeństwa jest wskazanie, że zadań tych nie mogą wykonywać osoby skazane za przestępstwa przeciwko ochronie informacji³⁷⁾. Daje to odpowiednią gwarancję, że zadania te będą wykonywały osoby dające rękojmię ich prawidłowej realizacji. Ograniczono się przy tym do przestępstw przeciwko ochronie informacji, ponieważ są one związane tematycznie z cyberbezpieczeństwem.

Osoba musi przedstawić zaświadczenie o niekaralności za ww. przestępstwa. Zaświadczenia w tym zakresie będą weryfikowane przez ich kierowników podmiotów kluczowych i podmiotów ważnych. Po otrzymaniu zaświadczenia kierownik dopuści taką osobę do realizacji zadań związanych z systemem zarządzania bezpieczeństwem informacji oraz zgłaszaniem incydentów. Weryfikacja personelu przed przydzieleniem zadań z zakresu

³⁷⁾ Czyli przestępstwa określone w rozdziale XXXIII Kodeksu karnego – art. 265 (ujawnienie informacji niejawnych), art. 266 (ujawnienie informacji służbowych), art. 267 (nielegalne uzyskanie informacji), art. 268 (niszczenie informacji), art. 268a (niszczenie danych w systemach), art. 269 (sabotaż komputerowy), art. 269a (zakłócanie sieci i systemów), art. 269b (bezprawne wykorzystanie programów i danych).

cyberbezpieczeństwa jest przewidywana przez normy techniczne, np. normę ISO 27001, a zatem nie jest to zupełna nowość. Podkreślić należy, że mogą tutaj wystąpić stosunek pracy, a także inne stosunki zatrudnienia, np. umowa zlecenia. Jest to istotne w kontekście przetwarzania danych osobowych, jako że dotyczy to danych o karalności w rozumieniu art. 10 RODO. Tak jak wyżej wspomniano, weryfikacja niekaralności personelu przed wykonywaniem zadań z zakresu cyberbezpieczeństwa jest zasadna. Osoby, które dopuściły się czynów zabronionych przeciwko ochronie informacji nie dają należytej rękojmi prawidłowego wykonywania zadań z zakresu cyberbezpieczeństwa. W interesie samego podmiotu kluczowego i podmiotu ważnego jest zatrudnienie wiarygodnego personelu. Ponadto sama dyrektywa NIS 2 wspomina o konieczności wdrożenia środków z zakresu bezpieczeństwa zasobów ludzkich. Stąd weryfikacja niekaralności personelu jest konieczna. Informacje o niekaralności będą przechowywane w dokumentacji pracowniczej albo w dokumentacji związanej z daną umową w przypadku innych stosunków zatrudnienia. Oczywiście, zgodnie z RODO, takie informacje będą musiały być należycie chronione. Wprowadza się również uprawnienie podmiotu kluczowego i podmiotu ważnego do wezwania osoby do ponownego przedstawienia zaświadczenia o niekaralności za przestępstwa przeciwko ochronie informacji, jeżeli podmiot poweźmie uzasadnione podejrzenie, że osoba ta została skazana za przestępstwo przeciwko ochronie informacji. Podejrzenie to musi być uzasadnione, w jakimś mierze uprawdopodobnione. Przy czym sam anonim czy zgłoszenie od sygnalisty może być niewystarczające w tej mierze, trzeba wziąć pod uwagę, że takie zgłoszenie może być po prostu aktem szkalującym inną osobę. Również uzasadnionym działaniem podmiotu kluczowego i podmiotu ważnego nie będzie cykliczne wzywanie danej osoby do przedstawienia zaświadczenia o niekaralności.

Koszt uzyskania zaświadczenia z Krajowego Rejestru Karnego wynosi 20 zł w wersji elektronicznej.

Wprowadzono wyjątek od obowiązku przedstawiania zaświadczenia o niekaralności – jest to sytuacja, gdy dana osoba posiada ważne poświadczenie bezpieczeństwa upoważniające w zakresie dostępu do informacji niejawnych o klauzuli „poufne” lub wyższej. Taka osoba została zweryfikowana w postępowaniu sprawdzającym, dlatego nie ma potrzeby dodatkowej weryfikacji jej niekaralności.

2.6.4. Obowiązki informacyjne dostawców usług zarządzanych z zakresu cyberbezpieczeństwa

Nawiązując do powszechnej międzynarodowej praktyki (publikowanie informacji na podstawie wzoru zawartego w pkt. 3.3 dokumentu RFC 2350³⁸⁾), nakłada się na dostawców usług zarządzanych z zakresu cyberbezpieczeństwa obowiązek udostępniania na stronie internetowej podstawowych informacji o swojej działalności. W celu zrealizowania tego obowiązku wystarczy zamieścić krótki plik tekstowy na stronie internetowej dostawcy usług zarządzanych z zakresu cyberbezpieczeństwa.

2.6.5. Dobrowolna wymiana informacji z zakresu cyberbezpieczeństwa

Przepisy projektu ustawy tworzą ramy do dobrowolnej wymiany informacji z zakresu cyberbezpieczeństwa pomiędzy podmiotami kluczowymi i podmiotami ważnymi. Jest to niezwykle istotne gdyż przekazanie informacji o zagrożeniach i atakach może pozwolić innym podmiotom zabezpieczyć swoje systemy i uchronić się przed zagrożeniem.

Dopuszczalna wymiana informacji w zakresie cyberbezpieczeństwa	
Rodzaj informacji	Opis informacji
<i>cyberzagrożenia</i>	wszelkie potencjalne okoliczności, zdarzenie lub działanie, które mogą wyrządzić szkodę, spowodować zakłócenia lub w inny sposób niekorzystnie wpłynąć w przypadku sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób
<i>potencjalnych zdarzeniach dla cyberbezpieczeństwa</i>	zdarzenie, które mogło mieć niekorzystny wpływ na bezpieczeństwo systemów informacyjnych jednak nie wystąpiło lub, któremu udało się zapobiec

³⁸⁾ <https://datatracker.ietf.org/doc/html/rfc2350>

Jako przykłady praktyki można wskazać:

<https://www.knf.gov.pl/knf/pl/komponenty/img/RFC2350.pdf>

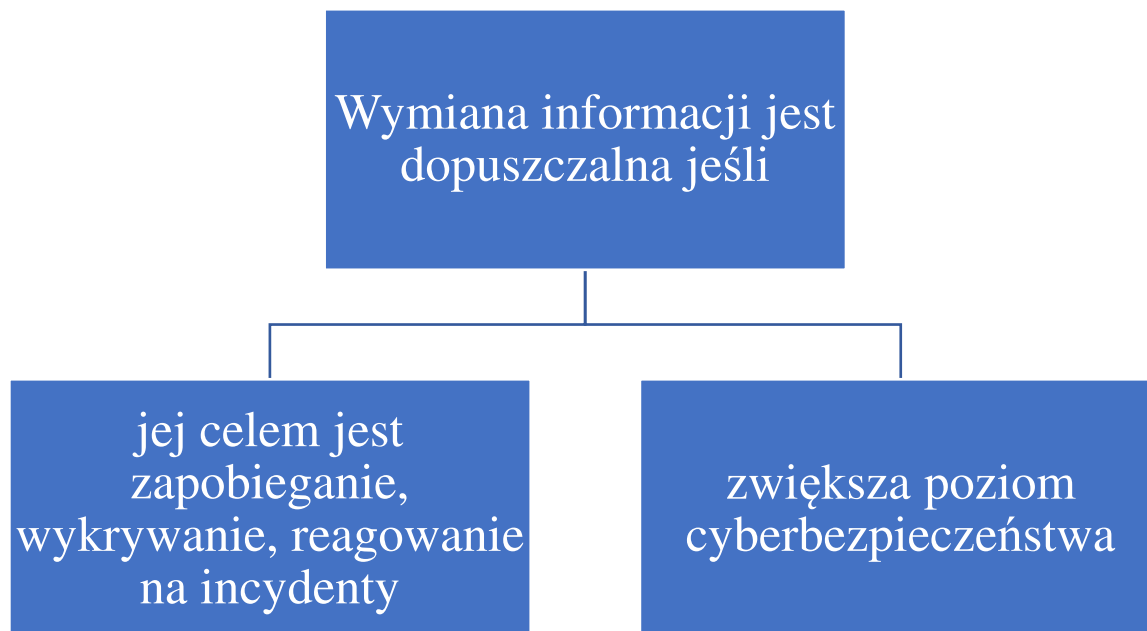
<https://www.csirt.gov.sk/csirt-sk-description-document-according-to-rfc-2350.html>

<https://www.ncsc.gov.ie/pdfs/RFC2350%20NCSC-IE.txt>

<i>podatność</i>	właściwości produktu ICT lub usługi ICT, która mogą być wykorzystane przez cyberzagrożenie
<i>techniki</i>	w tym kontekście - szczegółowy opis zachowania „actor” w kontekście jego taktyki – por. NIST-SP-800-150 ³⁹⁾
<i>procedury</i>	drobiazgowy opis działania aktora w kontekście jego techniki – por. NIST-SP-800-150
<i>oznaki naruszenia integralności systemu informacyjnego</i>	ang. indicators of compromise - mogą to być artefakty lub zdarzenia wskazujące na naruszenie integralności systemu – por. NIST-SP-800-150
<i>wrogie taktyki</i>	generalny opis działania <i>actora</i> – por. NIST-SP-800-150
<i>grupy przestępcze</i>	grupy sponsorowane przez obce państwa działające agresywnie w cyberprzestrzeni grupy typu Private Sector Offensive Actors typowe grupy cyberprzestępców hacktywiści
<i>ostrzeżenia dotyczące cyberbezpieczeństwa</i>	porady, biuletyny, informacje o podatnościach, exploitach itd. przykładowo alerty amerykańskiej agencji CISA
<i>zalecenia dotyczące konfiguracji narzędzi bezpieczeństwa</i>	informacje o ustawieniu i skonfigurowaniu narzędzi służących automatycznemu zbieraniu, wymianie analizie

³⁹⁾ C. Johnson i in., Guide to Cyber Threat Information Sharing, National Institute of Standards and Technology, 4 października 2016 r., <https://csrc.nist.gov/pubs/sp/800/150/final>.

	i wykorzystaniu informacji o cyberzagrożeniach



Komunikacja w tych sprawach ma odbywać się za pomocą systemu teleinformatycznego S46, który będzie dedykowanym kanałem komunikacji do kwestii cyberbezpieczeństwa. Podmioty krajowego systemu cyberbezpieczeństwa mogą również zawierać porozumienia dotyczące wzajemnej wymiany informacji. Takie porozumienia mogą stać się podstawą do wymiany informacji w danym sektorze i pozwolą usprawnić przepływ informacji tak, aby informacje docierały do podmiotów, które tego najbardziej potrzebują. Porozumienia mogą być zawierane również przez organizacje społeczne zrzeszające podmioty kluczowe i podmioty ważne – przykładowo izby gospodarcze. Należy podkreślić, że przepis ten umieszcza w ramach ustawy również już funkcjonujące porozumienia, np. ISAC-Kolej. Nie zdecydowano się przy tym na nadanie osobowości prawnej inicjatywom typu ISAC tudzież nadania im statusu ułamnej osoby prawnej. W polskiej praktyce kilka istniejących tego typu inicjatyw ma charakter luźnych porozumień. Postanowiono więc nie zmieniać tego stanu rzeczy. Wprowadzenie formy prawnej ISAC jako (ułamnej) osoby prawnej powodowałoby dodatkowe obowiązki po stronie ISAC np. obowiązek prowadzenia uproszczonej rachunkowości. Wprowadzono przy tym przepis względnie obowiązujący, zgodnie z którym koszt wykonania porozumień o wymianie informacji ponoszą w równych częściach strony porozumienia, chyba, że

postanowią one inaczej. Przykładowo może zaistnieć z pozoru błaha kwestia – kto ma zapłacić za utrzymanie strony internetowej ISAC.

Wskazano przy tym, że wymieniając informacje o cyberbezpieczeństwie podmioty kluczowe i podmioty ważne oznaczają zakres odbiorców tych informacji. Odbiorca informacji może ją udostępniać w zakresie określonym przez wytwórcę informacji. W praktyce nadawca informacji może skorzystać z zestawu *Traffic Light Protocol* ustandaryzowanego przez organizację FIRST⁴⁰⁾.

Źródło: <https://cert.pl/tlp/>

Traffic Light Protocol jest to zestaw reguł, pogrupowanych w 4 kategorie, używanych w celu lepszego zdefiniowania grupy odbiorców wrażliwych informacji. Dla ułatwienia kategorie opisywane są czterema kolorami (czerwony, pomarańczowy, zielony oraz biały). Zakwalifikowanie do odpowiedniej kategorii leży po stronie organizacji, z której pochodzą informacje. Jeśli odbiorca chciałby podzielić się uzyskanymi informacjami z szerszym gronem, musi uzyskać odpowiednią akceptację od autora wiadomości.

Znaczenie kolorów TLP dla odbiorców wiadomości

TLP:RED

Odbiorcy nie mogą dzielić się przekazanymi informacjami z nikim, z wyjątkiem innych odbiorców tych wiadomości.

TLP:AMBER

Odbiorcy mogą dzielić się informacjami jedynie w obrębie swojej organizacji (a także jej klientów i konsultantów) z osobami, które muszą poznać wiadomości oraz jedynie w zakresie niezbędnym do podjęcia stosownych działań. Dodatkowe ograniczenia mogą zostać wyspecyfikowane przez nadawcę w dowolnym zakresie i muszą być przestrzegane. Jednym ze standardowych ograniczeń jest oznaczenie **TLP:AMBER+STRICT**, które pozwala dzielić się informacjami wyłącznie w obrębie organizacji.

TLP:GREEN

Odbiorcy mogą dzielić się informacjami ze swoimi współpracownikami, w ramach swojej i partnerskich organizacji oraz w swoim środowisku. Nie można jednak udostępniać tych informacji przez publiczne kanały informacyjne.

TLP:CLEAR

Dystrybucja informacji nie podlega żadnym ograniczeniom (z wyjątkiem praw autorskich).

Znaczenie kolorów TLP dla autorów wiadomości

TLP:RED

Oznaczenie wiadomości, które mogą za sobą nieść poważne zagrożenie ujawnienia wrażliwych danych w wyniku ich nieprawidłowego przetworzenia, jak również, gdy ich wykorzystanie przez innych niż odbiorcy nie ma sensu.

⁴⁰⁾ <https://www.first.org/tlp/>

TLP:AMBER

Oznaczenie wiadomości wymagających podjęcia odpowiednich kroków przez dodatkowe osoby. Informacje te niosą ze sobą ryzyko ujawnienia zbyt wielu wrażliwych danych, jeśli zostałyby przekazane podmiotom innym niż bezpośrednio zaangażowanym.

TLP:GREEN

Oznaczenie wiadomości niosących ze sobą informacje ogólnie przydatne dla wszystkich organizacji partnerskich oraz w obrębie środowiska.

TLP:CLEAR

Oznaczenie wiadomości, których wykorzystanie nie powinno wiązać się z żadnym bądź minimalnym ryzykiem niewłaściwego użycia.

Informację o użytym TLP umieszczamy w nagłówku lub stopce przekazywanej wiadomości, przeważnie stosując zapis w formacie: "TLP:[Kolor]". Należy mieć na uwadze, że Traffic Light Protocol nie ma zastosowania do informacji niejawnych.

Nie wprowadza się obowiązku korzystania z TLP, ale jest to bardzo popularny standard oznaczania wiadomości. Nadawca informacji może określić inaczej zakres udostępniania informacji.

Odbiorca informacji może odpowiadać cywilnie za wyrządzenie szkody wywołanej przez ujawnienie informacji niezgodnie z zakresem przedstawionym przez nadawcę informacji.

Należy przy tym traktować przepisy ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych jako *lex specialis* względem proponowanego uprawnienia do wymiany informacji – w szczególności dotyczy do klasyfikacji informacji jako niejawnych i udostępnianie ich w ściśle określonym trybie.

2.6.6. Kolizja przepisów ustawy i rozporządzenia DORA

W zakresie sektora bankowości i infrastruktury rynków finansowych ustawa wskazuje, że pierwszeństwo przed nią mają przepisy rozporządzenia DORA. Ma to wyeliminować wątpliwości wynikające z funkcjonowania w tym obszarze, tych dwóch aktów prawnych. Dyrektywa NIS 2 w artykule 4 wskazuje na pierwszeństwo sektorowych aktów unijnych z zakresu cyberbezpieczeństwa w zakresie środków zarządzania ryzykiem oraz zgłaszania incydentów. Komunikat Komisji – Wytoczne Komisji dotyczące stosowania art. 4 ust. 1 i 2 dyrektywy (UE) 2022/2555 (NIS 2) 2023/C 328/02 (Dz. Urz. UE C 328 z 18.9.2023, str. 2) wskazuje, że rozporządzenie DORA jest takim aktem w zakresie podmiotów kluczowych i podmiotów ważnych z sektora bankowości i infrastruktury rynków finansowych. Zgodnie

z proponowanym art. 8i w ustawie o KSC pierwszeństwo nad ustawą o KSC mają regulacje DORA, z tym że do podmiotów kluczowych i podmiotów ważnych z sektora bankowości i infrastruktury rynków finansowych stosuje się przepisy art. 3a (czynności dopuszczalne w ramach obsługi incydentów), art. 5 ust. 1–3 (kryteria podmiotu kluczowego i podmiotu ważnego), art. 7–7m (przepisy o wykazie podmiotów kluczowych i podmiotów ważnych), art. 8 ust. 1 pkt 1 (obowiązek prowadzenia systematycznego szacowania ryzyka wystąpienia incydentu) i pkt 2 lit. j (obowiązek stosowania podstawowych zasad cyberhigieny), art. 8h (dopuszczalność wymiany informacji), art. 9 (obowiązki w zakresie wyznaczenia osób kontaktowych), art. 11 ust. 1 pkt 5 i 6 (współdziałanie z CSIRT podczas zgłoszenia incydentów), art. 13 (dobrowolne przekazywanie informacji do CSIRT), art. 15 (audyty), art. 16 (stosowanie obowiązków po raz pierwszy), art. 26a ust. 2–4 (zgłoszenia podatności w ramach skoordynowanego ujawniania podatności), art. 32 (uprawnienie CSIRT do wykonywania niezbędnych działań technicznych), art. 33 ust. 5, 7 oraz 8 (rekomendacje Pełnomocnika), art. 36a, art. 36b (ocena bezpieczeństwa), art. 37 (wyłączenie ustawy z dnia 6 września 2021 r. o dostępie do informacji publicznej przy informacjach o podatnościach, incydentach i cyberzagrożeniach), art. 43 (uprawnienie organu do żądania informacji), art. 45 ust. 3, art. 46 ust. 1 pkt 1, 2, 4–7 i oraz ust. 4–6 (obowiązek korzystania z systemu teleinformatycznego S46), art. 67a (rekomendacje Pełnomocnika), art. 67c, art. 67d oraz, art. 67g, art. 67h oraz art. 67i (postępowanie w sprawie uznania za dostawcę wysokiego ryzyka oraz polecenie zabezpieczające) ustawy o KSC.

2.6.7. Obowiązki podmiotów kluczowych w zakresie kontaktów z innymi podmiotami i użytkownikami

Podmioty kluczowe i podmioty ważne muszą również wyznaczyć dwie osoby do kontaktów z innymi podmiotami krajowego systemu cyberbezpieczeństwa. To rozwiązanie wynika z dotychczasowych doświadczeń w ramach krajowego systemu cyberbezpieczeństwa. Dotychczasowy obowiązek wyznaczenia jednej osoby do kontaktu sprawiał, że w przypadku gdy osoba ta przebywała na zwolnieniu lekarskim lub z innych powodów była nieobecna w pracy, zespoły CSIRT miały trudności ze skontaktowaniem się z podmiotami, w których wystąpił incydent. Dwie osoby mają zagwarantować, że zawsze będzie można nawiązać kontakt. Podmiot będący mikroprzedsiębiorcą lub małym przedsiębiorcą wyznaczy jedną osobę, ponieważ obowiązek wyznaczenia dwóch osób mógłby być zbyt dużym obciążeniem.

Podmioty te mają również obowiązek zapewniania użytkownikowi usługi dostępu do wiedzy pozwalającej na zrozumienie cyberzagrożeń i stosowanie skutecznych sposobów

zabezpieczania się przed tymi zagrożeniami w zakresie związanym ze świadczonymi usługami. Użytkownicy muszą posiadać aktualne informacje, aby być w stanie chronić się przed zagrożeniami. Wprowadza się przy tym pewne ułatwienie w stosowaniu tego przepisu – będzie można wykonać ten obowiązek przez odesłanie do stron internetowych organu właściwego do spraw cyberbezpieczeństwa, CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT sektorowego.

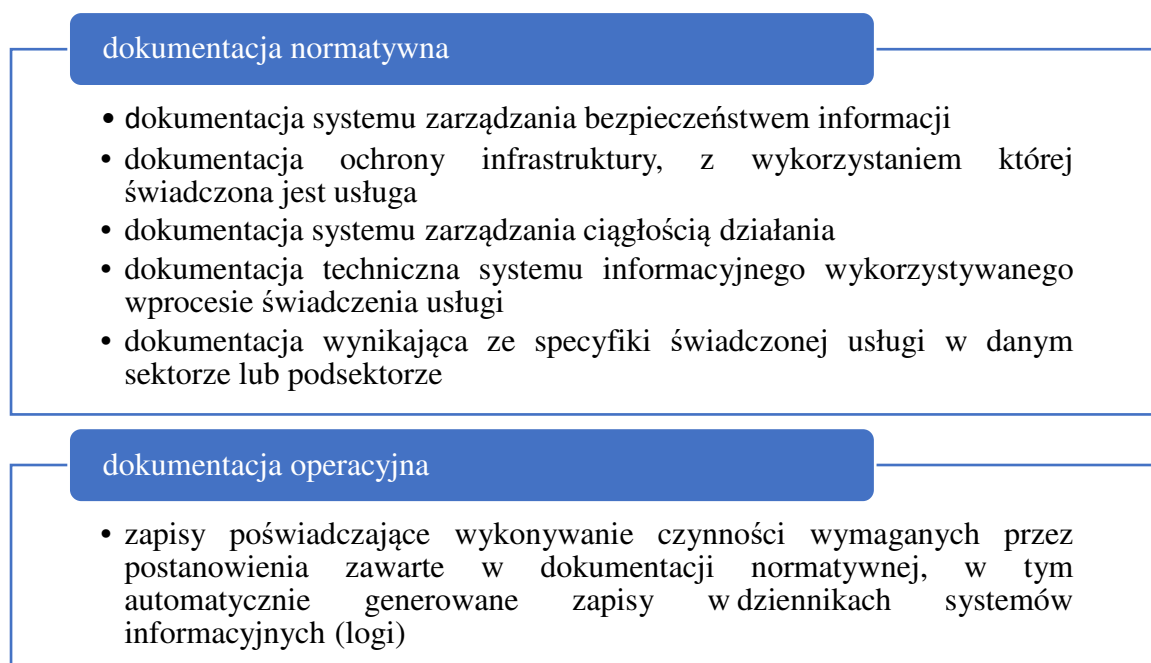
Każdy podmiot kluczowy oraz podmiot ważny powinien zapewnić możliwość zgłaszania przez swoich użytkowników cyberzagrożeń, podatności czy incydentu związanego z usługą świadczoną przez podmiot. Forma zgłoszenia należy już do podmiotu – czy to będzie odrębny adres poczty elektronicznej, czat na stronie internetowej, adres do doręczeń elektronicznych w przypadku podmiotów zobowiązanych do stosowania ustawy o doręczeniach elektronicznych.

2.6.8. Dokumentacja SZBI

Przepisy projektu ustawy precyzują również kwestię dokumentacji jaką muszą przechowywać podmioty kluczowe i podmioty ważne. W tym zakresie przeniesiono dotychczasowe przepisy rozporządzenia i nadano im rangę ustawową. Dokumentacja dotyczy bezpieczeństwa systemu informacyjnego wykorzystywanego w procesie świadczenia usługi i może być prowadzona w postaci elektronicznej lub w postaci papierowej.

Zakres dokumentacji podzielono na 2 części. Dokumentacja normatywna to ta część dokumentacji, która opisuje świadczoną usługę, systemy, infrastrukturę oraz funkcjonowanie bezpieczeństwa informacji w podmiocie. Dokumentacja operacyjna potwierdza wykonywanie czynności opisanych w dokumentacji normatywnej.

Rysunek 2 Dokumentacja w nowelizacji ustawy o KSC



Rysunek 3 Zakres przedmiotowy dokumentacji ochrony infrastruktury

Dokumentacja ochrony infrastruktury obejmuje:	charakterystykę usługi oraz infrastruktury, w której świadczona jest usługa
	ocenę aktualnego stanu ochrony infrastruktury
	szacowanie ryzyka dla obiektów infrastruktury
	plan postępowania z ryzykiem
	opis zabezpieczeń technicznych obiektów infrastruktury
	zasady organizacji i wykonywania ochrony fizycznej infrastruktury
dane o specjalistycznej uzbrojonej formacji ochronnej, o której mowa w art. 2 pkt 7 ustawy z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz. U. z 2021 r. poz. 1995), chroniącej infrastrukturę	

Podkreślić należy, że przepis wskazuje zakres przedmiotowy dokumentacji. Może powstać z tego jeden dokument albo kilka. To należy już do decyzji podmiotu kluczowego i podmiotu ważnego. Istotne jest, aby zakres dokumentacji został zachowany.

Ważne jest, aby podmiot dbał o bezpieczeństwo dokumentacji. Należy zapewnić dostępność dokumentacji dla uprawnionych osób (zasada need to know) w zakresie niezbędnym do realizacji zadań. Ograniczy to ryzyko ujawnienia informacji z dokumentacji osobom

nieuprawnionym. Organizacja powinna ustalić kto i w jakim zakresie ma dostęp do dokumentacji – na żądanie kontroli należy przedstawić dowód przypisania dostępu do dokumentacji. Podmiot powinien także chronić dokumenty pod kątem fizycznym – ochrona przed uszkodzeniem (uszkodzenie papieru czy dysku), zniszczeniem, utratą, nieuprawnionym dostępem, niewłaściwym użyciem lub utratą integralności. Konieczne jest wskazanie kto odpowiada za dokumentację, kto ma ją chronić oraz jakie środki wdrożono, aby chronić dokumentację np. szkolenia, środki fizyczne (przechowywanie papierowej dokumentacji w zamkniętym pomieszczeniu czy szafie), środki techniczne np. szyfrowanie plików z dokumentacją. Pamiętać także należy o oznaczaniu kolejnych wersji dokumentów – ułatwi to identyfikację zmian i odnalezienie aktualnej wersji.

Dla celów zapewnienia efektywnej kontroli podtrzymuje się dotychczasowy przepis ustawy o przechowywaniu dokumentacji. Dostosowuje się go tylko do zmian terminologicznych i wprowadza zmiany redakcyjne.

Aby potwierdzić, że zniszczona dokumentacja w ogóle zaistniała czynność zniszczenia potwierdza się protokołem brakowania. Te protokoły przechowuje się w sposób trwały, aby były dostępne dla kontrolerów.

2.7. Zgłaszanie incydentów

Dyrektywa NIS 2 wprowadziła nowe rozwiązania w zakresie zgłaszania incydentów poważnych. Zgodnie z proponowanymi rozwiązaniami incydenty poważne zgłaszane będą do CSIRT sektorowego. Wskazanie CSIRT sektorowego jako podmiotu przyjmującego zgłoszenie o incydencie związane jest z zadaniami jakie CSIRT ten będzie realizował, tj. oprócz reagowania na incydenty, współpraca z podmiotami kluczowymi i ważnymi z danego sektora, dzięki temu CSIRT sektorowy będzie znał specyfikę danego sektora co umożliwi skuteczną obsługę incydentów. Zgłoszenie wczesnego ostrzeżenia i zgłoszenie incydentu poważnego będzie dokonywane za pośrednictwem systemu teleinformatycznego S46, takie rozwiązanie spowoduje, iż informacja o tych zgłoszeniach będzie dostępna dla pozostałych CSIRT, w tym również CSIRT poziomu krajowego. W pierwszej kolejności podmiot kluczowy i podmiot ważny zobowiązany będzie do zgłoszenia wczesnego ostrzeżenia o incydencie poważnym niezwłocznie nie później niż w ciągu 24 godzin od momentu wykrycia incydentu poważnego. Zgłoszenie wczesnego ostrzeżenia może zawierać wniosek o wskazanie wytycznych dotyczących możliwych do wdrożenia środków ograniczających skutki incydentu poważnego lub o dodatkowe wsparcie techniczne przy obsłudze incydentu. Jeżeli incydent

poważny wyczerpuje znamiona przestępstwa CSIRT sektorowy przekazuje informacje o sposobie zgłoszenia tego faktu organom ścigania. CSIRT sektorowy zobowiązany będzie w terminie 24 godzin udzielić wsparcia zgodnie z treścią wniosku.

Wczesne ostrzeżenie zawiera m.in.

- 1) dane podmiotu zgłaszającego – w tym firmę przedsiębiorcy, numer z właściwego rejestru, siedzibę i adres – chodzi o konieczność zapewnienia identyfikacji podmiotu zgłaszającego wczesne ostrzeżenie;
- 2) imię i nazwisko, numer telefonu służbowego oraz służbowy adres poczty elektronicznej osoby dokonującej zgłoszenia;
- 3) imię i nazwisko, numer telefonu służbowego oraz adres służbowej poczty elektronicznej osoby uprawnionej do składania wyjaśnień dotyczących zgłaszanych informacji. W zależności od okoliczności osoba dokonująca zgłoszenia może być jednocześnie osobą uprawnioną do składania wyjaśnień. Może być też inaczej, stąd zasadne jest wyodrębnienie tych kategorii osób;
- 4) wskazanie momentu wystąpienia i wykrycia incydentu poważnego oraz czas jego trwania – jest to istotne dla CSIRT który może również dokonać korelacji tych danych z innymi dostępnymi informacjami o innych incydentach i np. zidentyfikować działania grup wrogich aktorów;
- 5) wskazanie, czy incydent poważny został wywołany działaniem bezprawnym lub działaniem w złej wierze, jeżeli możliwe jest dokonanie takiej oceny – dzięki tej informacji CSIRT będzie wiedział, czy konieczne jest zaangażowanie organów ścigania;
- 6) określenie, czy incydent dotyczy innych państw członkowskich Unii Europejskiej – jest to konieczne do określenia ewentualnego wpływu transgranicznego.

Natomiast w ciągu 72 godzin podmiot kluczowy i podmiot ważny zgłasza incydent poważny wraz z dodatkowymi informacjami o tym incydencie:

- 1) opis wpływu incydentu poważnego na świadczenie usługi, w tym:
 - a) wskazanie usługi zgłaszającego, na które incydent poważny miał wpływ.

Aby pomóc podmiotowi zgłaszającemu incydent CSIRT musi wiedzieć na świadczenie jakich usług wpływa incydent,

- b) liczbę użytkowników usługi, na których incydent poważny miał wpływ.

Chodzi o szacunkowe określenie liczby użytkowników na których oddziałuje incydent,

c) zasięg geograficzny obszaru, którego dotyczy incydent poważny.

Chodzi o określenie obszaru na który wpływa incydent poważny, przykładowo ten obszar może obejmować niedostępność usług telekomunikacyjnych na terenie dwóch powiatów, albo brak prądu w mieście wojewódzkim spowodowany awarią systemów sterowania,

d) wpływ incydentu poważnego na świadczenie usługi przez inne podmioty.

Podmiot kluczowy i podmiot ważny powinien, w ramach analizy kontekstu organizacji ustalić podmioty z którymi współpracuje i którym świadczy usługi. Będzie więc mógł określić, czy incydent wpływa na te podmioty czy nie;

- 2) opis przyczyn tego incydentu, sposób jego przebiegu oraz prawdopodobne skutki oddziaływania na systemy informacyjne lub świadczone usługi.

Przykładowo należy wskazać oznaki naruszenia integralności systemu (indicators of compromise);

- 3) informacje o podjętych działaniach zapobiegawczych;
- 4) informacje o podjętych działaniach naprawczych;
- 5) aktualizację informacji przekazanych we wczesnym ostrzeżeniu, jeżeli nastąpiła ich zmiana.

Nie zawsze wszystkie informacje będą dostępne w trakcie zgłaszania incydentu poważnego, dlatego podmiot kluczowy lub podmiot ważny będzie obowiązany zgłosić te informacje, o których wie na moment zgłoszenia. Będzie przy tym zobligowany uzupełnić te informacje później w trakcie obsługi incydentu.

Dostawcy usług zaufania zgodnie z dyrektywą NIS 2 zgłaszają incydenty poważne nie w terminie 72 godzin od jego wystąpienia, tylko w terminie 24 godzin od ich wystąpienia. Odzwierciedlono to w przepisach projektu ustawy.

Dane przekazywane w zgłoszeniu incydentu mogą stanowić tajemnice prawnie chronione w tym tajemnicę przedsiębiorstwa. Jednocześnie są one potrzebne aby zespół CSIRT był w stanie efektywnie pomóc podmiotowi. Dlatego podmiot kluczowy lub podmiot ważny zgłaszający incydent ma obowiązek przekazać we wczesnym ostrzeżeniu lub w zgłoszeniu incydentu informacje stanowiące tajemnice prawnie chronione. Jednocześnie zespoły CSIRT są obowiązane zachować te informacje w tajemnicy. Informacje te powinny być stosownie oznaczone we wczesnym ostrzeżeniu lub zgłoszeniu incydentu, aby CSIRT wiedział które informacje w szczególny sposób musi chronić.

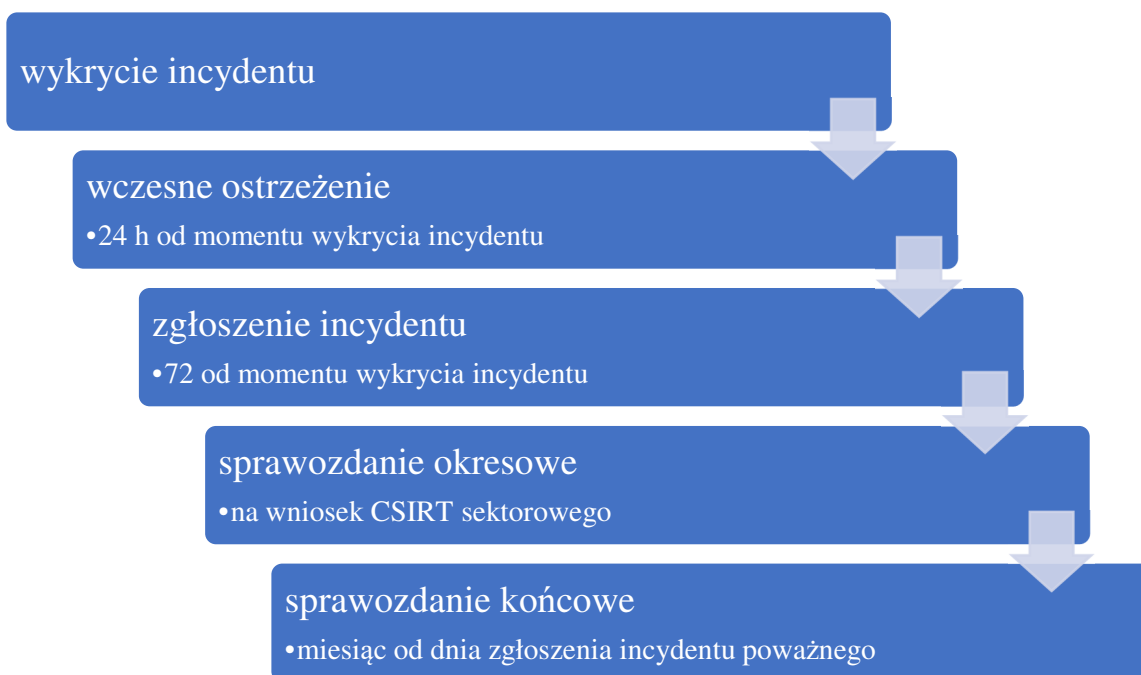
Może się okazać, że do realizacji zadań CSIRT – przede wszystkim zadania reagowania na incydenty – przekazane informacje są niewystarczające. Dlatego zespoły CSIRT są uprawnione do zwracania się do podmiotu kluczowego i podmiotu ważnego o uzupełnienie wczesnego ostrzeżenia czy zgłoszenia incydu.

W trakcie obsługi incydu powaźnego podmiot zgłaszający incydent, na wniosek CSIRT sektorowego, przekazują sprawozdanie okresowe z obsługi tego incydu. Natomiast sprawozdanie końcowe z obsługi incydu powaźnego przekazywane będzie nie później niż w ciągu miesiąca od dnia zgłoszenia incydu. Podsumowuje ono obsługę incydu powaźnego. Zawiera ono:

- 1) szczegółowy opis incydu powaźnego, w tym spowodowane zakłócenia i szkody;
- 2) rodzaj zagrożenia lub przyczynę, która prawdopodobnie była źródłem incydu;
- 3) zastosowane i wdrażane środki ograniczające ryzyko;
- 4) w odpowiednich przypadkach transgraniczne skutki incydu.

Podsumowując sprawozdanie końcowe opisuje co się stało, przyczynę, działania następce oraz transgraniczne skutki incydu. Dzięki takiemu sprawozdaniu zarówno podmiot kluczowy i podmiot ważny jak i zespół CSIRT są w stanie wyciągnąć wnioski z incydu na przyszłość, ewentualnie wrócić do dokumentacji obsługi konkretnego incydu, jeżeli w przyszłości pojawi się inny podobny incydent. Świadomość tego jak postąpiło się z podobnym incydem pomoże przy obsłudze kolejnych tego typu zdarzeń.

Jeżeli jednak obsługa incydu powaźnego nie zakończyła się w terminie miesiąca podmiot zgłaszający incydent powaźny przesyła sprawozdanie z postępu obsługi incydu, a sprawozdanie końcowe w terminie miesiąca od zakończenia obsługi tego incydu.



Progi uznania incydentu za incydent poważny zostaną określone w drodze rozporządzenia przez Radę Ministrów. Przy czym w tym rozporządzeniu nie będą określone progi incydentów dla podmiotów, dla których progi te ustaliła Komisja Europejska w bezpośrednio stosownym akcie wykonawczym wydanym na podstawie art. 23 ust. 11 dyrektywy NIS 2. Prawo krajowe nie może wkraczać w kwestie uregulowane bezpośrednio stosownym akcie prawa unijnego.

Przepisy dyrektywy NIS 2 jak i nowelizacji przewidują także obowiązek poinformowania użytkowników podmiotu kluczowego lub podmiotu ważnego o możliwych środkach zapobiegawczych przed poważnym cyberzagrożeniem. Przydatny do realizacji tego obowiązku może być ten szablon⁴¹⁾:

1. Informacja o cyberzagrożeniu	
1.1. Nazwa	Ogólna nazwa zagrożenia
1.2. Data	data
1.3. Opis	Krótki opis zagrożenia
1.4. Źródła	Źródło pozyskania informacji o cyberzagrożeniu
1.5. Charakter cyberzagrożenia	Np. awaria systemu, błąd ludzki, zjawiska naturalne, złośliwe działanie (malicious action), błędy po stronie osób trzecich

⁴¹⁾ Szablon opracowano na podstawie: . European Union Agency for Cybersecurity, *Cyber threats outreach in telecom: guidelines for national authorities and telecom providers on outreach to users about cyber threats.*, 2022, s. 27. <https://www.enisa.europa.eu/publications/cyber-threats-outreach-in-telecom>.

1.6. Prawdopodobny wpływ na systemy informacyjne i usługi	Opisać prawdopodobny wpływ na systemy i usługi na podstawie dostępnej wiedzy.
2. Kiedy komunikować?	
2.1. Właściwości techniczne cyberzagrożenia	Krótki opis szczegółów technicznych cyberzagrożenia
2.2. Czy cyberzagrożenie może mieć wpływ na bezpieczeństwo systemów informacyjnych?	Tak lub Nie
2.3. Czy cyberzagrożenie może mieć wpływ na użytkowników?	Tak lub NIE
2.4. Czy ten wpływ jest poważny?	Należy oszacować wpływ w oparciu o przyjętą w organizacji metodę szacowania ryzyka. Na pewno wpływ cyberzagrożenia będzie większy, jeśli nie jest to typowe lub generalnie występujące cyberzagrożenie. Ponadto
<i>Jeśli na 2.2 lub 2.3 oraz 2.4 odpowiedź brzmi TAK</i>	
2.5. Czy może wywołać szkodę materialną – jaką?	Opisać krótko możliwe szkody materialne, które może wywołać cyberzagrożenie – wedle najlepszej dostępnej wiedzy – nie chodzi o wycenianie potencjalnej szkody materialnej, ale o jej świadomość np. cyberzagrożenie może spowodować przestoje w dostawach prądu, co uniemożliwi prowadzenie działalności gospodarczej.
2.6. Czy może wywołać szkodę niematerialną – jaką?	Opisać krótko możliwe szkody niematerialne, np. szkody wizerunkowe, szkody zdrowotne.
<i>Jeśli na 2.5 lub 2.6 odpowiedź brzmi TAK</i>	
2.7. Czy szkoda może być poważna?	Ocenić potencjalną szkodę.
2.8. Czy należy zakomunikować środki zaradcze?	Jeśli zidentyfikowano, że cyberzagrożenie może mieć poważny wpływ na bezpieczeństwo systemów informacyjnych lub użytkowników oraz może spowodować poważną szkodę – materialną lub niematerialną – należy zakomunikować środki zapobiegawcze użytkownikom.
3. Komunikacja	
3.1. Kanał komunikacji	Wybrać kanał komunikacji adekwatny do zagrożenia i użytkowników – wiadomość email, SMS, media społecznościowe, aplikacja mobilna, strona internetowa
3.2. Środki zapobiegawcze	W komunikacji wskazać środki, które użytkownicy mogą podjąć, aby zabezpieczyć się lub ograniczyć skutki poważnego cyberzagrożenia, np. rekomendacja instalacji oprogramowania antywirusowego, włączenie wieloskładnikowego uwierzytelnienia, edukacja z zakresu nowych zagrożeń,

3.3. Czy informować o samym poważnym cyberzagrożeniu?	Oszacować ryzyko dla komunikacji informacji o samym cyberzagrożeniu.
4. Ewaluacja – czy komunikacja była skuteczna?	
4.1. Czy komunikacja dotarła do użytkowników?	Przeanalizować dostępne logi z użytych kanałów komunikacji np. liczba unikalnych wejść na stronę.
4.2. Czy użytkownicy podjęli działania?	Przeanalizować dostępne informacje zwrotne od użytkowników np. reakcje w mediach społecznościowych.
4.3. Inne mierniki	Przeanalizować inne mierniki, jeśli są dostępne.

Wprowadza się także przepis, zgodnie z którym podmiot kluczowy lub podmiot ważny ma obowiązek poinformować użytkowników swoich usług o incydencie poważnym, jeżeli ma on niekorzystny wpływ na świadczenie usług. Niekorzystny wpływ to taki wpływ, który przynosi straty dla użytkowników, np. tracą czas, pieniądze czy w niektórych przypadkach zdrowie. Stąd też w takich sytuacjach należy ich informować o incydencie poważnym.

Obecny art. 13 ustawy o KSC umożliwia dobrowolne zgłaszanie do zespołów CSIRT poziomu krajowego jak również CSIRT sektorowego informacji o incydentach nie podlegających obowiązkowemu zgłoszeniu, o cyberzagrożeniach, wynikach szacowania ryzyka, podatnościach, potencjalnych zdarzeniach dla cyberbezpieczeństwa czy wykorzystywanych technologiach⁴²⁾. Przepis ten dostosowano do innych zmian, rozszerzając te uprawnienie na wszystkie podmioty kluczowe i podmioty ważne. Dodatkowo wskazano, że zgłoszenia te są dokonywane za pomocą systemu teleinformatycznego S46. Jest to ważny przepis ponieważ umożliwia dzielenie się informacjami z zespołami CSIRT, które mogą przeanalizować je i wyciągnąć wnioski, które pozwolą na lepsze wspieranie podmiotów kluczowych i podmiotów ważnych. Przykładowo informacje o podatnościach pozwolą na opracowanie sposobów ich mitygacji. Zapewniono przy tym możliwość ochrony informacji prawnie chronionych – w tym celu podmiot kluczowy i podmiot ważny ma obowiązek oznaczyć tego rodzaju informacje.

2.8. Realizacja obowiązków z zakresu cyberbezpieczeństwa

Tak jak przy obecnej treści ustawy o KSC przepisy będą od tej pory wskazywać, że podmiot kluczowy lub podmiot ważny realizuje zadania za pomocą wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo (np. komórka organizacyjna w danym podmiocie, niezależnie od jej nazwy, ale zajmująca się cyberbezpieczeństwem) lub zawiera umowę

⁴²⁾ Technologie należy rozumieć szeroko, jako produkty, usługi, procesy ICT.

z dostawcą usług zarządzanych w zakresie cyberbezpieczeństwa. Kluczowy jest tutaj spójnik „lub” – chodzi o możliwość outsourcingu tylko niektórych zadań. Decyzja o wyborze modelu realizacji zadań należy do podmiotu kluczowego lub podmiotu ważnego. Podkreślić jednak należy, że musi być ona rozsądna. Zadania z zakresu cyberbezpieczeństwa nie powinny być powierzane np. przeciążonemu działowi help-desk, ponieważ nie będą one realizowane efektywnie.

Traci moc rozporządzenie Ministra Cyfryzacji z dnia 4 grudnia 2019 r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo (Dz. U. poz. 2479), które było wydane na podstawie obecnego art. 14 ustawy o KSC. Przede wszystkim dotychczasowe podmioty świadczące usługi z zakresu cyberbezpieczeństwa staną się pod rządami znowelizowanej ustawy dostawcami usług zarządzanych z zakresu cyberbezpieczeństwa i będą podlegały wymogom wdrożenia systemu zarządzania bezpieczeństwem informacji. Wprowadzanie odrębnych wymogów dla nich jest zbędne, wobec tego przepisy ww. rozporządzenia wymagają uchylenia.

2.9. Audyt

Podmioty kluczowe mają obowiązek zapewnić przeprowadzenie, na własny koszt, co najmniej raz na 3 lata, audytu bezpieczeństwa systemu informacyjnego wykorzystywanego w procesie świadczenia usługi. Musi on być przeprowadzony przez podmiot posiadający odpowiednią akredytację, dwóch audytorów legitymujących się odpowiednimi certyfikatami i doświadczeniem lub przez CSIRT sektorowy. Audyty na zgodność należy rozumieć jako przeprowadzane na zgodność z przepisami ustawy. Audyt, o którym mowa w projektowanym art. 15 ust. 1, może być audytem wewnętrznym lub zewnętrznym. Te przepisy są analogiczne do obecnych rozwiązań w tym zakresie i nie wprowadzają istotnych zmian. Audyt powinien dotyczyć całego systemu informacyjnego wykorzystywanego przez dany podmiot, a nie jedynie jego części związanych z konkretną usługą. Wynika to z tego, że dzięki powiązaniom między poszczególnymi systemami można poprzez inne elementy systemu wpłynąć na kluczową działalność danego podmiotu.

Raportu z audytu musi być przekazany w postaci elektronicznej do organu właściwego do spraw cyberbezpieczeństwa w terminie 3 dni roboczych od otrzymania go od audytorów przez podmiot kluczowy. Jest to niezbędne, gdyż analiza raportów audytowych będzie jednym ze

skuteczniejszych środków nadzorczych przy tak dużej liczbie podmiotów podlegających ustawie. Wskazać jednak należy, że przekazanie raportu w tym terminie odnosi się do kopii tego raportu i dokonywane jest drogą elektroniczną.

Ponadto wdrożono tutaj postanowienia dyrektywy NIS 2 i wskazano, że organ właściwy do spraw cyberbezpieczeństwa będzie mógł nakazać przeprowadzenie audytu doraźnego przez podmiot kluczowy lub podmiot ważny. Audyt ten jest audytem zewnętrznym. W stosunku do podmiotów kluczowych będzie on mógł zostać zlecony w każdym czasie. Wynika to z charakteru nadzoru nad podmiotami kluczowymi – prowadzony jest on prewencyjnie i następczo. W stosunku do podmiotów ważnych taki audyt będzie mógł zostać zlecony wyłącznie w przypadku wystąpienia incydentu poważnego lub innego naruszenia przepisów ustawy. W decyzji nakazującej przeprowadzenie audytu doraźnego organ właściwy do spraw cyberbezpieczeństwa określi termin przekazania raportu z przeprowadzonego audytu i wskaże podmioty uprawnione do jego przeprowadzenia uwzględniając przepisy ustawy. Będzie mógł także określić zakres audytu. Brak określenia zakresu audytu równoważny jest z obowiązkiem przeprowadzenia audytu w pełnym zakresie. Decyzja nakazująca przeprowadzenie audytu doraźnego podlega natychmiastowemu wykonaniu.

Audyt systemu zarządzania bezpieczeństwem informacji musi być przeprowadzany przez audytorów obiektywnych, którzy nie będą stronniczy wobec podmiotu audytowanego. Dlatego wprowadza się regulację, zgodnie z którą audyt nie może być przeprowadzony przez osoby, które w podmiocie audytowanym przez rok przed rozpoczęciem audytu realizowały zadania z zakresu systemu zarządzania bezpieczeństwem informacji oraz zgłaszania i reagowania na incydenty lub realizują je nadal.

Ponadto realizacja obowiązku co do zapewnienia przeprowadzenia audytu bezpieczeństwa systemu informacyjnego wykorzystywanego w procesie świadczenia usługi nie zwalnia administratora – wykonawcy obowiązków z ustawy o KSC – z obowiązków wynikających z RODO w zakresie realizacji zasady poufności i integralności i konieczności wdrożenia odpowiednich środków technicznych i organizacyjnych z uwzględnieniem analizy ryzyka.

2.10. Wdrożenie obowiązków przez podmioty kluczowe i podmioty ważne po raz pierwszy

Należało przesądzić od kiedy podmioty kluczowe i podmioty ważne będą miały obowiązek wdrożenia obowiązków wynikających z nowelizacji ustawy o KSC. Obecnie momentem, od którego liczą się terminy na wdrożenie obowiązków przez operatorów usług kluczowych, jest

doręczenie decyzji o uznaniu za operatora usługi kluczowej. W projektowanych przepisach wskazano, że podmiot kluczowy i podmiot ważny realizuje swoje obowiązki w terminie 6 miesięcy od dnia spełnienia przesłanek uznania za podmiot kluczowy lub podmiot ważny. Audyt systemu będzie realizowany po raz pierwszy w terminie 24 miesięcy od dnia spełnienia przesłanek uznania za podmiot kluczowy.

2.11. Zadania i obowiązki rejestrów nazw domen najwyższego poziomu oraz zadania i obowiązki podmiotów świadczących usługi rejestracji nazw domen

Projekt ustawy nakłada szczególne obowiązki na rejestr nazw domen najwyższego poziomu (TLD) oraz podmioty świadczące usługi rejestracji nazw domen w zakresie gromadzenia i zachowywania z należytą starannością danych dotyczących rejestracji nazw domen. Podmioty te mają wprowadzić polityki i procedury, w tym procedury weryfikacji, służące zapewnieniu, aby bazy danych rejestracji domen zawierały dokładne i kompletne dane. Jest to szczególnie istotne gdyż informacje o domenach mogą być szczególnie istotne przy wykrywaniu źródeł cyberataków oraz niebezpiecznego ruchu sieciowego.

Podmioty świadczące usługi rejestracji nazw domen muszą współpracować z rejestrem nazw domen najwyższego poziomu dla danej domeny. Aby uniknąć dublowania obowiązków przepisy przewidują, że rejestr nazw domen najwyższego poziomu może umożliwić podmiotom świadczącym usługi rejestracji nazw domen wprowadzanie do bazy danych rejestru aktualnych danych o domenach.

Podkreślić należy, że zgodnie z definicją z dyrektywy NIS 2 podmiotem świadczącym usługi rejestracji nazw domen jest nie tylko rejestrator ale również i agent działający w imieniu rejestratorów. Przy czym działalność poprzez agenta nie zwalnia rejestratora z obowiązków wskazanych w przepisach ustawy o KSC.

Baza danych dotyczących rejestracji nazw domen zawiera:

- 1) nazwę domeny – jest to dosyć oczywiste, bez tej informacji ta baza nie ma sensu;
- 2) datę rejestracji;
- 3) imię i nazwisko lub nazwę abonenta nazwy domeny oraz adres poczty elektronicznej i numer telefonu;
- 4) adres poczty elektronicznej i numer telefonu, pod którymi można skontaktować się z punktem kontaktowym zarządzającym nazwą domeny, w przypadku gdy różnią się od adresu poczty elektronicznej i numeru telefonu abonenta nazwy domeny, a w przypadku gdy usługi punktu kontaktowego zarządzającego nazwą domeny nie są dopuszczone dla

konkretnej domeny najwyższego poziomu (TLD), należy podać co najmniej dane identyfikujące podmiot świadczący usługi rejestracji nazw domen.

Aby przepisy spełniały swój cel baza danych dotycząca rejestracji nazw domen musi być aktualna. Dlatego podmioty świadczące usługi rejestracji nazw domen oraz rejestry nazw domen najwyższego poziomu są obowiązane opracować i wdrożyć polityki i procedury weryfikacji danych. Muszą one być wzajemnie zgodne. Obejmują możliwość weryfikacji danych na etapie rejestracji domeny jak i po rejestracji.

Wyjaśnienia wymaga przepis, zgodnie z którym „w przypadku gdy podanie danych, w tym adresu poczty elektronicznej abonenta nazwy domeny, wymaga uzyskania zgody, obowiązek jej uzyskania obciąża podmiot przetwarzający te dane jako pierwszy”. Jest to związane przede wszystkim z tym, że abonent domeny zawiera umowę z rejestrem nazw domen najwyższego poziomu za pośrednictwem podmiotu świadczącego usługi rejestracji nazw domen. To podmiot świadczący usługi rejestracji nazw domen uzyskuje dane od abonenta jako pierwszy. I to ten podmiot powinien uzyskać zgodę, w tym zgodę w rozumieniu art. 7 ust. 1 RODO. Dane wobec których uzyskano zgodę są przekazywane do rejestru nazw domen najwyższego poziomu. Następnie ten rejestr publikuje te dane w ogólnodostępnej światowej bazie domen WHOIS. Zgodnie z informacjami NASK dotyczącymi publikacji informacji o abonentach w bazie WHOIS – „Dane te publikowane są, by zapewnić należyte poszanowanie praw użytkowników Internetu, właścicieli znaków towarowych, praw autorskich i innych dóbr prawnie chronionych. Zgodnie z przepisami prawa o ochronie danych osobowych, nie są publikowane dane abonentów będących osobami fizycznymi.”.

Polityki w tym zakresie muszą też być podane do publicznej wiadomości co gwarantuje transparentność tego procesu. Dane z rejestru będą również udostępniane na wniosek:

- 1) sądu – w celu przeprowadzenia dowodu w postępowaniu karnym, postępowaniu w sprawach o wykroczenia lub w postępowaniu cywilnym;
- 2) prokuratora – w celu przeprowadzenia dowodu w postępowaniu karnym lub postępowaniu w sprawach o wykroczenia;
- 3) Policji oraz innych upoważnionych organów w postępowaniu karnym i postępowaniu w sprawach o wykroczenia, w celu przeprowadzenia dowodu w postępowaniu karnym, postępowaniu w sprawach o wykroczenia oraz czynności w ramach postępowaniu o wykroczenia;
- 4) CSIRT sektorowego – w celu przeprowadzenia obsługi incydentu poważnego przez CSIRT sektorowy związanego z daną domeną;

- 5) CSIRT MON, CSIRT NASK lub CSIRT GOV – w celu przeprowadzenia obsługi incydentu poważnego lub incydentu krytycznego związanego z daną domeną;
- 6) podmiotowi wykonującemu postanowienie sądu w przedmiocie zabezpieczenia środka dowodowego, o którym mowa w art. 479¹⁰⁰ §1 ustawy z dnia 17 listopada 1964 r. – Kodeks postępowania cywilnego (Dz. U. z 2024 r. poz. 1568 i 1841 oraz z 2025 r. poz. 620, 1172 i 1302). Postanowienie to wydaje sąd w sprawach własności intelektualnej na wniosek uprawnionego, który uprawdopodobnił roszczenie, jak również interes prawny w zabezpieczeniu. Czyli sąd już zbadał interes prawny uprawnionego. Zwykle podmiotem wykonującym to postanowienie będzie komornik. Rozwiązanie to dodano z uwagi na to, że dyrektywa NIS 2 dopuszcza dostęp do danych dla osób z interesem prawnym, które np. chcą pozwać osobę dysponującą tytułem prawnym do domeny, na której naruszono prawa własności intelektualnej;
- 7) Prezesa Urzędu Komunikacji Elektronicznej – celu weryfikacji czy podmiot składający sprzeciw wobec wpisania domeny na listę ostrzeżeń, o którym mowa w art. 21 ust. 1 ustawy z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej (Dz. U. z 2024 r. poz. 1803) dysponuje do tej domeny tytułem prawnym Prezes Urzędu Komunikacji Elektronicznej rozpatruje sprzeciwy wobec wpisania domeny na listę ostrzeżeń prowadzoną przez CSIRT NASK. Aby móc zweryfikować, czy sprzeciw złożyła osoba uprawniona do danej domeny potrzebny jest dostęp do danych z bazy rejestracji nazw domen.

Pozwoli to na zwiększenie skuteczności walki z przestępczością w internecie, a w szczególności ze stronami internetowymi służącymi podszywaniu się pod inne podmioty.

Żądanie o udostępnienie danych będzie składane w postaci elektronicznej i opatrywane kwalifikowanym podpisem elektronicznym, podpisem zaufanym, podpisem osobistym albo kwalifikowaną pieczęcią elektroniczną.

Rejestry nazw domen najwyższego poziomu oraz podmioty świadczące usługi rejestracji nazw domen będą obowiązane do udzielenia odpowiedzi nie później niż w ciągu 72 godzin od dnia otrzymania żądania udostępnienia danych. Dyrektywa NIS 2 dała dużo swobody tym podmiotom, gdyż zgodnie z dyrektywą to rejestratorzy określają politykę i procedurę ujawniania danych dotyczących rejestracji domen.

2.12. Uchylenie rozdziału o obowiązkach dostawców usług cyfrowych i podmiotów publicznych

Ze względu na zmiany w strukturze krajowego systemu cyberbezpieczeństwa uchyla się rozdziały 4 i 5 ustawy o KSC dotyczące obowiązków dostawców usług cyfrowych i podmiotów publicznych. Te podmioty, zgodnie z dyrektywą NIS 2, staną się podmiotami kluczowymi i podmiotami ważnymi, w związku z czym nie jest zasadne utrzymywanie dla nich osobnych regulacji.

2.13. Uwspólnienie zadań z zakresu cyberbezpieczeństwa w podmiotach publicznych

Przepisy projektu ustawy umożliwiają ministrowi kierującemu działem administracji publicznej, kierownikowi urzędu centralnego, wojewodzie oraz jednostce samorządu terytorialnego wyznaczenie jednostki, która będzie realizowała zadania z zakresu cyberbezpieczeństwa w pozostałych jednostkach podległych danemu organowi. Rozwiązanie to ma być elastyczne i z jednej strony zapewnić, że nawet najmniejsze jednostki budżetowe będą w krajowym systemie cyberbezpieczeństwa, z drugiej strony, że obowiązki te będą realizowane przez wyspecjalizowany podmiot działający na rzecz wielu podmiotów publicznych. Przepisy wprowadzają obowiązek współpracy podmiotów publicznych z jednostką, która realizuje tym podmiotom zadania z zakresu cyberbezpieczeństwa. Katalog ten wskazano w sposób otwarty celowo. W przypadku jednostek samorządu terytorialnego odwołano się do już obecnych systemowych rozwiązań zawartych w już obecnych przepisach odpowiednio art. 10a–10d ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2025 r. poz. 1153), art. 6a–6d ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym (Dz. U. z 2024 r. poz. 107 i 1907) oraz art. 8c–8f ustawy z dnia 5 czerwca 1998 r. o samorządzie województwa (Dz. U. z 2025 r. poz. 581). Zgodnie z tymi przepisami organ stanowiący jednostki samorządu terytorialnego określa w drodze uchwały jednostki obsługujące, jednostki obsługiwane oraz zakres obowiązków powierzonych jednostkom obsługującym w ramach wspólnej obsługi.

Wprowadza się także możliwość aby dwie lub więcej jednostek samorządu terytorialnego mogło zawrzeć porozumienie i powierzyć jednej z nich zadanie wspólnej realizacji obowiązków z zakresu cyberbezpieczeństwa. W takim porozumieniu trzeba będzie wskazać jednostki organizacyjne, samorządowe osoby prawne lub spółki komunalne objęte porozumieniem, czyli tym, którym będzie świadczona wspólna obsługa. Jednostka samorządu

terytorialnego, której powierzono wspólną obsługę wyznaczy do realizacji tego zadania własną jednostkę organizacyjną, samorządową osobę prawną lub spółkę komunalną. Aby osadzić tę regulację w systemie prawa samorządowego wskazano, że do tych porozumień stosuje się odpowiednio art. 74 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym czyli przepis, który reguluje zawieranie porozumień międzygminnych.

Istotą koncepcji jest to, że zadania z zakresu cyberbezpieczeństwa oraz odpowiedzialność za ich wykonywanie jest przenoszona na jednostkę wyznaczoną do realizacji tych zadań. Podmiot publiczny, któremu te zadania są realizowane, nadal jest przy tym podmiotem kluczowym i podmiotem ważnym, który będzie wykazany w wykazie podmiotów kluczowych i podmiotów ważnych. To jednostka wyznaczona będzie odpowiadała za wdrożenie systemu zarządzania bezpieczeństwem informacji w podmiotach publicznych, stworzenie niezbędnej dokumentacji, zgłaszanie incydentów, przekazanie sprawozdań okresowych oraz sprawozdań końcowych do właściwego CSIRT sektorowego, weryfikację personelu, wskazanie osoby kontaktowej. Kierownik tej jednostki będzie odpowiadał za niewykonanie obowiązków wynikających z ustawy – dlatego też uzyskał prawo do podejmowania decyzji w sprawie systemu zarządzania bezpieczeństwem informacji w podmiotach, którym realizuje zadania z zakresu cyberbezpieczeństwa – z drugiej strony jednostka ma obowiązek wykonać te decyzje. Wprowadza się także uprawnienie dla kierownika jednostki wyznaczonej aby mógł wyznaczyć podmiotom publicznym terminy na przekazanie informacji o incydentach. Kierownik jednostki wyznaczonej będzie ponosił odpowiedzialność karnoadministracyjną za niewykonanie obowiązków. Co jednak w sytuacji, gdy nie wykonał on obowiązku, ponieważ to podmiot publiczny, któremu jednostka wyznaczona realizuje zadania, nie współpracował? Kierownik jednostki wyznaczonej będzie mógł uchronić się od odpowiedzialności wykazując, że nie przyczynił się do tego stanu rzeczy.

Wskazać przy tym należy, że przepisy dotyczące uwspólnienia zadań z zakresu cyberbezpieczeństwa umożliwiają na powołanie bądź wyznaczenie zarówno jednej jednostki jak i kilku jednostek realizujących zadania z zakresu cyberbezpieczeństwa.

2.14. Zadania zespołów CSIRT

2.14.1. Zadania CSIRT

Zadania CSIRT zostały rozszerzone i doprecyzowane w dyrektywie NIS 2 co znalazło odzwierciedlenie w ich nowym katalogu. Należy podkreślić, że część z tych zadań, np. przetwarzanie danych kryminalistycznych, było już realizowane przez zespoły CSIRT

na podstawie obecnych przepisów. Projektowane przepisy pozwolą uporządkować te zadania i zwiększyć spójność krajowego systemu cyberbezpieczeństwa.

W związku z nową rolą CSIRT sektorowych wskazano, że udzielając wsparcia podmiotom krajowego systemu cyberbezpieczeństwa informuje o tym odpowiedni CSIRT sektorowy. Pozwoli to uniknąć dublowania działań przez te podmioty.

Projektowane przepisy dają też możliwość Pełnomocnikowi zlecenia udzielenia wsparcia przez CSIRT poziomu krajowego innemu podmiotowi krajowego systemu cyberbezpieczeństwa. W przypadku CSIRT MON i CSIRT GOV na takie zlecenie muszą wyrazić zgodę organy prowadzące taki CSIRT. To uprawnienie pozwoli Pełnomocnikowi skutecznie reagować na zagrożenia i szybko zapewnić niezbędne wsparcie podmiotom dotkniętym incydentami. Przepisy dopuszczają wyrażenie zgody na udzielenie zgody ustnie oraz z wykorzystaniem środków porozumiewania się na odległość. Jest to konieczne, aby reakcja była odpowiednio szybka w sytuacji incydentu.

Przepisy dotyczące zadań CSIRT MON, CSIRT NASK, CSIRT GOV zostały dostosowane w zakresie zmian terminologicznych – czyli zamiast „sektorowy zespół cyberbezpieczeństwa” wprowadzono „CSIRT sektorowy” a zamiast „zagrożenie cyberbezpieczeństwa” wprowadzono „cyberzagrożenie”. Dostosowano również przepisy o przekazywaniu informacji do innych państw członkowskich Unii Europejskiej informacji o incydentach poważnych dotyczących dwóch lub większej liczby państw a także uzupełniono katalog informacji przekazywanych do Pojedynczego Punktu Kontaktowego.

Wprowadzono również nowe zadania wynikające z dyrektywy NIS 2:

- w odpowiednich przypadkach gromadzenie i zabezpieczanie danych na potrzeby postępowań karnych,
- współpraca z sektorowymi i międzysektorowymi społecznościami podmiotów kluczowych lub podmiotów ważnych oraz, w odpowiednich przypadkach, wymieniają z nimi informacje,
- współpraca z krajowymi zespołami reagowania na incydenty bezpieczeństwa komputerowego z państw trzecich,
- udział we wdrażaniu bezpiecznych narzędzi wymiany informacji z podmiotami kluczowymi i podmiotami ważnymi oraz innymi podmiotami,
- prowadzenie działań na rzecz podnoszenia poziomu bezpieczeństwa systemów informacyjnych podmiotów krajowego systemu cyberbezpieczeństwa przez:

- wykonywanie oceny bezpieczeństwa,
- identyfikowanie podatności systemów dostępnych w otwartych sieciach teleinformatycznych, a także powiadamianie właścicieli tych systemów o wykrytych podatnościach oraz cyberzagrożeniach,
- promowanie, przyjmowanie i stosowanie wspólnych lub znormalizowanych praktyk, systemów klasyfikacji i systematyki związanych z:
 - procedurami obsługi incydentu,
 - zarządzaniem kryzysowym w obszarze cyberbezpieczeństwa,
 - ujawnianiem podatności,
- przekazywanie Pełnomocnikowi sprawozdania z wykonywania swoich zadań ustawowych zawierającego w szczególności informacje o zgłoszonych do CSIRT incydentach krytycznych, incydentach poważnych, incydentach, cyberzagrożeniach oraz potencjalnych zdarzeniach dla cyberbezpieczeństwa.

Należy podkreślić, że CSIRT przy udzielaniu wsparcia w obsłudze incydentu nie staje się administratorem danych osobowych w rozumieniu RODO, gdyż nie ma on wpływu na cel przetwarzania danych osobowych, którymi dysponuje podmiot, u którego wystąpił incydent.

Zmiany w zakresie właściwości zespołów CSIRT.

W przypadku CSIRT MON precyzuje się, że do jego właściwości należą incydenty zgłaszane przez Ministra Obrony Narodowej.

W przypadku CSIRT NASK precyzuje się, że do jego właściwości należą incydenty zgłaszane przez:

- międzynarodowe instytuty badawcze;
- Centrum Łukasiewicz;
- instytuty działające w ramach Sieci Badawczej Łukasiewicz.

Podmioty kluczowe oraz podmioty ważne, z wyjątkiem tych, które wchodzą w zakres właściwości CSIRT MON albo CSIRT GOV.

Ponadto wprowadza się dosyć istotną zmianę – pierwotnie było wskazane, że CSIRT NASK odpowiada za przyjmowanie zgłoszeń incydentów od jednostek samorządu terytorialnego, zwanych dalej „JST”. Tymczasem JST to są wspólnoty samorządowe z odrębnym numerem REGON. Tak naprawdę istotne są incydenty zgłaszane nie przez JST tylko przez urzędy obsługujące JST.

W przypadku CSIRT GOV precyzuje się, że zespół ten odpowiada za reagowanie na incydent zgłaszane przez:

- organy władzy publicznej, w tym organy administracji rządowej, organy kontroli państwowej i ochrony prawa oraz sądy i trybunały,
- Zakład Ubezpieczeń Społecznych i zarządzane przez niego fundusze oraz Kasa Rolniczego Ubezpieczenia Społecznego i fundusze zarządzane przez Prezesa Kasy Rolniczego Ubezpieczenia Społecznego,
- Narodowy Fundusz Zdrowia oraz
- urzędy obsługujące ww. podmioty.

W obecnym brzmieniu interpretując dosłownie przepisy organ władzy publicznej – np. minister kierujący działem administracji rządowej zgłasza incydenty do CSIRT GOV, ale jednostka budżetowa go obsługująca zgłasza do CSIRT NASK. Aby przeciąć ten absurd doprecyzowano przepis, uwzględniając też wieloletnią, rozsądną, praktykę w przepisach. Ponadto uwzględnia się w zakresie właściwości CSIRT GOV:

- Polską Agencję Żeglugi Powietrznej,
- Polską Agencję Prasową,
- Państwowe Gospodarstwo Wodne Wody Polskie,
- Polski Fundusz Rozwoju i inne instytucje rozwoju, o których mowa w art. 2 ust. 1 pkt 3–6 ustawy z dnia 4 lipca 2019 r. o systemie instytucji rozwoju (Dz. U. z 2024 r. poz. 923 oraz z 2025 r. poz. 352, 769 i 1216),
- Urząd Komisji Nadzoru Finansowego.

Wprowadza się możliwość udzielenia dotacji celowej przez ministra właściwego do spraw informatyzacji dla CSIRT NASK na zakup, utrzymanie i rozbudowę infrastruktury teleinformatycznej niezbędnej do wykonywania zadań CSIRT NASK. Działalność CSIRT NASK jest finansowana rokrocznie w drodze dotacji podmiotowej z cz. 27 budżetu państwa – informatyzacja. Dotacja podmiotowa nie umożliwia jednak dokonywanie zakupów inwestycyjnych. Stąd też dla zapewnienia prawidłowej realizacji zadań przez zespół CSIRT NASK wprowadza się możliwość udzielenia dotacji celowej na zakup inwestycyjny związany z infrastrukturą teleinformatyczną.

Wprowadza się przepis umożliwiający zespołom CSIRT poziomu krajowego udział w procesie oceny wzajemnej, o której mowa w art. 19 dyrektywy NIS 2. Szczegóły dotyczącej tej oceny są zawarte w art. 40a.

Wprowadza się także przepisy dotyczące realizacji zadań zespołów CSIRT NASK lub CSIRT GOV wobec podmiotów finansowych w rozumieniu rozporządzenia DORA.

2.14.2. Ujawnianie podatności

CSIRT NASK będzie realizował zadania w zakresie skoordynowanego ujawniania podatności w Unii Europejskiej. W tym zakresie będzie on przyjmował zgłoszenia o wystąpieniu podatności, a następnie kontaktował się z producentami lub dostawcami danych produktów i usług w celu ustalenia sposobu i harmonogramu likwidacji podatności. Należy podkreślić, że CSIRT nie będzie posiadał kompetencji władczych w tym zakresie, w związku z czym eliminacja podatności i jej sposób pozostaną w gestii właściciela danego produktu lub usługi. Równocześnie przepisy ustawy pozwalają CSIRT wydać ostrzeżenie lub zwrócić się do Pełnomocnika o wydanie rekomendacji dotyczących niekorzystania z określonego sprzętu. W związku z tym, posiada on narzędzia, którymi może wpływać na te podmioty. Pozwoli to zwiększyć bezpieczeństwo produktów ICT i usług ICT dostępnych dla konsumentów.

Podatność może zgłosić każdy – przepis wskazuje, że mogą to być osoby fizyczne, osoby prawne albo jednostki organizacyjne nieposiadające osobowości prawnej. Zgłaszanie będzie się odbywało w postaci elektronicznej za pomocą formularza przygotowanego przez CSIRT NASK. Formularz ten powinien umożliwiać zgłoszenie podatności z możliwością zachowania anonimowości przez zgłaszających. Wprowadza się również podstawę prawną dla CSIRT NASK do przetwarzania danych osobowych zawartych w zgłoszeniach podatności.

W ramach tych zadań informacje o podatnościach będą przesyłane do Agencji Unii Europejskiej do spraw Bezpieczeństwa Sieci i Informacji, zwanej dalej „ENISA”, tak aby chronić konsumentów w całej Unii Europejskiej.

2.14.3. Obowiązki Ministra Obrony Narodowej w zakresie udostępniania listy przedsiębiorców, wobec których nałożono obowiązki realizacji zadań na rzecz Sił Zbrojnych

CSIRT MON jest właściwy jako CSIRT dla przedsiębiorców, wobec których wydano decyzję administracyjną na podstawie art. 648 ustawy z dnia 11 marca 2022 r. o obronie Ojczyzny (Dz. U. z 2025 r. poz. 825, 1014 i 1080), czyli decyzje o nałożeniu obowiązku realizacji zadań na rzecz Sił Zbrojnych. Aby więc ustalić zakres właściwości zespołów CSIRT – i skutecznie rozgraniczyć właściwość zespołów CSIRT – Minister Obrony Narodowej będzie miał obowiązek udostępnienia zespołowi CSIRT NASK listy przedsiębiorców wobec których nałożono obowiązki realizacji zadań na rzecz Sił Zbrojnych.

2.14.4. Weryfikacja personelu w CSIRT MON, CSIRT NASK, CSIRT GOV

Podobnie jak w przypadku podmiotów kluczowych i podmiotów ważnych również osoby skazane prawomocnym wyrokiem sądu za przestępstwa przeciwko ochronie informacji nie będą mogły realizować zadań CSIRT MON, CSIRT NASK lub CSIRT GOV. Jest to konieczne, aby zapewnić bezpieczeństwo osobowe w tych podmiotach oraz uniknąć sabotażu czy wycieku informacji.

2.14.5. Przepisy dotyczące współpracy z Pojedynczym Punktem Kontaktowym

Zmiany w tym zakresie mają na celu zastąpienie wyrazów „operator usługi kluczowej” na „podmiot kluczowy lub podmiot ważny”. Uchyła się przy tym przepis dotyczący informowania za pomocą Pojedynczego Punktu Kontaktowego innych państw członkowskich Unii Europejskiej o incydentach istotnych, ponieważ nie będzie już takiego pojęcia jak „incydent istotny” – dyrektywa NIS 2 nie odróżnia takiego incydentu.

2.14.6. Przepisy dotyczące zgłaszania incydentów przez podmioty spoza krajowego systemu cyberbezpieczeństwa

Przepis art. 30 ustawy KSC umożliwia każdemu podmiotowi, który nie jest podmiotem krajowego systemu cyberbezpieczeństwa na zgłoszenie incydentu do CSIRT NASK. Przepis ten wymaga dostosowania do nowej terminologii ustawy – zmiany w tym zakresie mają na celu zastąpienie wyrazów „operator usługi kluczowej” na „podmiot kluczowy lub podmiot ważny”.

2.14.7. Określenie sposobu zgłoszenia incydentu

Do tej pory zespoły CSIRT MON, CSIRT NASK, CSIRT GOV, określały sposób przekazywania zgłoszeń o incydencie poważnym i udostępniały informację o tym na swoich stronach internetowych. Co do zasady pozostawiono to rozwiązanie, z tą różnicą, że chodzi o określenie sposobu zgłoszenia incydentu poważnego w przypadku, gdy system teleinformatyczny S46 będzie czasowo niedostępny.

2.14.8. Działania w zakresie obsługi incydentu

Przepisy projektu ustawy doprecyzowują działania zespołów CSIRT w zakresie koordynacji obsługi incydentu. W trakcie koordynacji obsługi incydentu poważnego lub krytycznego CSIRT MON, CSIRT NASK lub CSIRT GOV mogą wystąpić do organu właściwego do spraw cyberbezpieczeństwa z wnioskiem, aby w wyznaczonym terminie usunął podatności lub o udzielenie informacji niezbędnych do koordynacji tego procesu. Daje to gwarancje,

że zespoły CSIRT będą w stanie szybko wprowadzić środki naprawcze przy obsłudze incydentu. Jest to szczególnie istotne w przypadku incydentów, które mają skutki dla wielu podmiotów, gdzie współpraca podmiotu dotkniętego incydem jest szczególnie istotna. Dzięki pozyskiwanym informacjom zespoły CSIRT poziomu krajowego oraz CSIRT sektorowe będą również w stanie skutecznie informować inne podmioty o wykrytych podatnościach, zwiększając ich bezpieczeństwo.

2.14.9. Badanie produktów ICT

Od 2018 r. zespoły CSIRT poziomu krajowego są uprawnione do prowadzenia badań urządzenia informatycznego lub oprogramowania w celu identyfikacji podatności, której wykorzystanie może zagrozić w szczególności integralności, poufności, rozliczalności, autentyczności lub dostępności przetwarzanych danych, które może mieć wpływ na bezpieczeństwo publiczne lub istotny interes bezpieczeństwa państwa.

W chwili obecnej badanie to jest przeprowadzane z inicjatywy jednego z CSIRT prowadzącego badanie. Wprowadza się zmianę zgodnie z którą badanie przeprowadza się również na wniosek Pełnomocnika lub przewodniczącego Kolegium – który to wniosek jest kierowany do organu prowadzącego lub nadzorującego zespół CSIRT. Ten wniosek ma zapoczątkować działania zespołów w celu przeprowadzenia badania.

Dodano także inną kwestię, która jest istotna dla podmiotów kluczowych i podmiotów ważnych. Mianowicie to badanie musi być przeprowadzone w środowisku testowym – czyli nie może być przeprowadzane na produktach ICT i usługach ICT, które funkcjonują w celu świadczenia usługi tzw. „na produkcji”. Ponadto badanie nie może wpłynąć na ciągłość świadczenia usług przez podmioty kluczowe oraz podmioty ważne. Jeżeli wskutek badania dojdzie do naruszenia ciągłości świadczenia usług oraz powstanie wtedy szkoda, to podmiot może domagać się odszkodowania na podstawie art. 417 §1 ustawy z dnia 23 kwietnia 1964 r. – Kodeks cywilny (Dz. U. z 2025 r. 1071 i 1172)⁴³⁾.

Dalej w przepisie dodano również licencję ustawową do prowadzenia technik mających na celu:

- obserwację i analizę pracy produktu ICT lub usługi ICT,
- uzyskanie dostępu do przetwarzanych danych,

⁴³⁾ § 1. Za szkodę wyrządzoną przez niezgodne z prawem działanie lub zaniechanie przy wykonywaniu władzy publicznej ponosi odpowiedzialność Skarb Państwa lub jednostka samorządu terytorialnego lub inna osoba prawna wykonująca tę władzę z mocy prawa.

- odtworzenie postaci źródłowej produktu ICT lub usługi ICT,
- zwielokrotnienie (powielenie) kodu programowego oraz tłumaczenie (translacja) jego formy,
- odtworzenie algorytmu przetwarzania danych,
- identyfikację realizowanych funkcji,
- usunięcie lub przełamanie zabezpieczeń przed badaniem,
- identyfikację podatności lub identyfikację nieudokumentowanych funkcji realizowanych przez produkt ICT lub usługę ICT.

Głównym powodem wprowadzenia tego przepisu jest fakt, że zgodnie z art. 77 ust. 1 w zw. z art. 33² ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych nie wolno korzystać z utworu będącego programem komputerowym dla celów bezpieczeństwa publicznego.

Doprecyzowano kwestie związane z prowadzeniem badań przez zespół CSIRT. CSIRT MON, CSIRT NASK i CSIRT GOV w czasie prowadzenia badania, nie będą związane postanowieniami umów licencyjnych badanych urządzeń i oprogramowania, które ograniczają możliwość przeprowadzenia badania. Ponadto wyraźnie wskazano, że badanie nie narusza autorskich praw majątkowych i osobistych oraz nie wymaga zgody licencjodawcy lub dysponenta produktu ICT lub usługi ICT.

Wskazane wyżej uprawnienia zespołu prowadzącego badanie są konieczne do zapewnienia ochrony bezpieczeństwa państwa. Niektóre postanowienia umów licencyjnych mogłyby uniemożliwić realizację tego zadania. Zespół CSIRT prowadzący badanie nie powinien być ograniczony licencją twórcy złośliwego oprogramowania, którego wykorzystanie zagraża bezpieczeństwu państwa, w tym np. bezpieczeństwu infrastruktury krytycznej. W zakresie badania sprzętu lub oprogramowania należy zwrócić uwagę, że standardowe umowy licencyjne nie przewidują możliwości dokonywania badania sprzętu pod kątem jego bezpieczeństwa ani też testowania konkretnych rozwiązań zastosowanych w danym produkcie. Konieczność uzyskania zgody właściciela licencji na takie działania często jest niemożliwa do uzyskania w drodze umowy zawieranej na ogólnych zasadach. Producenci nie mają bowiem interesu w umożliwianiu podmiotom zewnętrznym takich działań. Równocześnie rosnąca liczba cyberzagrożeń oraz zależność kluczowych usług od systemów teleinformatycznych sprawia, że konieczne jest, by administracja publiczna dysponowała narzędziem, które pozwoli jej przeprowadzić takie badanie. Brak tych przepisów

mógłby prowadzić do powstania sytuacji, w której CSIRT poziomu krajowego musiałby uzyskać zgodę dostawcy potencjalnie niebezpiecznego sprzętu na przeprowadzenie jego badania, nawet w wypadku gdyby powstało uzasadnione podejrzenie, że dany produkt może być wykorzystany do wywołania incydentu. W związku z powyższym, przepisy te są niezbędne dla zapewnienia bezpieczeństwa podmiotom krajowego systemu cyberbezpieczeństwa.

Celem regulacji jest umożliwienie zespołom CSIRT poziomu krajowego skuteczne badanie produktów ICT i usług ICT pod kątem zagrożeń dla bezpieczeństwa narodowego.

Zaproponowana regulacja jest w stanie doprowadzić do realizacji tego celu – wprowadza bowiem licencję ustawową na badanie tych produktów i usług. Ta licencja ustawowa jest niezbędna do ochrony bezpieczeństwa państwa – wykorzystywanie produktów ICT i usług ICT zawierających podatności umożliwiające np. zaprzestanie działania systemów automatyki przemysłowej elektrowni, uniemożliwienie dostaw paliw czy znaczne zwiększenie chloru w zakładzie wodociągowych grozi zagrożeniem dla funkcjonowania państwa i jego obywateli. Proponowane rozwiązania są proporcjonalne – korzyści dla państwa i obywateli z identyfikacji niebezpiecznych produktów i usług przewyższają obciążenia dla producentów oprogramowania. Licencja jest powiązana tylko z badaniem, o którym mowa w projektowanym art. 33 ustawy o KSC. Licencja nie może służyć np. uzyskaniu oprogramowania do bieżącej działalności zespołów CSIRT. Stąd też należy uznać, że przepisy te spełniają wymóg testu proporcjonalności.

W obecnym art. 33 ustawy o KSC nie zostało wskazane w jaki sposób powinny być publikowane rekomendacje Pełnomocnika dotyczące stosowania urządzeń informatycznych lub oprogramowania. Dlatego proponuje się, aby były one publikowane w Biuletynie Informacji Publicznej, zwanym dalej „BIP”, na stronie podmiotowej Pełnomocnika (nowy ust. 4c). W ślad za tą zmianą proponuje się zmianę w ust. 5 – termin 14 dni na złożenie przez podmiot krajowego systemu cyberbezpieczeństwa zastrzeżenia do rekomendacji będzie liczony od momentu opublikowania rekomendacji w BIP, a nie od momentu otrzymania przez podmiot tych rekomendacji.

Wprowadza się także uprawnienie dla CSIRT MON, CSIRT NASK i CSIRT GOV zażądania od dostawcy badanego produktu ICT, usługi ICT lub procesu ICT dokumentacji, co pozwoli na skuteczne przeprowadzenie badania. Doświadczenia z dotychczasowych badań

wykazały niechęć do przekazywania informacji przez producentów sprzętu lub oprogramowania, co utrudniało przeprowadzenie badania.

2.14.10. Współpraca CSIRT z innymi podmiotami

Modyfikuje się przepisy o współpracy zespołów CSIRT z innymi rodzajami podmiotów. Uzupełnia się, że także zespoły CSIRT sektorowe mają współpracować z organami ścigania i wymiaru sprawiedliwości oraz służbami specjalnymi przy realizacji ich ustawowych zadań. Pojęcie podmiotów świadczących usługi z zakresu cyberbezpieczeństwa zastępuje się wyrażeniem „dostawcy usług zarządzanych w zakresie cyberbezpieczeństwa” – ten rodzaj podmiotu także będzie współpracował z organami ścigania i wymiaru sprawiedliwości oraz służbami specjalnymi przy realizacji ich ustawowych zadań. Ponadto dodaje się, że zespoły CSIRT sektorowe będą współpracować również z organem właściwym do spraw ochrony danych osobowych. Mając na uwadze brzmienie art. 13 ust. 4 dyrektywy NIS 2 wskazano, że zespoły CSIRT poziomu krajowego oraz CSIRT sektorowe będą współpracowały również z Prezesem Urzędu Lotnictwa Cywilnego, Prezesem Urzędu Komunikacji Elektronicznej oraz Komisją Nadzoru Finansowego.

W swojej opinii Europejski Bank Centralny wskazał na konieczność współpracy zespołów CSIRT z Narodowym Bankiem Polskim, który odpowiada za bezpieczeństwo systemów płatności. Stąd też dodano odpowiedni przepis, który daje podstawę do takiej współpracy.

2.15. Zespół Incydentów Krytycznych

Przepisy dotyczące działań związanych z reagowaniem na incydenty krytyczne dostosowuje się i uwzględnia się udział CSIRT sektorowego w wymianie informacji o incydentach krytycznych. Ponadto dodaje się zadanie związane z wymianą informacji o incydentach w cyberbezpieczeństwie na dużą skalę. Przepisy dostosowuje się także do zmian terminologicznych np. zamienia się wyrażenie „zagrożenie cyberbezpieczeństwa” na „cyberzagrożenie”. Ponadto wskazuje się, że informacja o incydencie krytycznym lub incydencie w cyberbezpieczeństwie na dużą skalę, wymieniana między zespołami CSIRT, może zawierać dane osobowe, gdy jest to niezbędne dla ochrony podmiotów krajowego systemu cyberbezpieczeństwa przed incydentami. Konieczne jest tutaj zachowanie zasady minimalizacji przetwarzanych danych.

Do członków Zespołu Incydentów Krytycznych dołączy przedstawiciel ministra właściwego do spraw zagranicznych, ponieważ incydent krytyczny to taki incydent, który

skutkuje znaczną szkodą dla m. in. dla interesów międzynarodowych – stąd zasadne, aby w Zespole Incydentów Krytycznych był przedstawiciel ministra właściwego do spraw zagranicznych.

Projekt ustawy zakłada, że prowadzenie Zespołu Incydentów Krytycznych przejmie od dyrektora Rządowego Centrum Bezpieczeństwa Pełnomocnik. Dotychczasowa praktyka prac Zespołu Incydentów Krytycznych pokazała, że takie rozwiązanie będzie bardziej efektywne.

Wprowadza się nowy przepis art. 35a, który umożliwia Prezesowi Rady Ministrów zobowiązanie, na podstawie propozycji użycia sił i środków niezbędnych do opanowania sytuacji kryzysowych przedstawioną przez Rządowy Zespół Zarządzania Kryzysowego (RZZK), Ministra Obrony Narodowej do udzielenia wsparcia zespołowi CSIRT poziomu krajowego koordynującemu obsługę incydentu krytycznego, przez jednostki podległe lub nadzorowane przez Ministra Obrony Narodowej. Obecne przepisy przewidują, że dyrektor Rządowego Centrum Bezpieczeństwa, działając na podstawie decyzji Zespołu ds. Incydentów Krytycznych, może zwrócić się do Prezesa Rady Ministrów o zwołanie RZZK. Może się tak wydarzyć, jeżeli incydent krytyczny jest sytuacją kryzysową, wymagającą działania na poziomie rządowym. Proponowany artykuł wpisuje się w ten model działania, umożliwiając udzielenie wsparcia zespołowi CSIRT przez wyspecjalizowane w zakresie cyberbezpieczeństwa jednostki podległe lub nadzorowane przez Ministra Obrony Narodowej. Decydującą rolę będzie miał tutaj Prezes Rady Ministrów, działający w oparciu o propozycję RZZK. Podkreślić należy, że dotychczasowa praktyka wskazuje, że zarówno Zespół do spraw Incydentów Krytycznych jak i RZZK są ciałami, które w sytuacjach nagłych są w stanie zebrać się szybko. Zaproponowane rozwiązanie jest zatem adekwatne.

2.16. Ocena bezpieczeństwa

Wprowadza się możliwość przeprowadzania przez CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT sektorowe, oceny bezpieczeństwa systemów informacyjnych wykorzystywanych przez podmioty krajowego systemu cyberbezpieczeństwa. Przepisy tego rozdziału były wzorowane na art. 32a ustawy o ABW i AW⁴⁴⁾. Wprowadzono jednak kilka istotnych zmian w stosunku do pierwotnego. Przede wszystkim wyłącza się stosowanie tego przepisu do ocen bezpieczeństwa systemów teleinformatycznych podmiotów krajowego systemu

⁴⁴⁾ Podsumowanie ocen bezpieczeństwa wykonywanych przez Agencję Bezpieczeństwa Wewnętrznego znajduje się w *Raporcie o stanie bezpieczeństwa cyberprzestrzeni RP w 2021 roku* str. 43–52 <https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/977,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2021-roku.html>.

cyberbezpieczeństwa, które znajdują się w zbiorze organów i podmiotów wymienionych w art. 32a ustawy o ABW i AW. Bez tego wyłączenia powstałyby dwie podstawy prawne do przeprowadzania ocen bezpieczeństwa wobec podmiotów krajowego systemu cyberbezpieczeństwa, które są jednocześnie operatorami infrastruktury krytycznej. Nie jest to sytuacja pożądana.

Ponadto wyłącza się stosowanie rozdziału 6b do systemów teleinformatycznych akredytowanych na podstawie art. 48 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2025 r. poz. 1209). Są to systemy służące przetwarzaniu informacji niejawnych i tutaj pierwszeństwo powinny mieć przepisy ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych.

Wprowadzono jasne określenie właściwości CSIRT poziomu krajowego do przeprowadzania ocen bezpieczeństwa – nawiązuje ono do ogólnej właściwości zespołów CSIRT określonej w art. 26 ust. 5–7. CSIRT sektorowe będą mogły przeprowadzać ocenę bezpieczeństwa wobec operatorów usług kluczowych w danym sektorze.

Wprowadza się również regułę, że przeprowadzanie oceny bezpieczeństwa powinno być uzgodnione z właściwym CSIRT poziomu krajowego. Jest to po to, aby w tym samym czasie nie były prowadzone oceny bezpieczeństwa przez kilka zespołów. Jednocześnie wprowadza się obowiązek poinformowania odpowiednio organu właściwego do spraw cyberbezpieczeństwa czy Prezesa Urzędu Komunikacji Elektronicznej o zamiarze wykonania oceny bezpieczeństwa.

Ocena bezpieczeństwa będzie mogła być przeprowadzona wyłącznie za zgodą podmiotu krajowego systemu cyberbezpieczeństwa wyrażoną w postaci pisemnej lub elektronicznej pod rygorem nieważności. Jest to duża różnica względem art. 32a ustawy o ABW i AW, zgodnie z którym Szef ABW decyduje o włączeniu systemu teleinformatycznego operatora infrastruktury krytycznej do rocznego planu przeprowadzania ocen bezpieczeństwa. Jednakże dyrektywa NIS 2 przewiduje także przeprowadzanie *security scans* wobec podmiotu kluczowego lub podmiotu ważnego. Dlatego wprowadza się możliwość przeprowadzenia oceny bezpieczeństwa na zlecenie organu właściwego do spraw cyberbezpieczeństwa.

Część urzędów administracji publicznej ma zagwarantowaną niezależność. Dlatego wprowadza się zasadę, że ocenę bezpieczeństwa systemów informacyjnych Kancelarii Sejmu, Kancelarii Senatu, Kancelarii Prezydenta Rzeczypospolitej Polskiej, Narodowego Banku Polskiego, Biura Rzecznika Praw Obywatelskich, Biura Rzecznika Praw Dziecka, Instytutu

Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu, Państwowej Inspekcji Pracy, Trybunału Konstytucyjnego, Sądu Najwyższego, sądów administracyjnych, Najwyższej Izby Kontroli, Krajowej Rady Radiofonii i Telewizji, Krajowego Biura Wyborczego, Urzędu Ochrony Danych Osobowych przeprowadza się wyłącznie po uzyskaniu zgody tych podmiotów.

Aby ograniczyć arbitralność organu właściwego do spraw cyberbezpieczeństwa przy wyborze podmiotu, którego system informacyjny będzie podlegał ocenie bezpieczeństwa wprowadza się obowiązek przeprowadzenia wcześniej przez organ analizy ryzyka. Wyniki analizy ryzyka stanowiąc będą podstawę do wyboru podmiotu do przeprowadzenia oceny bezpieczeństwa.

Celem oceny bezpieczeństwa jest pomoc w identyfikacji podatności. Ma ona charakter prewencyjny. Jednakże prowadzenie tej oceny nie może zaszkodzić systemowi informacyjnemu, a szerzej podmiotowi, który korzysta z tego systemu i świadczy usługi dla swoich klientów. Dlatego wprowadza się zasadę, zgodnie z którą czynności przeprowadzane w ramach oceny bezpieczeństwa powinny w jak najmniejszym stopniu zakłócać funkcjonowanie tego systemu lub ograniczać jego dostępność. Tym bardziej nie jest dopuszczalne, aby działania te doprowadziły do nieodwracalnego zniszczenia danych w systemie poddanym ocenie. Przepis ten ma stanowić ogólną zasadę dla osób przeprowadzających ocenę bezpieczeństwa i stanowi gwarancję dla podmiotu krajowego systemu cyberbezpieczeństwa, wobec którego prowadzona jest ocena bezpieczeństwa. Dodatkowo wprowadzono katalog sytuacji w których ocena bezpieczeństwa nie może być przeprowadzona, a rozpoczętą przerywa się. Są to sytuacje, gdy:

- 1) podmiot krajowego systemu cyberbezpieczeństwa nie posiada kopii bezpieczeństwa badanego systemu⁴⁵⁾;
- 2) istnieje zagrożenie nieodwracalnego zniszczenia danych przetwarzanych w systemie;
- 3) czas potrzebny na przywrócenie systemu z kopii bezpieczeństwa może w istotny sposób zakłócić pracę systemu lub ograniczyć jego dostępność;

⁴⁵⁾ Pamiętać należy, że podmiot kluczowy i podmiot ważny taką kopię powinien mieć, bowiem przepis art. 8 nakazuje stosowanie środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego wykorzystywanego do świadczenia usługi, w tym stosowanie mechanizmów zapewniających poufność, integralność, dostępność i autentyczność danych przetwarzanych w systemie informacyjnym. Ponadto podmiot ma zapewnić bezpieczeństwo w procesie (...) utrzymania i eksploatacji systemu informacyjnego. Brak kopii bezpieczeństwa może zostać wykryty w trakcie kontroli organu właściwego do spraw cyberbezpieczeństwa. Poza tym brak kopii bezpieczeństwa może zostać wykryty w trakcie audytu prowadzonego na podstawie art. 15.

- 4) czynności podejmowane podczas oceny bezpieczeństwa mogą doprowadzić do uszkodzenia produktów ICT wchodzących w skład tego systemu oraz innych systemów informacyjnych podmiotu kluczowego;
- 5) istnieje zagrożenie ograniczenia dostępności usług świadczonych przez podmiot krajowego systemu cyberbezpieczeństwa.

Po uzyskaniu zgody od podmiotu krajowego systemu cyberbezpieczeństwa albo po otrzymaniu zlecenia od organu właściwego do spraw cyberbezpieczeństwa, CSIRT przeprowadzający ocenę bezpieczeństwa będzie obowiązany uzgodnić tryb i ramowe warunki przeprowadzania tej oceny, w szczególności datę rozpoczęcia, harmonogram oraz zakres i rodzaj przeprowadzanych w ramach oceny bezpieczeństwa testów bezpieczeństwa. Aby przeprowadzić taką ocenę zespół CSIRT musi otrzymać niezbędne informacje techniczne i organizacyjne dotyczące systemu. Dlatego podmiot, którego system podlega ocenie będzie przekazywał te informacje do zespołu CSIRT. Dodatkowo wskaże on: imię i nazwisko, służbowy adres poczty elektronicznej oraz służbowy numer telefonu osoby upoważnionej do reprezentacji podmiotu a także osoby upoważnionej do udzielania wyjaśnień CSIRT w trakcie przeprowadzania oceny bezpieczeństwa. Dzięki temu zespół CSIRT będzie wiedział, z kim skontaktować się celem ustalenia szczegółów dotyczących przeprowadzania oceny bezpieczeństwa.

Zespół CSIRT przeprowadzający ocenę bezpieczeństwa otrzyma dwa ważne uprawnienia, które są niezbędne do skutecznego przeprowadzenia takiej oceny.

Po pierwsze, będzie uprawniony do wytworzenia lub pozyskania urządzeń lub oprogramowania przystosowanych do popełnienia przestępstw określonych w art. 165 § 1 pkt 4⁴⁶⁾, art. 267 § 3⁴⁷⁾, art. 268a⁴⁸⁾ § 1 albo § 2 w związku z § 1, art. 269 § 1⁴⁹⁾ lub 2 albo art. 269a⁵⁰⁾

⁴⁶⁾ Przestępstwo polegające na spowodowaniu niebezpieczeństwa dla życia lub zdrowia wielu osób albo dla mienia w wielkich rozmiarach w ramach którego sprawca zakłóca, uniemożliwia lub w inny sposób wpływa na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych.

⁴⁷⁾ Przestępstwo, w którym sprawca w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem.

⁴⁸⁾ Przestępstwo, w którym sprawca nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa, zmienia lub utrudnia dostęp do danych informatycznych albo w istotnym stopniu zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych.

⁴⁹⁾ Przestępstwo, w którym sprawca niszczy, uszkadza, usuwa lub zmienia dane informatyczne o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego albo zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych.

⁵⁰⁾ Przestępstwo, w którym sprawca nie będąc do tego uprawnionym, przez transmisję, zniszczenie, usunięcie, uszkodzenie, utrudnienie dostępu lub zmianę danych informatycznych, w istotnym stopniu zakłóca pracę systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej.

Kodeksu karnego, aby móc sprawdzić, czy oceniany system jest podatny na tego rodzaju oprogramowanie.

Po drugie, używając ww. urządzeń lub programów zespół CSIRT będzie uprawniony do dostępu do informacji dla niego nieprzeznaczonej, przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie. Będzie mógł uzyskać dostęp do całości lub części ocenianego systemu. Wprowadza się przy tym kontratyp, zgodnie z którym osoba wykonująca te czynności nie popełnia przestępstwa, o którym mowa w art. 267 § 1 Kodeksu karnego.

Bez tego rodzaju szczególnych uprawnień zespół CSIRT nie będzie w stanie zidentyfikować podatności, które mogą być wykorzystane przez przestępców komputerowych do zaatakowania podmiotu krajowego systemu cyberbezpieczeństwa.

Aby zapewnić gwarancje dla podmiotu, u którego jest przeprowadzana ocena, wprowadza się przepis, na mocy którego informacje uzyskane w wyniku oceny stanowią tajemnicę prawnie chronioną. Zespół CSIRT nie będzie mógł wykorzystać ich do realizacji innych zadań ustawowych. Informacje te będą podlegały niezwłocznemu, komisijnemu i protokolarnemu zniszczeniu. Zniszczeniu nie podlegają informacje o czynnościach przeprowadzanych w ramach oceny bezpieczeństwa oraz o wykrytych podatnościach systemu informacyjnego.

Końcowym etapem oceny bezpieczeństwa będzie sporządzenie przez CSIRT raportu, który będzie zawierał podsumowanie przeprowadzonych w ramach oceny bezpieczeństwa czynności oraz wskazanie wykrytych podatności systemu informacyjnego. Raport będzie przekazany do podmiotu, którego system był poddany ocenie bezpieczeństwa. Dzięki temu podmiot będzie mógł przeanalizować np. jak jego personel, odpowiedzialny za bezpieczeństwo systemu, zachowywał się podczas oceny bezpieczeństwa, czy procedury bezpieczeństwa zadziałały prawidłowo, a także czy i jakie podatności zostały wykryte podczas oceny bezpieczeństwa.

W wyniku prowadzonej przez zespół CSIRT oceny bezpieczeństwa może zostać zidentyfikowana podatność, która może występować w innych systemach informacyjnych, które np. wykorzystują to samo oprogramowanie zawierające podatność. W takiej sytuacji zasadne jest, aby zespół CSIRT był obowiązany poinformować o tym:

- 1) ministra właściwego do spraw informatyzacji – z uwagi na to, że minister jest właściwy w sprawach systemów i sieci teleinformatycznych administracji publicznej⁵¹⁾;
- 2) Pełnomocnika – z uwagi na to, że do zadań Pełnomocnika należy ocena funkcjonowania krajowego systemu cyberbezpieczeństwa, a także może on przekazywać Radzie Ministrów wnioski oraz rekomendacje dotyczące działań, które powinny podejmować podmioty krajowego systemu cyberbezpieczeństwa w celu zapewnienia cyberbezpieczeństwa na poziomie krajowym i przeciwdziałania zagrożeniom, w tym zakresie (art. 63 ustawy o KSC).

Dodano także upoważnienie ustawowe dla Rady Ministrów do określenia, w drodze rozporządzenia:

- 1) trybu przeprowadzania oceny bezpieczeństwa,
 - 2) szczegółowych informacji przekazywanych do CSIRT niezbędnych do przeprowadzenia oceny bezpieczeństwa;
 - 3) rodzaje przeprowadzanych testów bezpieczeństwa w ramach oceny bezpieczeństwa,
 - 4) sposobu niszczenia materiałów zawierających informacje, które zespół CSIRT uzyskał w trakcie przeprowadzania oceny bezpieczeństwa,
 - 5) trybu działania komisji,
 - 6) wzoru protokołu zniszczenia materiałów zawierających informacje
- mając na uwadze konieczność zapewnienia sprawnego przeprowadzenia oceny bezpieczeństwa, bezpieczeństwo systemów informacyjnych podlegających ocenie, rodzaj materiałów podlegających zniszczeniu i konieczność zapewnienia efektywności i przejrzystości prowadzonych działań komisji.

2.17. Zasady udostępniania informacji i przetwarzania danych osobowych

2.17.1. Zmiany w zakresie przepisów o przetwarzaniu danych osobowych

Obecne przepisy o przetwarzaniu danych osobowych dostosowano do zmian wprowadzonych w pozostałej części ustawy. Przyznano uprawnienia zespołom CSIRT sektorowym do przetwarzania danych osobowych co jest konieczne do realizacji ich zadań.

Dodano wyłączenie stosowania ustawy z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego, do udostępniania informacji

⁵¹⁾ Art. 12a ustawy z dnia 4 września 1997 r. o działach administracji rządowej (Dz. U. z 2025 r. poz. 1275).

o podatnościach, incydentach i cyberzagrożeniach oraz o ryzyku wystąpienia incydentów. Wskazać należy, że zgłoszenie incydentu może zawierać wrażliwe dane dotyczące kluczowych dla państwa podmiotów gospodarczych, takich właśnie jak podmioty kluczowe i podmioty ważne. Udostępnienie informacji o tym, że u konkretnego operatora usługi kluczowej, np. elektrociepłowni, szpitalu czy kopalni, wystąpiły podatności w systemach informacyjnych czy incydenty poważne, może zachęcić przestępców lub podmioty nieprzychylne Państwu do dokonania cyberataku na te podmioty. Z tego też powodu projektodawca uważa, że znajdzie zastosowanie artykuł 1 ust. 2 dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/1024 z dnia 20 czerwca 2019 r. w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego (Dz. Urz. UE L 2019/1024 z 26.06.2019) ze względu na konieczność ochrony bezpieczeństwa narodowego. Natomiast wprowadzono dopisek, zgodnie z którym podlegają udostępnieniu informacje o incydentach, podatnościach i cyberzagrożeniach, których udostępnienie nie zagrażałoby bezpieczeństwu państwa lub bezpieczeństwu publicznemu.

Incydenty mogą być związane z różnymi rodzajami danymi, w tym z danymi osobowymi. Jako przykład można wskazać zdarzenie, w którym dzienniki połączeń konsumentów zostały wykradzione lub numery telefonów użytkowników końcowych oraz numery IMSI zostały upublicznione. Atak na sieć, z której korzysta podmiot świadczący usługi OTT może spowodować utratę poufności i dostęp do wiadomości o użytkownikach, np. komunikatorów internetowych. Z kolei wskutek ataku mogłaby zostać zaszyfrowana baza abonentów przedsiębiorcy komunikacji elektronicznej, wskutek czego tymczasowo niemożliwe lub utrudnione może być świadczenie usług komunikacji elektronicznej.

Aby skutecznie zareagować na tego rodzaju zdarzenia, zespoły CSIRT poziomu krajowego oraz CSIRT sektorowe muszą otrzymać niezbędne dane m.in. po to, aby dokonać czynności z zakresu informatyki śledczej. Niezbędne będzie przekazanie dzienników zdarzeń (logów), które mogą zawierać informacje kto, kiedy, jakiej czynności dokonał. Innym przykładem będzie przekazanie zaszyfrowanej bazy danych abonentów. Wśród tych danych często będą znajdować się dane osobowe, jak wskazano wyżej. Może być też tak, że w skład tych danych będą znajdować się informacje umożliwiające identyfikację osób, które przyczyniły się do powstania incydentu. W tej sytuacji niezbędne jest zapewnienie możliwości przetwarzania przez ww. zespoły CSIRT danych osobowych. Zespoły CSIRT będą przetwarzać dane osobowe pozyskane dopiero przy zaistnieniu szczególnego rodzaju zdarzenia, jakim będzie incydent poważny.

Wprowadza się jeszcze dodatkowy przepis regulujący zasady usuwania danych osobowych pozyskanych przez ministra właściwego do spraw informatyzacji, Pełnomocnika, Dyrektora Rządowego Centrum Bezpieczeństwa, Prezesa Urzędu Komunikacji Elektronicznej w związku z wykonywaniem zadań wynikających z ustawy o KSC. Przepis wypełnia lukę prawną, która obecnie występuje w ustawie o KSC.

W dotychczasowych przepisach o przetwarzaniu danych osobowych przez zespoły CSIRT poziomu krajowego oraz CSIRT sektorowe wprowadzono możliwość przetwarzania danych nie tylko określonych w art. 9 RODO ale także dotyczące danych osobowych dotyczących wyroków skazujących i czynów zabronionych (art. 10 RODO). Jest to związane z tym, że incydent polegający np. na naruszeniu poufności danych w danym podmiocie (np. sądzie, jednostce penitencjarnej, czy ośrodku zdrowia) może naruszać te szczególne kategorie danych osobowych. Specjaliści z zespołu CSIRT, analizujący incydent muszą zorientować się jakich danych dotyczy incydent, aby móc go obsłużyć. Są oczywiście związani przy tym tajemnicą.

Tak jak jest to w obecnej ustawie o KSC nie uregulowano kwestii przetwarzania danych osobowych przez CSIRT GOV działający w Agencji Bezpieczeństwa Wewnętrznego. Kwestia ta była omawiana w trakcie procesu legislacyjnego projektu ustawy o krajowym systemie cyberbezpieczeństwa w 2018 r.⁵²⁾. Ostatecznie zostało przesądzone, że ustawie o KSC nie będą regulowane kwestie przetwarzania danych osobowych przez CSIRT GOV, ponieważ zastosowanie znajdzie tutaj art. 34 ustawy z dnia 24 maja 2022 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, który reguluje kwestie przetwarzania danych osobowych przez Agencję Bezpieczeństwa Wewnętrznego.

Wprowadza się uprawnienie ministra właściwego do spraw informatyzacji do przetwarzania danych osobowych – imienia i nazwiska oraz numeru PESEL osób fizycznych, które w imieniu podmiotu kluczowego lub podmiotu ważnego korzystają z systemu teleinformatycznego S46 w celu uwierzytelnienia tych osób w systemie. Uwierzytelnienie będzie odbywać się za pomocą Węzła krajowego, który dopuszcza uwierzytelnianie za pomocą nr PESEL lub niepowtarzalnego identyfikatora środka identyfikacji elektronicznej, o którym mowa w przepisach wydanych na podstawie art. 12 ust. 8 rozporządzenia 910/2014.

W chwili obecnej ustawa o KSC wyłącza stosowanie art. 15, art. 16, art. 18 ust. 1 lit. a i d oraz art. 19 zdanie drugie RODO w zakresie danych pozyskanych przez CSIRT poziomu

⁵²⁾ Por. pkt I.2 pisma DBN.WP.141.1.4.2018.KM z 22 marca 2018 r.
<https://legislacja.rcl.gov.pl/docs//2/12304650/12466734/12466736/dokument337595.pdf>.

krajowego. RODO wskazuje jednak, że prawa zawarte w ww. artykułach można ograniczyć a nie całkiem wyłączyć. Z tego powodu zrezygnowano z formuły wyłączania stosowania tych artykułów tylko zaproponowano, że realizacja uprawnień wynikających z tych artykułów RODO jest możliwa po zakończeniu obsługi incydentu, w związku z którym dane zostały pozyskane lub po zakończeniu obsługi incydentu, do którego obsługi te dane są niezbędne. Ograniczenie tych uprawnień np. prawa do sprostowania ma na celu zachowanie danych w takiej postaci, jakie zostały pozyskane – jest to niezbędne do przeprowadzenia analizy próbek, każda modyfikacja pliku spowoduje błędne wnioski.

W przepisach dotyczących zadań ministra właściwego do spraw informatyzacji wprowadzono możliwość opublikowania przez niego zestawienia wymogów dokumentów normalizacyjnych, których spełnienie oznacza spełnienie wymogów ustawy. Dokument ten będzie obowiązkowo podlegał konsultacjom publicznym. W związku z tym wprowadzono podstawę prawną do przetwarzania danych osobowych przez ministra pozyskanych w trakcie konsultacji publicznych. Przetwarzanie dotyczy danych osobowych zawartych w stanowiskach do projektu dokumentu. Może to obejmować także dane szczególnie chronione, o których mowa w art. 9 ust. 1 RODO – przykładowo – danymi szczególnie chronionymi są dane o przynależności do związków zawodowych, a przecież uwagi w trakcie konsultacji publicznych mogą zgłosić przedstawiciele związków zawodowych.

2.17.2. Przetwarzanie danych przez CSIRT NASK w celu tworzenia usługi online (art. 26c i zmiany w art. 39 ustawy o KSC)

Wycieki danych na przestrzeni lat stają się coraz powszechniejsze co często wiąże się z poważnymi konsekwencjami takimi jak utrata prywatności, kradzież tożsamości, czy negatywnymi skutkami finansowymi. Z tego względu, dla zapewnienia bardziej efektywnej ochrony użytkowników i w celu minimalizacji ryzyka powstania szkód materialnych i niematerialnych związanych z nieuprawnionym upublicznieniem danych osobowych w sieci internet, CSIRT NASK będzie tworzył i udostępniał usługę online umożliwiającą sprawdzenie przez osobę fizyczną, czy jej dane osobowe nie zostały ujawnione w sieci internet w sposób nieuprawniony, na skutek incydentu lub cyberzagrożenia.

Projektowane przepisy art. 26c i art. 39 ustawy o KSC określają wyraźne podstawy do gromadzenia i przetwarzania danych pozyskanych w związku z incydentami i cyberzagrożeniami. Tym samym CSIRT NASK może gromadzić i przetwarzać dane pozyskane m.in. przy obsłudze incydentów lub przy prowadzeniu czynności operacyjnych

i wykorzystywać je do świadczenia usługi online, o której mowa w przepisach. Projektowany art. 26c ust. 2 ustawy o KSC wskazuje ponadto zakres danych, które mogą być przetwarzane przy realizacji tej usługi. Katalog ten wydaje się być szeroki, natomiast CSIRT NASK na podstawie przepisów odrębnych zobowiązany jest do minimalizacji przetwarzanych danych, co będzie miało miejsce także przy realizacji usługi online. Szeroki zakres wynika przede wszystkim z technicznych uwarunkowań profilu zaufanego, a dokładniej węzła krajowego, w którym przetwarzane są wszystkie te dane i przekazywane w momencie logowania użytkownika. CSIRT NASK musi być zatem uprawniony do przetwarzania danych, które uzyska w momencie logowania się przez użytkownika.

Jednocześnie nie sposób przewidzieć zakresu danych, jakie zostaną upublicznione w sposób nieuprawniony w sieci internet. Katalog możliwych do gromadzenia i przetwarzania danych musi zatem być na tyle szeroki, aby umożliwiać prawidłowe funkcjonowanie usługi online, pozwalające na realizację założonego w ustawie celu.

Realizacja usługi online przez CSIRT NASK przy pomocy gromadzonych przez ten podmiot danych oznacza, że CSIRT NASK będzie administratorem danych zgromadzonych i przetwarzanych w tej usłudze. Usługa ta – co wynika z przepisów odrębnych – musi być zgodna z RODO oraz z minimalnymi wymaganiami dla systemów teleinformatycznych wydanych na podstawie art. 18 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2024 r. poz. 1557 i 1717 oraz z 2025 r. poz. 1006, 1019 i 1158).

Wszelkie techniczne aspekty tworzenia i udostępniania usługi online, o której mowa w art. 26c ust. 1 ustawy o KSC, zostaną opracowane w dokumentacji technicznej.

Zgromadzone dane będą przez CSIRT NASK anonimizowane w terminie 5 lat od dnia ich zgromadzenia co pozostaje w zgodzie z terminem na anonimizację danych pozyskanych do realizacji pozostałych zadań wynikających z ustawy. Termin ten jest adekwatny z punktu widzenia realizacji samej usługi – użytkownik musi mieć możliwość sprawdzenia historycznych wycieków, których skutki mogą być widoczne po kilku latach. Nie można wykluczyć sytuacji, że użytkownik skorzysta z funkcjonalności usługi nie od razu po wycieku, a dopiero po roku, 2 czy nawet 4 latach.

W związku z tym, że zadanie to będzie ustawowym zadaniem CSIRT NASK, finansowane będzie przez ministra właściwego do spraw informatyzacji na zasadzie dotacji podmiotowej.

2.17.3. Ocena wzajemna

CISRT MON, CISRT NASK, CSIRT GOV, CSIRT sektorowe oraz organy właściwe do spraw cyberbezpieczeństwa będą mogły również uczestniczyć w ocenie wzajemnej organów z państw członkowskich Unii Europejskiej. Jest to proces, w ramach którego podmioty z poszczególnych państw członkowskich Unii Europejskiej badają nawzajem funkcjonowanie swoich zespołów CSIRT oraz procedur postępowania w przypadku wystąpienia incydentu. Metodyka przeprowadzania tych ocen zostanie ustalona przez państwa członkowskie Unii Europejskiej przy współudziale Komisji Europejskiej oraz ENISA. Udział w ocenie wzajemnej jest dobrowolny i każdy z podmiotów mogących wziąć w nim udział będzie mógł zdecydować czy chce brać w nim udział.

Aby umożliwić realizację tych procesów niezbędne jest również stworzenie podstawy prawnej do przekazywania informacji ekspertom biorącym udział w tym procesie, tak aby mogli zapoznać się ze szczegółami spraw jakimi zajmowały się zespoły CSIRT.

Udział w tym procesie pozwoli krajowym ekspertom zapoznać się z metodami postępowania wypracowanymi w innych krajach, a następnie wykorzystać je w ramach swojej pracy. Udział w ocenie wzajemnej pozwoli również wykorzystać wiedzę ekspertów z innych krajów do usprawnienia funkcjonowania krajowych instytucji zajmujących się cyberbezpieczeństwem.

2.18. Zmiany w obszarze organów właściwych do spraw cyberbezpieczeństwa

W przepisach o właściwości organów właściwych do spraw cyberbezpieczeństwa pozostawiono właściwość dotychczasowych organów właściwych do spraw cyberbezpieczeństwa. Uzupełniono ją w przypadku nowych sektorów.

Nowe organy właściwe do spraw cyberbezpieczeństwa dla sektorów kluczowych:

- 1) dla sektora podsektora komunikacji elektronicznej – Prezes Urzędu Komunikacji Elektronicznej – zgodnie z ustawą z dnia 12 lipca 2024 r. – Prawo komunikacji elektronicznej Prezes Urzędu Komunikacji Elektronicznej nadzoruje przedsiębiorców komunikacji elektronicznej, więc rozsądne jest aby nadzorował ich także pod kątem cyberbezpieczeństwa świadczonych usług komunikacji elektronicznej;
- 2) dla sektora ścieków – minister właściwy do spraw gospodarki wodnej – zgodnie z art. 11 ust. 1 pkt 7 ustawy z dnia 4 września 1997 r. o działach administracji rządowej (Dz. U.

z 2025 r. poz. 1275) dział gospodarka wodna obejmuje sprawy określenia zasad i warunków zbiorowego odprowadzania ścieków;

- 3) dla sektora zarządzania usług ICT – minister właściwy do spraw informatyzacji – zgodnie z art. 12a ust. 1 pkt 7 ustawy z dnia 4 września 1997 r. o działach administracji rządowej dział informatyzacja obejmuje sprawy rozwoju usług świadczonych drogą elektroniczną;
- 4) dla sektora przestrzeni kosmicznej – minister właściwy do spraw gospodarki – zgodnie z art. 9 ust. 2 pkt 14 stawy z dnia 4 września 1997 r. o działach administracji rządowej do zadań tego ministra należy kształtowanie i prowadzenie polityki kosmicznej;
- 5) dla sektora produkcji, wytwarzania i dystrybucji chemikaliów – minister właściwy do spraw gospodarki – zgodnie z art. 9 ust. 1 ustawy z dnia 4 września 1997 r. o działach administracji rządowej dział gospodarka obejmuje sprawy gospodarki, w tym przemysłu;
- 6) dla sektora produkcji, przetwarzania i dystrybucji żywności – minister właściwy do spraw rolnictwa – zgodnie z art. 22 ust. 1 pkt 1 i 3 ustawy z dnia 4 września 1997 r. o działach administracji rządowej dział rolnictwo obejmuje sprawy produkcji roślinnej i zwierzęcej;
- 7) dla sektora produkcji, z wyłączeniem podsektora produkcja wyrobów medycznych i wyrobów medycznych do diagnostyki in vitro – minister właściwy do spraw gospodarki – zgodnie z art. 9 ust. 1 ustawy z dnia 4 września 1997 r. o działach administracji rządowej dział gospodarka obejmuje sprawy gospodarki, w tym przemysłu;
- 8) dla podsektora produkcji wyrobów medycznych i wyrobów medycznych do diagnostyki in vitro – minister właściwy do spraw zdrowia – zgodnie z art. 33 ust. 1 pkt 2 1 ustawy z dnia 4 września 1997 r. o działach administracji rządowej dział zdrowie obejmuje sprawy nadzoru nad wyrobami medycznymi, wyrobami medycznymi do diagnostyki in vitro.

Organami właściwymi do spraw cyberbezpieczeństwa dla podmiotów ważnych są:

- 1) dla sektora usług pocztowych – Prezes Urzędu Komunikacji Elektronicznej – zgodnie z ustawą z dnia 23 listopada 2012 r. – Prawo pocztowe (Dz. U. z 2025 r. poz. 366 i 820), Prezes Urzędu Komunikacji Elektronicznej jest regulatorem rynku pocztowego;
- 2) dla sektora gospodarowania odpadami – minister właściwy do spraw klimatu – zgodnie z art. 13a ust. 1 pkt 7 ustawy z dnia 4 września 1997 r. o działach administracji rządowej dział klimat obejmuje sprawy gospodarki odpadami;
- 3) dla sektora dostawców usług cyfrowych – minister właściwy do spraw informatyzacji – zgodnie z art. 12a ust. 1 pkt 7 ustawy z dnia 4 września 1997 r. o działach administracji

rządowej dział informatyzacja obejmuje sprawy rozwoju usług świadczonych drogą elektroniczną;

- 4) dla sektora badań naukowych – minister właściwy do spraw nauki – zgodnie z art. 26 ust. 1 ustawy z dnia 4 września 1997 r. o działach administracji rządowej dział szkolnictwo wyższe i nauka obejmuje sprawy działalności naukowej.

Przypisując właściwość organów właściwych do spraw cyberbezpieczeństwa kierowano się właściwością wynikającą z ustawy z dnia 4 września 1997 r. o działach administracji rządowej albo ustawami regulującymi poszczególne sektory gospodarki.

W przypadku sektora podmiotów publicznych organami właściwymi do spraw cyberbezpieczeństwa będą:

- 1) w zakresie podmiotów zgłaszających incydenty do CSIRT NASK – minister właściwy do spraw informatyzacji, przy czym zadania nadzorcze z wyjątkiem wydawania decyzji administracyjnych będą mogły być powierzone CSIRT NASK;
- 2) w zakresie podmiotów podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych – Minister Obrony Narodowej;
- 3) w zakresie jednostek organizacyjnych podległych ministrowi właściwemu do spraw finansów publicznych lub przez niego nadzorowanych, urzędu obsługującego tego ministra oraz spółki, o której mowa w art. 2 ust. 1 ustawy o szczególnych zasadach wykonywania niektórych zadań dotyczących informatyzacji w zakresie działów administracji rządowej budżet i finanse publiczne – minister właściwy do spraw finansów publicznych.

Podział ten jest konieczny z uwagi na bardzo dużą liczbę podmiotów publicznych. Co do zasady minister właściwy do spraw informatyzacji jest odpowiedzialny za bezpieczeństwo w cyberprzestrzeni w wymiarze cywilnym (art. 12a ust. 1 pkt 10 ustawy z dnia 4 września 1997 r. o działach administracji rządowej). Stąd co do zasady to on będzie organem właściwym do spraw cyberbezpieczeństwa dla podmiotów publicznych. Minister Obrony Narodowej jest z kolei odpowiedzialny za bezpieczeństwo cyberprzestrzeni w wymiarze militarnym (art. 19 ust. 1 pkt 1a ustawy z dnia 4 września 1997 r. o działach administracji rządowej). Stąd też to on powinien nadzorować podmioty publiczne jemu podległe albo przez niego nadzorowane.

Wprowadzono przy tym regułę, że jeśli podmiot publiczny znajduje się również w innym sektorze niż sektor podmioty publiczne, to wtedy organem właściwym

do spraw cyberbezpieczeństwa dla niego nie będzie minister właściwy do spraw informatyzacji tylko będzie organ z innego sektora – przykładowo dla Polskiej Agencji Kosmicznej będzie to minister właściwy do spraw gospodarki. Rozwiązanie ma na celu uprościć właściwość organów. Nie będzie się go jednak stosować przy samorządowych podmiotach publicznych, ponieważ mogą one potencjalnie znajdować się w wielu sektorach, np. prowadząc działalność telekomunikacyjną, zaopatrując w wodę mieszkańców itd. – proponowana regulacja uniemożliwiałaby wtedy ustalenie właściwości organów.

Katalog zadań organów właściwych do spraw cyberbezpieczeństwa został uzupełniony zgodnie z innymi przepisami ustawy, wskazano na kompetencje do bieżącej analizy podmiotów spełniających kryteria podmiotu kluczowego lub podmiotu ważnego, zadania związane z wykazem podmiotów kluczowych lub podmiotów ważnych.

Dodatkowo dodaje się także uprawnienie do odpytywania podmiotów, np. przedsiębiorców, o przekazanie informacji umożliwiających stwierdzenie, czy są one podmiotami kluczowymi czy podmiotami ważnymi. To uprawnienie jest konieczne, aby zapewnić skuteczność ustawy.

Nowym zadaniem, związanym ze sprawowaniem nadzoru, jest prowadzenie przez organ właściwy do spraw cyberbezpieczeństwa wykazu osób wobec których wydana została decyzja o zastosowaniu środka nadzorczego, o którym mowa w art. 53 ust. 9 pkt 6 ustawy o KSC. Środek ten dotyczy tymczasowego zakazu pełnienia funkcji zarządczych w podmiocie kluczowym przez kierownika podmiotu. Prowadzenie wykazu związane jest z obowiązkiem przekazywania informacji na temat stosowania tego środka celem ujawnienia w Krajowym Rejestrze Sądowym. Zgodnie z art. 21 ust. 1 ustawy z dnia 20 sierpnia 1997 r. o Krajowym Rejestrze Sądowym (Dz. U. z 2025 r. poz. 869), zwanej dalej „ustawą o KRS”, organy administracji rządowej są obowiązane niezwłocznie informować właściwy sąd rejestrowy o zdarzeniach, które podlegają obowiązkowi wpisu do Krajowego Rejestru Sądowego z urzędu. Wskutek objęcia osoby takim zakazem, w Krajowym Rejestrze Sądowym prowadzonym dla danego podmiotu kluczowego należy dokonać z urzędu wykreślenia takiej osoby z rejestru (art. 24 ust. 6 ustawy o KRS). Osoba ta może zostać wpisana ponownie na ogólnych zasadach, jeżeli zostanie złożony stosowny wniosek w tym przedmiocie. Organy właściwe do spraw cyberbezpieczeństwa obowiązane będą także do regularnego aktualizowania wykazu. Oznacza to, że w przypadku uchylecia decyzji, o zastosowaniu środka nadzorczego, o którym mowa w art. 53 ust. 9 pkt 6, dane dotyczące tego kierownika podmiotu kluczowego zostaną usunięte z wykazu.

2.19. CSIRT sektorowe

Wprowadza się obowiązek powołania przez organ właściwy do spraw cyberbezpieczeństwa CSIRT sektorowego właściwego dla danego sektora lub podsektora, który będzie wspierał podmioty kluczowe i podmioty ważne tego sektora w obszarze reagowania na incydenty.

Do obligatoryjnych zadań CSIRT sektorowego będzie należało przyjmowanie zgłoszeń o incydentach oraz reagowanie na incydenty. Dotychczas sektorowe zespoły cyberbezpieczeństwa miały za zadanie przyjmować zgłoszenia o incydentach poważnych i reagować na nie. Zmiana ta pozwoli CSIRT sektorowemu uzyskiwać więcej zgłoszeń o incydentach, dzięki czemu zespół będzie mógł szybciej zdobywać doświadczenie i wiedzę w ciągle zmieniającej się sytuacji w cyberprzestrzeni. Przełoży się to na skuteczną pomoc dla podmiotów kluczowych i podmiotów ważnych zmagających się z incydentami. Podkreślić przy tym należy, że nadal podmioty kluczowe i podmioty ważne będą prawnie obowiązani zgłaszać tylko incydenty poważne do CSIRT sektorowego. Dobrowolnie będą mogli zgłosić każdy incydent, nawet ten który nie spełnia progów incydentu poważnego.

Innymi zadaniami CSIRT sektorowego będzie:

- 1) gromadzenie informacji o podatnościach i cyberzagrożeniach;
- 2) współpraca z podmiotami kluczowymi i podmiotami ważnymi w zakresie wymiany dobrych praktyk oraz informacji o podatnościach i cyberzagrożeniach, organizacja i uczestniczenie w ćwiczeniach oraz wspieranie inicjatyw szkoleniowych;
- 3) współpraca z CSIRT MON, CSIRT NASK i CSIRT GOV w koordynowanym przez nie reagowaniu na incydenty, w szczególności w zakresie wymiany informacji o cyberzagrożeniach oraz stosowanych środkach zapobiegających i ograniczających wpływ incydentów; przepis podkreśla nadrzędną rolę zespołów CSIRT poziomu krajowego;
- 4) współpraca z innymi CSIRT sektorowymi w zakresie wymiany informacji o podatnościach i cyberzagrożeniach.

Otrzymają również fakultatywną kompetencję zapewniania dynamicznej analizy ryzyka i incydentów oraz koordynacji incydentów w sektorze, a także będą mogły, w uzgodnieniu z podmiotem kluczowym lub podmiotem ważnym, wspierać go w wykonywaniu jego obowiązków określonych w ustawie o KSC. Będą one również uprawnione do przeprowadzania, w określonych sytuacjach, testów bezpieczeństwa. Katalog zadań CSIRT sektorowego jest katalogiem otwartym, mając na względzie, że CSIRT sektorowy powinien być dostosowany do sektora, do podmiotów, które wspiera. Zależnie od oceny organu

właściwego do spraw cyberbezpieczeństwa ustawowe zadania CSIRT sektorowego mogłyby być uzupełnione o inne np. o wsparcie operatorów usług kluczowych w zakresie zarządzania ciągłością działania, czy o zadania związane z proaktywnym przeciwdziałaniem incydom, tworzeniem oprogramowania bezpieczeństwa, czy monitoring technologii⁵³⁾. Otwartość katalogu jest spowodowana także tym, że nie ma CSIRT, który zapewniałby wszystkie usługi zawarte w metodykach⁵⁴⁾, dlatego niezbędna jest tutaj zdrowa elastyczność. Projekt zakłada, że część zadań CSIRT sektorowego może być ustalona w akcie tworzącym CSIRT (np. w statucie jednostki budżetowej działającej jako CSIRT). Oczywiście te fakultatywne zadania nie mogą prowadzić do nałożenia pozaustawowych obowiązków na podmioty kluczowe lub podmioty ważne. Organ właściwy do spraw cyberbezpieczeństwa ustanawiając te zadania powinien się kierować uznanymi metodykami tworzenia takich zespołów oraz koniecznością zapewnienia jak najlepszego wsparcia operatorom usług kluczowych.

CSIRT sektorowy będzie niezwłocznie (maksymalnie w ciągu 8 godzin) przekazywał zgłoszenie o incydencie poważnym do właściwego CSIRT MON, CSIRT NASK albo CSIRT GOV. Takie rozwiązanie gwarantuje, że zespoły CSIRT poziomu krajowego będą posiadały aktualną wiedzę o występowaniu incydentów w systemie.

Wprowadzono również regułę kolizyjną – CSIRT sektorowy, który omyłkowo otrzymał zgłoszenie incydomu do którego obsługi nie jest właściwy ma obowiązek niezwłocznie przekazać go do właściwego CSIRT sektorowego.

W przepisach podkreślono, że CSIRT sektorowy w sektorze bankowości i infrastruktury rynków finansowych może realizować swoje zadania także w zakresie poważnych incydomów związanych z ICT zgłaszanych przez podmioty kluczowe i podmioty ważne oraz podmioty finansowe. Jest to konieczne ze względu na styk regulacji NIS 2 z rozporządzeniem DORA oraz w związku z tym, że rozporządzenie DORA posługuje się własną definicją incydomu – poważny incydom związany z ICT. Ta definicja jest bardzo podobna do definicji z dyrektywy NIS 2, ale żeby przeciąć wątpliwości wskazano wyraźnie w przepisie, że ten CSIRT sektorowy może również obsługiwać tego rodzaju incydomy.

Dzięki wprowadzonym zmianom podmiotom kluczowym i podmiotom ważnym zostanie zapewnione najlepsze możliwe wsparcie przy obsłudze incydomów. Ponadto nowy system

⁵³⁾ Por. Martijn van der Heide, *Establishing a CSIRT*, str. 25. <https://www.first.org/resources/guides/Establishing-CSIRT-v1.2.pdf>

⁵⁴⁾ *Ibidem*.

zgłaszania incydentów zmniejsza obciążenia administracyjne ciążące na operatorach usług kluczowych.

Należy przy tym wskazać na doświadczenia płynące z funkcjonowania CSIRT KNF – jedyne obecnie sektorowe zespoły cyberbezpieczeństwa. W 2021 r. CSIRT KNF przekazał podmiotom rynku finansowego 22 ostrzeżenia o zagrożeniach cyberbezpieczeństwa wraz z sugerowanymi działaniami mitygującymi te zagrożenia. Zespół ten systematycznie monitoruje kampanie złośliwego oprogramowania ukierunkowane na instytucje i klientów polskiego rynku finansowego. Prowadzi działalność edukacyjną poprzez szkolenia dla podmiotów nadzorowanych, publikowanie artykułów w prasie czy w mediach społecznościowych⁵⁵⁾. Niezależnie od tego zespół ten wspiera 20 operatorów usług kluczowych w sektorze bankowości i infrastrukturze rynków finansowych w obsłudze incydentów poważnych. W 2021 r. w tym sektorze doszło do 30 incydentów poważnych⁵⁶⁾, a od dnia 1 stycznia do dnia 8 grudnia 2022 r. do 21 incydentów poważnych⁵⁷⁾. Dzięki istnieniu wyspecjalizowanego dla tego sektora zespołu CSIRT podmioty rynku finansowego mogły liczyć na szybką i konkretną pomoc przy incydentach poważnych związanych ze świadczeniem usług bankowości elektronicznej.

Opierając się na tych doświadczeniach projektodawca jest zdania, że powołanie analogicznych zespołów w innych sektorach gospodarki pozytywnie wpłynie na zdolności operatorów usług kluczowych w zakresie cyberbezpieczeństwa.

Organ właściwy do spraw cyberbezpieczeństwa będzie mógł powierzyć realizację zadań CSIRT sektorowego jednostkom podległym lub nadzorowanym⁵⁸⁾ albo organowi przez niego nadzorowanemu jak również urzędowi, który obsługuje organ właściwy do spraw cyberbezpieczeństwa.

Przykładowo zadania CSIRT sektorowego będą mogły być powierzone jednostce budżetowej podległej danemu organowi właściwemu do spraw cyberbezpieczeństwa. Finansowanie CSIRT sektorowego odbędzie się co do zasady z budżetu państwa – jednostka

⁵⁵⁾ Sprawozdanie z działalności Urzędu Komisji Nadzoru Finansowego oraz Komisji Nadzoru Finansowego w 2021 roku, str. 151–154.

https://www.knf.gov.pl/?articleId=78355&p_id=18.

⁵⁶⁾ Źródło <https://dane.gov.pl/pl/dataset/1992,statystyki-zespołu-cert-polska/resource/35639/table>.

⁵⁷⁾ Źródło <https://dane.gov.pl/pl/dataset/1992,statystyki-zespołu-cert-polska/resource/43252/table>.

⁵⁸⁾ Należy przy tym podkreślić, że chodzi tutaj o jednostki organizacyjne, o których mowa w art. 33 ust. 1d ustawy z dnia 8 sierpnia 1996 r. o Radzie Ministrów (Dz. U. z 2025 r. poz. 780).

budżetowa będąca CSIRT sektorowym powinna być ustanowiona dysponentem⁵⁹⁾ środków budżetu państwa drugiego lub trzeciego stopnia z części budżetowej, której dysponentem jest organ właściwy do spraw cyberbezpieczeństwa. Do decyzji organu właściwego do spraw cyberbezpieczeństwa należeć będzie czy zadania CSIRT sektorowego zostaną powierzone istniejącej jednostce budżetowej czy też zostanie w tym celu utworzona nowa jednostka budżetowa zgodnie z art. 12 lub 13 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych.

Projekt przewiduje możliwość powierzenia zadań także jednostce nadzorowanej przez organ właściwy do spraw cyberbezpieczeństwa. W szczególności CSIRT sektorowy mógłby zostać utworzony w państwowym instytucie badawczym. Zgodnie z art. 22 pkt 2 lit b ustawy z dnia 30 kwietnia 2010 r. o instytutach badawczych (Dz. U. z 2024 r. poz. 534 oraz z 2025 r. poz. 1017 i 1080), do zadań państwowego instytutu badawczego należy wykonywanie m.in. zadań szczególnie ważnych dla planowania i realizacji polityki państwa, których wykonanie jest niezbędne dla zapewnienia obronności i bezpieczeństwa publicznego, które dotyczą monitoringu i zapobiegania skutkom zjawisk i wydarzeń mogących stwarzać zagrożenie publiczne. Niewątpliwie zapobieganie i reagowanie na incydenty poważne stanowi materię bezpieczeństwa publicznego. Z tego powodu zasadne jest powierzenie zadań CSIRT sektorowego państwowemu instytutowi badawczemu.

Jednostka której powierzono zadania CSIRT sektorowego będzie mogła otrzymać na ten cel dotację celową. Chodzi oczywiście o jednostki, które nie są jednostkami budżetowymi.

Przewiduje się także możliwość powierzenia zadania CSIRT sektorowego państwowej osobie prawnej – chodzi o możliwość wykorzystania już istniejących zasobów w podmiotach, które są kontrolowane przez Skarb Państwa. Dodatkowym warunkiem jest dysponowanie przez taką osobę prawną zdolnościami technicznymi i organizacyjnymi niezbędnymi do wypełniania zadań CSIRT sektorowego w danym sektorze lub podsektorze. Warunek ten zabezpiecza przed powierzeniem realizacji zadania CSIRT państwowym osobom prawnym, które nie mają odpowiedniej dojrzałości, aby realizować zadania CSIRT.

Wprowadza się także możliwość porozumienia się organów właściwych ds. cyberbezpieczeństwa i wyznaczenia wspólnego CSIRT sektorowego dla kilku sektorów. Takie rozwiązanie pozwoli na efektywne wykorzystanie dostępnych zasobów przez administrację. W tym przypadku konieczne będzie zawarcie porozumienia pomiędzy organami

⁵⁹⁾ Zgodnie z rozporządzeniem Ministra Finansów z dnia 15 stycznia 2014 r. w sprawie szczegółowego sposobu wykonywania budżetu państwa (Dz. U. z 2021 r. poz. 259 oraz z 2022 r. poz. 2846).

właściwymi do spraw cyberbezpieczeństwa jak również jednostką, której powierza się zadania CSIRT sektorowego. Porozumienie musi objąć zakres powierzonych zadań (czy wszystkie zadania CSIRT czy może tylko niektóre), zasady sprawowania kontroli nad prawidłowym wykonywaniem powierzonych zadań (np. możliwość żądania informacji od CSIRT przez organ właściwy ds. cyberbezpieczeństwa) a także określać sposób finansowania zadań – czy będzie to dotacja celowa (w przypadku jednostek organizacyjnych, które nie są jednostkami budżetowymi) czy też jednostka budżetowa realizująca zadania CSIRT sektorowego zostanie ustanowiona dysponentem środków budżetu państwa drugiego lub trzeciego stopnia z części budżetowej, której dysponentem jest organ właściwy do spraw cyberbezpieczeństwa.

Przewidziano także sytuację, gdy minister jest organem właściwym do spraw cyberbezpieczeństwa dla kilku sektorów, ponieważ kieruje kilkoma działami administracji rządowej. Będzie mógł wtedy wydać decyzję o wyznaczeniu jednego CSIRT sektorowego dla wszystkich nadzorowanych podmiotów – a następcy prawni ministra będą mogli zawrzeć porozumienie, w którym zdecydują jaka jednostka dalej będzie pełniła funkcje CSIRT sektorowego dla nadzorowanych przez nich sektorów. Ta decyzja nie będzie decyzją w rozumieniu Kodeksu postępowania administracyjnego, ponieważ minister będzie ją wydawał wobec podmiotów, wobec których posiada władczość. Wprowadza się przy tym obowiązek publikacji decyzji w dzienniku urzędowym organu właściwego do spraw cyberbezpieczeństwa, co umożliwi poinformowanie wszystkich zainteresowanych o powierzeniu zadań CSIRT sektorowego.

Organ właściwy będzie mógł także, alternatywnie, porozumieć się z organami prowadzącymi CSIRT MON, CSIRT NASK, CSIRT GOV i powierzyć im realizację zadań CSIRT sektorowego.

Szczególną regulację zastosowano wobec powierzenia zespołowi CSIRT MON zadań CSIRT sektorowego – tutaj Minister Obrony Narodowej będzie mógł wydać decyzję o powierzeniu zadań zespołowi CSIRT MON. Z uwagi na charakter militarny ta decyzja nie będzie podlegała ogłoszeniu.

Tego rodzaju przepisy zapewnią elastyczność i efektywne wykorzystanie zasobów przy powoływaniu zespołów CSIRT sektorowych.

Konieczne jest określenie przepisów dotyczących finansowania zadań CSIRT sektorowego. Oczywiście jest, że zadania te są finansowane przede wszystkim z budżetu państwa – z części budżetu państwa, której dysponentem jest minister albo centralny organ

administracji rządowej⁶⁰⁾, będący organem właściwym do spraw cyberbezpieczeństwa. Należało przy tym dodać, że zadania te mogą być dofinansowywane:

- ze środków pochodzących z budżetu Unii Europejskiej,
- ze środków przeznaczonych na realizację programów finansowanych z udziałem środków pochodzących z budżetu Unii Europejskiej.

Zespołem CSIRT sektorowym może być jednostka organizacyjna (instytucja gospodarki budżetowej, państwowa osoba prawna itd.), która nie jest jednostką budżetową. Taka jednostka nie mogła by otrzymać bezpośrednio środków z budżetu państwa na realizację zadań CSIRT sektorowego. Dlatego więc przewidziano możliwość udzielania dotacji celowej na realizację zadań CSIRT sektorowego z części budżetowej której dysponentem jest minister będący organem właściwym do spraw cyberbezpieczeństwa dla danego sektora lub podsektora. Zapewni to możliwość finansowania zadań. W tym miejscu warto podkreślić oczywisty fakt – jednostka budżetowa nie może otrzymać dotacji z budżetu państwa, gdyż jest to sprzeczne z istotą jednostki budżetowej i przepisami ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2024 r. poz. 1530, z późn. zm.).

Konieczne jest uregulowanie sytuacji zespołu CSIRT sektorowego dla kilku sektorów, który funkcjonuje w jednostce budżetowej. Przepisy ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych pozwalają na przenoszenie środków pomiędzy częściami budżetowymi tylko w rzadkich sytuacjach. Co do zasady nie jest to jednak możliwe. Dlatego wprowadza się regułę, że taka jednostka budżetowa otrzymuje środki z części budżetowych, których dysponentami są organy właściwe do spraw cyberbezpieczeństwa dla danego sektora lub podsektora, które zawarły porozumienie o powierzeniu tej jednostce zadań CSIRT sektorowego. Czyli taka jednostka budżetowa będzie z mocy prawa finansowana z 2 (ew. więcej) części budżetowych. Bez tego rozwiązania nie byłoby prawnych możliwości przekazania środków finansowych na zespół CSIRT realizujący zadania dla kilku sektorów.

Komunikaty o porozumieniach w sprawie powierzenia realizacji zadań CSIRT sektorowego będą ogłaszane w dzienniku urzędowym organu właściwego do spraw cyberbezpieczeństwa oraz w BIP Pełnomocnika. Zapewni to wszystkim zainteresowanym dostęp do informacji o jednostkach realizujących zadania CSIRT sektorowych.

⁶⁰⁾ Tutaj takim organem będzie Prezes Urzędu Komunikacji Elektronicznej, który ma swoją część budżetu państwa – cz. 76.

Jednostka organizacyjna, której organ właściwy do spraw cyberbezpieczeństwa powierzył rolę CSIRT sektorowego stanie się oczywiście administratorem danych osobowych przetwarzanych w ramach obsługi incydentów.

Organy właściwe do spraw cyberbezpieczeństwa będą raz w roku, do dnia 31 stycznia, przedkładać Pełnomocnikowi Rządu do Spraw Cyberbezpieczeństwa sprawozdania z funkcjonowania CSIRT sektorowych, które zapewni niezbędne informacje do prowadzenia oceny funkcjonowania krajowego systemu cyberbezpieczeństwa zgodnie z art. 62 ust. 1 pkt 1 ustawy o KSC.

2.20. Kompetencje ministra właściwego do spraw informatyzacji

2.20.1. Kompetencje ministra

Zmiany w zakresie kompetencji ministra właściwego do spraw informatyzacji wynikają ze zmian w zakresie struktury krajowego systemu cyberbezpieczeństwa i nowych definicji oraz dostosowują je do tych zmian. Wskazano, że minister ten będzie prowadził wykaz podmiotów kluczowych i podmiotów ważnych. Nowym zadaniem ministra właściwego do spraw informatyzacji, wynikającym z dyrektywy NIS 2, będzie przygotowanie i monitorowanie wykonania Krajowego Planu reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę i monitorowania jego wykonania. Minister właściwy do spraw informatyzacji będzie pełnił rolę organu odpowiedzialnego za zarządzanie incydentami i zarządzanie kryzysowe w cyberbezpieczeństwie na dużą skalę w wymiarze cywilnym. Pozwoli to zbliżyć reżim krajowego systemu cyberbezpieczeństwa oraz zarządzania kryzysowego zapewniając przepływ niezbędnych informacji i synergii działań.

W wymiarze międzynarodowym minister właściwy do spraw informatyzacji będzie współpracował w obszarze cyberbezpieczeństwa z państwami trzecimi – obejmuje to działalność nie tylko w ramach Unii Europejskiej ale także poza nią, np. uczestnictwo w konferencjach dyplomatycznych, współpraca bilateralna, przygotowywanie wspólnych deklaracji. Te działania oczywiście będą wykonywane we współpracy z ministrem właściwym do spraw zagranicznych.

Wprowadza się także możliwość aby minister właściwy do spraw informatyzacji opublikował zestawienie wymogów dokumentów normalizacyjnych, o których mowa w art. 2 pkt 3 ustawy z dnia 12 września 2002 r. o normalizacji (Dz. U. z 2015 r. poz. 1483), których wykonywanie realizuje obowiązki wynikające z przepisów ustawy oraz z przepisów wydanych na podstawie art. 8a. Celem tego rozwiązania jest ułatwienie funkcjonowania podmiotom

kluczowym i podmiotom ważnym i wskazanie różnych norm, standardów i innych dokumentów, które spełniają wymogi ustawy. To zestawienia będzie miało charakter tzw. prawa miękkiego. W razie jakichkolwiek wątpliwości zawsze wiążące będą przepisy ustawy. Jeżeli podmiot wykona przepisy ustawy w oparciu o normę nie znajdującą się w tym zestawieniu i wykaże ponad wszelką wątpliwość zgodność z ustawą, to takie działanie nie będzie z ustawą sprzeczne. Zestawienie to powinno być skutkiem dialogu między administracją a przedsiębiorcami i organizacjami społecznymi. Dlatego przed jego wydaniem minister właściwy do spraw informatyzacji przeprowadzi 30-dniowe konsultacje publiczne – które też powinny objąć organy właściwe do spraw cyberbezpieczeństwa. Skutkiem konsultacji powinien być raport zawierający główne tezy zawarte w stanowiskach zgłoszonych do projektu zestawienia oraz odniesienie się do tych stanowisk. Ma to wymiar praktyczny – nie tylko będzie taki raport prostszy do sporządzenia względem długiej tabeli uwag ale również łatwiej będzie się zapoznać ze stanowiskami i odpowiedzieć na nie. W ramach jawności życia publicznego projekt zestawienia, uwagi, raport będą opublikowane w BIP ministra właściwego do spraw informatyzacji. Nie będzie to dotyczyło oczywiście danych osobowych osób fizycznych biorących udział w konsultacjach publicznych. W przepisach o przetwarzaniu danych osobowych zawarto uprawnienie dla ministra do przetwarzania danych osobowych osób uczestniczących w tych konsultacjach, w tym także danych szczególnych z art. 9 RODO – są ku temu 2 argumenty: 1. Podobnie jest tak unormowane w ustawie o Radzie Ministrów, 2. Dane szczególne z art. 9 RODO to także dane o przynależności związkowej – nie jest wykluczone że uwagi zgłoszą przedstawiciele związków zawodowych.

Rozbudowuje się obecną kompetencję ministra właściwego do spraw informatyzacji do udzielania wsparcia finansowego w ramach programów rządowych lub innych programów np. unijnych. Obecnie brzmienie jest szczątkowe i należy je uzupełnić przynajmniej o rodzaje projektów, na które można udzielić tego wsparcia.

Wsparcia udziela się na realizację projektów, których celem jest:

- 1) tworzenie i rozwój produktów ICT, usług ICT oraz procesów ICT z zakresu cyberbezpieczeństwa;
- 2) rozwój kompetencji w obszarze cyberbezpieczeństwa;
- 3) zapewnianie cyberbezpieczeństwa w danej jednostce organizacyjnej;
- 4) promocja dobrych praktyk, programów edukacyjnych, kampanii i szkoleń na rzecz poszerzania wiedzy i budowania świadomości z zakresu cyberbezpieczeństwa;
- 5) wsparcie w obszarze standaryzacji i certyfikacji cyberbezpieczeństwa;

- 6) rozwój infrastruktury służącej zapewnianiu cyberbezpieczeństwa;
- 7) wsparcie badań naukowych, rozwoju technologicznego i projektów pilotażowych związanych z cyberbezpieczeństwem;
- 8) wsparcie w obsłudze incydentów;
- 9) identyfikacja i mitygacja podatności produktów ICT, usług ICT i procesów ICT;
- 10) zwiększenie rozpoznawalności produktów lub usług z zakresu cyberbezpieczeństwa;
- 11) inne działania służące rozwojowi cyberbezpieczeństwa.

Cele opisano szeroko, aby w jak największy sposób umożliwić udzielanie wsparcia.

Wsparcie finansowe może być udzielone tylko podmiotom, które mają zdolności do realizacji wyżej wskazanych projektów. Takie rozwiązanie uniemożliwia wydawanie pieniędzy unijnych dla podmiotów, które nie są w stanie zrealizować projektów, na które otrzymają wsparcie.

Wsparcie finansowe może mieć charakter pomocy publicznej dla podmiotów prywatnych czy pomocy de minimis oraz dofinansowania dla podmiotów publicznych.

Projekty będą wybierane w trybie konkursowym albo pozakonkursowym. Ten drugi typ może być przydatny przy udzielaniu wsparcia dla konkretnego rodzaju podmiotów jak np. CSIRT sektorowe czy organy właściwe do spraw cyberbezpieczeństwa albo wąska grupa podmiotów kluczowych lub podmiotów ważnych w ramach konkretnego sektora.

Wsparcie finansowe będzie udzielane na podstawie rozporządzenia ministra właściwego do spraw informatyzacji. Dotychczasowe upoważnienie ustawowe do wydania rozporządzenia zostało dostosowane do nowej treści przepisów. Określi ono szczegółowe warunki udzielania tego wsparcia finansowego – czyli jakie przesłanki musi spełnić dany podmiot aby otrzymać pomoc – w tym także kryteria oceny projektu, formę udzielania wsparcia finansowego – czy jest to pomoc publiczna, pomoc de minimis albo dofinansowanie dla podmiotów publicznych, a także tryb udzielania wsparcia – konkursowy albo pozakonkursowy. Przewiduje się, że na podstawie tego upoważnienia ustawowego będzie wydawanych wiele rozporządzeń, które będą musiały być spójne z programami finansowymi oraz z przepisami krajowymi jak i unijnymi regulującymi dany rodzaj udzielania pomocy.

Obecnie istnieje wyspecjalizowana jednostka budżetowa, podległa ministrowi właściwemu do spraw informatyzacji, która posiada wieloletnie doświadczenie, wiedzę i kompetencje w zakresie udzielania różnego rodzaju wsparcia finansowego. Jest to Centrum

Projektów Polska Cyfrowa. Aby wykorzystać efektywnie ten zasób wprowadza się możliwość udzielenia wsparcia finansowego przez podmiot podległy ministrowi właściwemu do spraw informatyzacji lub przez niego nadzorowany.

Dodano także zasady wyboru projektów do wsparcia finansowego – wybór ma być dokonany w sposób przejrzysty, rzetelny i bezstronny na podstawie obiektywnych kryteriów oceny. Pozwoli to na sprawiedliwe udzielenie wsparcia finansowego podmiotom, które rzeczywiście go potrzebują i przy zachowaniu neutralności. Podstawą dofinansowania projektu będzie umowa o dofinansowanie zawarta między beneficjentem a podmiotem, który udziela dofinansowania – z reguły będzie to Centrum Projektów Polska Cyfrowa. Beneficjent może wykorzystywać wsparcie tylko na wydatki służące realizacji wcześniej wymienionych celów związanych z cyberbezpieczeństwem. Jeżeli wyda na inne wydatki, to środki te musi zwrócić w terminie nie dłuższym niż 15 dni od określonego w umowie dnia wykonania zadania. Beneficjent musi informować podmiot udzielający wsparcie o postępach w realizacji projektu w terminach wskazanych w umowie.

Do umowy o dofinansowanie stosować się będzie odpowiednio art. 150 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych w ten sposób, że w umowie zostanie określony:

- 1) szczegółowy opis projektu, w tym cel, na jaki dofinansowanie zostało przyznane, i termin jego wykonania;
- 2) wysokość udzielonego dofinansowania;
- 3) termin wykorzystania dofinansowania, nie dłuższy niż do dnia 31 grudnia danego roku budżetowego;
- 4) termin i sposób rozliczenia udzielonego dofinansowania;
- 5) termin zwrotu niewykorzystanej części dofinansowania, nie dłuższy niż 15 dni od określonego w umowie dnia wykonania zadania, a w przypadku zadania realizowanego za granicą - 30 dni od określonego w umowie dnia jego wykonania;
- 6) tryb kontroli wykonania projektu.

2.20.2. System teleinformatyczny S46

Obecnie funkcjonujący system teleinformatyczny S46 zostanie dostosowany do tego, aby stać się głównym środkiem komunikacji pomiędzy podmiotami krajowego systemu cyberbezpieczeństwa. W związku z koniecznością dodania do tego systemu bardzo dużej liczby podmiotów zrezygnowano z zawierania porozumienia o dołączeniu do systemu. Ponadto dołączenie do systemu nie będzie już wymagało zakupu specjalnych urządzeń, ale będzie odbywało się za pomocą rozwiązań chmurowych. Podmioty kluczowe i podmioty

ważne będą obowiązane zapewnić zgodność swoich systemów informacyjnych z minimalnymi wymaganiami technicznymi i funkcjonalnymi podłączenia do systemu teleinformatycznego S46 w terminie 3 miesięcy od ich udostępnienia. Podmioty te będą więc miały odpowiedni czas na dostosowanie swoich systemów.

Wskazano w przepisie, że zespoły CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT sektorowe, organy właściwe do spraw cyberbezpieczeństwa oraz Prezes Urzędu Ochrony Danych Osobowych korzystają z systemu w celu realizacji swoich zadań ustawowych. Głównie chodzi o sprawowanie nadzoru nad podmiotami kluczowymi i podmiotami ważnymi oraz przyjmowanie zgłoszeń incydentów a także reagowanie na incydenty jak i wymiana informacji o cyberbezpieczeństwie. Przepisy te nie naruszają uprawnień Prezesa Urzędu Ochrony Danych Osobowych wynikających z RODO.

Dla podmiotów kluczowych i podmiotów ważnych wprowadzono obligatoryjność korzystania z systemu teleinformatycznego S46 – na to podmioty będą miały czas 6 miesięcy od spełnienia przesłanek uznania za podmiot kluczowy lub podmiot ważny. Za pomocą tego systemu podmioty kluczowe oraz podmioty ważne będą zgłaszały incydenty do zespołów CSIRT sektorowych, ale również zwrotnie będą otrzymywały informacje o cyberzagrożeniach, podatnościach i innych incydentach, aby mogły rozwijać się pod kątem cyberbezpieczeństwa.

W systemie tym będzie prowadzony również wykaz podmiotów kluczowych i podmiotów ważnych. Oprócz tego system będzie wspierał wykonywanie zadań nadzorczych organów właściwych do spraw cyberbezpieczeństwa – np. będzie mógł ułatwić analizę sprawozdań audytowych poprzez zastosowanie sztucznej inteligencji. Innym nowym zadaniem będzie wymiana informacji ministra właściwego do spraw informatyzacji, Pełnomocnika i organów właściwych do spraw cyberbezpieczeństwa mających charakter generalny – są to w szczególności rekomendacje Pełnomocnika z art. 33 oraz z art. 67a, zestawienie dokumentów normalizacyjnych ministra właściwego do spraw informatyzacji.

Obowiązki z zakresu cyberbezpieczeństwa oraz ochrona danych osobowych często wzajemnie się przenikają. W obydwu przypadkach należy wdrożyć proporcjonalne środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych. Bardzo często incydent w rozumieniu ustawy o KSC stanowi jednocześnie naruszenie ochrony danych osobowych. Przepisy prawa przewidują także obowiązek notyfikacji tych zdarzeń. W przypadku incydentów cyberbezpieczeństwa podmioty krajowego systemu cyberbezpieczeństwa

zgłaszają incydenty do jednego z zespołów CSIRT poziomu krajowego, a w przypadku naruszeń – do Prezesa Urzędu Ochrony Danych Osobowych.

Mnogość obowiązków informacyjnych może utrudnić ich realizację. Tymczasem art. 67 pkt 2 oraz 3 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców, nakazuje przy projektowaniu aktów normatywnych dążenie do ograniczenia obowiązków informacyjnych oraz umożliwienie ich realizacji w postaci elektronicznej.

Z tego powodu wprowadza się możliwość zgłaszania naruszeń ochrony danych osobowych za pomocą systemu teleinformatycznego S46. Takie rozwiązanie z pewnością ułatwi zgłaszanie zdarzeń, będących zarówno incydentami jak i naruszeniami ochrony danych osobowych.

Uwierzytelnienie w systemie teleinformatycznym S46 będzie się odbywać tak, jak to przewiduje ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne. Jest to ogólny sposób uwierzytelniania w systemach podmiotów realizujących zadania publiczne, dobrze też znany.

Uwierzytelnienie użytkownika będzie więc dostępne za pomocą bezpłatnych profilu zaufanego oraz profilu osobistego, a także środków identyfikacji elektronicznej dostarczanych przez banki jak również za pomocą danych weryfikowanych za pomocą kwalifikowanego certyfikatu podpisu elektronicznego, jeżeli te dane pozwalają na identyfikację i uwierzytelnienie.

Na prośbę Ministra Obrony Narodowej dodano możliwość, aby zespoły CSIRT poziomu krajowego mogły otrzymywać informacje przetwarzanych w systemie teleinformatycznym S46 dotyczących danego podmiotu kluczowego lub podmiotu ważnego. Informacje te będą przydatne zespołom CSIRT, które prowadzą szacowanie ryzyka na poziomie krajowym.

Dopuszcza się korzystanie przez podmioty resortu obrony narodowej z własnych odrębnych środków komunikacji elektronicznej do zgłaszania incydentów do CSIRT MON i CSIRT sektorowych.

Wprowadza się również przepisy regulujące kwestie doręczania dokumentów w postaci elektronicznej w systemie teleinformatycznym S46. Co do zasady doręczenie jest skuteczne, jeżeli adresat potwierdzi odbiór pisma w systemie. Aby jednak przeciwdziałać próbom unikania doręczenia organ po upływie 7 dni, licząc od dnia wysłania pisma, przesyła zawiadomienie o możliwości odebrania tego pisma. Po 14 dniach od dnia wysłania pisma doręczenie uważa się za dokonane – jest to tzw. fikcja doręczenia.

2.20.3. Powierzenie realizacji zadań ministra właściwego do spraw informatyzacji

Dostosowano przepis, który obecnie umożliwia powierzenie realizacji zadań ministra właściwego do spraw informatyzacji jego jednostkom podległym lub przez niego nadzorowanym. Uzupełniono katalog zadań, które mogą być powierzone – są to zadania własne ministra takie jak monitorowanie wdrożenia Strategii, prowadzenie systemu teleinformatycznego S46 jak również udzielanie wsparcia finansowego na projekcie z zakresu cyberbezpieczeństwa.

Wskazano przy tym, że minister właściwy do spraw informatyzacji może udostępniać jednostkom, którym powierzył realizację zadań dane z wykazu podmiotów kluczowych i podmiotów ważnych w zakresie i w celu realizacji zadań im powierzonych. Udostępnianie to musi być zgodne z RODO i uwzględniać poufność, integralność, dostępność i autentyczność danych. Przepis ten ma pełnić funkcję gwarancyjną.

2.20.4. Pojedynczy punkt kontaktowy

Przepisy ustawy o KSC w zakresie pojedynczego punktu kontaktowego zostały dostosowane do nowej struktury pojęciowej oraz do zmian jakie zostały wprowadzone, w tym wśród instytucji unijnych. Zapewni to sprawną i efektywną wymianę informacji w obszarze cyberbezpieczeństwa. Pojedynczy punkt kontaktowy będzie przekazywał Agencji Unii Europejskiej do Spraw Cyberbezpieczeństwa (ENISA) aktualne dane o podmiotach z sektorów infrastruktury cyfrowej, zarządzania ICT i dostawców usług cyfrowych, a także Komisji Europejskiej oraz Grupie Współpracy informacje o podmiotach znajdujących się w wykazie podmiotów kluczowych i podmiotów ważnych – konieczność ta wynika wprost z przepisów dyrektywy NIS 2. Wskazano przy tym katalog danych przekazywanych do ENISA.

Zgodnie z dyrektywą NIS 2 Pojedynczy Punkt Kontaktowy przekazywać będzie do ENISA sprawozdanie o zgłoszonych incydentach poważnych, incydentach, cyberzagrożeniach oraz potencjalnych zdarzeniach dla cyberbezpieczeństwa.

Z uwagi na transgraniczną działalność podmiotów z sektorów infrastruktury cyfrowej, zarządzania ICT i dostawców usług cyfrowych dyrektywa NIS 2 wprowadziła zadanie dla ENISA w postaci prowadzenia rejestru tych podmiotów. Dane o tych podmiotach będą szczególnie przydatne przy obsłudze incydentów. Dlatego oprócz obowiązku dostarczania danych do rejestru ENISA dyrektywa NIS 2 nadała państwom członkowskim uprawnienie do żądania udostępnienia danych z tego rejestru – np. podmiotów z innych państw, które to dane są istotne do obsługi incydentu. W projektowanej ustawie uprawnienie do przysługuje

organom właściwym do spraw cyberbezpieczeństwa, CSIRT sektorowym oraz CSIRT poziomowi krajowego. Wniosek będzie składany do ENISA za pośrednictwem Pojedynczego Punktu Kontaktowego. Wniosek będzie zawierał zakres żądanych danych.

Polska jako państwo członkowskie Unii Europejskiej jest obowiązana przekazywać Komisji Europejskiej informacje liczbie podmiotów kluczowych i podmiotów ważnych w podziale na sektory, oraz wskazane jakie usługi świadczą te podmioty jak również podstawę prawną wskazania tych podmiotów. Te informacje są potrzebne Komisji Europejskiej do analizy funkcjonowania dyrektywy NIS 2.

ENISA dysponuje wiedzą teoretyczną i praktyczną w zakresie budowy i funkcjonowania zespołów CSIRT. Z tego powodu, zgodnie z dyrektywą NIS2, wprowadza się uprawnienie dla podmiotów odpowiedzialnych za utworzenie CSIRT do zwrócenie do ENISA o pomoc w rozwijaniu tych zespołów. Tak jak w innych przypadkach uprawnienie to jest realizowane za pomocą Pojedynczego Punktu Kontaktowego.

2.21. Zadania Ministra Obrony Narodowej

Katalog zadań Ministra Obrony Narodowej został dostosowany do nowej struktury krajowego systemu cyberbezpieczeństwa. Nowymi zadaniami w zakresie cyberbezpieczeństwa są:

- 1) kierowanie, za pośrednictwem CSIRT MON, działaniami związanymi z obsługą incydentów, a także koordynowanie działań CSIRT NASK i CSIRT GOV w czasie stanu wojennego oraz w czasie wojny;
- 2) ocenę cyberzagrożeń w każdym ze stanów gotowości obronnej państwa oraz przedstawianie właściwym organom propozycji dotyczących działań obronnych;
- 3) koordynację, we współpracy z ministrem właściwym do spraw wewnętrznych i ministrem właściwym do spraw informatyzacji, realizacji zadań organów administracji rządowej i jednostek samorządu terytorialnego w czasie stanu wojennego lub w czasie wojny dotyczących działań obronnych w przypadku cyberzagrożenia;
- 4) koordynację działania organów państwa w przypadku wystąpienia sytuacji kryzysowej w cyberbezpieczeństwie dotyczącej obrony Państwa oraz Sił Zbrojnych Rzeczypospolitej Polskiej.

Zadania te podkreślają kluczową rolę Ministra Obrony Narodowej w przypadku wprowadzenia stanu wojennego oraz przy przygotowywaniu rozwiązań związanych z obroną państwa. Ponadto przepisy powierzają Ministrowi Obrony Narodowej zadania związane z zarządzaniem kryzysowym w cyberbezpieczeństwie w zakresie w jakim dotyczy to obrony państwa oraz Sił

Zbrojnych Rzeczypospolitej Polskiej. Takie rozwiązanie gwarantuje, że w zakresie Sił Zbrojnych i obrony państwa Minister Obrony Narodowej będzie miał kluczową rolę.

2.22. Zadania ministra właściwego do spraw energii

Procedowany projekt służy nie tylko wdrożeniu dyrektywy NIS 2, ale także rozporządzenia delegowanego Komisji (UE) 2024/1366 z dnia 11 marca 2024 r. uzupełniającego rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/943 poprzez ustanowienie kodeksu sieci dotyczącego zasad sektorowych w zakresie aspektów cyberbezpieczeństwa w transgranicznych przepływach energii elektrycznej. Rozporządzenie to jest bezpośrednio stosowane. Do państw członkowskich Unii Europejskiej należy wyznaczenie organu właściwego, który będzie wykonywał obowiązki wynikające z tego rozporządzenia. Kierując się przepisami art. 7a ust. 2 pkt 3 ustawy z dnia 4 września 1997 r. o działach administracji rządowej przypisano te zadania ministrowi właściwemu do spraw energii. W szczególności wskazano, że ten minister identyfikuje podmioty o dużym wpływie i podmioty o krytycznym wpływie. Identyfikacja ta jest inną czynnością z zakresu administracji publicznej – uproszczono więc znacznie postępowanie w sprawie identyfikacji, ale zapewniono możliwość złożenia skargi do sądu administracyjnego na tą czynność. Zgodnie z art. 24 ust. 6 rozporządzenia 2024/1366 minister właściwy do spraw energii musi powiadomić o identyfikacji podmiot w terminie 9 miesięcy od otrzymania powiadomienia o ogólnounijnym sprawozdaniu z oceny ryzyka w cyberprzestrzeni, stąd też nie dodawano kolejnego przepisu, który powtarzałaby tę normę.

Kryteria identyfikacji tych podmiotów są zawarte w dokumentach unijnych – istotny będzie tutaj wskaźnik wpływu na cyberbezpieczeństwo w odniesieniu do energii elektrycznej oraz progi dużego wpływu i progów krytycznego wpływu zawarte w ogólnounijnym sprawozdaniu z oceny ryzyka w cyberprzestrzeni zgodnie z art. 19 ust. 3 lit. b rozporządzenia 2024/1366.

Celem wykonania przepisów rozporządzenia 2024/1366 wprowadzono podstawę prawną dla ministra właściwego do spraw energii do wystąpienia do podmiotu kluczowego lub podmiotu ważnego z podsektora energii o udzielenie informacji, które pozwolą na wstępną ocenę, czy dany podmiot należy uznać za podmiot o dużym wpływie lub podmiot o krytycznym wpływie zgodnie z art. 24 rozporządzenia 2024/1366. Wprowadzono przy tym odesłanie do odpowiedniego stosowania art. 53c ust. 1–3 – jest to przepis o żądaniu informacji przez organ właściwy do spraw cyberbezpieczeństwa. Odpowiednie stosowanie tego przepisu polega na tym, że uprawnienie w nim zawarte przysługuje ministrowi właściwemu do spraw energii.

Obowiązany do udzielenia informacji będzie podmiot kluczowy lub podmiot ważny z podsektora energii elektrycznej, do którego zostało skierowane wystąpienie.

Minister właściwy do spraw energii otrzyma także uprawnienie do prowadzenia kontroli podmiotów zidentyfikowanych jako podmioty o krytycznym wpływie, o których mowa w rozporządzeniu 2024/1366. Zgodnie z tym rozporządzeniem mogą być prowadzone kontrole tych podmiotów. Nie nakłada się jednak administracyjnych kar pieniężnych.

2.23. Zadania ministra właściwego do spraw zagranicznych

W nowelizacji podkreślono wiodącą rolę ministra właściwego do spraw zagranicznych w obszarze cyberdyplomacji. Wskazano, że prowadzi działalność dyplomatyczną w obszarze cyberbezpieczeństwa w stosunkach z państwami trzecimi i organizacjami międzynarodowymi oraz koordynuje tę współpracę. Podkreślenie „prowadzenia tej działalności” ma na celu umożliwienie podejmowania samodzielnych działań w tym obszarze. Minister właściwy do spraw zagranicznych będzie też otrzymywał od ministra właściwego do spraw informatyzacji wszelkie informacje które przechodzą przez Pojedynczy Punkt Kontaktowy, a dotyczą relacji międzynarodowych. Zgodnie z zasadą minimalizacji danych nie będzie otrzymywał danych osobowych zawartych w przekazywanych dokumentach i informacjach.

2.24. Organy odpowiedzialne za zarządzanie incydentami i zarządzanie kryzysowe w cyberbezpieczeństwie na dużą skalę

Zgodnie z dyrektywą NIS 2 należało wyznaczyć organy odpowiedzialne za zarządzanie incydentami i zarządzanie kryzysowe w cyberbezpieczeństwie na dużą skalę. W wymiarze cywilnym będzie to minister właściwy do spraw informatyzacji – ponieważ zgodnie z ustawą z dnia 4 września 1997 r. o działach administracji rządowej jest on odpowiedzialny za bezpieczeństwo w cyberprzestrzeni w wymiarze cywilnym. Jednakże w sprawach dotyczących zagrożeń terrorystycznych oraz zagrożeń związanych ze szpiegostwem organem odpowiedzialnym za zarządzanie incydentami i zarządzanie kryzysowe w cyberbezpieczeństwie będzie Szef Agencji Bezpieczeństwa Wewnętrznego, co wpisuje się w zadania Agencji Bezpieczeństwa Wewnętrznego. Minister Obrony Narodowej z kolei będzie pełnił rolę organu odpowiedzialnego za zarządzanie incydentami i zarządzanie kryzysowe w cyberbezpieczeństwie na dużą skalę w wymiarze militarnym, co również jest zgodne z ustawą z dnia 4 września 1997 r. o działach administracji rządowej.

Wprowadzono również przepis zgodnie z którym organy odpowiedzialne za zarządzanie incydentami i zarządzanie kryzysowe w cyberbezpieczeństwie na dużą skalę koordynują

działania organów państwa zgodnie z Krajowym planem reagowania na incydenty i sytuacje kryzysowe.

2.25. Nadzór i środki egzekwowania przepisów

2.25.1. Organy nadzoru, środki nadzoru i egzekwowania przepisów

Zmiany art. 53 ustawy o KSC wynikają przede wszystkim z obowiązku implementacji postanowień art. 31 i art. 32 dyrektywy NIS 2.

Nadzór sprawować będą organy właściwe do spraw cyberbezpieczeństwa w zakresie wykonywania przez podmioty kluczowe i podmioty ważne wynikających z ustawy obowiązków. Wskazać należy, że może dojść do sytuacji zbiegu nadzoru kiedy podmiot kluczowy lub podmiot ważny będzie tym podmiotem w kilku sektorach, dla których różny jest organ nadzorczy. W takiej sytuacji nadzór nad tym podmiotem sprawuje kilka organów właściwych do spraw cyberbezpieczeństwa jednak wyłącznie we właściwym dla tego organu sektorze. Tym samym organ nadzorczy właściwy dla danego sektora uprawniony jest do stosowania środków nadzorczych tylko w zakresie obejmującym sektor, który został mu przypisany. W pozostałym zakresie (dotyczącym innego sektora) nie wykonuje środków nadzorczych, gdyż robi to inny organ właściwy. W sytuacji zbiegu nadzoru oraz niemożliwości rozdzielania właściwości rozwiązaniem będzie stworzenie przez organy właściwe do spraw cyberbezpieczeństwa wspólnych metodyk nadzoru, w których zostaną określone te kwestie. Ponadto możliwe będzie wspólne prowadzenie nadzoru, w tym kontroli, a także wyznaczenie organu wiodącego w tym zakresie. Organy właściwe do spraw cyberbezpieczeństwa obowiązane będą do informowania się wzajemnie o zamiarze wszczęcia kontroli, co pozwoli na sprawne i efektywne zarządzanie nadzorem bez ryzyka podwójnej kontroli i zbiegu kompetencji.

Określone zostały również środki nadzoru, a więc uprawnienia organu nadzoru w stosunku do podmiotów kluczowych i podmiotów ważnych. Do takich środków nadzoru należą m.in. kontrole prowadzone na miejscu lub zdalnie, występowanie z wnioskami o udzielenie informacji, dostępu do danych, dokumentów i informacji. Organ właściwy do spraw cyberbezpieczeństwa będzie mógł zobowiązać podmiot w drodze decyzji do przeprowadzenia audytu bezpieczeństwa. Takie zobowiązanie znajdzie zastosowanie w stosunku do podmiotów kluczowych w każdym czasie (z uwagi na prewencyjny i następczy charakter nadzoru), a w stosunku do podmiotów ważnych wyłącznie wtedy gdy wystąpi poważny incydent lub sytuacja naruszenia przepisów ustawy. Realizacja uprawnień nadzorczych będzie mogła

przyjąć postać zlecenia CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT sektorowemu dokonania oceny bezpieczeństwa w podmiocie.

W sytuacji uzasadnionego podejrzenia, że działania lub zaniechania podmiotu kluczowego mogą naruszać przepisy niniejszej ustawy, organ właściwy do spraw cyberbezpieczeństwa będzie kierował pismo z ostrzeżeniem, w którym wskaże te działania lub zaniechania oraz czynności, jakie należy podjąć w celu zapobiegnięcia lub zaprzestania przepisów ustawy. Przez uzasadnione podejrzenie należy rozumieć wszelkie wiarygodne informacje, które organ uzyskał. W szczególności dowody, wskazówki, informacje podane przez inne organy właściwe i pozostałe podmioty krajowego systemu cyberbezpieczeństwa, obywateli, media lub z innych źródeł. Mogą być to informacje dostępne publicznie lub mogą one wynikać z innych działań prowadzonych przez właściwe organy podczas wykonywania ich zadań, w tym w ramach czynności operacyjnych.

Organ właściwy do spraw cyberbezpieczeństwa zyska uprawnienie do nakazania podmiotom podjęcia określonych czynności dotyczących obsługi incydentu, a także nakazania w drodze decyzji administracyjnej zaprzestania naruszania przepisów ustawy, zapewnienia zgodności środków zarządzania ryzykiem w cyberbezpieczeństwie czy wdrożenia w określonym terminie zaleceń wydanych w wyniku audytu bezpieczeństwa systemu informacyjnego. Może także wyznaczyć na określony czas (nie dłuższy jednak niż miesiąc), spośród osób zatrudnionych w urzędzie obsługującym ten organ, urzędnika monitorującego do nadzorowania wykonywania obowiązków, o których mowa w rozdziale 3 ustawy o KSC. Organ właściwy do spraw cyberbezpieczeństwa będzie musiał wskazać ściśle określone zadania, które urzędnik powinien realizować w tym czasie. W przypadku nakazu dotyczącego podjęcia określonych czynności dotyczących obsługi incydentu zdecydowano się wyłączyć decyzję administracyjną. Incydent wymaga podejmowania zdecydowanych i szybkich działań, aby zapobiec lub zminimalizować negatywne skutki. Nakaz podjęcia określonych czynności powinien być zatem wydany w jak najkrótszym czasie i mieć jak najprostszą formę, która zapewni maksymalną efektywność w sytuacji wystąpienia incydent.

Postępowanie prowadzone w powyższym zakresie jest jednoinstancyjne, a na decyzję organu właściwego do spraw cyberbezpieczeństwa przysługiwać będzie skarga do sądu administracyjnego. Również w przypadku nakazu, o którym mowa w projektowanym art. 53 ust. 5 pkt 1 ustawy o KSC, który jest inną czynnością z zakresu administracji publicznej, podmiotowi przysługuje skarga do sądu administracyjnego. Wskazać nadto należy, że oznacza to, że w przypadku wniesienia skargi do sądu administracyjnego, właściwe zastosowanie

znajdą przepisy dotyczące postępowania sądowo-administracyjnego. Tym samym podmiotom będzie przysługiwało uprawnienie, o którym mowa w art. 61 ust 2 ustawy z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi (Dz. U. z 2024 r. poz. 935 i 1685 oraz z 2025 r. poz. 769), zwanej dalej „PPSA”, tzn. możliwe będzie wstrzymanie wykonania decyzji lub czynności z zakresu administracji publicznej do czasu rozpatrzenia sprawy przez sąd. Wprowadza się jednak miesięczny termin instrukcyjny dla sądu do rozpatrzenia skargi na ww. środki nadzoru i egzekwowania przepisów. Zabieg ten jest konieczny z punktu widzenia zgodności z prawem europejskim i obowiązkiem nałożonym na państwa członkowskie Unii Europejskiej, aby zapewnić, że środki nadzoru będą skuteczne. Zawieszenie możliwości stosowania dalej idących środków nadzoru przy braku określenia terminu instrukcyjnego na rozpatrzenie skargi przez sąd administracyjny skutkowałoby nieprawidłowym wdrożeniem dyrektywy NIS 2. Jednocześnie wprowadzenie takiego instrukcyjnego terminu polepsza sytuację podmiotu, który wniósł skargę. Długie rozpatrywanie skargi na środek nadzorczy, który został zastosowany w sposób nieprawidłowy może bowiem negatywnie wpływać na prowadzenie działalności przez ten podmiot, zarówno pod względem finansowym jak i wizerunkowym.

Projekt ustawy przewiduje ponadto dalej idące uprawnienia organu nadzoru w sytuacji, w której dany podmiot nie zastosował się w określonym terminie, do postanowień decyzji administracyjnej. Przed realizacją tych uprawnień oraz przed wydaniem decyzji administracyjnej organ zobowiązany jest poinformować podmiot o wstępnych ustaleniach wraz ze szczegółowym uzasadnieniem, a podmiot ten uprawniony jest do przedstawienia stanowiska w sprawie niezwłocznie, nie później niż w terminie 7 dni od poinformowania o wstępnych ustaleniach. Określono także zamknięty katalog wyjątków od obowiązku informowania o wstępnych ustaleniach. Środków, o których mowa w projektowanym art. 53 ust. 9 ustawy o KSC, nie stosuje się do czasu rozstrzygnięcia sprawy przez sąd, jeśli podmiot kluczowy wniósł skargę do sądu administracyjnego. Środków tych nie stosuje się także do podmiotów publicznych. Środki nadzorcze określone w art. 53 ust. 9 mają charakter tymczasowy, a w stosunku do kierownika podmiotu kluczowego mogą być stosowane wyłącznie o ile nie doprowadzi to do uniemożliwienia funkcjonowania podmiotu w zakresie jaki jest niezbędny do naprawienia naruszeń. Oznacza to, że zastosowanie wobec kierownika podmiotu środka polegającego na zakazie pełnienia funkcji zarządczych w podmiocie kluczowym nie może uniemożliwić realizacji celu tego środka tj. usunięcia uchybień lub

zaprzestania naruszeniom. Zakaz pełnienia funkcji zarządczych nie może zatem obejmować tych uprawnień, których wykonywanie jest niezbędne do realizacji ww. celu.

W projektowanym art. 53e ustawy o KSC wskazano procedurę związaną z realizacją środków nadzorczych określonych w projektowanym art. 53 ust. 9 ustawy o KSC. Przepis ten reguluje sposób postępowania organu właściwego do spraw cyberbezpieczeństwa w związku z wydaniem decyzji o zastosowaniu środków nadzorczych oraz uprawnienia podmiotu kluczowego i organu właściwego do spraw cyberbezpieczeństwa zmierzające do przywrócenia stanu sprzed zastosowania tych środków. Przepisy określają jakie informacje powinna zawierać decyzja, jaki jest maksymalny termin stosowania tych środków, a także procedurę wydawania decyzji o stosowaniu tych środków na dalszy okres, w przypadku gdy uchybienia nie zostały usunięte w pierwotnym terminie. W takiej sytuacji będzie wydawana ponowna decyzja o zastosowaniu środka, z tym zastrzeżeniem, że nie będą miały zastosowania przepisy art. 53 ust. 13–16 ustawy o KSC. Wynika to z faktu, że nie jest to inne naruszenie wobec którego konieczne jest przeprowadzenie całej procedury związanej z nadzorem od początku. Procedura wydawania ponownej decyzji, po zrealizowaniu się właściwych przesłanek, ma mieć charakter uproszczony, niemal automatyczny. W praktyce ma być to przedłużenie czasu trwania zastosowanych środków nadzorczych wobec podmiotu kluczowego bądź kierownika podmiotu. Należy jednak podkreślić, że organ będzie obowiązany do uchylenia decyzji o zastosowaniu środka w przypadku, w którym usunięcie uchybień lub zaprzestanie naruszeń będzie miało miejsce szybciej niż upływ terminu, na który został orzeczony środek. Środki określone w art. 53 ust. 9 ustawy o KSC mogą być stosowane wielokrotnie do czasu usunięcia uchybień lub zaprzestania naruszeń na zasadach określonych w przepisach określających sposób i termin ich ponownego zastosowania.

Zgodnie z art. 59e ust. 5 ustawy o KSC organ z urzędu uchyla decyzję o zastosowaniu tych środków jeśli poweźmie informację o usunięciu uchybień lub zaprzestaniu dokonywania naruszeń przez podmiot kluczowy na skutek np. stosowania innych środków nadzorczych, określonych w art. 53 ust. 1, 4 i 5 ustawy o KSC. Może to nastąpić zatem w szczególności w wyniku kontroli doraźnej lub kontroli na zasadach ogólnych.

Z uwagi na tymczasowość tych środków oraz określenie procedury weryfikacji zasadności ich dalszego stosowania, możliwości uchylenia, zarówno z urzędu jak i na wniosek, postępowanie ma charakter jednoinstancyjny. Od decyzji przysługiwać będzie natomiast skarga do sądu administracyjnego.

Organy właściwe do spraw cyberbezpieczeństwa obowiązane będą do publikowania w swoim BIP informacji o zastosowaniu wobec podmiotu kluczowego lub kierownika podmiotu kluczowego środków określonych w art. 53 ust. 9 ustawy o KSC, z zastrzeżeniem, że publikacja nie obejmuje tajemnicy przedsiębiorstwa, jak również innych informacji podlegających ochronie na podstawie odrębnych przepisów. Rozumieć przez to należy przede wszystkim inne rodzaje tajemnic, takie jak tajemnice państwowe i służbowe, tajemnice zawodowe czy techniczne. Publikowana będzie także informacja o uchyleniu decyzji w przedmiocie stosowania środka. Celem publikowania informacji w BIP jest zapewnienie transparentności i pewności obrotu.

Podkreślenia wymaga, że w okresie stosowania środka, o którym mowa w art. 53 ust. 9 ustawy o KSC, podmiot kluczowy nie może wykonywać żadnej działalności, której środek dotyczy. Przykładowo – jeśli zastosowany wobec podmiotu kluczowego środek dotyczy tymczasowego wstrzymania koncesji, oznacza to, że podmiot kluczowy nie może wykonywać działalności, której ta koncesja dotyczy. Należy traktować podmiot tak, jak by tej koncesji nie miał. Tym samym każda działalność podmiotu wykonywana podczas obowiązywania środka i wbrew temu środkowi będzie uznawana za prowadzenie działalności bez koncesji. Jednocześnie podmiot kluczowy ma obowiązek niezwłocznie podjąć działania zmierzające jedynie do usunięcia uchybień bądź zaprzestania naruszeń. W tym celu może w szczególności składać oświadczenia woli i wiedzy, podejmować czynności procesowe w postępowaniach, przedsiębiorzać czynności faktyczne, jeżeli nie stoją one w sprzeczności z celem stosowanego środka lub nie zmierzają do jego obejścia. Związane jest to z faktem, że wstrzymanie działalności gospodarczej w rozumieniu ustawy o KSC nie jest równoznaczne w skutkach z zawieszeniem działalności gospodarczej, która dokonywana może być na wniosek przedsiębiorcy na podstawie ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców. Wstrzymanie działalności nie oznacza, że podmiot kluczowy nie może podejmować żadnych działań związanych z działalnością. Niekiedy do naprawienia naruszeń czy zaprzestania dopuszczania się uchybień konieczne będzie np. zawarcie bądź rozwiązanie jakiejś umowy. Przyjęcie odmiennego stanowiska skutkowałoby brakiem realizacji celu stosowania środka nadzorczego oraz nadrzędnego celu dyrektywy NIS 2 i ustawy o KSC. Możliwe będzie zatem podejmowanie działań, które mają doprowadzić do usunięcia uchybień bądź zaprzestania naruszeń. Podejmowanie tych działań będzie jednak możliwe wyłącznie wtedy, jeżeli nie stoi w sprzeczności z celem stosowanego środka lub nie zmierza do jego obejścia. To zastrzeżenie gwarantuje, że podmiot kluczowy nie będzie świadczył usług (wynikających z zobowiązania

podmiotu) pomimo zastosowanego środka nadzorczego w postaci wstrzymania działalności gospodarczej, koncesji, czy zezwolenia.

W zakresie nieuregulowanym zastosowanie mają przepisy odrębne, właściwe dla danego rodzaju koncesji, zezwolenia, czy rodzaju działalności gospodarczej. Związane jest to z liczbą i zróżnicowaniem sektorów, które podlegać mogą pod odrębne przepisy związane z koncesjami bądź zezwoleniami. Koncesje mogą być związane np. z działalnością energetyczną (dystrybucja energii elektrycznej, obrót energią elektryczną, dystrybucja paliw gazowych, wytwarzanie ciepła itp.), czy działalnością górniczą. W tym zakresie należy odpowiednio stosować np. ustawę z dnia 9 czerwca 2011 r. – Prawo geologiczne i górnicze lub ustawę z dnia 10 kwietnia 1997 r. – Prawo energetyczne.

Podkreślenia wymaga również, że wstrzymanie całości albo części działalności obejmuje swoim zakresem usługi świadczone przez podmiot. Na podstawie art. 53 ust. 9 ustawy o KSC organ właściwy do spraw cyberbezpieczeństwa może zatem wstrzymać część usług podmiotu kluczowego, np. tylko jedną – jeśli uzna to za uzasadnione i wystarczające w konkretnym przypadku.

Organ nie wybiera środka egzekwowania przepisów czy środka nadzoru na zasadzie dobrowolności. Z tego względu proponuje się, aby organ właściwy do spraw cyberbezpieczeństwa, dokonując wyboru określonego środka, brał pod uwagę m.in. wagę naruszenia i znaczenie naruszonych przepisów, czas trwania naruszenia, istotne wcześniejsze naruszenia, spowodowane szkody majątkowe i niemajątkowe, umyślny lub nieumyślny charakter czynu, środki zastosowane przez podmiot, aby zapobiec szkodom majątkowym i niemajątkowym lub je ograniczyć, stopień współpracy podmiotu z organami właściwymi do spraw cyberbezpieczeństwa.

Wskazać również należy, że podmioty kluczowe objęte są kompleksowym systemem nadzoru *ex ante* (prewencyjnym) i *ex post* (następczym), a podmioty ważne uproszczonym systemem nadzoru – *ex post* – co wynika przede wszystkim z odmiennej roli jaką pełnią w systemie cyberbezpieczeństwa. Oznacza to zatem, że podmioty kluczowe podlegają nadzorowi prewencyjnemu i następczemu aby zapewnić, że podmioty kluczowe i świadczone przez nich usługi spełniają wymogi określone w niniejszej ustawie. W przypadku podmiotów ważnych nadzór został zawężony do nadzoru następczego, w oparciu o podejście reaktywne. Może być on uruchamiany w przypadku podejrzenia, że zachodzi możliwość naruszenia przepisów niniejszej ustawy. Jak wskazano wyżej, takie podejrzenie może być wynikiem uzyskania przez

organ właściwy do spraw cyberbezpieczeństwa dowodów, wskazówek, informacji podanych przez inne organy właściwe, pozostałe podmioty krajowego systemu cyberbezpieczeństwa, obywateli, media lub inne źródła. Mogą być to informacje dostępne publicznie lub mogą one wynikać z innych działań prowadzonych przez właściwe organy podczas wykonywania ich zadań, w tym w ramach czynności operacyjnych. Podkreślić należy, że przepisy nadzorcze i egzekwowania przepisów odnoszące się do podmiotów kluczowych mają zastosowanie również do podmiotów ważnych, ale z tym zastrzeżeniem, że stosuje się do nich tylko te środki, które mogą być zastosowane *ex post*. Oznacza to, że organ właściwy do spraw cyberbezpieczeństwa wykonując swoje uprawnienia wobec podmiotów ważnych będzie musiał podjąć adekwatne środki uwzględniając, że mogą mieć one wyłącznie charakter następczy.

W dodawanym w ustawie o KSC art. 53d określono ponadto uprawnienia jakie przysługują urzędnikowi monitorującemu w ramach nadzoru realizacji przez podmiot kluczowy obowiązków określonych w rozdziale 3 ustawy o KSC. Zaproponowany zakres uprawnień pozwoli na skuteczne wykonywanie przez niego zadań, a informacje pozyskane w toku monitorowania będą mogły stanowić podstawę do podjęcia przez organ właściwy do spraw cyberbezpieczeństwa innych, koniecznych środków nadzoru, w tym w szczególności kontrolę doraźną. Wyraźnie należy podkreślić, że instytucja urzędnika monitorującego jest środkiem nadzoru i instytucją odrębną od kontroli. Do nadzorowania przez urzędnika monitorującego wykonywania przez podmiot kluczowy obowiązków stosuje się jedynie odpowiednio art. 58 ustawy o KSC, a więc przepis stanowiący o sporządzeniu protokołu z kontroli – w tym wypadku z prowadzonego monitoringu. Jednym z elementów protokołu jest wyszczególnienie wniosków. Podmiot nadzorowany będzie miał zatem wiedzę na temat tego czy należy coś poprawić i w jakim obszarze. Celem instytucji urzędnika monitorującego jest bowiem realizacja nadzoru prewencyjnego, czyli sprawdzenie czy podmiot kluczowy na bieżąco prawidłowo realizuje obowiązki wynikające z ustawy, a także zasygnalizowanie podmiotowi kluczowemu obszarów wymagających poprawy zanim dojdzie do incydentu. Jednocześnie wskazać należy, że realizując swoje obowiązki urzędnik monitorujący obowiązany jest do poszanowania tajemnicy prawnie chronionej na podstawie odrębnych przepisów. Przykładowo dostęp do informacji niejawnych będzie zależny od tego czy wyznaczony urzędnik posiada dostęp do informacji klauzulowanych. Jeśli nie posiada takiego dostępu, to nie będzie on mógł zapoznawać się z takimi dokumentami. Wyznaczona osoba będzie pełniła w podmiocie wyłącznie funkcję monitorującą realizację obowiązków. Urzędnik monitorujący nie może

naruszać polityk bezpieczeństwa, nie będzie dokonywał żadnych zmian w stosowanej w podmiocie technologii, infrastrukturze, urządzeniach, sieciach czy systemach operacyjnych. Takie działanie stanowiłoby wykroczenie poza obowiązki urzędnika monitorującego. Urzędnik monitorujący będzie każdorazowo wyznaczany przez organ właściwy do spraw cyberbezpieczeństwa z konkretnie wskazanymi zadaniami do realizacji i na określony czas. Dobór właściwej osoby będzie uzależniony m.in. od rodzaju podmiotu i rodzaju tych zadań, tak aby zapewnić skuteczność środka nadzoru przez odpowiednie umiejętności osoby wyznaczonej. Organ obowiązany jest zatem wyznaczać osoby do sprawowania tej funkcji według zarówno zaplecza kadrowego jak i potrzeb nadzorczych.

Urzędnik monitorujący w zakresie przetwarzania przez niego danych osobowych będzie związany przepisami RODO jako osoba realizująca zadania w imieniu i na rzecz administratora.

Wskazane jest, żeby urzędnik monitorujący i podmiot kluczowy współpracowali ze sobą. Jest to w interesie podmiotu kluczowego m.in. z tego względu, że ten środek nadzorczy ma charakter prewencyjny, a więc co do zasady ma dążyć do zapobiegania naruszeniom ustawy i wystąpieniu incydentu. Za uniemożliwianie bądź utrudnianie urzędnikowi monitorującemu realizacji jego zadań bądź uprawnień, przewidzianych w projektowanym art. 53d ust. 1 ustawy o KSC, podmiot kluczowy będzie podlegał karze pieniężnej. Przez uniemożliwianie lub utrudnianie należy rozumieć w szczególności niewydanie urzędnikowi monitorującemu przepustki.

Ze względu na zróżnicowanie w zakresie prowadzenia nadzoru nad podmiotami kluczowymi i podmiotami ważnymi, przepisy dotyczące nadzoru nad podmiotami kluczowymi stosuje się odpowiednio do nadzoru nad podmiotami ważnymi.

Zmiany wprowadzane w art. 53 ustawy o KSC i w dodawanym w tej ustawie art. 53d w jasny sposób określają zarówno organy nadzoru, ich uprawnienia nadzorcze i zmierzające do egzekwowania przepisów w stosunku do podmiotów kluczowych i podmiotów ważnych, co przekładać się będzie na wysoki poziom bezpieczeństwa usług.

2.25.2. Metodyki nadzoru i hierarchia priorytetów zadań nadzorczych

Przepisy określające możliwość tworzenia metodyk nadzoru oraz ustanawiania hierarchii priorytetów w odniesieniu do zadań nadzorczych mają na celu zapewnienie skutecznego nadzoru w zakresie stosowania przepisów ustawy przez podmioty kluczowe i podmioty ważne.

Celem utworzenia metodyk nadzoru jest dostosowanie metod nadzoru do określonego sektora oraz podmiotu nadzorowanego co pozwoli na usystematyzowanie i ujednolicenie sposobu przeprowadzania nadzoru, lepsze wykorzystanie dostępnych zasobów i zwiększenie efektywności działań nadzorczych. Metodyki nadzoru powinny w szczególności określać zakres nadzoru, a więc m.in. rodzaje czynności nadzorczych, sposób przeprowadzania nadzoru obejmujący np. etapy nadzoru, stosowane narzędzia i techniki oraz kryteria oceny, które pozwolą na wyprowadzenie odpowiednich wniosków w zakresie tego, czy dany podmiot prawidłowo realizuje nałożone na niego obowiązki. Należy mieć na uwadze, że każdy organ właściwy do spraw cyberbezpieczeństwa będzie określał adekwatne dla swojego sektora zakres nadzoru, sposób jego przeprowadzenia i kryteria oceny. Z tego względu nie zdecydowano się na precyzyjne wskazanie w przepisie co należy rozumieć jako zakres, sposób oraz kryteria. Metodyka nadzoru powinna być dobrana w taki sposób, aby zapewnić skuteczność oraz zgodność z przepisami prawa, a także właściwą i pełną realizację zarówno obowiązków nałożonych na podmioty nadzorowane jak i zadań organów sprawujących nadzór. Dodatkowo organy nadzoru mogą określać inne elementy w metodykach nadzoru jeśli uznają to za stosowne. Metodyki nadzoru będą także rozwiązaniem problemu wielosektorowości danego podmiotu to znaczy sytuacji, w której dany podmiot kluczowy lub podmiot ważny jest nadzorowany przez różne organy właściwe do spraw cyberbezpieczeństwa. W sytuacji braku możliwości rozdzielenia działań nadzorczych z uwagi na niemożliwość wyodrębnienia sektorów, sporządzenie przez organy właściwe do spraw cyberbezpieczeństwa wspólnych metodyk nadzoru pozwoli na porozumienie organów właściwych do spraw cyberbezpieczeństwa, np. co do zakresu sprawowanego przez nich nadzoru i pozwoli uniknąć sporów kompetencyjnych. Metodyki nadzoru można uznać w tym przypadku za porozumienia pomiędzy organami właściwymi do spraw cyberbezpieczeństwa.

Ponadto ustanowienie hierarchii priorytetów w odniesieniu do zadań nadzorczych, które oparte będzie na analizie ryzyka przeprowadzanej przez organ właściwy do spraw cyberbezpieczeństwa, pozwoli na dobór efektywnej formy nadzoru dostosowanej do sytuacji nadzorowanego podmiotu. W celu zapewnienia maksymalnej efektywności w sytuacji, w której organy zdecydują się wprowadzić metodykę nadzoru zobowiązane będą do jej przeglądu i oceny co 2 lata.

W celu przeprowadzenia analizy ryzyka organ właściwy do spraw cyberbezpieczeństwa będzie mógł skorzystać z kompetencji określonej w projektowanym art. 53c ust. 1 ustawy o KSC.

2.25.3. Obowiązek przekazywania danych, informacji i dokumentów

W celu zagwarantowania prawidłowego realizowania kompetencji nadzorczych, a tym samym podjęcia adekwatnych i efektywnych działań, wprowadza się w ustawie o KSC art. 53c, który nakłada na podmioty kluczowe i podmioty ważne obowiązek dostarczenia organom właściwym do spraw cyberbezpieczeństwa na ich żądanie wszelkich danych, informacji i dokumentów niezbędnych do wykonywania przez te organy ich uprawnień i obowiązków określonych w ustawie.

Określono również elementy, które żądanie organu właściwego do spraw cyberbezpieczeństwa powinno zawierać. Istotnym obwarowaniem jest również określenie, iż żądanie powinno być proporcjonalne do celu jakiemu ma służyć. Oznacza to, że nie jest możliwe żądanie udostępnienia takich informacji, dokumentów czy danych, które nie są konieczne, adekwatne i proporcjonalne do wykonywania przez organ jego obowiązków i uprawnień.

2.25.4. Czynności kontrolne

W toku przeglądu przepisów ustawy o KSC oraz na podstawie doświadczeń z przeprowadzonych na podstawie tych przepisów czynności kontrolnych, zidentyfikowano problemy znacznie utrudniające prawidłowe realizowanie tych czynności. Z tego względu zdecydowano się na wprowadzenie zmian w art. 54 i art. 58 ustawy o KSC.

Zmiany w art. 54 ustawy o KSC mają charakter dostosowujący i są konsekwencją zmian poczynionych w pozostałych przepisach.

W nowym brzmieniu art. 58 ustawy o KSC wskazano wyraźnie, że kontrolowany w przypadku zastrzeżeń co do ustaleń zawartych w protokole kontroli ma prawo odmówić jego podpisania, a także złożyć umotywowane pisemne zastrzeżenia do tego protokołu w terminie 7 dni od dnia przedstawienia mu protokołu kontroli do podpisu. Nie tylko podkreślono zatem uprawnienie kontrolowanego do odmowy podpisania protokołu ale i postanowiono, że pisemne zastrzeżenia powinny być umotywowane.

Obowiązek analizy zastrzeżeń przekazano na kierownika komórki do spraw kontroli jednocześnie zdejmując ten obowiązek z osoby prowadzącej czynności kontrolne. Kierownik komórki do spraw kontroli po analizie odrzuca zastrzeżenia i informuje o tym fakcie podmiot kontrolowany albo uwzględnia zastrzeżenia w całości lub w części lub je oddala. Kierownik komórki obowiązany jest również do sporządzenia stanowiska wobec złożonych zastrzeżeń. W tym miejscu należy wskazać, że kierownik komórki do spraw kontroli nie oznacza, że organ właściwy do spraw cyberbezpieczeństwa obowiązany jest posiadać specjalnie wyodrębnioną

komórkę do spraw kontroli. Przez komórkę do spraw kontroli należy rozumieć komórkę organizacyjną, która w ramach swoich zadań zajmuje się kontrolą. Kontrola może być zatem jednym z wielu zadań realizowanych w tej komórce.

Osoba prowadząca czynności kontrole w razie potrzeby, w związku ze zgłoszonymi zastrzeżeniami, podejmuje dodatkowe czynności kontrolne, a w przypadku stwierdzenia przez kierownika komórki do spraw kontroli zasadności zastrzeżeń zmienia lub uzupełnia odpowiednią część protokołu w formie aneksu.

Zmiana procedury w przypadku zastrzeżeń do protokołu w zaproponowanym brzmieniu pozwoli na zapewnienie większej efektywności i obiektywności.

Zgodnie z NIS 2 wprowadzono także regulację dotyczącą współpracy nadzorczej organów właściwych do spraw cyberbezpieczeństwa z organami innych państw członkowskich Unii Europejskiej. Współpraca ta dotyczy nadzoru nad podmiotami, które świadczą usługi na terytorium Rzeczypospolitej Polskiej, ale ich siedziba znajduje się w innym państwie – albo sytuacji odwrotnej. Należy tą współpracę rozumieć szeroko, w ramach tej współpracy organy właściwe do spraw cyberbezpieczeństwa będą mogły konsultować się w ramach nadzoru nad podmiotem, który świadczy usługi na terytorium Polski. Polski organ właściwy do spraw cyberbezpieczeństwa będzie zobligowany do udzielenia wsparcia w sprawowaniu nadzoru nad podmiotami kluczowymi lub podmiotami ważnymi, których systemy informacyjne znajdują się na terytorium Rzeczypospolitej Polskiej. Odmowa udzielenia tej pomocy będzie możliwa, gdy polski organ właściwy do spraw cyberbezpieczeństwa nie jest właściwy w sprawie, żądana pomoc jest nieproporcjonalna do realizowanych przez organ zadań z zakresu nadzoru lub organ innego państwa członkowskiego Unii Europejskiej żąda udostępnienia informacji lub dokumentów, których udostępnienie narusza podstawowy interes bezpieczeństwa państwa, bezpieczeństwa i porządku publicznego lub obronności.

Wprowadzono także możliwość prowadzenia wspólnych czynności nadzorczych z organem innego państwa członkowskiego Unii Europejskiej. Wprowadzono także przepisy o współpracy z organami innych państwa członkowskich Unii Europejskiej właściwych do stosowania rozporządzenia DORA.

Dodano także przepisy o informowaniu Prezesa Urzędu Ochrony Danych Osobowych o podejrzeniu nadużycia ochrony danych osobowych.

Nadzór nad przetwarzaniem danych osobowych przez sądy powszechne sprawuje prezes sądu wyższego rzędu, a w przypadku Sądu Najwyższego – Krajowa Rada Sądownictwa.

W przypadku prokuratur rejonowych ten rodzaj nadzoru sprawuje prokurator okręgowy, prokuratury okręgowej – prokurator regionalny, a w przypadku prokuratur regionalnych i Prokuratury Krajowej – Prokurator Krajowy. Z tego względu ustawa przewiduje, że to te podmioty będą informowane przez organ właściwy do spraw cyberbezpieczeństwa, jeśli w toku czynności nadzorczych stwierdzone zostanie podejrzenie naruszenia danych osobowych odpowiednio w sądach powszechnych lub prokuraturach.

Wprowadza się także instytucję kontroli doraźnej (projektowany art. 59c ustawy o KSC), która jest jednym ze środków nadzorczych. Kontrola doraźna może zostać wszczęta w przypadkach uzasadnionych charakterem sprawy lub pilnością przeprowadzenia czynności kontrolnych wynikających z ochrony bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego lub w przypadku potrzeby realizacji wzajemnej pomocy, o której mowa w art. 59b ust. 1 lub potrzeby sprawdzenia, czy podmiot kluczowy usunął uchybienia lub zaprzestał dokonywania naruszeń. Wskazano przykładowe sytuacje, w których wszczęcie jest możliwe – będzie to m.in. kontrola wszczynana w razie potrzeby sprawdzenia informacji uzyskanej od urzędnika monitorującego, że podmiot kluczowy może naruszać przepisy ustawy albo sprawdzenia, w celu podjęcia działań na podstawie art. 53e ust. 4 i 5, czy podmiot kluczowy usunął uchybienia lub zaprzestał dokonywania naruszeń. Z racji otwartego katalogu przesłanek wszczęcia kontroli doraźnej możliwe będzie również jej wszczęcie w celu sprawdzenia informacji zawartych w skargach i wnioskach, jeśli będzie to uzasadnione kwestiami bezpieczeństwa państwa, porządku publicznego czy będzie wynikało z potrzeby realizacji wzajemnej pomocy. Kontrola ta jest z reguły szybsza i prostsza, w związku z tym wyłącza się w stosunku do niej niektóre czynności, które mają miejsce przy kontroli przeprowadzanej na zasadach ogólnych. W nieuregulowanym zakresie stosuje się odpowiednio przepisy dotyczące kontroli sprawowanej na zasadach ogólnych, a zatem tych określonych m.in. w ustawie o KSC, ustawie z dnia 15 lipca 2011 r. o kontroli w administracji rządowej, czy ustawie z dnia 6 marca 2018 r. – Prawo przedsiębiorców. Z kontroli doraźnej sporządzane będzie sprawozdanie bądź protokół kontroli, w zależności od rodzaju podmiotu kontrolowanego. Wyłączone są w stosunku do kontroli doraźnej art. 47 ust 1 i 2 oraz art. 54 ust. 1 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców. Jest to podyktowane w szczególności potrzebą zapobiegnięcia sytuacji, w której zajdzie zbieg nadzoru. Podmiot kluczowy lub podmiot ważny może naruszać przepisy ustawy w różny sposób w kilku sektorach. Brak powyższego wyłączenia skutkowałby tym, że co najmniej jeden z organów właściwych do spraw cyberbezpieczeństwa sprawujących nadzór nad podmiotem kluczowym lub podmiotem ważnym nie mógłby realizować swoich

obowiązków i kompetencji. Zachodzi to również w sytuacji, w której kontrola dokonywana jest przez organ spoza ustawy o KSC, na podstawie przepisów odrębnych. W przypadku cyberbezpieczeństwa istotny jest czas, a czynności kontrolne powinny być realizowane bez żadnych przeszkód. Nie można zatem dopuścić do sytuacji, w której organ właściwy do spraw cyberbezpieczeństwa nie mógłby przeprowadzić kontroli niezwłocznie z uwagi na to, że prowadzi ją w podmiocie inny organ na podstawie przepisów niezwiązanych z krajowym systemem cyberbezpieczeństwa. W takiej sytuacji bowiem nie zachodzi możliwość uwspólnienia zadań z zakresu nadzoru, gdyż podstawą kontroli są różne podstawy prawne. Wyłączenie art. 47 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców ma natomiast na celu wyłączenie obowiązku przeprowadzania analizy prawdopodobieństwa naruszenia prawa przez podmiot kontrolowany, a także kolizji jaka może zajść pomiędzy przesłankami z niniejszej ustawy i z art. 47. Pozostawienie obowiązku przeprowadzania analizy prawdopodobieństwa naruszenia prawa w przypadku kontroli doraźnej, która ma być z zasady szybka i uproszczona byłoby niecelowe i sprzeczne z założeniami tego środka nadzorczego.

2.26. Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa

Nowe przepisy przewidują, że Pełnomocnikiem może być minister właściwy do spraw informatyzacji, sekretarz stanu albo podsekretarz stanu w urzędzie obsługującym ministra właściwego do spraw informatyzacji. Takie rozwiązanie zapewni stabilność w zakresie obsługi tego Pełnomocnika oraz jego odpowiednią rangę. Należy podkreślić, że minister właściwy do spraw informatyzacji nadzoruje NASK-PIB, w której zlokalizowany jest CSIRT NASK. Dzięki temu Pełnomocnik ma łatwy dostęp do dodatkowej wiedzy eksperckiej i kompetencji z zakresu cyberbezpieczeństwa.

Dotychczasowa praktyka pokazała, że takie rozwiązanie jest korzystne gdyż zapewnia Pełnomocnikowi dodatkowe informacje i zasoby niezbędne do realizacji jego zadań. Przepisy te zapewnią również stabilizację funduszy Pełnomocnika, wskazując z której części budżetowej jest finansowany.

Pełnomocnik będzie również mógł zlecać przeprowadzanie badań i ekspertyz oraz tworzyć zespoły robocze. Te kompetencje zapewnią mu dodatkowe narzędzia do realizacji jego zadań. Wprowadzono również regulację, że inne organy państwa mają obowiązek udzielania wsparcia Pełnomocnikowi, tak aby w sytuacji gdy dane zagadnienie dotyczy ich właściwości otrzymał on niezbędne wsparcie.

Przy Pełnomocniku zostanie utworzone Połączone Centrum Operacyjne Cyberbezpieczeństwa, zwane dalej „PCOC”, będące organem pomocniczym w sprawach koordynowania działań i realizowania polityki rządu w zakresie zapewnienia cyberbezpieczeństwa. W jego skład będą wchodzić przedstawiciele najważniejszych instytucji rządowych zapewniających cyberbezpieczeństwo w kraju. Do zadań PCOC należeć będzie:

- 1) wymiana informacji na temat cyberzagrożeń, incydentów i podatności na poziomie krajowym;
- 2) wymiana informacji o wynikach szacowania ryzyka związanego z ujawnionymi cyberzagrożeniami oraz zaistniałymi incydentami;
- 3) wymiana informacji o przeprowadzanych badaniach, o których mowa w art. 33 ust. 1 ustawy o KSC;
- 4) wymiana informacji dotyczących sytuacji kryzysowych w cyberprzestrzeni;
- 5) przygotowywanie bieżących informacji na temat sytuacji w cyberprzestrzeni dla Pełnomocnika;
- 6) wymiana informacji dotycząca procesów i współpracy międzynarodowej w zakresie bezpieczeństwa w cyberprzestrzeni.

Dotychczasowa inicjatywa spotkań koordynujących cyberbezpieczeństwo w Polsce będzie unormowana na poziomie ustawowym. Formuła ta sprawdza się przy intensywnej sytuacji w cyberprzestrzeni.

Wprowadza się również stanowisko sekretarza PCOC, analogicznie jak przy Kolegium. Sekretarz organizuje pracę PCOC i może żądać od organów administracji rządowej informacji niezbędnych do organizacji posiedzenia PCOC.

Dodatkowo Pełnomocnikowi umożliwia się wydanie zarządzenia określającego sposób działania PCOC. Zdaniem projektodawcy wydanie aktu prawa wewnętrznego w tym zakresie jest możliwe, mając na względzie, że PCOC będzie działał przy Pełnomocniku i na jego rzecz, a Pełnomocnik przewodniczy PCOC. Podobna sytuacja ma miejsce przy Rządowym Zespole Zarządzania Kryzysowego – tryb działania jest określany w zarządzeniu Prezesa Rady Ministrów, który przewodniczy temu Zespołowi.

Pełnomocnik będzie mógł dokonywać zakupów sprzętu lub oprogramowania dla uczestników posiedzeń Połączonego Centrum Operacyjnego Cyberbezpieczeństwa. Rozwiązanie to ma na celu uprościć zakupy z zakresu cyberbezpieczeństwa dla kluczowych podmiotów w Polsce

odpowiadających za cyberbezpieczeństwo. Dzięki hurtowym zakupom będzie możliwe uzyskanie tańszej ceny za sprzęt lub oprogramowanie.

2.27. Kolegium do Spraw Cyberbezpieczeństwa

Zmiana ustawy poszerza skład Kolegium, zakres jego zadań i precyzuje pewne kwestie związane z jego funkcjonowaniem.

W projektowanej ustawie zostały określone nowe rodzaje analiz jakie będą mogły być zlecane CSIRT MON, CSIRT NASK lub CSIRT GOV. Będą to analizy dotyczące wpływu konkretnych produktów ICT, usług ICT lub procesów ICT na bezpieczeństwo usług świadczonych przez podmioty określone w art. 67b ust. 1 ustawy o KSC oraz analizy dotyczące trybu i zakresu, w jakim dostawca sprawuje nadzór nad procesem wytwarzania i dostarczania produktów ICT, usług ICT lub procesów ICT. Analizy te będą wykonywane na wniosek Przewodniczącego Kolegium i będą mogły posłużyć jako dowód w ramach postępowania o uznaniu dostawcy za dostawcę wysokiego ryzyka.

Rozszerzono katalog zadań Kolegium m.in. o wyrażanie opinii o decyzji w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka.

Proponuje się rozszerzenie składu Kolegium– nowymi członkami będą organy właściwe do spraw cyberbezpieczeństwa.

W posiedzeniach Kolegium będą mogli także uczestniczyć:

- 1) Dowódca Komponentu Wojsk Obrony Cyberprzestrzeni albo jego zastępca;
- 2) Prokurator Generalny albo jego zastępca;
- 3) Szef Agencji Wywiadu albo jego zastępca;
- 4) Szef Służby Wywiadu Wojskowego albo jego zastępca.

Ponadto umożliwiono, aby pozostali szefowie służb (wymienieni w znowelizowanym art. 66 ust. 4 ustawy o KSC) mogli także desygnować na posiedzenia Kolegium swoich zastępców.

W ślad za odpowiednimi zmianami w innych przepisach, uzupełniono katalog kompetencji przewodniczącego Kolegium o możliwość:

- 1) wnioskowania o przeprowadzenie badania produktu ICT, usługi ICT lub procesu ICT;
- 2) zlecenia zespołom CSIRT MON, CSIRT NASK lub CSIRT GOV, przeprowadzenie analizy dotyczącej wpływu konkretnych produktów ICT, usług ICT lub procesów ICT na bezpieczeństwo usług świadczonych przez podmioty kluczowe i podmioty ważne oraz największych przedsiębiorców telekomunikacyjnych;

- 3) zlecenia CSIRT MON, CSIRT NASK lub CSIRT GOV, przeprowadzenie analizy dotyczącej trybu i zakresu, w jakim dostawca sprzętu i oprogramowani sprawuje nadzór nad procesem wytwarzania i dostarczania produktów ICT, usług ICT lub procesów ICT, o której mowa w art. 65a ust. 2 ustawy o KSC;
- 4) wnioskowania o wszczęcie postępowania w sprawie uznania dostawcy sprzętu i oprogramowania za dostawcę wysokiego ryzyka.

Ustawa o KSC nie przewiduje sytuacji nieobecności sekretarza Kolegium na przykład spowodowanej czasowymi problemami zdrowotnymi. Aby zapewnić ciągłość obsługi Kolegium proponuje się wprowadzenie instytucji zastępcy sekretarza Kolegium. Sekretarz Kolegium jest powoływany przez Przewodniczącego Kolegium – czyli Prezesa Rady Ministrów. Aby nie nakładać nadmiernych obowiązków na Prezesa Rady Ministrów zastosowano zasadę pomocniczości – zastępcę sekretarza Kolegium będzie powoływał jak również odwoływał sekretarz Kolegium. Będzie to też oznaczało, że sekretarz Kolegium odpowiada przed Przewodniczącym Kolegium za wybór danej osoby na zastępcę. Kryteria wyboru zastępcy sekretarza będą takie same, jak dla sekretarza – zastępca będzie musiał spełniać wymagania określone w przepisach o ochronie informacji niejawnych w zakresie dostępu do informacji niejawnych o klauzuli „tajne”.

W przepisie wskazano jasno, że zastępca sekretarza Kolegium wykonuje obowiązki sekretarza w razie nieobecności tego ostatniego, w szczególności zastępuje go na posiedzeniu Kolegium.

2.28. Szczególne działania na rzecz zapewnienia cyberbezpieczeństwa na poziomie krajowym

2.28.1. Rekomendacje Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa

Nowe przepisy umożliwią wydawanie przez Pełnomocnika rekomendacji określających środki techniczne i organizacyjne stosowane w celu zwiększenia bezpieczeństwa systemów informacyjnych podmiotów krajowego systemu cyberbezpieczeństwa. Ten dokument będzie publikowany na stronie podmiotowej Pełnomocnika w BIP. W takiej formie będą mogły być wydawane Narodowe Standardy Cyberbezpieczeństwa, o których mowa w Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej, a także inne zbiory dobrych praktyk. Podkreślić należy, że rekomendacje będą formalnie niewiążące. Decyzja o uwzględnieniu tych środków będzie należała wyłącznie do podmiotów krajowego systemu cyberbezpieczeństwa. Dzięki rekomendacjom uzyskają one fachową wiedzę, dzięki czemu będą mogły wprowadzić adekwatne do oszacowanego ryzyka zabezpieczenia.

2.28.2. Dostawca Wysokiego Ryzyka

Zawarty w rozdziale I Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. art. 20 stanowi o ustroju gospodarczym Rzeczypospolitej Polskiej. Opiera się on między innymi na wolności prowadzenia działalności gospodarczej, która polega na możliwości: podejmowania działalności gospodarczej w wybranej formie, swobodnego podejmowania decyzji gospodarczych oraz decyzji w sprawie zakończenia działalności. Z kolei art. 22 Konstytucji Rzeczypospolitej Polskiej dopuszcza ograniczenie wolności działalności gospodarczej w drodze ustawy ze względu na ważny interes publiczny. W ślad za tym artykułem Trybunał Konstytucyjny podkreślał w swoim orzecznictwie, że wolność działalności gospodarczej nie ma charakteru absolutnego. W jednym z wyroków Trybunał zaznaczył, że działalność gospodarcza może podlegać różnego rodzaju ograniczeniom w stopniu większym niż prawa i wolności o charakterze osobistym bądź politycznym⁶¹⁾. Państwo może więc wprowadzić takie przepisy ustawowe, które pozwolą zminimalizować niekorzystne skutki mechanizmów wolnorynkowych, jeżeli skutki te ujawniają się w sferze, która nie może pozostać obojętna dla państwa ze względu na ochronę powszechnie uznawanych wartości⁶²⁾. Z kolei w innym orzeczeniu Trybunał zaznaczył, że rezygnacja z niezbędnych środków kontroli przez państwo niektórych dziedzin gospodarki mogłaby doprowadzić do zagrożenia bezpieczeństwa państwa, porządku publicznego, a także prawno-międzynarodowym zobowiązaniom państwa⁶³⁾. W tym kontekście należy wskazać, że bezpieczeństwo państwa zostało uznane przez Trybunał Konstytucyjny za element dobra wspólnego, a każdy obywatel jest zobowiązany do troski o dobro wspólne. Obowiązkiem Rady Ministrów jest zapewnienie bezpieczeństwa wewnętrznego i zewnętrznego państwa (art. 146 ust. 4 pkt 7 i 8 Konstytucji Rzeczypospolitej Polskiej).

Opierając się na powyższych przesłankach, projektodawca proponuje wprowadzenie mechanizmu pozwalającego na uznanie określonego dostawcy sprzętu lub oprogramowania dla szczególnego rodzaju podmiotów gospodarczych i społecznych, za dostawcę wysokiego ryzyka. Wskazane w decyzji zakresy produktów ICT, rodzaje usług ICT lub konkretne procesy ICT pochodzące od dostawcy wysokiego ryzyka, będą musiały być wycofane z tych podmiotów. Rozwiązanie to ma na celu zapewnienie ochrony ważnego interesu państwowego w postaci bezpieczeństwa państwa.

⁶¹⁾ Wyrok Trybunału Konstytucyjnego z dnia 8 kwietnia 1998 r., sygn. K 10/97.

⁶²⁾ Ibidem.

⁶³⁾ Wyrok Trybunału Konstytucyjnego z dnia 10 października 2001 r., sygn. K 28/01.

Obecnie nie ma żadnych środków prawnych umożliwiających nakazanie wycofywania z eksploatacji produktów ICT, usług ICT i procesów ICT zagrażających bezpieczeństwu kluczowych podmiotów w Polsce, a przez to funkcjonowaniu państwa. W szczególności dotyczy to kluczowych przedsiębiorców telekomunikacyjnych, którzy będą świadczyć usługi w oparciu o mobilne sieci 5G⁶⁴). Sieć 5G będzie oferowała możliwość przetwarzania znacznie większej liczby danych oraz wyższe prędkości przekazywania danych w porównaniu do dotychczasowej sieci 3G oraz 4G. Dzięki sieci 5G możliwe będzie podłączenie znacznie większej liczby urządzeń Internetu Rzeczy niż do tej pory. Umożliwi to znacznie większe możliwości przekazywania danych pomiędzy obywatelami oraz wpłynie pozytywnie na rozwój gospodarki.

Wdrożenie sieci 5G wiąże się z ryzykami, szczególnie tymi związanymi z bezpieczeństwem. Dzięki tym sieciom będzie możliwe świadczenie wielu usług niezbędnych do funkcjonowania rynku wewnętrznego oraz utrzymania i realizacji podstawowych funkcji społecznych i gospodarczych – takich jak energetyka, transport, bankowość i opieka zdrowotna oraz systemy sterowania produkcją. Potencjalny cyberatak mógłby doprowadzić do naruszenia dostępności danej usługi na niespotykaną dotąd skalę. Możliwy byłby atak na sieć 5G, który doprowadziłby do przejęcia kontroli nad infrastrukturą krytyczną, jak np. sieci energetyczne. Przejęcie kontroli nad siecią 5G mogłoby doprowadzić do naruszenia poufności ogromnej liczby przesyłanych danych. Skutki takich incydentów byłyby bardzo poważne.

Kwestia bezpieczeństwa sieci 5G została podjęta na poziomie unijnym. W motywie 3 i 4 zaleceń Komisji (UE) 2019/534 wskazano, że:

„(3) Z powodu uzależnienia wielu usług o krytycznym znaczeniu od sieci 5G konsekwencje systemowych i rozległych zakłóceń byłyby szczególnie poważne. W rezultacie zapewnienie cyberbezpieczeństwa sieci 5G jest kwestią o strategicznym znaczeniu dla Unii w czasie, gdy cyberataki przybierają na sile i są coraz bardziej wyrafinowane.

⁶⁴) Jako sieci 5G Komisja Europejska zdefiniowała: *zbiór wszystkich istotnych elementów infrastruktury sieciowej z zakresu technologii łączności ruchomej i bezprzewodowej, wykorzystywanej na potrzeby łączności i usług o wartości dodanej, o zaawansowanych parametrach eksploatacyjnych, takich jak bardzo wysoka prędkość przesyłu danych i przepustowość łączy, łączność charakteryzująca się niskim opóźnieniem, ekstremalnie wysoka niezawodność bądź zdolność obsługi dużej liczby podłączonych urządzeń. Mogą one obejmować elementy dotychczasowych sieci wykorzystujących technologię łączności ruchomej i bezprzewodowej poprzednich generacji, takich jak 4G lub 3G. Sieci 5G należy rozumieć jako obejmujące wszystkie istotne części sieci.* Pkt II.2.a Zalecenie Komisji (UE) 2019/534 z dnia 26 marca 2019 r. Cyberbezpieczeństwo sieci 5G (Dz. Urz. UE L 88 z 29.3.2019, s. 42.).

(4) Ponadnarodowy charakter infrastruktury stanowiącej podstawę ekosystemu cyfrowego, która charakteryzuje się siecią wzajemnych powiązań, jak również transgraniczny charakter zagrożeń oznaczają, że wszelkie istotne luki bezpieczeństwa lub cyberincydenty dotyczące sieci 5G występujące w jednym państwie członkowskim miałyby wpływ na całą Unię. Dlatego też należy przewidzieć środki w celu zapewnienia wysokiego wspólnego poziomu cyberbezpieczeństwa sieci 5G.”.

Komisja Europejska zaleciła, aby państwa członkowskie Unii Europejskiej przeprowadziły krajową ocenę ryzyka bezpieczeństwa sieci 5G, zgodnie z jej rekomendacjami. Ponadto Komisja Europejska zaleciła, że w oparciu o krajową ocenę ryzyka państwa członkowskie powinny:

- 1) zaktualizować wymogi w zakresie bezpieczeństwa oraz metody zarządzania ryzykiem stosowane w odniesieniu do sieci 5G;
- 2) zaktualizować odpowiednie obowiązki nakładane na przedsiębiorstwa udostępniające publiczne sieci łączności lub świadczące publicznie dostępne usługi łączności elektronicznej zgodnie z art. 13a i art. 13b dyrektywy 2002/21/WE;
- 3) obwarować ogólne zezwolenia warunkami dotyczącymi zabezpieczenia sieci publicznych przed nieuprawnionym dostępem oraz uzyskać od przedsiębiorstw uczestniczących w przyszłych postępowaniach o udzielenie praw użytkowania częstotliwości radiowych w pasmach 5G zobowiązanie do przestrzegania wymogów w zakresie bezpieczeństwa sieci na podstawie dyrektywy 2002/20/WE;
- 4) stosować inne środki zapobiegawcze mające na celu ograniczenie potencjalnych zagrożeń dla cyberbezpieczeństwa.

Środki te powinny obejmować obowiązki nakładane na dostawców oraz operatorów celem zapewnienia bezpieczeństwa sieci 5G.

W wyniku powyższych zaleceń powstała unijna skoordynowana ocena ryzyka cyberbezpieczeństwa sieci 5G⁶⁵⁾ oraz Unijny zestaw środków dla cyberbezpieczeństwa sieci 5G – tzw. Toolbox 5G⁶⁶⁾. W dokumentach tych wskazano na ryzyka związane z sieciami 5G, w tym także tymi związanymi z dostawcami sprzętu i oprogramowania dla tej sieci.

⁶⁵⁾ Report on the EU coordinated risk assessment on cybersecurity in Fifth Generation (5G) networks https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6049, zwana dalej Unijną oceną cyberbezpieczeństwa sieci 5G”.

⁶⁶⁾ Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures <https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures>.

Jedno ze wskazanych ryzyk dotyczy dostawców, którzy znajdują się pod wpływem państw prowadzących agresywne działania w cyberprzestrzeni. Takie państwo może wpływać na dostawcę, aby wykorzystał ukryte podatności w sprzęcie lub oprogramowaniu dostarczonemu innemu państwu, aby uzyskać dostęp do wrażliwych danych przesyłanych przez ten sprzęt czy też wpływać na dostępność usług świadczonych poprzez ten sprzęt. Dostawca taki będzie działał na rzecz interesów państwa, pod którego wpływem znajduje się. Prawdopodobieństwo zaistnienia tej sytuacji zależy od stopnia, w jakim dostawca ma dostęp do sieci, w szczególności jej krytycznych funkcji⁶⁷⁾.

Natomiast ryzyka dotyczą również aspektów technicznych, np. tego czy dostawca jest w stanie zapewnić bezpieczeństwo swoich produktów, jak reaguje na incydenty związane z tymi produktami, jak zarządza podatnościami własnych produktów. Niska jakość sprzętu i oprogramowania dostarczanego przez dostawcę, w tym ukryte podatności, może umożliwić cyberatak na sieć dokonywany przez agresywne państwa w cyberprzestrzeni, grupy *Advanced Persistent Threat* czy grupy przestępcze⁶⁸⁾.

Z wyżej wskazanych dokumentów wynika więc, że mogą istnieć dostawcy sprzętu lub oprogramowania, którzy poprzez dostarczany sprzęt lub oprogramowanie mogą zagrażać państwom członkowskim Unii Europejskiej, w tym także Polsce. Przyjęło się określać takich dostawców jako „dostawców wysokiego ryzyka” (high risk vendors).

Toolbox 5G wskazuje środki strategiczne, które będą w stanie zmitigować ryzyka wskazane w Unijnej ocenie cyberbezpieczeństwa sieci 5G. Przede wszystkim Toolbox 5G zaleca środki strategiczne:

- 1) SM01 – wzmocnienie roli władz krajowych – środek ten polega m.in. na wyposażeniu władz krajowych w kompetencje do zakazu, ograniczenia lub wprowadzenia wymagań odnośnie produktów dla sieci 5G, biorąc pod uwagę m.in. bezpieczeństwo krytycznych (critical and sensitive) części sieci 5G, ryzyka związane z wpływem państw trzecich na łańcuchy dostaw 5G czy ryzyka dla bezpieczeństwa narodowego;
- 2) SM03 – ocena ryzyka dostawców – przeprowadzenie rygorystycznej oceny ryzyka dostawców, a następnie wprowadzenie niezbędnych wyłączeń w krytycznych zasobach.

⁶⁷⁾ Unijna ocena cyberbezpieczeństwa sieci 5G str. 22, przypis 14 i 15, str. 27; Toolbox str. 43 i 44.

⁶⁸⁾ Unijna ocena cyberbezpieczeństwa sieci 5G pkt 2.51, Toolbox 5G str. 43.

W swoim komunikacie z dnia 29 stycznia 2020 r. Komisja Europejska potwierdziła, że „państwa członkowskie zgodziły się co do konieczności oceny profilu ryzyka poszczególnych dostawców i w konsekwencji stosowania odpowiednich ograniczeń wobec dostawców uznanych za stwarzających wysokie ryzyko, w tym niezbędnych wyłączeń, aby skutecznie łagodzić ryzyko w odniesieniu do kluczowych aktywów, jak wskazano w zestawie narzędzi”⁶⁹⁾.

Biorąc pod uwagę powyższe stanowisko unijne zasadne jest wprowadzenie procedury umożliwiającej zbadanie ryzyk związanych z danym dostawcą sprzętu lub oprogramowania. W przypadku, gdyby ryzyka dla bezpieczeństwa państwa okazały się zbyt wysokie, taki dostawca powinien być uznany za stwarzający wysokie ryzyko.

W przepisach nowelizacji została dodana kompetencja ministra właściwego do spraw informatyzacji do przeprowadzenia postępowania w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Postępowanie to będzie prowadzone w celu ochrony ważnych interesów państwowych w postaci bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego. Tak jak wyżej wspomniano kwestia cyberbezpieczeństwa sieci 5G jest kwestią strategiczną dla Unii Europejskiej z uwagi na współzależności pomiędzy sieciami telekomunikacyjnymi państw członkowskich Unii Europejskiej. Ze względu na potencjalne szkody, które może przynieść zakłócenie funkcjonowania tych sieci jest to również materia dotycząca bezpieczeństwa państwa. Jednakże przepis nie zamyka się wyłącznie do sieci 5G. Postępowaniu będzie mógł być poddany dostawca produktów, usług i procesów ICT nie tylko dla sieci 5G, ale również dla innych systemów informacyjnych – jeżeli będzie spełniona przesłanka zapewnienia ochrony bezpieczeństwa państwa.

Dostawcą sprzętu lub oprogramowania jest dostawca produktów ICT, usług ICT lub procesów ICT⁷⁰⁾. Zgodnie z definicją dostawcy może to być producent, importer, dystrybutor. Dzięki temu postępowaniem będą mogły być objęte wszystkie podmioty kluczowe w łańcuchu dostaw. Postępowanie nie będzie dotyczyło wszystkich produktów ICT, usług ICT i procesów

⁶⁹⁾ https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=COM:2020:0050:FIN&_sm_au_=iVVZRW54FHZ10n2PVkFHNKt0jRsMJ

⁷⁰⁾ Dla przypomnienia: produktem ICT jest element lub grupę elementów systemu informacyjnego, usługą ICT jest usługa polegająca w pełni lub głównie na przekazywaniu, przechowywaniu, pobieraniu lub przetwarzaniu informacji za pośrednictwem systemów informacyjnych, procesem ICT jest zestaw czynności wykonywanych w celu projektowania, budowy, rozwijania, dostarczania lub utrzymywania produktów ICT lub usług ICT. Zauważyć przy tym należy, że definicja systemu informacyjnego obejmuje także sieć telekomunikacyjną - por. Sejm RP VIII kadencji, druk nr 2505, Rządowy projekt ustawy o krajowym systemie cyberbezpieczeństwa, uzasadnienie str. 18-19. <https://sejm.gov.pl/Sejm8.nsf/druk.xsp?nr=2505>.

ICT pochodzących od konkretnego dostawcy sprzętu lub oprogramowania, lecz tylko tych, które są wykorzystywane przez podmioty kluczowe i podmioty ważne z wyłączeniem podsektora komunikacji elektronicznej lub przedsiębiorców komunikacji elektronicznej, których roczne przychody z tytułu wykonywania działalności telekomunikacyjnej w poprzednim roku obrotowym były wyższe od kwoty 10 milionów złotych.

Podmioty te są szczególnie ważne dla zapewnienia bezpieczeństwa państwa, dlatego konieczne jest, żeby korzystały z bezpiecznego sprzętu lub oprogramowania w trakcie świadczenia usług na rzecz państwa i obywateli.

Do postępowania w sprawie uznania dostawcy za dostawcę wysokiego ryzyka będą miały zastosowanie przepisy ustawy z dnia 14 czerwca 1960 r. Kpa. Dzięki temu dostawca sprzętu lub oprogramowania będzie brał udział w postępowaniu na prawach strony, z odmiennosciami wynikających ze szczególnych regulacji wynikających z przepisów nowelizacji. W postępowaniu nie będą stosowane następujące przepisy Kpa:

- 1) art. 28 – projekt wprowadza wyjątek, że w tym szczególnym postępowaniu stroną postępowania jest każdy wobec kogo zostało wszczęte postępowanie w sprawie uznania za dostawcę wysokiego ryzyka;
- 2) art. 31 – wyłącza się udział organizacji społecznej w postępowaniu;
- 3) art. 51 – wyłącza się przepis, który zawęży osobiste stawiennictwo do obrębu gminy lub miasta, w którym zamieszkuje albo przebywa osoba, jak również sąsiedniej gminy albo miasta;
- 4) art. 66a – wyłącza się przepis dotyczący prowadzenia metryki sprawy;
- 5) art. 79 – wyłącza się przepis o udziale strony w przeprowadzeniu dowodu;

Wyłączenie tych przepisów Kpa jest niezbędne ze względu na szczególny charakter tego postępowania, które ma na celu zapewnienie bezpieczeństwa narodowego.

W celu usprawnienia przebiegu postępowania i wzmocnienia trwałości rozstrzygnięć konieczne jest zawężenie przymiotu strony oraz udziału organizacji społecznej, mając na względzie, że do każdego takiego postępowania, według zasad ogólnych mogłoby przystąpić na prawach strony nawet setki podmiotów korzystających z konkretnych produktów pochodzących od konkretnego dostawcy sprzętu lub oprogramowania.

Wyłączenie art. 28 Kpa jest konieczne, ponieważ postępowanie jest wszczynane z urzędu przez ministra albo na wniosek przewodniczącego Kolegium – co za tym idzie stroną jest każdy

wobec kogo zostało wszczęte postępowanie w sprawie uznania za dostawcę wysokiego ryzyka. Podobne rozwiązanie znajduje się w art. 88 ust. 1 ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. z 2024 r. poz. 1616 oraz z 2025 r. poz. 794).

Z kolei wyłączenie art. 31 Kpa wynika ze szczególnego związku tego postępowania z kwestiami bezpieczeństwa narodowego.

Ze względu na ogólnopolski zasięg decyzji jaka ma zostać wydana w tym postępowaniu został wyłączony art. 51 Kpa.

Kwestia metryki sprawy przy tego typu postępowaniu jest złożona. Obowiązkowo w ramach postępowania o uznaniu dostawcy za dostawcę wysokiego ryzyka będą przeprowadzane szerokie analizy podmiotu, którego dotyczy postępowanie oraz jego produktów. Ujawnienie nazwisk osób, które przeprowadzały te analizy mogłoby narazić ich na działania ze strony podmiotów zainteresowanych konkretnym wynikiem sprawy. Ponadto wiele z tych osób to funkcjonariusze, których tożsamość, ze względu na wykonywane zadania, musi być chroniona. Z powyższych względów wyłączony został art. 66a Kpa.

W związku z wrażliwym charakterem informacji, jakie będą wykorzystywane w ramach tego postępowania, konieczne jest wyłączenie udziału strony z przeprowadzanych dowodów.

Jednocześnie umożliwiono przystąpienie do postępowania na prawach strony kilkunastu największych przedsiębiorców komunikacji elektronicznej. Będą to tacy przedsiębiorcy komunikacji elektronicznej, którzy w poprzednim roku obrotowym uzyskali przychód z tytułu prowadzenia działalności telekomunikacyjnej w wysokości co najmniej dwudziestotysięcznej krotności przeciętnego wynagrodzenia w gospodarce narodowej, wskazanego w ostatnim komunikacie Prezesa Głównego Urzędu Statystycznego, o którym mowa w art. 20 pkt 1 lit. a ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych (Dz. U. z 2024 r. poz. 1631 i 1674 oraz z 2025 r. poz. 718, 769 i 1159). Aby przystąpić do postępowania taki przedsiębiorca będzie obowiązany złożyć stosowny wniosek. Zmiana odpowiada na postulaty strony społecznej, jednocześnie zapewniając sprawny przebieg postępowania.

Umożliwia się wypowiedzenie się w toku postępowania izbom gospodarczym. Będą one mogły przedstawić stanowisko co do dostawcy sprzętu lub oprogramowania, wobec którego wszczęto postępowanie, oraz dostarczanych przez niego produktów ICT, usług ICT oraz procesów ICT. Minister właściwy do spraw informatyzacji, przed wydaniem decyzji, udostępnia w BIP na swojej stronie podmiotowej raport ze złożonych stanowisk, wskazując

w szczególności główne uwagi zawarte w stanowiskach. Rozwiązanie to zapewnia z jednej strony możliwość wypowiedzenia się reprezentantów przedsiębiorców w sprawie tego postępowania, a z drugiej strony nie spowoduje to przewlekłości postępowania.

Minister właściwy do spraw informatyzacji stanowisko zajmuje w drodze decyzji administracyjnej, co umożliwi dostawcy ewentualne złożenie skargi do wojewódzkiego sądu administracyjnego.

W przypadku, gdy dostawcą sprzętu lub oprogramowania jest strona niemająca siedziby na terytorium państwa członkowskiego Unii Europejskiej, Konfederacji Szwajcarskiej albo państwa członkowskiego Europejskiego Porozumienia o Wolnym Handlu (EFTA) zawiadomienie o wszczęciu postępowania publikowane jest na stronie podmiotowej BIP ministra właściwego do spraw informatyzacji. Publikacja ma skutek doręczenia po upływie 14 dni od dnia jej dokonania. Przepis ten stanowi szczególną regulację w stosunku do zasad doręczeń określonych w Kpa.

Zawiadomienie o wszczęciu postępowania wobec dostawcy, który ma siedzibę na terytorium Unii Europejskiej, Konfederacji Szwajcarskiej czy państwa członkowskiego EFTA będzie doręczane na zasadach ogólnych wynikających z Kpa. Natomiast po otrzymaniu potwierdzenia doręczenia informacja o tym będzie publikowana na stronie BIP ministra właściwego do spraw informatyzacji, aby uprawnieni przedsiębiorcy telekomunikacyjni mogli złożyć wniosek o dopuszczenie do postępowania na prawach strony.

Postępowanie w sprawie uznania dostawcy za dostawcę wysokiego ryzyka będzie wszczynane z urzędu przez ministra właściwego do spraw informatyzacji lub na wniosek Przewodniczącego Kolegium. Minister właściwy do spraw informatyzacji jest odpowiedzialny za bezpieczeństwo cyberprzestrzeni w wymiarze cywilnym, stąd też zasadne jest, aby to on prowadził tego rodzaju postępowanie. Przed wydaniem decyzji minister właściwy do spraw informatyzacji będzie obowiązany zwrócić się do Kolegium o wydanie opinii w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Kolegium będzie miało 3 miesiące, od dnia wystąpienia o opinię, na przekazanie jej do ministra. Termin od dnia wystąpienia o opinię do dnia otrzymania opinii nie będzie wliczał się do terminu załatwienia sprawy.

Wskazano elementy analizy, która ma być zawarta w opinii Kolegium. W większości nawiązują one do pkt. 2.37 raportu Unii Europejskiej dotyczącego unijnej oceny ryzyka cyberbezpieczeństwa sieci 5G⁷¹⁾.

Celem opinii Kolegium jest kompleksowa analiza działalności dostawcy sprzętu lub oprogramowania. Mając na uwadze, że w skład Kolegium wchodzi ministrowie kluczowi dla bezpieczeństwa państwa a także szefowie służb specjalnych, będą w stanie pozyskać niezbędne informacje do oceny dostawcy od swoich jednostek podległych lub nadzorowanych.

Zasadne jest, aby opinia obejmowała kwestie zagrożeń, które stwarza dostawca. Nie są to jednak zwykłe zagrożenia, lecz takie, które wpływają na bezpieczeństwo narodowe. Przepis dalej precyzuje, że chodzi o zagrożenia w wymiarze ekonomicznym⁷²⁾, wywiadowczym⁷³⁾ oraz terrorystycznym⁷⁴⁾. Ponadto konieczna będzie analiza zagrożeń, które stwarza dostawca dla zobowiązań sojuszniczych (np. w ramach NATO czy innych umów międzynarodowych) a także europejskich. Niewątpliwie zobowiązaniem europejskim jest zapewnienie na poziomie unijnym wysokiego poziomu bezpieczeństwa systemów informacyjnych (co wynika z dyrektywy NIS 2).

Kolejnym aspektem opinii powinna być analiza prawdopodobieństwa, z jakim dostawca znajduje się pod wpływem państwa. Ta część opinii skupia się na powiązaniach dostawcy sprzętu lub oprogramowania z państwem spoza Unii Europejskiej oraz NATO. Wpływ ten może obejmować prawodawstwo danego państwa, które reguluje stosunki między państwem a dostawcą (np. w zakresie swobody działalności gospodarczej czy bezpieczeństwa przetwarzanych danych). Co istotne Kolegium powinno pochylić się także nad praktyką stosowania tych przepisów, aby sprawdzić, jak one funkcjonują, np. czy gwarancje zawarte w tych przepisach rzeczywiście są respektowane przez dane państwo.

⁷¹⁾ Report on the EU coordinated risk assessment on cybersecurity in Fifth Generation (5G) networks https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6049.

⁷²⁾ Np. zagrożenia które uniemożliwiają rozwój ekonomiczny i osłabiają potencjał gospodarczo-obronny państwa. Przykładowo sieci w technologii 5g przyczynia się do rozwoju gospodarczego ponieważ szybki przesyłanie danych poprzez technologię *Ultra Reliable Low Latency Communications* ułatwi prowadzenie działalności gospodarczej przez wiele podmiotów - przykłady - inteligentne urządzenia portowe umożliwiające szybki rozładunek, inteligentne systemy transportowe u zarządców dróg, inteligentne sieci energetyczne - smart grids. Dostawca wysokiego ryzyka wpływający na funkcjonowanie tych podmiotów wpływa na innych przedsiębiorców korzystających z tych usług.

⁷³⁾ Np. chodzi o zagrożenie eksfiltracji danych poprzez sprzęt dostarczany przez dostawcę - w tym także szpiegostwo gospodarcze.

⁷⁴⁾ Np. cyberterrorizm w postaci ataków na infrastrukturę krytyczną państwa.

Z uwagi na to, że współcześnie coraz więcej danych osobowych jest przesyłanych poza Unię Europejską ważna jest także kwestia ochrony danych osobowych w danym państwie i kwestia faktycznego stosowania tych przepisów.

Opinia będzie także zawierała analizę struktury własnościowej dostawcy sprzętu lub oprogramowania – w celu ustalenia kto faktycznie sprawuje kontrolę własnościową nad dostawcą. Finalnie powinny być sprawdzone możliwości wpływu danego państwa na dostawcę.

Opinia będzie dotyczyła otoczenia regulacyjnego dostawcy, faktycznego stosowania prawa, struktury własnościowej oraz faktycznego wpływu państwa na dostawcę. Po dokonaniu analiz uzyskany zostanie całościowy obraz relacji między dostawcą a państwem.

Rozporządzeniem wykonawczym Rady (UE) 2020/1125 z dnia 30 lipca 2020 r. wykonującym rozporządzenie (UE) 2019/796 w sprawie środków ograniczających w celu zwalczania cyberataków zagrażających Unii Europejskiej lub jej państwom członkowskim (Dz. Urz. UE L 2020/1125 z 30.07.2020) Unia Europejska wskazała podmioty, które dokonują cyberataków na Unię Europejską lub jej państwa członkowskie. Wskazane jest, aby opinia Kolegium dotyczyła również tego, jakie są relacje pomiędzy tymi podmiotami a dostawcą sprzętu lub oprogramowania.

Jak już wyżej wskazano ryzyka dotyczą również aspektów technicznych produktów ICT, usług ICT i procesów ICT dostarczanych przez dostawcę. Dlatego do technicznych aspektów opinii należy analiza:

- 1) liczby i rodzajów wykrytych podatności i incydentów dotyczących zakresu typów produktów ICT lub rodzajów usług ICT lub konkretnych procesów ICT dostarczanych przez dostawcę sprzętu lub oprogramowania oraz sposobu i czasu ich eliminowania;
- 2) trybu i zakresu, w jakim dostawca sprzętu lub oprogramowania sprawuje nadzór nad procesem wytwarzania i dostarczania sprzętu lub oprogramowania dla podmiotów, o których mowa w art. 67b ust. 1 ustawy o KSC, oraz ryzyka dla procesu wytwarzania i dostarczania sprzętu lub oprogramowania;
- 3) treści wydanych wcześniej rekomendacji, o których mowa w art. 33 ust. 4 ustawy o KSC, dotyczących sprzętu lub oprogramowania danego dostawcy.

Jest to związane z potencjalnymi ryzykami, które wiążą się z niską jakością sprzętu lub oprogramowania. Jak wyżej wspomniano podatności mogą być wykorzystane do cyberataków

przez państwa, grupy APT czy grupy przestępcze – dlatego warto zbadać jakość produktów dostarczanych przez dostawcę.

Realizując postulaty strony społecznej dodano wymóg, aby prowadząc opinię Kolegium uwzględniło także certyfikaty produktów, usług i procesów ICT dostarczanych przez dostawcę oraz wyniki analiz łańcuchów dostaw, które przeprowadziły zespoły CSIRT poziomu krajowego.

Określono procedurę sporządzania opinii Kolegium. Opinia zostanie przygotowana przez zespół opiniujący w skład, którego wchodzi przedstawiciele członków Kolegium. Każdy członek zespołu opiniującego przygotowuje stanowisko w zakresie swojej właściwości. Przewodniczący Kolegium będzie miał kompetencję do rozstrzygnięcia ewentualnego negatywnego sporu co do zakresu tej właściwości poprzez wskazanie właściwego członka zespołu opiniującego. Wprowadzono obowiązek przeprowadzenia analiz łańcuchów dostaw, zanim zostanie sporządzona opinia Kolegium w sprawie dostawcy.

Po przeprowadzeniu postępowania minister właściwy do spraw informatyzacji wyda decyzję uznającą dostawcę sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, jeżeli z przeprowadzonego postępowania wynika, że dostawca ten stanowi zagrożenie dla podstawowego interesu bezpieczeństwa państwa. Decyzja będzie zawierać wskazanie typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT pochodzących od dostawcy uwzględnionych w postępowaniu w sprawie uznania za dostawcę wysokiego ryzyka – ponieważ one też stwarzają zagrożenie.

Pojęcie podstawowego interesu bezpieczeństwa państwa jest wskazane w art. 346 Traktatu o funkcjonowaniu Unii Europejskiej⁷⁵⁾. Zdaniem Rzecznika Generalnego N. Emiliou termin bezpieczeństwa państwa z art. 346 TFUE odpowiada terminom „bezpieczeństwo publiczne” i „bezpieczeństwo narodowe”, oraz w znacznym stopniu pokrywa się z terminem „bezpieczeństwo wewnętrzne”⁷⁶⁾.

⁷⁵⁾ Traktat o funkcjonowaniu Unii Europejskiej (wersja skonsolidowana) Dz. Urz. UE C 326 z 26.10.2012, s. 47.

⁷⁶⁾ Opinia Rzecznika Generalnego N. Emiliou przedstawiona w dniu 2 marca 2023 r. Komisja Europejska przeciwko Rzeczypospolitej Polskiej. Uchybienie zobowiązaniom państwa członkowskiego – Zamówienia publiczne na usługi – Drukarnia państwowa – Wytwarzanie dokumentów tożsamości i innych dokumentów urzędowych oraz układów do zarządzania tymi dokumentami – Przepisy krajowe przewidujące udzielanie zamówień dotyczących tego wytwarzania przedsiębiorstwu prawa publicznego bez uprzedniego postępowania o udzielenie zamówienia – Artykuł 346 ust. 1 lit. a) TFUE – Dyrektywa 2014/24/UE – Artykuł 1 ust. 1 i 3 – Artykuł 15 ust. 2 i 3 – Szczególne środki bezpieczeństwa – Ochrona podstawowych interesów w zakresie bezpieczeństwa państwa członkowskiego. Sprawa C-601/21., <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:62021CC0601>, [4 listopad 2024 r.].

Zdaniem Trybunału Sprawiedliwości Unii Europejskiej bezpieczeństwem narodowym jest: „*pierwszorzędny interes w ochronie podstawowych funkcji państwa i podstawowych interesów społeczeństwa, a także zapobieganie i ściganie działalności mogącej poważnie zdestabilizować podstawowe struktury konstytucyjne, polityczne lub społeczne kraju, w szczególności bezpośrednio zagrozić społeczeństwu, ludności lub państwu jako takiemu, zwłaszcza takiej jak działalność terrorystyczna*⁷⁷⁾”. Rzecznik Generalny rozwinął to, wskazując, że ten „*termin odnosi się do kwestii związanych z bezpieczeństwem instytucji i ludności państwa członkowskiego w obliczu zagrożeń o określonym znaczeniu, wynikających z okoliczności mających w stosunku do tego państwa charakter wewnętrzny (przestępczość zorganizowana, zamieszki itp.) lub zewnętrzny (działania wywiadowcze lub kontrwywiadowcze, cyberwojna itp.)*⁷⁸⁾”.

Należy jeszcze wyjaśnić na czym polega pojęcie „podstawowego interesu”. Rzecznik Generalny wskazuje, że „*pojęcie należy rozumieć tak, iż zawęża ono możliwość stosowania rozpatrywanych odstępstw do głównych elementów realizowanej przez państwa członkowskie polityki bezpieczeństwa, skutkując wyłączeniem z ich zakresu kwestii, które są tylko pośrednio lub luźno związane z bezpieczeństwem publicznym*⁷⁹⁾”. Dzięki prawnemu zidentyfikowaniu dostawcy wysokiego ryzyka będzie możliwe wprowadzenie dodatkowych środków mitygujących zagrożenie, jakie stwarza sprzęt lub oprogramowanie dostarczane przez dostawcę wysokiego ryzyka. Ze względu na charakter sprawy – stwierdzenie zagrożenia dla podstawowego interesu bezpieczeństwa państwa – decyzja ta będzie podlegała natychmiastowej wykonalności. Wskazać należy, że zastosowane w przepisie przesłanki w żaden sposób nie odnoszą się do pochodzenia dostawcy. Za dostawcę wysokiego ryzyka może być uznany zarówno podmiot zagraniczny jak również podmiot działający na terytorium Rzeczypospolitej Polskiej. Wszyscy przedsiębiorcy są obowiązani do działania w sposób niezagrażający bezpieczeństwu państwa polskiego.

⁷⁷⁾ La Quadrature du Net i in przeciwko Premier ministre i in, <https://eur-lex.europa.eu/legal-content/pl/TXT/?uri=CELEX:62018CJ0511>, [2 grudzień 2024 r.].

⁷⁸⁾ *Opinia rzecznika generalnego N. Emiliou przedstawiona w dniu 2 marca 2023 r. Komisja Europejska przeciwko Rzeczypospolitej Polskiej. Uchybienie zobowiązaniom państwa członkowskiego – Zamówienia publiczne na usługi – Drukarnia państwowa – Wytwarzanie dokumentów tożsamości i innych dokumentów urzędowych oraz układów do zarządzania tymi dokumentami – Przepisy krajowe przewidujące udzielanie zamówień dotyczących tego wytwarzania przedsiębiorstwu prawa publicznego bez uprzedniego postępowania o udzielenie zamówienia – Artykuł 346 ust. 1 lit. a) TFUE – Dyrektywa 2014/24/UE – Artykuł 1 ust. 1 i 3 – Artykuł 15 ust. 2 i 3 – Szczególne środki bezpieczeństwa – Ochrona podstawowych interesów w zakresie bezpieczeństwa państwa członkowskiego. Sprawa C-601/21., nr. 49.*

⁷⁹⁾ Ibidem, nr 50.

Jeżeli w trakcie postępowania zostanie stwierdzone, że dostawca nie stanowi poważnego zagrożenia dla podstawowego interesu bezpieczeństwa państwa, to zgodnie z zasadami ogólnymi Kpa zostanie wydana decyzja o umorzeniu postępowania.

Aby podmioty obowiązane do wycofania sprzętu mogły zastosować się do obowiązków wynikających z wydania tej decyzji administracyjnej, minister właściwy do spraw informatyzacji opublikuje ją w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski”, na stronie podmiotowej ministra właściwego do spraw informatyzacji w BIP, a także na stronie internetowej urzędu obsługującego tego ministra.

Od decyzji w sprawie uznania za dostawcę wysokiego ryzyka nie będzie przysługiwał wniosek o ponowne rozpatrzenie sprawy. Prawa strony postępowania będą zagwarantowane poprzez możliwość złożenia skargi do sądu administracyjnego.

Następstwem prawnego zidentyfikowania dostawcy wysokiego ryzyka powinno być zmiętygowanie ryzyka, które on stwarza. Wprowadza się więc niezbędne wymogi bezpieczeństwa dla podmiotów kluczowych i podmiotów ważnych w związku z wykorzystywaniem sprzętu lub oprogramowania pochodzącego od dostawcy wysokiego ryzyka.

Podmioty kluczowe i podmioty ważne nie będą mogły wprowadzać do użytkowania zakresów typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT w zakresie objętym decyzją, dostarczanych przez dostawcę wysokiego ryzyka. Dotyczyć to będzie zarówno nowych produktów ICT, usług ICT lub procesów ICT, jak i używanych. Celem jest, aby nie wprowadzać kolejnych produktów ICT, usług ICT lub procesów ICT, żeby nie zwiększać już i tak wysokiego ryzyka związanego z nimi.

Innym obowiązkiem będzie wycofanie z użytkowania zakresów typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT w zakresie objętym decyzją, dostarczanych przez dostawcę wysokiego ryzyka, jednak nie później niż 7 lat od dnia opublikowania informacji o decyzji. Chodzi tutaj o sytuację, w której w chwili wydania decyzji o uznaniu za dostawcę wysokiego ryzyka dany podmiot już używa lub korzysta z produktów ICT, usług ICT lub procesów ICT uwzględnionych w decyzji o uznaniu za dostawcę wysokiego ryzyka. Będzie więc musiał wycofać go w terminie 7 lat. Jest to związane z tym, że natychmiastowe wycofanie produktów ICT, usług ICT lub procesów ICT mogłoby być niemożliwe w praktyce, gdyż mogłoby spowodować zaprzestanie świadczenia usług.

Natomiast najwięksi przedsiębiorcy telekomunikacyjni, posiadający lub korzystający z typów produktów ICT, rodzajów usług ICT lub konkretnych procesów ICT wskazanych w decyzji i określonych w wykazie kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług w załączniku nr 3 do ustawy o KSC, będą musieli wycofać je w ciągu 4 lat od ogłoszenia decyzji. Takie skrócenie okresu na wycofanie jest spowodowane szczególnym znaczeniem dla bezpieczeństwa państwa usług telekomunikacyjnych, szczególnie sprzętu lub oprogramowania wykorzystywanych do realizowania funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku nr 3 do ustawy o KSC.

Jednocześnie wprowadzono przepis umożliwiający użytkowanie dotychczas posiadanych typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT w zakresie objętym decyzją w sprawie uznania za dostawcę wysokiego ryzyka, dostarczanych przez dostawcę wysokiego ryzyka, w zakresie naprawy, modernizacji, wymiany elementu lub aktualizacji. Będzie to możliwe wyłącznie, jeśli jest to niezbędne dla zapewnienia odpowiedniej jakości i ciągłości świadczonych usług, w szczególności dokonywania niezbędnych napraw awarii lub uszkodzeń. Te same przepisy zostały zastosowane do podmiotów publicznych, które już zakupiły określony sprzęt w drodze zamówienia publicznego. Jest to niezbędne rozwiązanie zarówno dla zapewnienia ciągłości świadczenia usług jak również ochrony dyscypliny finansów publicznych.

Wyżej zaproponowana interwencja prawodawcy jest konieczna ze względu na istotność dla bezpieczeństwa państwa usług świadczonych przez podmioty obowiązane do wycofania sprzętu lub oprogramowania. Podmioty te mogą być związane wieloletnimi umowami z dostawcą wysokiego ryzyka na dostarczanie sprzętu lub oprogramowania czy świadczenie usług serwisowych. Bez prawnego obowiązku stopniowego wycofania sprzętu lub oprogramowania pochodzącego od dostawcy wysokiego ryzyka podmioty te nie wycofają sprzętu lub oprogramowanie m. in. z uwagi na ryzyko odpowiedzialności kontraktowej wobec dostawcy. W konsekwencji ryzyko związane ze sprzętem lub oprogramowaniem pochodzącym od dostawcy wysokiego ryzyka nie zostanie skutecznie zmitigowane.

Podkreślić należy, że jest to wyjątek od podstawowej reguły zakazu wprowadzania do użytkowania i obowiązku wycofania ww. sprzętu lub oprogramowania w ciągu 5–7 lat. Wyjątek ten nie może być interpretowany rozszerzająco.

Wyjaśnienia wymaga termin użytkowania użyty w tym przepisie. Nie należy go utożsamiać z użytkowaniem z przepisów ustawy z dnia 23 kwietnia 1964 r. – Kodeks

cywilny, które jest ograniczonym prawem rzeczowym. Użytkowanie w rozumieniu projektowanego art. 66b ustawy o KSC oznacza każdy przypadek używania czy korzystania z produktu ICT, usługi ICT lub procesu ICT do świadczenia usług przez dany podmiot.

Należy podkreślić, że w zaproponowanych przepisach prawa nie ma mechanizmu nakazującego natychmiastowe wycofanie sprzętu lub oprogramowania wskazanego w ocenie ryzyka dostawców. Podmioty krajowego systemu cyberbezpieczeństwa, w tym operatorzy usług kluczowych, czy przedsiębiorcy telekomunikacyjni, zostaną zobowiązani do wycofania danego sprzętu lub oprogramowania w określonym czasie. W proponowanych przepisach jest mowa o 5–7 latach – termin ten jest często uznawany za średni okres użytkowania sprzętu lub oprogramowania, czyli tzw. cykl życia urządzenia. Raport BEREC wskazuje, że w przypadku sprzętu 5G wykorzystywanego w radiowej sieci dostępowej (RAN) cykl życia urządzenia wynosi w większości przypadków od 5 do 10 lat⁸⁰⁾.

Proponowane rozwiązania mają wpływ na swobodę działalności gospodarczej podmiotów zobowiązanych do wycofania sprzętu – wpływają bowiem na wolność podejmowania decyzji gospodarczych. Mają także wpływ na wykonywanie niektórych atrybutów prawa własności, tj. prawa do używania produktów. Wskazać należy, że przepisy te mają na celu mitygację ryzyk związanych ze sprzętem lub oprogramowaniem pochodzącym od dostawcy wysokiego ryzyka. Tak jak wyżej wspomniano korzystanie z takiego sprzętu mogłoby doprowadzić do poważnych ryzyk naruszenia poufności danych oraz naruszenia dostępności usługi. Co za tym idzie doprowadziłoby to do poważnego utrudnienia funkcjonowania obywateli – współczesnego społeczeństwa informacyjnego, a także do ryzyka przejęcia kontroli nad infrastrukturą krytyczną państwa. Wycofanie sprzętu lub oprogramowania pochodzących od dostawcy wysokiego ryzyka jest zatem konieczne do zapewnienia funkcjonowania demokratycznego państwa prawnego.

Proponowane rozwiązania nie naruszają istoty swobody prowadzenia działalności gospodarczej. Ogranicza się wykorzystywanie przez przedsiębiorców konkretnego sprzętu lub oprogramowania do świadczenia usług – w pozostałym zakresie przedsiębiorcy będą mogli swobodnie podejmować decyzje biznesowe. Przepisy te nie naruszają również istoty prawa własności. Tak jak wyżej wskazano nie ma mechanizmu natychmiastowego wycofania sprzętu lub oprogramowania – przez czas wycofywania z użytkowania podmioty te będą mogły

⁸⁰⁾ <https://www.berec.europa.eu/en/document-categories/berec/reports/berec-report-secure-5g-networks> str. 24.

w pełni wykonywać prawo własności. Ponadto w czasie wycofywania będzie można wprowadzić dotychczas posiadany sprzęt lub oprogramowanie pochodzący od dostawcy wysokiego ryzyka, aby dokonać niezbędnych napraw usterek czy awarii, aby zapewnić ciągłość świadczenia usługi – pokazuje to, że istota prawa własności nie została naruszona. Należy również zaznaczyć, że sprzęt lub oprogramowanie, które pochodzą od dostawcy wysokiego ryzyka i tak podlegałyby stopniowej wymianie ze względu na zużycie czy postęp technologiczny. Zatem proponowane rozwiązanie wpisuje się w mechanizm stopniowej wymiany sprzętu.

Proponowane rozwiązanie wpłynie na swobodę prowadzenia działalności gospodarczej przez dostawcę wysokiego ryzyka. Należy jednak podkreślić, że będzie to związane z poważnym zagrożeniem dla państwa, które stwarza ten dostawca. Jednakże istota prowadzenia działalności gospodarczej przez dostawcę wysokiego ryzyka nie zostanie naruszona. Taki dostawca nadal będzie mógł prowadzić działalność gospodarczą.

Podkreślić należy, że wartością konstytucyjną, która w tej sytuacji powinna być bardziej chroniona od swobody prowadzenia działalności gospodarczej czy prawa własności jest bezpieczeństwo państwa. Państwo powinno odpowiednio zaadresować problem dostawcy wysokiego ryzyka, który może, dzięki podatnościom w sprzęcie lub oprogramowaniu, które dostarczył, doprowadzić do ataku na infrastrukturę krytyczną państwa (np. inteligentne sieci energetyczne, sieci telekomunikacyjne), zakłócać funkcjonowanie organów państwa (np. poprzez ataki man in the middle, kradzież danych), czy zakłócić działanie kluczowych dla społeczeństwa usług (np. poprzez atak na systemy i urządzenia szpitalne, bez których znacznie utrudnione jest wykonywanie operacji ratujących życie). Może to się odbyć poprzez celowo zaprojektowane ukryte podatności lub również ukryte podatności powstałe w wyniku aktualizacji oprogramowania dostarczonego przez dostawcę wysokiego ryzyka. Wykorzystanie podatności w infrastrukturze telekomunikacyjnej, której elementy dostarczył taki dostawca, mogłoby utrudnić lub uniemożliwić funkcjonowanie usług komunikacji elektronicznej na danym obszarze.

Demokratyczne państwo prawne nie może być bezbronne i musi zawczasu identyfikować poważne zagrożenia dla jego funkcjonowania oraz skutecznie je mitygować. Ryzyka stwarzanego przez dostawcę wysokiego ryzyka (który działa pod wpływem obcych służb wywiadowczych lub grup przestępczych) oraz jego sprzęt lub oprogramowanie nie da się inaczej zmitygować, jak tylko poprzez stopniowe wycofanie takiego sprzętu. Podmioty korzystające z tych produktów ICT, usług ICT lub procesów ICT nie będą w stanie

zidentyfikować ukrytych podatności, poprzez które dostawca wysokiego ryzyka będzie mógł dokonywać ataków. W związku z tym nie jest możliwe zmitigowanie ryzyka stwarzanego przez dostawcę wysokiego ryzyka poprzez wprowadzenie dodatkowych środków bezpieczeństwa, innych niż wycofanie sprzętu lub oprogramowania, ponieważ będą one nieskuteczne wobec ukrytych podatności pozwalających np. nagle wyłączyć sprzęt czy zakłócić telekomunikację między podmiotami.

Warto podkreślić, że postępowanie w sprawie uznania za dostawcę wysokiego ryzyka będzie postępowaniem administracyjnym, a zatem dostawca będzie mógł przedstawić swoje racje w postępowaniu zanim zostanie uznany za dostawcę wysokiego ryzyka. Decyzja będzie mogła być zaskarżona do sądu administracyjnego, co zapewnia dostawcy możliwość obrony swoich praw. Dostawca będzie mógł być uznany za dostawcę wysokiego ryzyka, jeżeli będzie spełniał szczególnego rodzaju przesłanki, tj. będzie stwarzał poważne zagrożenie dla obronności, bezpieczeństwa państwa.

Podsumowując, zanim dostawca zostanie uznany za dostawcę wysokiego ryzyka jego sprawa zostanie wszechstronnie wyjaśniona – nastąpi to poprzez opinię Kolegium oraz czynności przeprowadzone przez ministra właściwego do spraw informatyzacji. Dostawca będzie mógł przedstawić swoje stanowisko, a w przypadku uznania za dostawcę wysokiego ryzyka – kwestionować to przed sądem administracyjnym.

Organy właściwe do spraw cyberbezpieczeństwa będą mogły zwracać się do podmiotów krajowego systemu cyberbezpieczeństwa o udzielenie informacji w sprawie wycofywanych produktów ICT, usług ICT i procesów ICT. Przepis wzmocni kompetencje organów i zapewni im możliwość monitorowania procesu wycofywania produktów ICT, usług ICT i procesów ICT.

Wprowadzono przepisy dotyczące procedury przed sądem administracyjnym, jest to więc przepis o charakterze *lex specialis* do PPSA. Jest on wzorowany na art. 38 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, która dotyczy rozpoznania skargi na decyzję o odmowie wydania poświadczenia bezpieczeństwa. Przepis ma za zadanie pogodzić dwie wartości prawne – prawo do złożenia skargi na decyzję administracyjną oraz ochronę informacji niejawnych, których ujawnienie mogłoby narazić państwo na niepowetowane szkody. Sąd administracyjny będzie rozpoznawał skargę na decyzję o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka na posiedzeniu niejawnym. Z kolei sentencja wyroku z uzasadnieniem zostanie doręczona tylko ministrowi właściwemu

do spraw informatyzacji. Skarżącemu doręcza się odpis wyroku z tą częścią uzasadnienia, która nie wymaga utajnienia ze względu na ochronę informacji niejawnych. Takie sformułowanie przepisu będzie zgodne z wyrokiem Trybunału Konstytucyjnego, który za niekonstytucyjne uznał brak doręczenia jawnych elementów wyroku sądu administracyjnego⁸¹⁾. Przepis stanowi niezbędne odstępienie od zasady ustności i jawności, jednakże strona będzie miała możliwość składania pism procesowych, jak w każdym innym postępowaniu przed sądem administracyjnym.

Rozwiązanie to jest konieczne dla zapewnienia bezpieczeństwa demokratycznego państwa prawnego – ujawnienie informacji niejawnych wykorzystanych w postępowaniu o uznaniu za dostawcę wysokiego ryzyka mogłoby narazić Rzeczpospolitą Polską na niepowetowane szkody. Nie została naruszona istota prawa do sądu, ponieważ w zakresie w jakim uzasadnienie nie zawiera informacji niejawnych (uzasadnienie prawne, kwestia wykładni, ustalenia organu niepodlegające utajnieniu) zostanie doręczone skarżącemu, dzięki czemu będzie mógł złożyć skargę kasacyjną. Rozwiązanie jest też proporcjonalne sensu stricto, bowiem sędziowie mają z urzędu dostęp do wszystkich materiałów niejawnych, które będą zgromadzone w sprawie. Będą więc mogli skrupulatnie zbadać legalność postępowania w sprawie uznania za dostawcę wysokiego ryzyka. Na poparcie tego rozwiązania warto tutaj odwołać się do wyroku Naczelnego Sądu Administracyjnego z 8 marca 2017 r. sygn. akt I OSK 1312/15: „strona skarżąca – z istoty sprawy mająca ograniczony dostęp do szeregu informacji z nią związanych – powinna móc działać w zaufaniu, że zasadniczo pełny dostęp do informacji posiada sąd, do którego zwraca się ona o kontrolę działania organu administracji publicznej, i że tę kontrolę sąd ten dokona w sposób niezależny i niezawisły w oparciu o pełną wiedzę wynikającą z ustaleń organu, w tym także niejawnych”.

Minister właściwy do spraw informatyzacji będzie prowadził w BIP wykaz decyzji o uznaniu za dostawcę wysokiego ryzyka w podziale na produkty, usługi i procesy w nich wskazane. Ułatwi to dostęp do informacji o niebezpiecznych produktach ICT, usługach ICT i procesach ICT.

2.28.2.1. Polecenie zabezpieczające

Przepisy nowelizacji ustawy o KSC wprowadzają regulację dotyczącą polecenia zabezpieczającego, które będzie mogło być wydane przez ministra właściwego do spraw informatyzacji w przypadku wystąpienia incydentu krytycznego, w celu skoordynowania

⁸¹⁾ Wyrok Trybunału Konstytucyjnego z dnia 23 maja 2018 r. sygn. akt SK 8/14.

efektywnej reakcji na ten incydent. Incydent krytyczny jest najbardziej dotkliwym w skutkach typem incydentu cyberbezpieczeństwa, skutkującym znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi. Incydent krytyczny jest klasyfikowany przez zespoły CSIRT poziomu krajowego, a więc najpierw operator usługi kluczowej, dostawca usługi cyfrowej lub podmiot publiczny zgłaszają właściwy incydent, który następnie – po przeprowadzeniu należytej oceny – może być uznany przez CSIRT poziomu krajowego za incydent krytyczny.

Obecnie państwo nie dysponuje środkami prawnymi, które umożliwiłyby skuteczną reakcję na incydent krytyczny. Oczywiście za obsługę incydentu krytycznego odpowiada jeden z zespołów CSIRT poziomu krajowego, który będzie współpracował z podmiotem, u którego wystąpił incydent krytyczny. Podkreślić jednak należy, że cyberataki mogą nie dotyczyć jednego podmiotu, a skutki takich ataków mogą się rozszerzać na inne podmioty w bardzo szybkim czasie. Zespoły CSIRT mogą nie nadążyć w obsłudze takiego incydentu krytycznego, który dotyczy wielu podmiotów. Jako przykład można podać sytuację, gdy cały świat zmagał się z podatnością Log4Shell. Była to krytyczna podatność, która mogła być wykorzystywana przez grupy advanced persistent threat⁸²⁾. Innym przykładem są ataki na wiele podmiotów administracji rządowej w Ukrainie.

Dlatego istnieje ważny interes publiczny w tym, aby państwo mogło nakazać, w niezbędnym i proporcjonalnym zakresie, przedsiębiorcom świadczącym istotne usługi dla społeczeństwa informacyjnego, zachowanie, które uchroni m.in. systemy informacyjne, sieci telekomunikacyjne wielu podmiotów przed skutkami incydentu krytycznego. Takim instrumentem będzie właśnie polecenie zabezpieczające.

Przed wydaniem polecenia zabezpieczającego niezbędne będzie przeprowadzenie analizy uzasadniającej wydanie tych środków nadzwyczajnych. Analiza będzie przeprowadzana wspólnie z Zespołem do spraw incydentów krytycznych. Zespół ten jest organem pomocniczym w sprawach obsługi incydentów krytycznych. W jego skład wchodzi przedstawiciele CSIRT MON, CSIRT NASK, Szefa Agencji Bezpieczeństwa Wewnętrznego realizującego zadania w ramach CSIRT GOV oraz Rządowego Centrum Bezpieczeństwa,

⁸²⁾ <https://www.crowdstrike.com/blog/overwatch-exposes-aquatic-panda-in-possession-of-log-4-shell-exploit-tools/>

Pełnomocnika oraz ministra właściwego do spraw informatyzacji. Jest to zespół ekspercki mający ułatwić reakcję na incydent krytyczny.

Natomiast minister właściwy do spraw informatyzacji będzie mógł wydać w drodze decyzji administracyjnej polecenie zabezpieczające w przypadku wystąpienia incydentu krytycznego. W poleceniu zabezpieczającym zawarte będzie wskazanie określonego zachowania, które zmniejszy skutki incydentu lub zapobiegnie jego rozprzestrzenianiu się. Katalog tych zachowań został wskazany w projektowanym art. 67g ust. 10 ustawy o KSC. Może to być m.in. nakaz zastosowania określonej poprawki bezpieczeństwa, nakaz szczególnej konfiguracji sprzętu lub oprogramowania, zakaz korzystania z określonego sprzętu lub oprogramowania. Jednocześnie należy wskazać, że zakaz korzystania z konkretnych usług i oprogramowania będzie dotyczył wyłącznie rozwiązań mających związek z trwającym incydentem krytycznym.

Polecenie zabezpieczające będzie miało charakter decyzji generalnej, a więc będzie skierowane w konkretnej sprawie do podmiotów ustalonych rodzajowo. Przemawia za tym fakt, że niemożliwe jest zidentyfikowanie ile dokładnie podmiotów mogłoby być dotkniętymi incydentem krytycznym.

Decyzje generalne są znane w prawie administracyjnym państw członkowskich Unii Europejskiej⁸³⁾, jak również w doktrynie i praktyce w polskim prawie sprzed 1997 r. Decyzja generalna to jeden z rodzajów aktu administracyjnego, a zatem akt stosowania prawa, a nie jego stanowienia (np. rozporządzenia czy ustawy)⁸⁴⁾. Ma charakter generalno-konkretny, czyli wymagają poczynienia ustaleń faktycznych i przyporządkowania (podciągnięcia) stanu faktycznego pod daną normę. Odróżnia je to od aktów normatywnych, które wiążą co do zasady wszystkich⁸⁵⁾.

Nie jest to nowa forma stanowienia prawa, a raczej specyficzny rodzaj aktu administracyjnego, działający obok, a nie zamiast decyzji administracyjnej. Decyzja administracyjna charakteryzuje się tzw. podwójną konkretnością (konkretny adresat i konkretna sprawa), natomiast akty normatywne są podwójnie ogólne (generalnie określony adresat

⁸³⁾ Przykładem mogą być: Niemcy, Grecja, Hiszpania i Portugalia oraz – jako przedstawiciel EOG – Norwegia.

⁸⁴⁾ Zbigniew Kmiecik (red.), *Raport Zespołu Eksperckiego z prac w latach 2012-2016 – Reforma prawa o postępowaniu administracyjnym*, Warszawa 2017.

⁸⁵⁾ E. Szewczyk, M. Szewczyk, *Między indywidualnym aktem administracyjnym a aktem normatywnym*, Warszawa 2014.

i abstrakcyjnie opisana sprawa). Akty generalne charakteryzują się natomiast ogólnie określonym adresatem i konkretnie określoną sprawą.

Decyzje generalne, mimo braku sformalizowanych zasad procedowania, są stosowane w polskim prawie. Przykładem mogą być niektóre uchwały Komisji Nadzoru Finansowego (dawny art. 71 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe (Dz. U. z 2024 r. poz. 1646, z późn. zm.)), Wykaz Produktów Leczniczych Dopuszczonych do Obrotu na terytorium Rzeczypospolitej Polskiej (art. 4 ust. 1 pkt 1 lit. j ustawy z dnia 18 marca 2011 r. o Urzędzie Rejestracji Produktów Leczniczych, Wyrobów Medycznych i Produktów Biobójczych (Dz. U. z 2023 r. poz. 1223), czy też rozstrzygnięcia Głównego Inspektora Sanitarnego (art. 27 ust. 1 i 2 ustawy z dnia 14 marca 1985 r. o Państwowej Inspekcji Sanitarnej (Dz. U. 2024 r. poz. 416)).

Do postępowania nie będą miały zastosowania przepisy art. 10, art. 34, art. 81, art. 81a, art. 107 § 1 pkt 3, art. 145 § 1 pkt 4 i art. 156 § 1 pkt 4 Kpa, a inne przepisy Kpa będą stosowane odpowiednio. Wyłączenia ww. przepisów są konieczne ponieważ w przypadku decyzji generalnych niemożliwe są do zidentyfikowania wszystkie strony postępowania. Wyłączenia w projekcie nawiązują do poglądów doktryny⁸⁶⁾.

W przypadku polecenia zabezpieczającego wyłączone wprost zostaną następujące przepisy Kpa odnoszące się do udziału strony w postępowaniu:

- 1) art. 10 – w przypadku decyzji generalnej, gdzie strona jest ustalona rodzajowo nie jest możliwe zapewnienie czynnego udziału wszystkim pomiotom, na których ten akt ma wpływ – ich prawa są chronione przez możliwość zaskarżenia decyzji do sądu administracyjnego;
- 2) art. 34 – z uwagi na to, że strona co do zasady nie będzie brała czynnego udziału w postępowaniu należy wyłączyć obowiązek organu dot. wystąpienia do sądu z wnioskiem o wyznaczenie przedstawiciela dla osoby nieobecnej lub niezdolnej do czynności prawnych;
- 3) art. 79 – z uwagi na rodzajowe określenie strony (a także potencjalną liczbę podmiotów, np. ok. 4000 przedsiębiorców telekomunikacyjnych) nie jest możliwe zawiadamianie ich o miejscu i terminie przeprowadzenia dowodu na siedem dni przed

⁸⁶⁾ Rozdział 7.4 E. Szewczyk, M. Szewczyk, *Generalny akt administracyjny: między indywidualnym aktem administracyjnym a aktem normatywnym*, Wolters Kluwer 2014.

terminem; tym bardziej nie będzie to możliwe w przypadku polecenia zabezpieczającego, gdzie istotny będzie czas reakcji na trwający incydent krytyczny;

- 4) art. 81 – z uwagi na rodzajowe określenie strony należy wyłączyć przepis o domniemaniu udowodnienia danego faktu, jeżeli strona miała możliwość wypowiedzenia się co do przeprowadzonych dowodów;
- 5) art. 81a – z uwagi na rodzajowe określenie strony należy wyłączyć przepis o zasadzie rozstrzygania wątpliwości faktycznych na korzyść strony;
- 6) art. 107 § 1 pkt 3 – wyłącza się przepis o wskazaniu strony w treści decyzji administracyjnej; w zamian w poleceniu zabezpieczającym będzie określony rodzaj podmiotów, do których skierowane będzie polecenie;
- 7) art. 145 § 1 pkt 4 – wyłącza się przepis o możliwości wznowienia postępowania, jeżeli strona nie brała z własnej winy udziału w postępowaniu – w przypadku decyzji generalnych, gdzie strona jest ustalona rodzajowo nie jest możliwe zapewnienie czynnego udziału wszystkim podmiotom, na których ten akt ma wpływ, stąd należy wyłączyć ten przepis, aby nie powstała podstawa do wzruszania tego aktu;
- 8) art. 156 § 1 pkt 4 – wyłącza się przepis o obowiązku stwierdzenia nieważności decyzji która została skierowana do osoby niebędącej stroną w sprawie – strona w przypadku decyzji generalnej jest określona rodzajowo.

Zawiadomienia w sprawie będą doręczane poprzez publiczne obwieszczenie na stronie podmiotowej ministra właściwego do spraw informatyzacji w BIP. Samo polecenie zabezpieczające będzie ogłoszone w dzienniku urzędowym ministra właściwego do spraw informatyzacji jako załącznik do komunikatu ministra oraz na stronie podmiotowej ministra w BIP lub na stronie internetowej urzędu obsługującego ministra.

Wskazane w poleceniu zabezpieczającym określone zachowanie ma być adekwatne do sytuacji – minister nie będzie mógł więc arbitralnie wskazać zachowania, tylko wybrać takie, które w świetle analizy, będzie proporcjonalne do sytuacji wywołanej incydem krytycznym.

Ze względu na fakt, że w dodawanym w ustawie o KSC art. 67g wprowadzona została decyzja generalna skierowana do bliżej nieokreślonego kręgu podmiotów, konieczne było wprowadzanie również kwestii precyzujących niektóre aspekty postępowania sądowo administracyjnego. Ze względu na specyfikę tej decyzji zdecydowano się wyraźnie wskazać,

że sąd administracyjny zarządza połączenie wszystkich oddzielnych spraw toczących się przed nim w celu ich łącznego rozpoznania i rozstrzygnięcia. Ma to ułatwić stosowanie tych przepisów oraz zapobiec powstaniu wątpliwości w zakresie postępowania ze skargami na decyzję stanowiącą polecenie zabezpieczające.

Rygor natychmiastowej wykonalności polecenia zabezpieczającego jest jedyną rzeczą, która zapewni skuteczne działanie tego środka prawnego i szybkie podjęcie działań ograniczających skutki incydentu krytycznego. Przykłady cyberataków m.in. związane z oprogramowaniem firmy SolarWinds, czy wykorzystujących niewykryte wcześniej podatności w programie Microsoft Exchange Server, dobitnie pokazują jak kluczowa w reagowaniu na takie ataki jest szybkość podjęcia działań mitygujących ryzyka i ograniczających skutki ataku. Jak krytyczne jest dokonywanie natychmiastowych aktualizacji oprogramowania pokazuje właśnie przykład podatności w przypadku produktu firmy Microsoft. Podatności, nie naprawione w porę natychmiast wykorzystali cyberprzestępcy, którzy mieli możliwość m.in. czytania wewnętrznej korespondencji mailowej.

Wyłączone zostały przepisy o ponownym rozpatrzeniu sprawy przez organ. Decyzja ta będzie oparta na specjalistycznej analizie opracowanej w warunkach wystąpienia incydentu krytycznego. Nie jest zasadne ponowne angażowanie osób w przeprowadzenie takiej analizy, w przypadku gdy wystąpiła znaczna szkoda dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi. Priorytetem w takiej sytuacji musi być podjęcie odpowiednich działań naprawczych. Prawa strony są odpowiednio chronione poprzez instytucję skargi do sądu administracyjnego.

Polecenie zabezpieczające wydaje się na czas koordynacji obsługi incydentu krytycznego lub na czas oznaczony, nie dłużej niż na dwa lata, a wygasa z dniem wskazanym w ogłoszeniu o zakończeniu koordynacji obsługi incydentu w dzienniku urzędowym ministra właściwego do spraw informatyzacji lub po upływie czasu, na które zostało wydane.

Wprowadzenie do polskiego porządku prawnego polecenia zabezpieczającego jest konieczne dla zapewnienia bezpieczeństwa narodowego, ponieważ cyberataki są coraz częstsze i coraz bardziej niebezpieczne. Należy podkreślić, że są one dokonywane zarówno przez zwykłych przestępców jak i sprawców powiązanych z określonymi państwami, którzy dysponują znaczną wiedzą i zasobami. Państwo zawczasu musi mieć odpowiednie prawne środki reakcji na incydenty krytyczne, aby bronić swojego społeczeństwa i gospodarki przed

skutkami tych incydentów. Polecenie zabezpieczające będzie skutecznym środkiem przeciwdziałania incydentom krytycznym. Będzie miało charakter proporcjonalny do cyberzagrożenia. Wpłynie ono wyłącznie w niezbędnym zakresie na swobodę działalności gospodarczej, aby uchronić kluczowe podmioty przed skutkami incydentu krytycznego, który jak wspomniano wyżej, w bardzo poważny sposób zagraża obywatelom, gospodarce czy szerzej bezpieczeństwu narodowemu. Katalog zachowań możliwych do nałożenia w drodze polecenia zabezpieczającego zostanie ustawowo ograniczony. Ponadto minister będzie zobligowany wybrać zachowanie adekwatne do cyberzagrożenia, jakie stwarza incydent krytyczny. Dlatego projektodawca jest zdania, że nie narusza ono istoty swobody działalności gospodarczej, a także jest ono proporcjonalne sensu stricto.

Z uwagi na konstytucyjną niezależność Narodowego Banku Polskiego nie będą do niego stosowały się przepisy dotyczące wycofania produktów ICT, usług ICT lub procesów ICT pochodzących od dostawcy wysokiego ryzyka. Minister właściwy do spraw informatyzacji będzie informował Prezesa Narodowego Banku Polskiego o wydaniu decyzji o uznaniu danego dostawcy za dostawcę wysokiego ryzyka. Prezes Narodowego Banku Polskiego zdecyduje zatem czy wycofa produkty ICT, usługi ICT oraz procesy ICT wskazane w decyzji o uznaniu dostawcy za dostawcę wysokiego ryzyka.

Dodano opcjonalną możliwość przekazania zadań zespołów CSIRT, określonych w art. 26 ustawy o KSC, Ministrowi Obrony Narodowej. Decyzję w tej sprawie podejmie Prezes Rady Ministrów, działając na podstawie rekomendacji Kolegium oraz w uzgodnieniu z Ministrem Obrony Narodowej. W decyzji zostaną określone m.in. zakres, czas powierzenia zadań, a także fakultatywnie szczegóły współpracy z CSIRT MON, CSIRT NASK i CSIRT GOV. Zadania te będą realizowane przez Ministra Obrony Narodowej za pomocą jego jednostek podległych lub przez niego nadzorowanych. Komunikat o powierzeniu realizacji zadań będzie ogłaszany w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski” przez Prezesa Rady Ministrów. Ponadto celem poinformowania podmiotów krajowego systemu cyberbezpieczeństwa informacja o komunikacie będzie udostępniana na stronach internetowych CSIRT MON, CSIRT NASK, CSIRT GOV lub w BIP na stronie podmiotowej Pełnomocnika.

2.29. Przepisy o karach pieniężnych

Zmiany poczynione w przepisach z zakresu kar pieniężnych obejmują dostosowanie katalogu kar w związku z nowymi obowiązkami jakim podlegają podmioty kluczowe lub podmioty

ważne. Przewidziano także możliwość nałożenia kary na podmiot, który nie wyznaczył osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami kluczowymi i podmiotami ważnymi lub na podmiot, który nie zapewnia użytkownikowi usługi dostępu do wiedzy pozwalającej na zrozumienie cyberzagrożeń i stosowanie skutecznych sposobów zabezpieczenia się przed tymi zagrożeniami w zakresie związanym ze świadczonymi usługami. Możliwość wymierzenia kary aktualizuje się wtedy, gdy przemawia za tym waga i znaczenie naruszonych przepisów. Doprecyzowano również, że karze pieniężnej podlegają podmioty kluczowe lub podmioty ważne także wtedy, gdy ich działanie lub zaniechanie ma charakter jednorazowy. Taki przepis pozwoli wyeliminować wątpliwości co do tego, czy np. niewykonywanie obowiązku musi mieć charakter ciągły lub powtarzalny, żeby wypełniało to znamiona czynu, za który nałożona może zostać kara pieniężna.

Dążąc do zapewnienia, że kary określone w ustawie będą skuteczne, proporcjonalne i odstraszające, określono minimalną wysokość kary na poziomie 20 000 zł w przypadku podmiotów kluczowych oraz 15 000 zł w przypadku podmiotów ważnych. Co do zasady jednak kara nie może przekroczyć 10 000 000 euro wyrażonej w złotych i ustalonej przy zastosowaniu kursu średniego ogłaszanego przez Narodowy Bank Polski obowiązującego w dniu wydania decyzji o wymierzeniu kary lub 2% przychodów osiągniętych przez podmiot kluczowy z działalności gospodarczej w roku obrotowym poprzedzającym wymierzenie kary. W przypadku kar nakładanych na podmioty ważne jej wysokość nie może przekroczyć 7 000 000 euro wyrażonej w złotych i ustalonej przy zastosowaniu kursu średniego ogłaszanego przez Narodowy Bank Polski obowiązującego w dniu wydania decyzji o wymierzeniu kary lub 1,4% przychodów osiągniętych przez ten podmiot z działalności gospodarczej w roku obrotowym poprzedzającym wymierzenie kary. Zastosowanie ma kara wyższa. Określenie granic wymiaru kary pieniężnej w powyższy sposób pozwala na miarkowanie represji, włącznie z jej ograniczaniem do minimum w uzasadnionych przypadkach. Tak szeroki zakres kar umożliwi indywidualne i adekwatne – zarówno surowe jak i łagodne – karanie podmiotów, które dopuszczają się naruszeń.

Przewidziano także sytuację, w której okres wykonywania działalności gospodarczej jest krótszy niż 12 miesięcy albo podmiot w ogóle nie osiągnął przychodu. W takiej sytuacji podstawą wymiaru kary w przypadku podmiotów kluczowych jest równowartość kwoty 500 000 euro, wyrażona w złotych i ustalana przy zastosowaniu kursu średniego ogłaszanego przez Narodowy Bank Polski obowiązujący w dniu wydania decyzji o wymierzeniu kary. W przypadku podmiotów ważnych jest to równowartość kwoty 250 000 euro.

Określając wymiar kary niezwykle istotną rolę odgrywają przychody osiągnięte przez podmiot z działalności gospodarczej w roku obrotowym poprzedzającym wymierzenie kary. Zdecydowano się na przyjęcie kategorii roku obrotowego z tego względu, że kara nakładana w powiązaniu z tym przychodem w większym stopniu uwzględnia sytuację majątkową podmiotu istniejącą w chwili wydania decyzji o nałożeniu kary. Zapewniono w ten sposób również zgodność z brzmieniem dyrektywy NIS 2.

W sytuacji, w której zidentyfikowane zostanie, że podmiot kluczowy albo podmiot ważny narusza przepisy ustawy, a przy tym powoduje bezpośrednie i poważne zagrożenie cyberbezpieczeństwa dla obronności, bezpieczeństwa państwa, bezpieczeństwa i porządku publicznego lub życia i zdrowia ludzi lub zagrożenie wywołania poważnej szkody majątkowej lub poważnych utrudnień w świadczeniu usług, organ właściwy nakłada karę w wysokości do 100 000 000 zł. Zwiększenie wymiaru kary w stosunku do obecnie obowiązujących przepisów wynika z nadrzędnego celu kar pieniężnych jaki określa implementowana dyrektywa NIS 2, a także z wagi tego naruszenia, które może mieć poważne skutki – również z punktu widzenia obecnej sytuacji międzynarodowej. Należy bowiem mieć na uwadze fakt, że przez długi czas, tj. od dnia 21 lutego 2022 r. utrzymywany był trzeci stopień alarmowy CRP (CHARLIE-CRP), co świadczy o wysokim stopniu zagrożenia bezpieczeństwa narodowego związanego z zagrożeniami w cyberprzestrzeni. Stopień ten jest wprowadzany w przypadku wystąpienia zdarzenia potwierdzającego prawdopodobny cel ataku o charakterze terrorystycznym w cyberprzestrzeni albo uzyskania wiarygodnych informacji o planowanym zdarzeniu. Aktualnie do dnia 30 listopada 2025 r. na całym terytorium Rzeczypospolitej Polskiej obowiązuje drugi stopień alarmowy CRP (BRAVO-CRP), który może być wprowadzony w przypadku zaistnienia zwiększonego i przewidywalnego zagrożenia wystąpieniem zdarzenia o charakterze terrorystycznym w cyberprzestrzeni, jednak konkretny cel ataku nie został zidentyfikowany.

Z tego względu każde naruszenie przepisów, które spełnia powyżej wskazane przesłanki, może wiązać się z poważnymi konsekwencjami dla państwa i jego obywateli, a tym samym powinno być obarczone odpowiednio wysoką sankcją, która będzie spełniać funkcję zarówno prewencyjną jak i represyjną. Oznacza to, że kara pieniężna ma odstraszać od kolejnych naruszeń i w związku z tym być odpowiednio dolegliwa. Jednocześnie należy wskazać, że w związku z zakazem podwójnego karania za te same naruszenia, organ właściwy do spraw cyberbezpieczeństwa może nałożyć wyłącznie jedną karę pieniężną. Oznacza to, że jeśli naruszenie wypełni znamiona określone w art. 73 ust. 5 ustawy o KSC, to organ właściwy

do spraw cyberbezpieczeństwa powinien nałożyć wyłącznie karę za to naruszenie, nie wymierzając już kary przewidzianej na zasadach ogólnych.

Za niewykonywanie obowiązków określonych w ustawie karze pieniężnej może podlegać także kierownik podmiotu kluczowego lub podmiotu ważnego. Co więcej, kara może zostać nałożona na kierownika podmiotu niezależnie od tego czy została nałożona na podmiot kluczowy lub podmiot ważny. Proponuje się, żeby kara mogła być wymierzona w kwocie nie większej niż 300% otrzymywanego przez ukaranego wynagrodzenia obliczanego według zasad obowiązujących przy ustalaniu ekwiwalentu pieniężnego za urlop. Wymierzając karę organ właściwy do spraw cyberbezpieczeństwa powinien kierować się w szczególności możliwościami finansowymi kierownika podmiotu.

W przypadku podmiotów kluczowych lub podmiotów ważnych, będących podmiotami publicznymi maksymalna wysokość kary dla kierownika podmiotu będzie mogła wynieść 100% otrzymywanego przez ukaranego wynagrodzenia obliczanego według zasad obowiązujących przy ustalaniu ekwiwalentu pieniężnego za urlop. Podkreślenia wymaga, że jeżeli taki podmiot kwalifikuje się także do innego sektora, niż sektor podmiotów publicznych, to wobec kierownika takiego podmiotu maksymalna wysokość kary może wynieść 300% otrzymywanego wynagrodzenia.

Kary pieniężne nakładane są przez organ właściwy do spraw cyberbezpieczeństwa w drodze decyzji. Decyzja ta co do zasady nie jest natychmiastowo wykonalna z wyjątkiem sytuacji, w której wymaga tego ochrona bezpieczeństwa lub porządku publicznego. Może mieć to miejsce w szczególności gdy organ właściwy do spraw cyberbezpieczeństwa, po analizie naruszenia na podstawie kryteriów określonych w projektowanym art. 53 ust. 12 ustawy o KSC, uzna, że naruszenie to ma charakter na tyle poważny, że decyzja o wymierzeniu kary zasługuje na nadanie klauzuli natychmiastowej wykonalności. Kolejnym przykładem, w którym przesłanki bezpieczeństwa lub porządku publicznego mogą zostać zrealizowane, to okresowe kary pieniężne. Można bowiem wyobrazić sobie sytuację, w której brak podjęcia czynności określonych przez organ właściwy do spraw cyberbezpieczeństwa w decyzji będzie wiązał się z istotnym zagrożeniem dla bezpieczeństwa lub porządku publicznego, które należy oceniać sytuacyjnie pod względem wewnętrznym jak i zewnętrznym. Podkreślić należy, że dążąc do zapewnienia bezpieczeństwa lub porządku publicznego działania podejmowane przez organ nie mogą polegać wyłącznie na zwalczaniu zagrożeń, które już się zrealizowały, ale wymaga to podejmowania działań prospektywnych. W takiej sytuacji nadrzędną wartością będzie zapewnienie skuteczności wymierzonych kar co w pełni zagwarantuje nałożenie

klauzuli natychmiastowej wykonalności na decyzję w przedmiocie wymierzenia okresowej kary pieniężnej.

Wpływy z tytułu kar pieniężnych stanowią przychód Funduszu Cyberbezpieczeństwa, o którym mowa w art. 2 ustawy z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1662 oraz z 2025 r. poz. 1017).

Organ właściwy do spraw cyberbezpieczeństwa ustalając wysokość kary i wydając decyzję o wymierzeniu kary pieniężnej zobowiązany jest do uwzględniania kryteriów określonych w projektowanym art. 53 ust. 12 ustawy o KSC oraz wysokości przychodu uzyskanego z działalności gospodarczej w roku obrotowym poprzedzającym wymierzenie kary, możliwości finansowych podmiotu kluczowego lub podmiotu ważnego będącego podmiotem publicznym albo możliwości finansowych kierownika podmiotu. Z tego powodu konieczne jest, aby podmiot kluczowy lub podmiot ważny, na żądanie organu właściwego do spraw cyberbezpieczeństwa, przekazał wszelkie niezbędne do wymierzenia kary dane. Chcąc jednocześnie zapobiec sytuacji, w której organ nie będzie mógł wymierzyć kary z powodu braku wykonania polecenia przez podmiot, organ ten będzie uprawniony do ustalenia podstawy wymiaru kary pieniężnej w sposób szacunkowy. W tym celu może skorzystać z ogólnodostępnych danych oraz wziąć pod uwagę specyfikę działalności podmiotu i jego wielkość. W przypadku podmiotów kluczowych lub podmiotów ważnych będących podmiotami publicznymi ich możliwości finansowe ustala się przede wszystkim biorąc pod uwagę środki finansowe w części budżetowej przeznaczonych dla danego podmiotu.

Jednocześnie wyłączeniu ulegnie art. 189a § 2 Kpa, co oznacza, że podmiot przy wymiarze kary poza przesłankami, na które wskazuje projekt ustawy powinien kierować się także dyrektywami wymiaru kary wskazanymi w art. 189d Kpa. Szczególne znaczenie przypadku kary nałożonej na kierownika podmiotu będzie miał stopień przyczynienia się kierownika podmiotu do powstania naruszenia prawa. Oznacza to, że np. w przypadku znikomego przyczynienia się (zawinienia) kierownika podmiotu będzie mogła zostać wymierzona niska kara (jeśli całokształt sytuacji zbadany według pozostałych przesłanek również będzie na to wskazywał), a nawet będzie można odstąpić od nałożenia kary, jeśli spełnione zostaną odpowiednie warunki.

Organ właściwy do spraw cyberbezpieczeństwa może odstąpić od nałożenia kary pieniężnej, o której mowa w art. 73 lub dodawanym art. 73a ustawy o KSC, w sytuacji, w której waga

i znaczenie naruszonych przepisów jest znikome, a podmiot albo kierownik podmiotu zaprzestał naruszania prawa lub naprawił wyrządzoną szkodę.

Istotną zmianą jest wprowadzenie możliwości nakładania na podmiot okresowej kary pieniężnej. Będzie to możliwe w sytuacji, w której podmiot opóźnia się z wykonaniem czynności określonych w decyzji wydanych na podstawie art. 53 ust. 5 pkt 2–8 ustawy o KSC. Za każdy dzień opóźnienia organ właściwy do spraw cyberbezpieczeństwa będzie mógł nałożyć karę pieniężną w wysokości od 500 zł do 100 000 zł. Należy zwrócić uwagę, że okresowa kara pieniężna różni się od kary nakładanej w artykułach poprzedzających tym, że karane nie jest samo naruszenie przepisów ustawy, a zwłoka w wykonaniu czynności zleconych przez organ, często w związku z tym naruszeniem. Okresowa kara pieniężna ma stanowić zatem narzędzie do efektywnego egzekwowania stosowania przepisów ustawy i wykonywania nałożonych na podmioty obowiązków.

Kara pieniężna jest także, zgodnie z wdrażaną dyrektywą NIS 2, środkiem nadzorczym, który może być stosowany niezależnie, a więc równolegle, do innych środków nadzorczych. Nałożenie kary pieniężnej na podmiot kluczowy lub podmiot ważny nie oznacza zatem, że organ właściwy do spraw cyberbezpieczeństwa nie może podjąć innych działań o charakterze nadzoru czy kontroli.

Doprecyzowano także, że w zakresie nieuregulowanym w rozdziale stanowiącym o karach stosuje się odpowiednio przepisy działu IVa Kpa.

2.30. Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej

Wprowadzono zmiany w przepisach dotyczących Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej, co bezpośrednio wynika z dyrektywy NIS 2. Zakres Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej został rozszerzony i uszczegółowiony, tak aby obejmował wszystkie kwestie kluczowe dla zapewnienia cyberbezpieczeństwa. Zmiana ta pozwoli zaadresować w tym dokumencie nowe istotne zagadnienia takie jak bezpieczeństwo łańcucha dostaw. Zmiana ta pozwoli też na uspoźnienie dokumentów w poszczególnych państwach członkowskich.

Strategia ma obejmować wszystkie sektory, w których znajdują się podmioty kluczowe i podmioty ważne.

Równocześnie ze Strategią Cyberbezpieczeństwa Rzeczypospolitej Polskiej będzie przygotowany plan działań do Strategii, który będzie stanowił jej załącznik i operacjonalizował jej zapisy, w tym uwzględniał koszty realizacji i źródła finansowania działań.

Strategię określa się na okres 5 lat ale również zapewnia się możliwość wprowadzenia w tym okresie zmian w Strategii w wyniku jej przeglądu. Okres 5 lat jest okresem, gdzie można już przeanalizować skutki długofalowych działań.

Dostosowano przepisy proceduralne dotyczące opracowania projektu Strategii – przy jej opracowaniu będzie brała udział Komisja Nadzoru Finansowego jako organ właściwy w rozumieniu rozporządzenia 2022/2554.

Ponadto dodany został przepis pozwalający ministrowi właściwemu do spraw informatyzacji, będącemu organem odpowiedzialnym za realizację Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej, uzyskiwać informacji o realizacji strategii od innych podmiotów zaangażowanych w jej realizację. Pozwoli to ministrowi na uzyskanie bieżących informacji o realizowanych zadaniach i na ewentualne podjęcie dodatkowych działań w danym obszarze. Wskazano również, że zespoły CSIRT poziomu krajowego, CSIRT sektorowe i organy właściwe do spraw cyberbezpieczeństwa będą corocznie informować ministra o postępach we wdrażaniu strategii.

Pozwoli to na skuteczniejszą realizację zadań z zakresu cyberbezpieczeństwa oraz bieżącą ocenę stanu realizacji Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej.

Wprowadza się obowiązek przeglądu i oceny skuteczności strategii nie rzadziej niż co 2 i pół roku. Proces ten ma prowadzić minister właściwy do spraw informatyzacji we współpracy z Pełnomocnikiem, innymi ministrami i właściwymi kierownikami urzędów centralnych w przegląd powinny być zaangażowane więc m. in. organy właściwe do spraw cyberbezpieczeństwa. W wyniku przeglądu i oceny Strategii powinien powstać dokument wskazujący kto dokonał przeglądu, kto był zaangażowany w przegląd i ocenę, kiedy przegląd i ocena miały miejsce, jakie problemy z realizacją strategii napotkano w praktyce, które elementy strategii są oceniane jako skuteczne, które są oceniane jako mniej skuteczne oraz podsumowanie zawierające wnioski.

2.31. Krajowy Plan reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę

Zgodnie z dyrektywą NIS 2 przyjęte zostały przepisy wprowadzające Krajowy Plan reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę, zwany dalej „Krajowym Planem”. Będzie to dokument strategiczny określający rolę organów, środki i procedury w przypadku wystąpienia sytuacji kryzysowej związanej z cyberbezpieczeństwem. Dokument ten ma posłużyć koordynacji działań z zakresu zapewniania cyberbezpieczeństwa i zarządzania kryzysowego w celu maksymalizacji ich efektywności.

Dokument ten będzie przyjmowany w drodze uchwały Rady Ministrów, a przygotowywany przez ministra właściwego do spraw informatyzacji. Dużą rolę w jego przygotowaniu będzie odgrywać również Rządowe Centrum Bezpieczeństwa gwarantując jego spójność z dokumentami z zakresu zarządzania kryzysowego.

Podobnie jak w przypadku Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej, minister będzie mógł zwracać się o informacje dotyczące realizacji Krajowego Planu do organów w nim wskazanych. Pozwoli mu to na bieżąco monitorować postępy we wdrażaniu Krajowego Planu i podejmować działania w razie wystąpienia nieprawidłowości.

2.32. Zmiany w podstawowych ustawach

Wprowadzone zmiany w zakresie podmiotów i funkcjonowania krajowego systemu cyberbezpieczeństwa wymagają również wprowadzenia zmian w szeregu innych ustaw. W szczególności nowelizacji wymagają poniższe ustawy.

2.32.1. Zmiany w ustawie z dnia 8 marca 1990 r. o samorządzie gminnym, ustawie z dnia 5 czerwca 1998 r. o samorządzie powiatowym oraz w ustawie z dnia 5 czerwca 1998 r. o samorządzie województwa

Zmiany w ustawach dotyczących ustroju samorządu terytorialnego mają na celu umożliwienie wspólnej obsługi podmiotów publicznych w zakresie cyberbezpieczeństwa przez spółki komunalne oraz żeby spółki komunalne mogły być obsługiwane przez centra usług wspólnych.

2.32.2. Zmiany w ustawie z dnia 21 marca 1991 r. o obszarach morskich Rzeczypospolitej Polskiej i administracji morskiej

Zmiany w ustawie z dnia 21 marca 1991 r. o obszarach morskich Rzeczypospolitej Polskiej i administracji morskiej (Dz. U. z 2024 r. poz. 1125 oraz z 2025 r. poz. 409) dotyczą wprowadzenia tam pojęcia usługi przetwarzania w chmurze, ponieważ obecna treść tej ustawy odwołuje się do obecnego załącznika nr 2 ustawy o KSC – a ten przepis jest zmieniany.

2.32.3. Zmiany w ustawie z dnia 24 sierpnia 1991 r. o Państwowej Straży Pożarnej

Zmiany w ustawie z dnia 24 sierpnia 1991 r. o Państwowej Straży Pożarnej (Dz. U. z 2024 r. poz. 1443, z późn. zm.) umożliwiają przyznanie strażakom wykonującym zadania z zakresu cyberbezpieczeństwa świadczenia teleinformatycznego. Funkcjonariusze, pracownicy korpusu służby cywilnej i pracownicy cywilni zatrudnieni w Państwowej Straży Pożarnej, analogicznie jak np. funkcjonariusze i osoby zatrudnione w Policji czy Straży Granicznej, w zakresie działania swoich organów realizują zadania z zakresu cyberbezpieczeństwa i ujęcie ich w art. 5 jest jak najbardziej wskazane i uzasadnione

2.32.4. Zmiany w ustawie z dnia 20 sierpnia 1997 r. o Krajowym Rejestrze Sądowym

Zmiany w tym akcie mają charakter dostosowujący, związany z ujawnianiem w Krajowym Rejestrze Sądowym informacji o tymczasowym zakazie pełnienia funkcji zarządczych w podmiocie kluczowym. Pozostają również w związku z nowym zadaniem organów właściwych do spraw cyberbezpieczeństwa w zakresie prowadzenia wykazu (projektowany art. 42 ust. 12). Nadrzędnym celem zmian jest jednak konieczność dochowania wymogów dyrektywy 2017/1132⁸⁷⁾ (zmienionej dyrektywą 2019/1151), która jest implementowana w przepisie art. 4d ustawy o KRS. Rzeczpospolita Polska ma obowiązek informowania w ramach Unii Europejskiej o nałożonych na osoby zakazach pełnienia funkcji kierowniczych. Dotyczy to także zakazów w ramach jednego podmiotu. Zaproponowane w ustawie zmiany pozwolą zachować pewność obrotu i skuteczność w wywiązywaniu się Polski ze zobowiązań wynikających z prawa Unii Europejskiej.

W przypadku powiadomienia sądu rejestrowego (w trybie art. 21 ust. 1 ustawy o KRS) przez organ właściwy do spraw cyberbezpieczeństwa o zastosowaniu środka, o którym mowa w art. 53 ust. 9 pkt 6 ustawy o KSC, sąd rejestrowy dokona z urzędu wpisu na podstawie art. 24 ust. 6 ustawy o KRS. Przepis ten stanowi bowiem, że w przypadkach uzasadnionych bezpieczeństwem obrotu sąd rejestrowy może dokonać z urzędu wykreślenia danych

⁸⁷⁾ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2017/1132 z dnia 14 czerwca 2017 r. w sprawie niektórych aspektów prawa spółek (Dz. Urz. UE L 169 z 30.06.2017, str. 46-127, z późn. zm.).

niezgodnych z rzeczywistym stanem rzeczy lub wpisu danych odpowiadających rzeczywistemu stanowi rzeczy, jeżeli dokumenty stanowiące podstawę wpisu lub wykreślenia znajdują się w aktach rejestrowych, a dane te są istotne. Dokumentem stanowiącym podstawę wpisu w trybie art. 24 ust. 6 ustawy o KRS będzie odpis decyzji organu ds. cyberbezpieczeństwa przesłany do właściwego sądu rejestrowego w ramach informacji w trybie art. 21 ust. 1 ustawy o KRS.

2.32.5. Zmiany w ustawie z dnia 29 sierpnia 1997 r. – Ordynacja podatkowa

Zmiany w ww. ustawie dotyczą umożliwienia Szefowi Krajowej Administracji Skarbowej przekazywania informacji organom właściwym do spraw cyberbezpieczeństwa oraz Zespołowi Reagowania na Incydenty Bezpieczeństwa Komputerowego działającemu na poziomie krajowym, prowadzonemu przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy. Dane te są niezbędne do realizacji ustawowych zadań tych podmiotów, a w szczególności do oceny czy dany podmiot spełnia przesłanki bycia podmiotem kluczowym lub podmiotem ważnym oraz co do jego znaczenia w danym sektorze gospodarki.

2.32.6. Zmiany w ustawie z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych

Zmiany w ustawie z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych (Dz. U. z 2025 r. poz. 350, z późn. zm.) umożliwią organom właściwym do spraw cyberbezpieczeństwa uzyskiwanie informacji o rocznej liczbie pracowników lub rocznej liczbie ubezpieczonych – co pozwoli na ustalenie wielkości przedsiębiorcy, a co za tym idzie statusu podmiotu kluczowego lub podmiotu ważnego.

2.32.7. Zmiany w ustawie z dnia 24 maja 2000 r. o Krajowym Rejestrze Karnym

Zmiana w ustawie z dnia 24 maja 2000 r. o Krajowym Rejestrze Karnym (Dz. U. z 2024 r. poz. 276 oraz z 2025 r. poz. 1235) umożliwi podmiotom kluczowym oraz podmiotom ważnym na złożenie zapytania do Krajowego Rejestru Karnego w sprawie weryfikacji niekaralności osoby zatrudnionej w podmiocie i realizującej zadania z zakresu cyberbezpieczeństwa. Ta ustawa dopuszcza obecnie sytuację, gdy to pracodawca może weryfikować niekaralność, jeżeli z przepisów odrębnych wynika wymóg niekaralności pracownika. Natomiast przy zadaniach z zakresu cyberbezpieczeństwa pojawiają się często inne stosunki zatrudnienia (B2B, umowy zlecenia, umowy o dzieło) stąd należało uzupełnić szerzej ten katalog.

2.32.8. Zmiany w ustawie z dnia 21 grudnia 2000 r. o dozorze technicznym

Zmiany w ustawie z dnia 21 grudnia 2000 r. o dozorze technicznym (Dz. U. z 2024 r. poz. 1194) pozwolą ministrowi właściwemu do spraw gospodarki powierzenie realizacji zadań CSIRT sektorowego dla sektorów produkcji, produkcji chemikaliów i przestrzeni kosmicznej Urzędowi Dozoru Technicznego, zwanego dalej „UDT”. Aby UDT mógł realizować zadania CSIRT sektorowego konieczna jest zmiana art. 37 ustawy o dozorze technicznym określającego zakres działania UDT. Zmiana dotyczy dopisania do katalogu zadań UDT wykonywanie zadań określonych w przepisach ustawy o KSC.

2.32.9. Zmiany w ustawie z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej

W drodze decyzji niepodlegającej ogłoszeniu, zostaną wydzielone z Dowództwa Komponentu Wojsk Obrony Cyberprzestrzeni oraz z jednostek podporządkowanych Dowódcy Komponentu Wojsk Obrony Cyberprzestrzeni zespoły specjalistów oraz zasoby materiałowe i sprzętowe, które będą podlegać Ministrowi Obrony Narodowej w przypadku mianowania Naczelnego Dowódcy Sił Zbrojnych i przejęcia przez niego dowodzenia Siłami Zbrojnymi. Takie rozwiązanie ma zapewnić, że w przypadku wprowadzenia stanu wojennego lub podobnej sytuacji, Minister Obrony Narodowej wciąż będzie dysponował personelem i zasobami niezbędnymi do realizacji ustawowych zadań.

2.32.10. Zmiany w ustawie z dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym

Zmiany w przedmiotowej ustawie polegają na uzupełnieniu strony przychodowej Urzędu Komisji Nadzoru Finansowego o dotacje z budżetu państwa, o których mowa w art. 42 ust. 9 oraz art. 44d ust. 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Są to dotacje na funkcjonowanie organu właściwego do spraw cyberbezpieczeństwa oraz CSIRT sektorowego dla sektora bankowości i infrastruktury rynków finansowych. Wskazano też, że z przychodów Urzędu Komisji Nadzoru Finansowego pokrywa się koszty funkcjonowania Urzędu Komisji i jego organów oraz koszty realizacji zadań Komisji wynikających z ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

2.32.11. Zmiany w ustawie z dnia 28 kwietnia 2011 r. o systemie i informacji w ochronie zdrowia

Zmiana w ustawie z dnia 28 kwietnia 2011 r. o systemie i informacji w ochronie zdrowia (Dz. U. z 2025 r. poz. 302 i 779) ma na celu likwidację odwołań do przepisów wykonawczych

wydanych na podstawie ustawy o informatyzacji podmiotów realizujących zadania publiczne. W praktyce przepis odwoływał się do wymogów systemu zarządzania bezpieczeństwem informacji zawartych w rozporządzeniu Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych. W zamian odwołanie będzie do art. 8 ustawy o krajowym systemie cyberbezpieczeństwa, który zawiera wymogi dla systemu zarządzania bezpieczeństwem informacji.

2.32.12. Zmiany w ustawie z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej

Zmiany w ustawie z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. z 2024 r. poz. 1725). Wprowadzono przepisy, które umożliwią administracji skorzystanie z informacji, które już zgromadziła a także uchylono przepisy, z których wynikały dotychczasowe obowiązki z zakresu cyberbezpieczeństwa dla dostawców usług zaufania – te obowiązki będą teraz wynikały ze znowelizowanej ustawy o KSC. Wynika to też z faktu, że dyrektywa NIS 2 uchyliła art. 19 rozporządzenia EIDAS dotyczący wymogów bezpieczeństwa dla dostawców usług zaufania. Ponadto przepis ma na celu likwidację odwołania do przepisów wykonawczych wydanych na podstawie ustawy o informatyzacji podmiotów realizujących zadania publiczne. W praktyce przepis odwoływał się do wymogów systemu zarządzania bezpieczeństwem informacji zawartych w rozporządzeniu Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. poz. 773). W zamian odwołanie będzie do art. 8 ustawy o krajowym systemie cyberbezpieczeństwa, który zawiera wymogi dla systemu zarządzania bezpieczeństwem informacji.

2.32.13. Zmiany w ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych

W ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781) wprowadza się zmiany w przepisie, który wskazuje przeznaczenie środków z kar nakładanych za naruszenie przepisów RODO). W przypadku kar nakładanych z tytułu naruszenia następujących przepisów RODO:

- 1) art. 5 ust. 1 lit. f (naruszenie integralności i poufności danych osobowych);
- 2) art. 25 ust. 1 i 2 (brak wdrożenia środków technicznych i organizacyjnych na etapie projektowania przetwarzania danych osobowych);

- 3) art. 28 ust. 3 lit. c (zapewnienie, że podmiot przetwarzający w imieniu administratora danych osobowych wdraża środki techniczne i organizacyjne zapewniające bezpieczeństwo danych osobowych);
- 4) art. 32 ust. 1 i 2 (brak wdrożenia środków technicznych i organizacyjnych zapewniających bezpieczeństwo danych osobowych).

Środki z powyższych kar w 50% będą stanowiły dochód budżetu państwa, a w 50% dochód Funduszu Cyberbezpieczeństwa. Powyższe przepisy dotyczą bezpieczeństwa danych osobowych i są pokrewne rozwiązaniom z dyrektywy NIS 2.

2.32.14. Zmiany w ustawie z dnia 11 września 2019 r. – Prawo zamówień publicznych

Wprowadza się również zmianę w art. 226 ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych (Dz. U. z 2024 r. poz. 1320, z późn. zm.). Artykuł ten reguluje sytuacje, w których zamawiający odrzuca ofertę złożoną w ramach postępowania o zamówienie publiczne. Kolejną przesłanką odrzucenia oferty będzie sytuacja, gdy oferta obejmuje produkt ICT, którego typ został określony w decyzji w sprawie uznania dostawcy za dostawcę wysokiego ryzyka, o której mowa w projektowanym art. 66a ust. 13 ustawy o KSC oraz usługę ICT lub proces ICT, określone w tej decyzji.

2.32. 15. Zmiany w ustawie z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa

Zmiany w ustawie z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa dotyczą:

- 1) dostosowania treści art. 5 ustawy i wskazanie, że świadczenie teleinformatyczne przysługuje pracownikom zatrudnionym w zespołach CSIRT sektorowych;
- 2) wskazanie, że świadczenie teleinformatyczne będzie przysługiwać również osobom realizującym zadania w zakresie zapewnienia cyberbezpieczeństwa w Urzędzie Ochrony Danych Osobowych⁸⁸⁾, w jednostkach organizacyjnych Krajowej

⁸⁸⁾ Urząd Ochrony Danych Osobowych sam musi również dbać o własne cyberbezpieczeństwo. W przeciwnym razie jego autorytet, jako urzędu obsługującego krajowy organ ochrony danych osobowych, ulegnie załamaniu. Poza tym Urząd Ochrony Danych Osobowych gromadzi dane w związku z postępowaniami nadzorczymi w sprawie kontroli stosowania przepisów o ochronie danych osobowych. Wyciek tych danych albo naruszenie integralności czy ich dostępności uniemożliwi realizację zadań Prezesa Urzędu Ochrony Danych Osobowych. Stąd też zasadne jest zapewnienie adekwatnych środków finansowych dla pracowników dbających o cyberbezpieczeństwo w Urzędzie Ochrony Danych Osobowych.

Administracji Skarbowej⁸⁹⁾, jednostkach Państwowej Straży Pożarnej⁹⁰⁾ oraz w sądach powszechnych⁹¹⁾, Generalnej Dyrekcji Dróg Krajowych i Autostrad, Głównym Inspektoracie Transportu Drogowego, instytutach badawczych nadzorowanych przez ministra właściwego do spraw gospodarki morskiej, gospodarki wodnej, transportu, żeglugi śródlądowej, Państwowym Gospodarstwie Wodnym Wody Polskie, Transportowym Dozorze Technicznym, Urzędzie do spraw Cudzoziemców, Urzędzie Lotnictwa Cywilnego, urzędzie morskim, Urzędzie Ochrony Danych Osobowych, urzędzie żeglugi śródlądowej;

- 3) uregulowania przychodu z kar pieniężnych, o których mowa w art. 101 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych, które staną się jednym z przychodów Funduszu Cyberbezpieczeństwa.

Zmiany te wpłyną na przychody Funduszu Cyberbezpieczeństwa co pozwoli na zwiększenie wsparcia udzielanego organom administracji na zapewnienie cyberbezpieczeństwa ich systemów informacyjnych.

Przewiduje się od 2026 r. wzrost kwoty dotacji przeznaczonej na zasilenie Funduszu Cyberbezpieczeństwa z budżetu państwa – kwota ta wzrośnie do 351,511 mln zł rocznie. Dzieje się tak z uwagi na wzrost liczby podmiotów uprawnionych do otrzymywania tego wsparcia. Koszty te będą sfinansowane z cz. 27 budżetu państwa.

Ponadto do obsługi Funduszu Cyberbezpieczeństwa dodaje się 4 etaty w urzędzie obsługującym ministra właściwego do spraw informatyzacji. Dzieje się tak z uwagi na konieczność obsługi dużej liczby wniosków o udzielenie wsparcia z Funduszu Cyberbezpieczeństwa również wynikającej z dodania nowych rodzajów podmiotów uprawnionych do wnioskowania o środki z tego Funduszu.

⁸⁹⁾ Systemy informacyjne Krajowej Administracji Skarbowej (KAS) zawierają informacje o postępowaniach karno-skarbowych. KAS dba również o należyta ściągłość podatków. Incydent w jednostkach organizacyjnych KAS może negatywnie wpłynąć na przychody budżetu państwa. Stąd też zasadne jest zapewnienie adekwatnych środków finansowych dla pracowników i funkcjonariuszy KAS dbających o cyberbezpieczeństwo w KAS.

⁹⁰⁾ W Państwowej Straży Pożarnej funkcjonuje system SWD PSP umożliwiający rejestrację zdarzeń i wspomagający dowodzenie jednostkami Państwowej Straży Pożarnej w tym dysponowanie jednostkami do zdarzeń czy sporządzaniem dokumentacji. Incydent w jednostkach organizacyjnych Państwowej Straży Pożarnej negatywnie wpływa na możliwość działania PSP w ramach Krajowego Systemu Ratowniczo-Gaśniczego. Stąd też zasadne jest zapewnienie adekwatnych środków finansowych dla pracowników i funkcjonariuszy PSP dbających o cyberbezpieczeństwo w PSP.

⁹¹⁾ Sądy powszechne przetwarzają w swoich systemach informacyjnych wrażliwe dane dotyczące postępowań sądowych. Ponadto podejmowane są dalsze reformy w zakresie informatyzacji sądów. Stąd też istotne jest zapewnienie adekwatnych wynagrodzeń dla pracowników dbających o cyberbezpieczeństwo w sądach powszechnych.

Koszty te będą sfinansowane z cz. 27 budżetu państwa. W związku z tym skorygowano regułę wydatkową w tej ustawie dodając do obecnej kwoty wynoszącej 250 mln zł – koszty zwiększenia wydatków.

2.32.16. W ustawie z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej

Zmiany w ustawie z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej (Dz. U. z 2024 r. poz. 1803) są wynikiem zmiany definicji podmiotu publicznego w ustawie o KSC.

2.32.17. Zmiany w ustawie z dnia 12 lipca 2024 r. – Prawo komunikacji elektronicznej

Ustawa z dnia 12 lipca 2024 r. – Prawo komunikacji elektronicznej (Dz. U. poz. 1221 oraz z 2025 r. poz. 637 i 820) w art. 40 w ust. 1 w pkt 2 w lit b pozwala Prezesowi Urzędu Komunikacji Elektronicznej w sytuacji szczególnego zagrożenia nałożenie w drodze decyzji na przedsiębiorcę telekomunikacyjnego obowiązków dotyczących odtwarzania dostarczania publicznych sieci telekomunikacyjnych lub przywrócenia świadczenia publicznie dostępnych usług telekomunikacyjnych, z uwzględnieniem pierwszeństwa m. in. dla operatorów usług kluczowych. Pojęcie operatorów usług kluczowych zastępuje się pojęciem podmiotów kluczowych.

23. 12. 18. W ustawie z 12 lipca 2024 r. – Przepisy wprowadzające ustawę – Prawo komunikacji elektronicznej

Poprzez przepis art. 68 ust. 3 ustawy z dnia 12 lipca 2024 r. – Przepisy wprowadzające ustawę – Prawo komunikacji elektronicznej (Dz. U. poz. 1222) tymczasowo utrzymano w mocy przepisy ustawy - Prawo telekomunikacyjne⁹²⁾, zawierające wymogi bezpieczeństwa sieci i usług telekomunikacyjnych do czasu pełnego wdrożenia dyrektywy NIS 2. Rozwiązanie to miało zapewnić, że nie powstanie luka w wymogach bezpieczeństwa dla przedsiębiorców telekomunikacyjnych między wejściem w życie Prawa komunikacji elektronicznej a wejściem w życie przepisów wdrażających dyrektywę NIS 2. Dla zapewnienia jednolitości systemu prawa należy uchylić art. 68 ust. 3 ustawy z dnia 12 lipca 2024 r. – Przepisy wprowadzające ustawę – Prawo komunikacji elektronicznej.

⁹²⁾ Konkretnie chodzi o przepisy art. 1 ust. 1 pkt 2, art. 2 pkt 1, 17, 27, 29, 31, 35, 41, 43, 46, 48, 49i 52, art. 9, art. 160 ust. 1 i 2, działu VIIa oraz art. 209 ust. 1 pkt 25a, 271 i 27a ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne.

2.33. Przepisy przejściowe, dostosowujące i końcowy

Projekt ustawy wskazuje, że postępowania karnoadministracyjne oraz kontrole wszczęte i niezakończone przed dniem wejścia w życie ustawy zostaną ukończone na podstawie przepisów dotychczasowych. Gwarantuje to, że podmioty, których te postępowania dotyczą nie zostaną zaskoczone nowymi zasadami i pozwoli zakończyć te postępowania w odpowiednim terminie. Dotychczasowe przepisy mają zastosowanie również do rozpoczętej obsługi incydentu, ponieważ w przypadku wystąpienia incydentu istotne jest postępowanie zgodnie z ustalonymi procedurami. Projektowane przepisy dotyczące obsługi incydentu wprowadziły szereg nowych obowiązków nałożonych na podmiot m.in. obowiązek sporządzenia raportu końcowego, dlatego też zdecydowano by trwające incydenty zostały obsługiwane na dotychczasowych zasadach. Pozwoli to uniknąć sytuacji, w której podmioty musiałyby zmieniać swoje wewnętrzne procedury przy jednoczesnym zwalczaniu skutków incydentu, co w znacznym stopniu mogłoby utrudnić prawidłową obsługę incydentu. Zachowane w mocy zostały rekomendacje Pełnomocnika, dotyczących stosowania urządzeń informatycznych lub oprogramowania, co wynika z zastosowania nowych przepisów do badań rozpoczętych i niezakończonych na podstawie obecnie obowiązującego art. 33 ust. 1 ustawy o KSC.

Minister właściwy do spraw informatyzacji uruchomi rejestr podmiotów kluczowych i podmiotów ważnych w ciągu miesiąca od dnia wejścia w życie ustawy. Rejestr będzie prowadzony elektronicznie w związku z czym taki termin gwarantuje czas niezbędny na jego uruchomienie i odpowiednie zabezpieczenie. Minister właściwy do spraw informatyzacji w komunikacie ogłoszonym w dzienniku urzędowym ministra właściwego do spraw informatyzacji określi termin złożenia wniosków o wpis do wykazu podmiotów kluczowych i podmiotów ważnych przez podmioty kluczowe i podmioty ważne oraz rozpoczęcia korzystania z systemu teleinformatycznego, o którym mowa w art. 46 ustawy o KSC.

W przepisach przejściowych rozstrzygnięto, że podmioty mające obecnie status operatorów usług kluczowych w momencie wejścia w życie ustawy zostaną również automatycznie wpisane na listę podmiotów kluczowych. Jest to niezbędne dla zapewnienia ciągłości realizowanych przez nie zadań, m.in. obsługi incydentów. Dzięki takiemu rozwiązaniu podmioty te nie będą również musiały przeprowadzać wewnętrznych analiz i dokonywać samoidentyfikacji co oszczędzi im czas. Należy podkreślić, że obecne przepisy dużo więcej definiują operatorów usług kluczowych niż wynika to z definicji podmiotów kluczowych.

W związku z czym nie ma wątpliwości, że podmioty te spełniają przesłanki dla podmiotów kluczowych.

W zakresie podmiotów świadczących usługi rejestracji nazw domen został zastosowany termin 6-miesięczny na dostosowanie baz danych oraz wdrożenie odpowiednich polityk i procedur. Nowe regulacje dotyczące tych podmiotów znacząco wpływają na ich działalność w związku z czym konieczne jest zapewnienie im odpowiedniego czasu na wprowadzenie niezbędnych rozwiązań technicznych.

Przepisy regulują przekazanie przez ministra właściwego do spraw informatyzacji danych dotyczących ilości podmiotów kluczowych i podmiotów ważnych i przepisów na podstawie których je zidentyfikowano w terminie do dnia 17 kwietnia 2025 r. do Komisji Europejskiej oraz Grupy Współpracy. Obowiązek ten wynika bezpośrednio z art. 3 ust. 5 dyrektywy NIS 2. Wykonanie tych przepisów pozwoli Komisji Europejskiej skutecznie oszacować liczbę podmiotów kluczowych i ważnych w całej Unii Europejskiej a następnie podejmować kolejne działania mające na celu zwiększenie ich cyberbezpieczeństwa. Minister właściwy do spraw informatyzacji przekaze też Komisji Europejskiej informacje dotyczące wyznaczenia krajowego organu do spraw zarządzania kryzysowego w cyberbezpieczeństwie. Do tych działań jesteśmy bezpośrednio zobligowani przepisami dyrektywy NIS 2.

Przepisy przewidują też rozszerzenie możliwości badania produktów przez zespoły CSIRT. Badaniu bezpieczeństwa nie mogą stać na drodze standardowe postanowienia licencji, które zakazują takich działań. Z tego względu w przepisach przejściowych dotyczących umów już obowiązujących konieczne były przesądzenie, że takie klauzule umowne utracą moc. Nie może być sytuacji by umowa cywilnoprawna uniemożliwiała organom państwa skuteczne działania w zakresie bezpieczeństwa.

W ramach zmian w funkcjonowaniu systemu teleinformatycznego S46 przewidziana jest rezygnacja z zawierania osobnych porozumień z przystępującymi obecnie podmiotami. Równocześnie w ramach tego systemu przyłączono już pewną liczbę podmiotów a ich prawa i obowiązki uregulowano w porozumieniach. W takim przypadku, dla zapewnienia efektywnej realizacji zadań zasadnym jest utrzymanie tych porozumień w mocy.

Dla zapewnienia ciągłości działań Kolegium konieczne jest utrzymanie w mocy rozporządzenia wydanego na podstawie art. 66 ust. 9 ustawy o KSC.

W dotychczasowym stanie prawnym CSIRT MON, CSIRT NASK i CSIRT GOV mogły zawierać porozumienia przekazujące określone podmioty do właściwości CSIRT innego niż

ten wskazany w ustawie. W związku ze zmianami w zakresie struktury podmiotowej krajowego systemu cyberbezpieczeństwa konieczne jest przesądzenie o sytuacji tych porozumień. Zawarte w ustawie rozwiązania zapewniają podmiotom czas na dostosowanie tych porozumień do zmian w przepisach.

Organy właściwe do spraw cyberbezpieczeństwa będą miały 18 miesięcy na utworzenie CSIRT sektorowych. Termin ten ma pozwolić na utworzenie nowych podmiotów, skompletowanie niezbędnej kadry oraz zapewnienie im zasobów do działań. Utworzenie CSIRT sektorowego podlega ogłoszeniu, w drodze komunikatu, w dzienniku urzędowym danego organu właściwego oraz na stronie internetowej, m.in. Pełnomocnika. Takie rozwiązanie pozwoli na precyzyjne określenie momentu od kiedy podmioty obowiązane będą miały realizować obowiązki do CSIRT sektorowych. Do tego czasu obowiązki te będą realizowane w stosunku do dotychczasowo właściwych CSIRT poziomu krajowego.

Przepisy określają też jakie informacje zostaną zamieszczone w sprawozdaniu z działania CSIRT sektorowego w roku, w którym został on utworzony. W tym okresie podstawową kwestią będzie zapewnienie takiemu podmiotowi wszystkich narzędzi i zasobów niezbędnych do realizacji jego działań. Może on w tym okresie nie zrealizować swoich standardowych zadań. Z tego względu sprawozdanie to będzie zawierało kwestie związane z jego utworzeniem.

Powołane już sektorowe zespoły cyberbezpieczeństwa staną się z chwilą wejścia w życie projektu ustawy CSIRT sektorowymi. Przepis ten pozwoli zapewnić pełną ciągłość ich działań.

Projekt ustawy dodaje nowe zdania, które do tej pory nie były planowane w budżecie państwa, stąd też w projekcie zostały dodane przepisy określające zwiększenie limitów wydatków w poszczególnych częściach budżetowych, a w przypadku ich przekroczenia nakazujące wprowadzenie mechanizmu korygującego. Wpływ projektowanej ustawy na sektor finansów publicznych został szczegółowo określony w Ocenie Skutków Regulacji.

2.34. Załączniki do ustawy o KSC

2.34.1. Załącznik nr 1

Załącznik nr 1 do ustawy o KSC określa sektory, i w ich obrębie, podsektory w ramach których działają podmioty kluczowe. Są to obszary, które zostały uznane za szczególnie istotne dla prawidłowego funkcjonowania państwa takie jak energetyka, transport, bankowość czy dostarczanie wody pitnej. Wystąpienie przerw w działaniu usług kluczowych podmiotów

w tych sektorach będzie miało natychmiastowy i znaczny wpływ na całe funkcjonowanie społeczeństwa na określonym obszarze i z tego powodu to właśnie je uznano za szczególnie istotne. Załącznik nr 1 do ustawy o KSC oparty jest na załączniku I do dyrektywy NIS 2, rozszerza jednak jego zakres o działalność w zakresie wydobywania kopalin, energii jądrowej oraz podmiotów publicznych.

Działalność w zakresie wydobywania kopalin to działalność, która również posiada bardzo istotny wpływ na funkcjonowanie innych podmiotów, zwłaszcza innych podmiotów z sektora energii i dlatego powinna być objęta tymi samymi regułami co przedsiębiorstwa wytwarzające i przesyłające prąd. Należy również podkreślić, że podmioty z tego sektora są obecnie objęte postanowieniami ustawy o KSC i mają już obecnie obowiązki z tego wynikające.

Projekt utrzymuje dotychczasowy sektor energii – w nowej wersji obejmuje on sektory energii elektrycznej, ciepło, ropa i paliwa, gaz i wodór. Podkreślić należy, że dyrektywa NIS 2 nie warunkuje statusu podmiotu kluczowego lub podmiotu ważnego od mocy instalacji wytwarzającej energię elektryczną przez dany podmiot – dyrektywa podeszła tutaj podmiotowo.

W ramach załącznika nr 1 do ustawy o KSC uwzględniono także obecne rodzaje podmiotów, które mogą być uznane za operatorów usług kluczowych. Przykładowo dotyczy to przedsiębiorców, którzy prowadzą aptekę ogólnodostępną – ten rodzaj podmiotu nie wynika z dyrektywy NIS 2, jednakże w polskiej transpozycji dyrektywy NIS został on uznany za operatora usług kluczowych.

1. Energia

Zapewnianie energii dla społeczeństwa i gospodarki jest kluczowe dla ich funkcjonowania. W łańcuchu dostaw poszczególnych rodzajów energii znajdują się różnorodne rodzaje podmiotów odpowiedzialne w szczególności za wytwarzanie, przesyłanie, dystrybucję i obrót energią. Infrastruktura energetyczna jest sterowana za pomocą przemysłowych systemów sterowania. Incydent może spowodować naruszenie ciągłości dostaw energii co powoduje wzrost cen energii czy ograniczenia w dostępności energii. Sektor energii jest też celem cyberterrorystów czy celem ataków grup APT. Z tego powodu zasadne jest objęcie go wymaganiami z zakresu cyberbezpieczeństwa i wsparciem zespołów CSIRT. Sektor energia występuje w ustawie o KSC od 2018 r. Jego zakres podmiotowy został dostosowany do wymogów dyrektywy NIS 2. Sektor ten dzieli się na kilka podsektorów.

1. 1. Podsektor wydobywanie kopalin

W ramach podsektora wydobywania kopalin wyróżnia się następujące podmioty:

- Podmioty prowadzące działalność gospodarczą w zakresie wydobywania gazu ziemnego na podstawie koncesji, o której mowa w art. 22 ust. 1 ustawy z dnia 9 czerwca 2011 r. – Prawo geologiczne i górnicze,
- Podmioty prowadzące działalność gospodarczą w zakresie wydobywania ropy naftowej na podstawie koncesji, o której mowa w art. 22 ust. 1 ustawy z dnia 9 czerwca 2011 r. – Prawo geologiczne i górnicze,
- Podmioty prowadzące działalność gospodarczą w zakresie wydobywania węgla brunatnego na podstawie koncesji, o której mowa w art. 22 ust. 1 ustawy z dnia 9 czerwca 2011 r. – Prawo geologiczne i górnicze,
- Podmioty prowadzące działalność gospodarczą w zakresie wydobywania węgla kamiennego na podstawie koncesji, o której mowa w art. 22 ust. 1 ustawy z dnia 9 czerwca 2011 r. – Prawo geologiczne i górnicze,
- Podmioty prowadzące działalność gospodarczą w zakresie wydobywania pozostałych kopalin na podstawie koncesji, o której mowa w art. 22 ust. 1 ustawy z dnia 9 czerwca 2011 r. – Prawo geologiczne i górnicze.

Podsektor wydobywanie kopalin występuje w ustawie o KSC od 2018 r. stąd został zachowany, co dopuszcza dyrektywa NIS 2.

Zaczynając od początku – dyrektywa NIS z 2016 r. dopuszczała, aby państwa członkowskie Unii Europejskiej zidentyfikowały dodatkowe sektory i przedsiębiorców, którzy powinni być objęci wymaganiami cyberbezpieczeństwa. Wiele państw członkowskich Unii Europejskiej skorzystało z tej możliwości, o czym wspomina sam OSR do projektu dyrektywy NIS⁹³⁾.

Dyrektywa NIS 2 dopuszcza, aby państwa członkowskie Unii Europejskiej uznały za podmioty kluczowe dotychczas wyznaczonych operatorów usług kluczowych. Wynika to wprost z motywu 17 dyrektywy oraz art. 3 ust. 1 lit. g dyrektywy.

⁹³⁾ **Annex 4: Methodology and criteria for determining the additional sectors, subsectors and services considered for the NIS scope in policy options 2 and 3** [w:] COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT REPORT Accompanying the document Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 PART 2/3, European Commission, 2020.

Co istotne angielska treść motywu posługuje się sformułowaniem “*Member States should be able to*” co wyraźnie wskazuje na to, że dyrektywa wyraźnie dopuszcza to uprawnienie.

Polska wskazała w 2018 r. jako dodatkowy podsektor „wydobywanie kopalin”. Podsektor ten obejmuje podmioty prowadzące działalność gospodarczą w zakresie wydobywania ropy naftowej, węgla kamiennego, węgla brunatnego i pozostałych kopalin na podstawie koncesji, o której mowa w art. 22 ust. 1 ustawy z dnia 9 czerwca 2011 r. – Prawo geologiczne i górnicze.

Warto odnieść się do danych statystycznych. Rocznik Statystyczny Przemysłu 2024⁹⁴⁾ podaje dane o zużyciu energii pierwotnej i pochodnej w przemyśle. W 2023 r. przetwórstwo przemysłowe odpowiadało za zużycie 57,9% energii w Polsce a przedsiębiorstwa energetyczne za kolejne 40,1%. Pokazuje to, jak istotne jest zapewnienie ciągłości łańcucha dostaw kopalin dla polskiego przemysłu. Incydenty cyberbezpieczeństwa w sektorze wydobywczym mogą zaburzyć dostawy kopalin dla polskiego przemysłu i unieruchomić inne przedsiębiorstwa. Stąd też zasadne jest utrzymanie tego podsektora w ramach krajowego systemu cyberbezpieczeństwa aby przedsiębiorstwa wydobywcze po pierwsze zapewniały własne cyberbezpieczeństwo a po drugie w przypadku incydentu poważnego, który uniemożliwia wydobywanie kopalin mogły uzyskać pomoc od zespołów CSIRT.

TABL. 15 (129). ZUŻYCIE ENERGII PIERWOTNEJ I POCHODNEJ W PRZEMYŚLE WEDŁUG SEKCJI						
CONSUMPTION OF PRIMARY AND DERIVED ENERGY IN INDUSTRY BY SECTIONS						
WYSZCZEGÓLNIENIE SPECIFICATION a - 2022 r. b - 2023 r.		Ogółem Total	Górnictwo i wydobywanie Mining and quarrying	Przetwórstwo przemysłowe Manufacturing	Wytwarzanie i zaopatrywanie w energię elektryczną, gaz, parę wodną i gorącą wodę ^D Electricity, gas, steam and air conditioning supply	Dostawa wody; gospodarowanie ściekami i odpadami; rekultywacja ^D Water supply; sewerage, waste management and remediation activities
Energia pierwotna ogółem						
Total primary Energy						
w TJ		368279				
.....	a	5	39715	2059321	1559107	24652
in TJ		337783				
.....	b	5	46148	1954712	1353619	23356
w %						
.....	a	100,0	1,1	55,9	42,3	0,7
in %		100,0				
.....	b	100,0	1,4	57,9	40,1	0,6

⁹⁴⁾ <https://stat.gov.pl/obszary-tematyczne/roczniki-statystyczne/roczniki-statystyczne/rocznik-statystyczny-przemyslu-2024,5,18.html>

w tym:						
of which:						
Węgiel kamienny						
Hard coal						
w tys. t	a	56640	76	16448	39963	153
in thousand tonnes	b	47858	54	14804	32857	143
w TJ	a	130976				
in TJ	b	5	2035	451328	852865	3540
	b	112113				
	b	7	1427	407907	708480	3323
Węgiel brunatny (lignit)						
Lignite						
w tys. t	a	54560	42	53	54465	—
in thousand tonnes	b	40077	31	44	40002	—
w TJ	a	443560	470	778	442312	—
in TJ	b	327131	326	608	326197	—
Ropa naftowa						
Crude oil						
w tys. t	a	26645	—	26645	—	—
in thousand tonnes	b	24979	—	24979	—	—
w TJ	a	113242				
in TJ	b	6	—	1132426	—	—
	b	106163				
	b	3	—	1061633	—	—
Gaz ziemny wysokometanowy						
High-methane natural gas						
w hm ³	a	9399	273	7536	1500	90
in hm ³	b	10293	434	7663	2111	85
w TJ	a	342094	9199	276243	53473	3179
in TJ	b	380491	15099	285650	76744	2998
Gaz ziemny zaazotowany						
Nitrified natural gas						
w hm ³	a	3152	1106	459	1583	4
in hm ³	b	3102	1148	403	1547	4
w TJ	a	79182	27902	11570	39595	115
in TJ	b	78481	29193	10278	38915	95

1.2 Energia elektryczna

W ramach podsektora energii elektrycznej wyróżnia się następujące podmioty:

- Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie wytwarzania energii elektrycznej,
- Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 24 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie przesyłania energii elektrycznej,
- Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 25 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie dystrybucji energii elektrycznej,
- Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie obrotu energią elektryczną,
- Podmioty o których mowa w art. 3 pkt 28b ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne.

Chodzi o wyznaczonego operatora rynku energii elektrycznej.

- Uczestnicy rynku świadczący usługę, o której mowa w art. 3 pkt 6e ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne.

Chodzi tutaj o uczestników rynku, którzy prowadzą działalność polegającą na łączeniu wielkości mocy lub energii elektrycznej oferowanej przez odbiorców, wytwórców energii elektrycznej lub posiadaczy magazynów energii elektrycznej, z uwzględnieniem zdolności technicznych sieci, do której są przyłączeni, w celu sprzedaży energii elektrycznej, świadczenia usług systemowych lub usług elastyczności na rynkach energii elektrycznej.

- Uczestnicy rynku świadczący usługę, o której mowa w art. 3 pkt 11j ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne,
- Uczestnicy rynku świadczący usługę, o której mowa w art. 3 pkt 59 i art. 3 pkt 59a ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne,
- Przedsiębiorcy odpowiedzialni za zarządzanie punktem ładowania i jego obsługę, świadczący usługę ładowania na rzecz użytkowników końcowych, w tym w imieniu i na rzecz dostawcy usług w zakresie mobilności.

1.3 Ciepło

Zgodnie z definicją ustawową pod pojęciem „ciepła” rozumie się energię cieplną w wodzie gorącej, parze lub w innych nośnikach.

W ramach podsektora „ciepło” wyróżnia się następujące podmioty:

- Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie wytwarzania ciepła,
- Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie obrotu ciepłem,
- Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie przesyłania ciepła,
- Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie dystrybucji ciepła.

Zakresem podmiotowym tego podsektora są objęte przedsiębiorstwa energetyczne odpowiedzialne za poszczególne elementy łańcucha dostaw ciepła czyli wytwarzanie, przesyłanie, dystrybucja i obrót ciepłem. Wszystkie podmioty z tego podsektora to podmioty, które muszą uzyskać koncesję na prowadzenie działalności. Ułatwia to podmiotom samoidentyfikację jako podmiot kluczowy lub podmiot ważny, muszą sprawdzić czy spełniają kryterium wielkościowe (co najmniej średnie przedsiębiorstwo) lub czy są np. podmiotem kluczowym ponieważ są podmiotem krytycznym w rozumieniu dyrektywy CER.

1.4 Ropa i paliwa

W ramach podsektora „Ropa i paliwa” wyróżnia się następujące podmioty:

- Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie wytwarzania paliw ciekłych, o której mowa w art. 32 ust. 1 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne,
- Podmioty prowadzące działalność gospodarczą w zakresie przesyłania ropy naftowej.

- Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie przesyłania paliw ciekłych siecią rurociągów, o której mowa w art. 32 ust. 1 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne,
- Podmiot prowadzący działalność gospodarczą w zakresie magazynowania ropy naftowej, w tym w zakresie bezzbiornikowego podziemnego magazynowania ropy naftowej, o którym mowa w art. 22 ust. 1 ustawy z dnia 9 czerwca 2011 r. – Prawo geologiczne i górnicze,
- Podmioty prowadzące działalność gospodarczą w zakresie przeładunku ropy naftowej,
- Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, wykonujące działalność gospodarczą w zakresie magazynowania paliw ciekłych, o którym mowa w art. 32 ust. 1 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, oraz podmiot prowadzący działalność w zakresie bezzbiornikowego podziemnego magazynowania paliw ciekłych, o którym mowa w art. 22 ust. 1 ustawy z dnia 9 czerwca 2011 r. – Prawo geologiczne i górnicze,
- Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, wykonujące działalność gospodarczą w zakresie przeładunku paliw ciekłych, o którym mowa w art. 32 ust. 1 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne,
- Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, wykonujące działalność gospodarczą w zakresie obrotu paliwami ciekłymi lub w zakresie obrotu paliwami ciekłymi z zagranicą, o którym mowa w art. 32 ust. 1 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne,
- Podmioty prowadzące działalność gospodarczą w zakresie wytwarzania paliw syntetycznych,
- Agencja wykonawcza utworzona na podstawie ustawy z dnia 17 grudnia 2020 r. o rezerwach strategicznych (Dz. U. z 2024 r. poz. 1598 i 1907).

Celem jest objęcie wymogami cyberbezpieczeństwa całego łańcuchu dostaw ropy i paliw ciekłych. Incydent w tym sektorze może w poważny sposób unieruchomić gospodarkę co pokazał w 2021 r. incydent Colonial Pipeline⁹⁵⁾.

1.5 Gaz

W ramach podsektora gazu wyróżnia się następujące podmioty:

- Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, prowadzące działalność w zakresie wytwarzania paliw gazowych, o którym mowa w art. 3 pkt 45 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne,
- Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie przesyłania paliw gazowych,
- Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie obrotu gazem ziemnym z zagranicą lub na wykonywanie działalności gospodarczej w zakresie obrotu paliwami gazowymi,
- Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 24 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, będące wyznaczonym przez Prezesa Urzędu Regulacji Energetyki operatorem systemu przesyłowego gazowego,
- Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 25 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, będące wyznaczonym przez Prezesa Urzędu Regulacji Energetyki operatorem systemu dystrybucyjnego gazowego,
- Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 26 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, będące wyznaczonym przez Prezesa Urzędu Regulacji Energetyki operatorem systemu magazynowania paliw gazowych,
- Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 27 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, będące wyznaczonym przez Prezesa Urzędu Regulacji Energetyki operatorem systemu skraplania gazu ziemnego,

⁹⁵⁾ <https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years>

- Przedsiębiorstwa energetyczne prowadzące działalność gospodarczą w zakresie rafinacji i przetwarzania gazu ziemnego.

Gaz ziemny i gaz zaazotowany jest wykorzystywany w górnictwie, przetwórstwie przemysłowym, w wytwarzaniu i zaopatrywaniu w energię elektryczną, gaz, parę wodną i gorącą wodę. Konieczne jest, zgodnie z dyrektywą NIS 2, zapewnienie bezpieczeństwa systemów informacyjnych automatyki przemysłowej wspierających wytwarzanie gazu i paliw gazowych, systemy przesyłowe, dystrybucyjne, magazynowania, skraplania gazu oraz te wspierające rafinację i przetwarzanie gazu ziemnego.

1.6 Energetyka jądrowa

Ze względu zarówno na:

- 1) znaczną doniosłość świadczonych usług (pozyskiwanie surowca, wytwarzanie paliwa, wykorzystanie paliwa do generacji elektryczności, ciepła oraz potencjalnie wodoru, postępowanie ze zużytym paliwem oraz innymi odpadami radioaktywnymi),
- 2) bezpieczeństwo jądrowe oraz ochronę radiologiczną

– zasadnym jest, aby operatorzy obiektów energetyki jądrowej zostali uznani za podmioty kluczowe – niezależnie od przewyższania wymogów dla średniego przedsiębiorstwa określonych w art. 2 ust. 1 załącznika I do rozporządzeniem 651/2014/UE (projektowany art. 5 ust. 1 pkt 1 ustawy o KSC).

Wdrażana dyrektywa NIS 2 oparta jest na zasadzie minimalnej harmonizacji (art. 5 dyrektywy). Wobec czego zasadnym jest przyjęcie szerszego niż przewidziany w dyrektywie katalogu podmiotów objętych regulacjami ustawy o KSC.

Mając na uwadze:

- 1) rozwój energetyki jądrowej w Polsce – zarówno programu rządowego jak i inicjatyw prywatnych;
- 2) znaczenie podmiotów z jądrowego cyklu paliwowego (od wydobywania rudy, poprzez wzbogacanie izotopowe, wytworzenie paliwa jądrowego, jego wykorzystanie, postępowanie z wypalonym paliwem jądrowym i odpadami radioaktywnymi) dla świadczenia usług wytwarzania energii, ciepła, a potencjalnie również wodoru;
- 3) znaczenie paliwa jądrowego dla funkcjonowania elektrowni jądrowych – generacji elektryczności, ciepła i wodoru;

- 4) ryzyka związane z paliwem jądrowym na każdym etapie postępowania z nim zasadnym jest poszerzenie katalogu podmiotów kluczowych o operatorów obiektów wskazanych w art. 2 ust. 2 ww. ustawy, tj. operatorów:
- a) zakładu do wydobywania rud uranu i toru ze złóż i do ich wstępnego przetwarzania,
 - b) zakładu wzbogacania izotopowego,
 - c) zakładu wytwarzania paliwa jądrowego,
 - d) elektrowni jądrowej,
 - e) zakładu przerobu wypalonego paliwa jądrowego,
 - f) przechowalnika wypalonego paliwa jądrowego,
 - g) obiektu do przechowywania odpadów promieniotwórczych,
 - h) składowisko odpadów promieniotwórczych.

Zakłady wskazane w lit. a–c są zaangażowane w wytwarzanie paliwa jądrowego do reaktorów jądrowych. Tym samym w zakresie energetyki jądrowej ich rola jest analogiczna do podmiotów, które odpowiadają za pozyskanie takich surowców jak węgiel, gaz czy ropa. Tak jak węgiel, gaz czy ropa stanowią nośniki energii pierwotnej (paliwa) do dalszego wykorzystania, podobną rolę pełni paliwo jądrowe dla reaktorów. Skoro więc za podmioty kluczowe uznaje się podmioty odpowiedzialne za pozyskanie węgla, gazu i ropy, a także przesył czy dystrybucję, również podmioty zaangażowane w cykl wytwarzania paliwa jądrowego powinny zostać objęte wymogami z zakresu cyberbezpieczeństwa.

Operator elektrowni jądrowej powinien zostać uznany za podmiot kluczowy niezależnie od kwestii z przewyższania wymogów dla średniego przedsiębiorstwa określonych w art. 2 ust. 1 załącznika I do rozporządzeniem 651/2014/UE (projektowany art. 5 ust. 1 pkt 1 ustawy o KSC).

Za „oderwaniem” operatora elektrowni jądrowej od kwestii wielkość przedsiębiorstwa przemawia nie tylko kwestia zapewnienia ciągłości pracy, ale również bezpieczeństwa jądrowego i ochrony radiologicznej. Stąd ujmowanie operatorów elektrowni jądrowych jako objętych regulacją ustawy o zmianie ustawy o KSC w ramach przedsiębiorstw energetycznych posiadających koncesje na wytwarzanie energii elektrycznej lub ciepła (załącznik nr 1 do ustawy o KSC w zw. z projektowanym art. 5 ust. 1 pkt 1 ustawy o KSC, sektor energia) jest niewystarczające, gdyż wiąże kwestie objęcia tą kategorią z przewyższaniem wymogów dla średniego przedsiębiorstwa określonych w art. 2 ust. 1 załącznika I do rozporządzeniem 651/2014/UE (projektowany art. 5 ust. 1 pkt 1 ustawy o KSC).

Pomiędzy osiągnięciem przez elektrownię jądrową zdolności operacyjnej, a uzyskaniem koncesji na wytwarzanie energii elektrycznej lub ciepła może wystąpić „luka” czasowa, która spowoduje okres ekspozycji na cyberzagrożenia – w tym wykorzystanie podatności przez zagrożenia, które aktywują się zarówno przed jak i po uzyskaniu koncesji. Moment identyfikacji powinien więc być wcześniejszy, o czym niżej.

Operatorzy obiektów jądrowych wymienionych w powyżej w lit. e–h są z kolei zaangażowani w postępowanie z wypalonym paliwem jądrowym oraz odpadami radioaktywnymi. Ich rola, w tym zakresie, jest więc analogiczna do roli podmiotów zaangażowanych w gospodarkę odpadami, które znalazły się w załączniku nr 2 jako podmioty kluczowe. Podmioty wymienione powyżej w lit. e–h nie wydają się jednak objęte załącznikiem. Załącznik nawiązuje do ustawy z dnia 14 grudnia 2012 r. o odpadach (Dz. U. z 2023 r. poz. 1587, z późn. zm.), której nie stosuje się do odpadów promieniotwórczych (art. 2 pkt 4 ustawy z dnia 14 grudnia 2012 r. o odpadach). Dodatkowo załącznik co do zasady wiąże status podmiotu kluczowego z przewyższaniem wymogów dla średniego przedsiębiorstwa określonych w art. 2 ust. 1 załącznika I do rozporządzeniem 651/2014/UE (projektowany art. 5 ust. 1 pkt 1 ustawy o KSC).

Składowisko odpadów promieniotwórczych – w chwili obecnej w Polsce funkcjonuje tylko jedno składowisko odpadów promieniotwórczych, prowadzone przez Zakład Unieszkodliwiania Odpadów Promieniotwórczych (ZUOP) – jednostkę nadzorowaną przez ministra właściwego do spraw energii, a po wejściu w życie uchwalonej przez Sejm ustawy o zmianie, będzie nadzorowany przez ministra do spraw gospodarki surowcami energetycznymi. W związku z rozwojem energetyki jądrowej konieczne będzie powstanie dalszych składowisk odpadów promieniotwórczych – zarówno powierzchniowych jak i głębokich. Obecnie nie wiadomo w jakiej formie prawnej będą funkcjonowały, ani czy ich operatorzy będą podlegali nadzorowi ze strony określonego ministra. Stąd zasadne jest uznanie operatora składowiska odpadów promieniotwórczych za podmiot kluczowy. Takie rozwiązanie zapewni odpowiedni poziom ogólności przepisów i ich elastyczność w przypadku, gdyby operatorzy nowych składowisk nie byli objęci kategorią jednostek nadzorowanych.

1.7 Wodór

W ramach podsektora wodoru wyróżnia się następujące podmioty:

- Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, prowadzące działalność w zakresie przesyłania wodoru,
- Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, prowadzące działalność w zakresie magazynowania wodoru,
- Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, prowadzące działalność w zakresie wytwarzania wodoru,
- Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, prowadzące działalność w zakresie dystrybucji wodoru.

Wodór przez ostatnich kilkanaście lat z powodzeniem stosuje się jako paliwo w różnych procesach technologicznych i napędowych, a także jest jedną z wiodących opcji magazynowania energii ze źródeł odnawialnych. Wodór i paliwa na bazie wodoru mogą też służyć do przesyłu i dystrybucji energii ze źródeł odnawialnych na duże odległości. Zasilanie urządzeń bez dostępu do sieci i magazynów energii, również w czasie kiedy wydajność systemów OZE jest niewystarczająca. Dostępnych jest wiele różnych typów ogniwo paliwowych o szerokim zakresie zastosowań. Małe ogniwa paliwowe mogą zasilać laptopy, a nawet telefony komórkowe, a także sprawdzać się w zastosowaniach wojskowych. Duże ogniwa paliwowe mogą dostarczać energię elektryczną na potrzeby zasilania awaryjnego w budynkach oraz w odległych od cywilizacji miejscach, które nie są podłączone do sieci elektroenergetycznych.

2. *Transport*

2.1 Podsektor Transport lotniczy

Transport lotniczy odgrywa duże znaczenie dla swobody przepływu osób oraz towarów w ramach Unii Europejskiej. Według statystyk Urzędu Lotnictwa Cywilnego w pierwszym półroczu 2024 r. polskie porty lotnicze obsłużyły:

- 1 719 742 pasażerów w ruchu krajowym - regularnym i czarterowym⁹⁶⁾,

⁹⁶⁾ https://ulc.gov.pl/download/statystyki/2024/II_kw_2024/wg_portow_krajowe_2kw2024_v2.pdf

- 94 329 761 kg *cargo on board* w ruchu krajowym i międzynarodowym⁹⁷⁾.

W lotnictwie cywilnym wykorzystywane są systemy zarządzania ruchem lotniczym, systemy nawigacyjne oraz systemy informatyczne dedykowane dla pasażerów, takie jak np. systemy rezerwacji biletów lotniczych w celu zapewnienia świadczenia usług⁹⁸⁾. Systemy te są narażone na cyberzagrożenia, przykładowo może dojść do ataków DDoS na systemy kontroli ruchu lotniczego, ataki na systemy rezerwacji biletów, w celu uzyskania danych osobowych, ataki typu Man in the Middle na systemy komunikacji radiowej, awarie techniczne systemów, błędy ludzkie⁹⁹⁾.

W ramach podsektora transportu lotniczego znajdują się następujące podmioty:

- Przewoźnik lotniczy, o którym mowa w art. 3 pkt 4 rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 300/2008 z dnia 11 marca 2008 r. w sprawie wspólnych zasad w dziedzinie ochrony lotnictwa cywilnego i uchylającego rozporządzenie (WE) nr 2320/2002 (Dz. Urz. UE L 97 z 09.04.2008, str. 72).

Zgodnie z definicją unijną przewoźnik lotniczy to przedsiębiorstwo transportu lotniczego posiadające ważną licencję na prowadzenie działalności lub jej odpowiednik,

- Zarządzający lotniskiem, o którym mowa w art. 2 pkt 7 ustawy z dnia 3 lipca 2002 r. – Prawo lotnicze (Dz. U. z 2023 r. poz. 2110, z późn. zm.).

Zarządzającym lotniskiem jest podmiot, który został wpisany jako zarządzający do rejestru lotnisk cywilnych. Rejestr ten jest prowadzony przez Prezesa Urzędu Lotnictwa Cywilnego.

- Przedsiębiorca, o którym mowa w art. 177 ust. 2 ustawy z dnia 3 lipca 2002 r. – Prawo lotnicze, wykonujący dla przewoźników lotniczych oraz innych użytkowników statków powietrznych jedną lub więcej kategorii usług, o których mowa w art. 176 tej ustawy, oraz przedsiębiorca, o którym mowa w art. 186b ust. 1 pkt 2 ustawy z dnia 3 lipca 2002 r. – Prawo lotnicze, wykonujący zadania związane z kontrolą bezpieczeństwa,
- Instytucja zapewniająca służby żeglugi powietrznej, o której mowa w art. 127 ust. 1 ustawy z dnia 3 lipca 2002 r. – Prawo lotnicze.

⁹⁷⁾ https://ulc.gov.pl/_download/statystyki/2024/II_kw_2024/wg_org_cargo_2kw2024_v2.pdf

⁹⁸⁾ E. Szczepaniuk, *Wybrane aspekty cyberbezpieczeństwa w lotnictwie cywilnym*, „Aviation and Security Issues” t. 3 nr 1 (2023), s. 111.

⁹⁹⁾ Ibidem, s. 114–115.

Instytucja zapewniająca służby żeglugi powietrznej jest wyznaczana w drodze decyzji administracyjnej przez ministra właściwego do spraw transportu po zasięgnięciu opinii Ministra Obrony Narodowej i Prezesa Urzędu Lotnictwa Cywilnego.

2.2 Podsektor transport kolejowy

W ramach podsektora transportu kolejowego znajdują się następujące podmioty:

- Zarządca infrastruktury kolejowej w rozumieniu art. 4 pkt 7 ustawy z dnia 28 marca 2003 r. o transporcie kolejowym (Dz. U. z 2025 r. poz. 1234), z wyłączeniem zarządców wyłącznie infrastruktury nieczynnej, o której mowa w art. 4 pkt 1b tej ustawy, infrastruktury prywatnej, o której mowa w art. 4 pkt 1c, oraz infrastruktury kolei wąskotorowej, o której mowa w art. 4 pkt 1d tej ustawy.

Zarządcą infrastruktury kolejowej jest podmiot odpowiedzialny za zarządzanie infrastrukturą kolejową, jej eksploatację, utrzymanie, odnowienie lub udział w rozwoju tej infrastruktury, a w przypadku budowy nowej infrastruktury, podmiot, który przystąpił do jej budowy w charakterze inwestora.

- Przewoźnik kolejowy, o którym mowa w art. 4 pkt 9 ustawy z dnia 28 marca 2003 r. o transporcie kolejowym, którego działalność podlega licencjonowaniu, oraz operator obiektu infrastruktury usługowej, o którym mowa w art. 4 pkt 52 ustawy z dnia 28 marca 2003 r. o transporcie kolejowym, jeżeli przedsiębiorca wykonujący funkcję operatora jest jednocześnie przewoźnikiem kolejowym.

Przewoźnikiem kolejowym jest przedsiębiorca uprawniony do wykonywania przewozów kolejowych, w tym przedsiębiorca świadczący wyłącznie usługę trakcyjną, na podstawie licencji i jednolitego certyfikatu bezpieczeństwa, lub przedsiębiorca uprawniony do wykonywania przewozów kolejowych na podstawie świadectwa bezpieczeństwa;

Operator obiektu infrastruktury usługowej to podmiot wykonujący działalność polegającą na zarządzaniu obiektem infrastruktury usługowej lub świadczeniu na rzecz przewoźników kolejowych co najmniej jednej z usług, o których mowa w ust. 2 i 3 załącznika nr 2 do ustawy.

Cyberbezpieczeństwo na kolei obejmuje w szczególności bezpieczeństwo systemów sterowania ruchem kolejowym, systemów odpowiedzialnych za informację o rozkładach jazdy, systemów biletowych czy systemów sterujących taborem kolejowym. Często systemy używane na kolei mają długi cykl życia, co utrudnia zapewnienie ich bezpieczeństwa.

2.3 Podsektor transport wodny

Incydenty związane z transportem wodnym mogą polegać na atakach na systemy przeładunkowe portów, wyłączanie kart sieciowych, blokada serwerów portów. Skutkować to może przerwą działalności portów i zaburzeniem łańcuchów dostaw¹⁰⁰⁾. Celem ataków mogą być nie tylko porty, obiekty morskie ale także armatorzy jak również systemy VTS.

W ramach podsektora transportu wodnego znajdują się następujące podmioty:

- Armator w transporcie morskim pasażerów i towarów zgodnie z definicją dla transportu morskiego w załączniku I do rozporządzenia (WE) nr 725/2004 Parlamentu Europejskiego i Rady z dnia 31 marca 2004 r. w sprawie podniesienia ochrony statków i obiektów portowych (Dz. Urz. UE L 129 z 29.04.2004, str. 6, z późn. zm.), z wyłączeniem poszczególnych statków, na których prowadzą działalność ci armatorzy,
- Armator, o którym mowa w art. 5 ust. 1 pkt 2 ustawy z dnia 21 grudnia 2000 r. o żegludze śródlądowej (Dz. U. z 2025 r. poz. 18),
- Podmiot zarządzający portem morskim, o którym mowa w art. 3 ust. 1 pkt 2 ustawy z dnia 4 września 2008 r. o ochronie żeglugi i portów morskich (Dz. U. z 2024 r. poz. 597),
- Podmiot zarządzający obiektem portowym, o którym mowa w art. 2 pkt 11 rozporządzenia (WE) 725/2004 Parlamentu Europejskiego i Rady z dnia 31 marca 2004 r. w sprawie podniesienia ochrony statków i obiektów portowych,
- Podmioty prowadzące na terenie portu działalność wspomagającą transport morski,
- VTS (Służba Kontroli Ruchu Statków) – aparat pomocniczy dyrektora urzędu morskiego powołany w celu monitorowania ruchu statków i przekazywania informacji, stanowiący część składową Narodowego Systemu SafeSeaNet, o którym mowa w art. 91 ustawy z dnia 18 sierpnia 2011 r. o bezpieczeństwie morskim (Dz. U. z 2025 r. poz. 883).

2.4 Podsektor transport drogowy

W ramach podsektora transportu drogowego znajdują się następujące podmioty:

¹⁰⁰⁾ A. Mrozowska, *Zarządzanie morskim cyberbezpieczeństwem*, „5 Wstęp”, s. 33.

- Zarządca drogi, o którym mowa w art. 19 ust. 2 pkt 1 ustawy z dnia 21 marca 1985 r. o drogach publicznych (Dz. U. z 2025 r. poz. 889),
- Podmioty świadczące usługę ITS, o której mowa w art. 4 pkt 36 ustawy z dnia 21 marca 1985 r. o drogach publicznych.

Ujęcie ww. podmiotów w ramach krajowego systemu cyberbezpieczeństwa pozwoli zabezpieczyć systemy związane z kierowaniem ruchem.

Inteligentne systemy transportowe pozwalają zapewnić większe bezpieczeństwo na drogach. Są jednak podatne na różnego rodzaju zagrożenia np. zagrożenia fizyczne – infrastruktura ITS jest dostępna przy drogach, stąd atakujący może podłączyć się do niezabezpieczonego urządzenia. W ten sposób może przechwytywać dane o ruchu drogowym, skanować topologię sieci, prowadzić ataki Man-in the middle, za pomocą ataków typu spoofing wpływać na komunikację między pojazdami (Vehicle-to-Vehicle communication) czy między pojazdami a infrastrukturą (Vehicle-to-infrastructure V2I).

3. Bankowość i infrastruktura rynków finansowych

W ramach tego sektora wyodrębniono następujące podmioty:

- Instytucja kredytowa, o której mowa w art. 4 ust. 1 pkt 17 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe (Dz. U. z 2024 r. poz. 1646, z późn. zm.),
- Bank krajowy, o którym mowa w art. 4 ust. 1 pkt 1 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe,
- Oddział banku zagranicznego, o którym mowa w art. 4 ust. 1 pkt 20 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe,
- Spółdzielcze kasy oszczędnościowo-kredytowe w rozumieniu ustawy z dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych,
- Podmiot prowadzący rynek regulowany, o którym mowa w art. 14 ust. 1 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi (Dz. U. z 2024 r. poz. 722, z późn. zm.),
- Podmiot, o którym mowa w art. 3 pkt 49 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi,
- Podmiot, o którym mowa w art. 48 ust. 7 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi,

- Podmiot prowadzący ASO w rozumieniu art. 3 pkt 2 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi,
- Podmiot prowadzący OTF w rozumieniu art. 3 pkt 10b ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi,
- Administratorzy kluczowych wskaźników referencyjnych,
- Podmiot utworzony na podstawie art. 67 ustawy – Prawo bankowe,
- Podmiot, o którym mowa w art. 3 pkt 21a ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi mający siedzibę na terytorium Rzeczypospolitej Polskiej.

Wszystkie te podmioty mają istotny wpływ na przeprowadzanie transakcji, a w konsekwencji na całą gospodarkę. Wystąpienie incydentu poważnego w takim podmiocie może też wiązać się z uzyskaniem dostępu do istotnych danych o transakcjach czy nawet może pozwolić na uzyskanie dostępu do środków należących do innych podmiotów. Dlatego konieczne jest szczególne zabezpieczenie tego sektora.

4. Ochrona zdrowia

W ramach sektora ochrony zdrowia wyróżniamy następujące podsektory:

Udzielanie świadczeń zdrowotnych i zdrowie publiczne:

- Podmiot leczniczy, o którym mowa w art. 4 ust. 1 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej,
- Laboratoria referencyjne UE, o których mowa w art. 15 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2371 z dnia 23 listopada 2022 r. w sprawie poważnych transgranicznych zagrożeń zdrowia oraz uchylenia decyzji nr 1082/2013/UE (Dz. Urz. UE L 314 z 06.12.2022, str. 1),
- Jednostka podległa ministrowi właściwemu do spraw zdrowia albo przez niego nadzorowana, właściwa w zakresie systemów informacyjnych ochrony zdrowia,
- Urzędy obsługujące organy Państwowej Inspekcji Sanitarnej,
- Krajowe Centrum Monitorowania Ratownictwa Medycznego, o którym mowa w art. 27a ustawy z dnia 8 września 2006 r. o Państwowym Ratownictwie Medycznym (Dz. U. z 2025 r. poz. 91 i 637),

- Jednostki organizacyjne publicznej służby krwi, o których mowa w art. 4 ust. 3 pkt 2 ustawy z dnia 22 sierpnia 1997 r. o publicznej służbie krwi (Dz. U. z 2024 r. poz. 1782),
- Podmioty udzielające świadczeń opieki zdrowotnej będące podwykonawcą dla podmiotów kluczowych lub ważnych w sektorze ochrona zdrowia, w rozumieniu art. 133 ustawy z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (Dz. U. z 2024 r. poz. 146, z późn. zm.),
- Świadczeniodawcy posiadający w swojej strukturze organizacyjnej Szpitalny Oddział Ratunkowy, Centrum Urazowe lub Centrum Urazowe dla Dzieci.

Produkcja i dystrybucja substancji czynnych, produktów leczniczych i wyrobów medycznych:

- Urząd Rejestracji Produktów Leczniczych, Wyrobów Medycznych i Produktów Biobójczych,
- Urzędy obsługujące organy Inspekcji Farmaceutycznej,
- Podmioty prowadzące działalność badawczo-rozwojową w zakresie produktów leczniczych zdefiniowanych w art. 1 pkt 2 dyrektywy 2001/83/WE Parlamentu Europejskiego i Rady z dnia 6 listopada 2001 r. w sprawie wspólnotowego kodeksu odnoszącego się do produktów leczniczych stosowanych u ludzi (Dz. Urz. UE L 311 z 28.11.2001, str. 67, z późn. zm.),
- Podmioty produkujące podstawowe substancje farmaceutyczne oraz leki i pozostałe wyroby farmaceutyczne, o których mowa w sekcji C dział 21 klasyfikacji NACE Rev. 2,
- Podmioty produkujące wyroby medyczne uznane za mające krytyczne znaczenie podczas danego stanu zagrożenia zdrowia publicznego („wykaz wyrobów medycznych o krytycznym znaczeniu w przypadku stanu zagrożenia zdrowia publicznego”) w rozumieniu art. 22 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/123 z dnia 25 stycznia 2022 r. w sprawie wzmocnienia roli Europejskiej Agencji Leków w zakresie gotowości na wypadek sytuacji kryzysowej i zarządzania kryzysowego w odniesieniu do produktów leczniczych i wyrobów medycznych (Dz. Urz. UE L 20 z 31.01.2022, str. 1, z późn. zm.),

- Przedsiębiorca prowadzący działalność polegającą na prowadzeniu hurtowni farmaceutycznej w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne (Dz. U. z 2025 r. poz. 750, 905 i 924),
- Przedsiębiorca lub podmiot prowadzący działalność gospodarczą w państwie członkowskim Unii Europejskiej lub państwie członkowskim Europejskiego Porozumienia o Wolnym Handlu (EFTA) – stronie umowy o Europejskim Obszarze Gospodarczym, który uzyskał pozwolenie na dopuszczenie do obrotu produktu leczniczego,
- Importer produktu leczniczego/substancji czynnej w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne,
- Wytwórca produktu leczniczego/substancji czynnej w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne,
- Importer równoległy w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne,
- Dystrybutor substancji czynnej w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne.

Przedsiębiorca prowadzący działalność w formie apteki ogólnodostępnej w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne. Wszystkie usługi związane z sektorem zdrowia mają szczególne znaczenie dla społeczeństwa, a nawet krótka przerwa w ich dostarczaniu może mieć bardzo niebezpieczne skutki. Podmioty te przechowują również wrażliwe dane dotyczące stanu zdrowia obywateli.

5. Zaopatrzenie w wodę pitną i jej dystrybucja

W ramach tego sektora wskazano następujący rodzaj podmiotu:

- Podmiot dostarczający wodę przeznaczoną do spożycia przez ludzi, w tym przedsiębiorstwo wodociągowo-kanalizacyjne, o którym mowa w art. 2 pkt 4 ustawy z dnia 7 czerwca 2001 r. o zbiorowym zaopatrzeniu w wodę i zbiorowym odprowadzaniu ścieków (Dz. U. z 2024 r. poz. 757), z wyłączeniem podmiotów, dla których dostarczanie wody przeznaczonej do spożycia przez ludzi jest inną niż istotną częścią ich ogólnej działalności.

Usługi użyteczności publicznej w coraz większym stopniu łączą się z sieciami cyfrowymi, aby m.in. usprawnić zaopatrzenie w wodę, odprowadzanie ścieków oraz zwiększyć efektywność oświetlenia i ogrzewania budynków. Te cyfrowe usługi użyteczności publicznej są narażone na cyberataki, a skuteczny cyberatak grozi obywatelom szkodami na dużą skalę ze względu na wzajemne powiązanie tych usług. W szczególności przerwa w zaopatrzeniu w wodę jest dotkliwa dla mieszkańców. Innym ryzykiem jest możliwość ataku do systemu zarządzającego uzdatnianiem wody i nieautoryzowana zmiana zawartości dezynfektantów w wodzie, co może doprowadzić do uszczerbku na zdrowiu czy na śmierci ludzi.

6. Zbiorowe odprowadzanie ścieków

W ramach tego sektora wskazano następujący rodzaj podmiotu:

- Podmiot odprowadzający lub oczyszczający ścieki, w tym przedsiębiorstwo wodociągowo-kanalizacyjne, o którym mowa w art. 2 pkt 4 ustawy z dnia 7 czerwca 2001 r. o zbiorowym zaopatrzeniu w wodę i zbiorowym odprowadzaniu ścieków, z wyłączeniem podmiotów, dla których odprowadzanie lub oczyszczanie ścieków jest inną niż istotną częścią ich ogólnej działalności.

Ten sektor został uwzględniony z tych samych powodów co sektor zaopatrzenia w wodę.

7. Infrastruktura cyfrowa

W ramach sektora infrastruktury cyfrowej wydzielono podsektor komunikacji elektronicznej, w którym znajdują się przedsiębiorcy telekomunikacyjni oraz podmioty świadczące usługę komunikacji interpersonalnej niewykorzystującej numerów. Podmioty te będą podlegały nadzorowi Prezesa Urzędu Komunikacji Elektronicznej. Pozostałe podmioty będą podlegały pod nadzór ministra właściwego do spraw informatyzacji

Infrastruktura cyfrowa z wyłączeniem komunikacji elektronicznej:

- Dostawca punktu wymiany ruchu internetowego,
- Dostawca usług DNS, z wyłączeniem operatorów głównych serwerów nazw,
- Rejestr nazw domen najwyższego poziomu (TLD),
- Dostawca chmury obliczeniowej,
- Dostawca usługi centrum przetwarzania danych,
- Dostawca sieci dostarczania treści,

- Dostawca usług zaufania,
- Podmiot świadczący usługę rejestracji nazw domen,

Komunikacja elektroniczna:

- Przedsiębiorca komunikacji elektronicznej.

Wszystkie usługi w tym sektorze związane są z przekazywaniem danych na odległość co ma istotny wpływ zarówno na funkcjonowanie gospodarki jak i bezpieczeństwo danych. Należy też zwrócić uwagę, że incydenty w tym sektorze mogą szczególnie łatwo wpłynąć na inne sektory. Niektóre z działalności wskazane wyżej są niezbędne do zapewnienia prawidłowego funkcjonowania internetu.

8. Zarządzanie usługami ICT

Jest to nowy sektor, do tej pory nie występujący w ustawie o KSC. Obejmuje on:

- Dostawcę usług zarządzanych,
- Dostawcę usług zarządzanych w zakresie cyberbezpieczeństwa.

Usługi wspierające inne podmioty w wykonywaniu zadań z zakresu cyberbezpieczeństwa powinny być objęte takimi samymi wymogami jakie dotyczą ich klientów, tak aby zapewnić jednolite standardy w tym zakresie.

9. Przestrzeń kosmiczna

Jest to nowy sektor, do tej pory nie występujący w ustawie o KSC. Obejmuje on:

- Operatora infrastruktury naziemnej, który wspiera świadczenie usług kosmicznych, z wyjątkiem przedsiębiorców dostawców publicznej sieci łączności elektronicznej,
- Polską Agencję Kosmiczną.

Coraz większe współzależności wynikają z coraz bardziej transgranicznej i współzależnej sieci świadczenia usług, dotyczy również usług związanych z przestrzenią kosmiczną, jeżeli chodzi o świadczenie niektórych usług zależnych od naziemnej infrastruktury. W takim wypadku incydent w tym obszarze wiąże się z poważnymi konsekwencjami i konieczne jest podjęcie odpowiednich działań aby mu zapobiec.

10. Podmioty publiczne

Sektor ten obejmuje:

- Podmioty z uwzględnieniem pkt 2–4:

- jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 1 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych oraz urzędy je obsługujące,
 - jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 3, –6, 8, 9, 11–13 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych,
 - Instytuty badawcze,
 - Narodowy Bank Polski,
 - Bank Gospodarstwa Krajowego,
 - Urząd Dozoru Technicznego,
 - Polska Agencja Żeglugi Powietrznej,
 - Polskie Centrum Akredytacji,
 - Urząd Komisji Nadzoru Finansowego,
 - Polska Agencja Prasowa,
 - Państwowe Gospodarstwo Wodne Wody Polskie, o którym mowa w ustawie z dnia 20 lipca 2017 r. – Prawo wodne (Dz. U. z 2025 r. poz. 960).
 - Polski Fundusz Rozwoju i inne instytucje rozwoju, o których mowa w art. 2 ust. 1 pkt 1 i 3–6 ustawy z dnia 4 lipca 2019 r. o systemie instytucji rozwoju.
 - Narodowy Fundusz Ochrony Środowiska i Gospodarki Wodnej,
 - wojewódzkie fundusze ochrony środowiska i gospodarki wodnej,
 - Państwowy Fundusz Rehabilitacji Osób Niepełnosprawnych,
 - Zakład Unieszkodliwiania Odpadów Promieniotwórczych z siedzibą w Otwocku-Świerku;
- w odniesieniu do samorządu województwa: jednostki budżetowe oraz zakłady budżetowe z wyłączeniem:
 - jednostek organizacyjnych, o których mowa w art. 2 ustawy z dnia 14 grudnia 2016 r. – Prawo oświatowe (Dz. U. z 2025 r. poz. 1043 i 1160) oraz ich zespołów,
 - jednostek organizacyjnych wspierania rodziny i systemu pieczy zastępczej, o których mowa w art. 2 ust. 3 ustawy z dnia 9 czerwca 2011 r. o wspieraniu rodziny i systemie pieczy zastępczej,
 - jednostek organizacyjnych, o których mowa w art. 6 pkt 5 ustawy z dnia 12 marca 2004 r. o pomocy społecznej, oprócz regionalnych ośrodków polityki społecznej,
 - wojewódzkich urzędów pracy,
 - parków krajobrazowych i ich zespołów,

- jednostek obsługujących, o których mowa w art. 8d ustawy z dnia 5 czerwca 1998 r. o samorządzie województwa (Dz. U. z 2025 r. poz. 581), w zakresie w jakim prowadzą wspólną obsługę jednostek, o których mowa w lit. a–e;
- w odniesieniu do samorządu powiatu: starostwo powiatowe.
- w odniesieniu do samorządu gminy: urząd gminy, jeżeli zatrudnia na dzień 1 stycznia danego roku w przeliczeniu na pełny wymiar czasu pracy na podstawie umowy o pracę co najmniej 50 osób.

Administracja publiczna jest częścią krajowego systemu cyberbezpieczeństwa od jego powstania w 2018 roku. Jest to sektor, w ramach którego realizowane są zadania publiczne na rzecz obywateli i przetwarzane są wrażliwe dane, dlatego konieczne jest objęcie tych podmiotów wymogami z zakresu cyberbezpieczeństwa. Równocześnie będą również prowadzone działania wspierające te podmioty w realizacji ich obowiązków zarówno pod kątem zapewnienia im środków jak i rozwoju ich kompetencji.

2.34.2. Załącznik nr 2

Załącznik nr 2 do projektu ustawy określa sektory, i w ich obrębie podsektory, dotyczące podmiotów ważnych. Należą do nich m.in. produkcja, przetwarzanie i dystrybucja żywności, gospodarowanie odpadami czy usługi pocztowe, produkcja i dystrybucja chemikaliów, produkcja, przetwarzanie i dystrybucja żywności i produkcja ogółem. Wszystkie z tych rodzajów działalności są istotne dla prawidłowego funkcjonowania społeczeństwa, ale równocześnie ich zakłócenie nie powoduje skutków w tak krótkiej perspektywie czasowej jak w przypadku podmiotów kluczowych. Tabela ta jest w całości oparta na załączniku II do dyrektywy NIS 2.

1. Sektor „usługi pocztowe”

Rodzaj podmiotu: Operator pocztowy, o którym mowa w art. 3 pkt 12 ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe.

Operatorem pocztowym jest przedsiębiorca, który ma uprawnienia do wykonywania działalności pocztowej na podstawie wpisu do rejestru operatorów pocztowych. Rejestr ten jest prowadzony przez Prezesa Urzędu Komunikacji Elektronicznej. Działalnością pocztową jest działalność gospodarcza polegająca na świadczeniu usług pocztowych w obrocie krajowym lub zagranicznym. Usługą pocztową jest wykonywane w obrocie krajowym lub zagranicznym, zarobkowe:

- 1) realizowane łącznie lub rozdzielnie przyjmowanie, sortowanie, doręczanie przesyłek pocztowych oraz druków bezadresowych;
- 2) przemieszczanie przesyłek pocztowych oraz druków bezadresowych, jeżeli jest wykonywane łącznie z przynajmniej jedną spośród czynności, o których mowa w pkt 1;
- 3) przesyłanie przesyłek pocztowych przy wykorzystaniu środków komunikacji elektronicznej, jeżeli na etapie przyjmowania, przemieszczania lub doręczania przekazu informacyjnego przyjmują one fizyczną formę przesyłki listowej;
- 4) prowadzenie punktów wymiany umożliwiających przyjmowanie i wymianę korespondencji między podmiotami korzystającymi z obsługi tych punktów;
- 5) realizowanie przekazów pocztowych.

Mimo postępującej informatyzacji operatorzy pocztowi nadal są niezbędni dla społeczeństwa i gospodarki. Zapewniają możliwość dostarczania przedmiotów o różnych gabarytach m.in. od sprzedawców do konsumentów i w obrocie biznesowym. Umożliwiają przesyłanie pieniędzy np. w celu wypłaty emerytur, rent i innych świadczeń. W celu zorganizowania obsługi świadczenia usług pocztowych posiadają systemy informacyjne umożliwiające rejestrowanie przesyłek, ich śledzenie i wyszukiwanie oraz umożliwiające rozpatrywanie ewentualnych reklamacji. Istotną rolę pełni przy tym operator wyznaczony. Więksi operatorzy pocztowi wykonują obowiązki z zakresu obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego. Zapewnienie ciągłości świadczenia usług pocztowych w sytuacjach kryzysowych oraz w sytuacjach stanów nadzwyczajnych ma duże znaczenie dla odporności państwa. Stąd też zasadne jest nałożenie na operatorów pocztowych obowiązków z zakresu cyberbezpieczeństwa – jako podmiotów ważnych – jest to zgodne z zał. 2 do dyrektywy NIS 2.

2. Sektor – inwestycje energetyki jądrowej

Sektor ten obejmuje:

- Podmioty będące inwestorami obiektu energetyki jądrowej określonego w art. 2 pkt 2 ustawy z dnia 29 czerwca 2011 r. o przygotowaniu i realizacji inwestycji w zakresie obiektów energetyki jądrowej oraz inwestycji towarzyszących, który uzyskał decyzję zasadniczą, o której mowa w art. 3a ust. 1 tej ustawy.

Już na etapie rozpoczynania inwestycji z zakresu energetyki jądrowej inwestorzy przetwarzają ważne dane związane choćby z lokalizacją inwestycji czy planem jej budowy. W związku z powyższym już na tym etapie powinny być one objęte obowiązkami z zakresu

cyberbezpieczeństwa, tak aby zapewnić cyberbezpieczeństwo ich systemów i przechowywanych w nich danych.

3. Sektor gospodarowanie odpadami

Dla porządku należy wskazać, że odpadem jest każdą substancję lub przedmiot, których posiadacz pozbywa się, zamierza się pozbyć lub do których pozbycia się jest obowiązany.

Zgodnie z ustawą z dnia 14 grudnia 2012 r. o odpadach pod pojęciem gospodarowania odpadami zbieranie, transport lub przetwarzanie odpadów, w tym sortowanie, wraz z nadzorem nad wymienionymi działaniami, a także późniejsze postępowanie z miejscami unieszkodliwiania odpadów oraz działania wykonywane w charakterze sprzedawcy odpadów lub pośrednika w obrocie odpadami.

Gospodarka odpadami pozwala zredukować ilość niewykorzystanych odpadów. W celu obsługi tych procesów powstały systemy informacyjne wspierające planowanie gospodarki odpadami, pozyskiwanie odpadów, naliczanie opłat, składowanie odpadów czy utylizację odpadów. Systemy wspomagają identyfikację rodzajów odpadów, lokalizacji czy klientów co pozwala na zarządzanie odpadami oraz generowanie raportów o liczbie i lokalizacji odpadów jak również wspomagają obsługę księgową podmiotów zaangażowanych w gospodarkę odpadami.¹⁰¹⁾

Incydent dotyczący systemów informacyjnych służących gospodarce odpadami może utrudnić sprawne zbieranie odpadów czy ich segregację co negatywnie wpłynie na środowisko.

3.1 Podsektor Zbieranie odpadów obejmuje:

- Przedsiębiorstwa świadczące usługi w rozumieniu ustawy z dnia 14 grudnia 2012 r. o odpadach, polegające na zbieraniu odpadów, zobowiązane do uzyskania wpisu w rejestrze, o którym mowa w art. 49 ust. 1 ustawy z dnia 14 grudnia 2012 r. o odpadach, z wyłączeniem przedsiębiorstw, dla których usługi te nie stanowią podstawowej działalności gospodarczej określonej zgodnie z przepisami wydanymi na podstawie art. 40 ust. 2 ustawy z dnia 29 czerwca 1995 r. o statystyce publicznej (Dz. U. z 2024 r. poz. 1799).

¹⁰¹⁾ A. Brzeszczak, D. Dziembek, *Technologie i systemy informatyczne wykorzystywane w gospodarce odpadami*, „Artykuły IZIP” t. 2 (2017), http://46.242.185.119/off_ptzp.org.pl/files/konferencje/kzz/artyk_pdf_2017/T2/t2_625.pdf.

Zbieranie odpadów to gromadzenie odpadów przed ich transportem do miejsc przetwarzania, w tym wstępne sortowanie nieprowadzące do zasadniczej zmiany charakteru i składu odpadów i niepowodujące zmiany klasyfikacji odpadów oraz tymczasowe magazynowanie odpadów.

3.2 Podsektor Transport odpadów obejmuje:

- Przedsiębiorstwa świadczące usługi w rozumieniu ustawy z dnia 14 grudnia 2012 r. o odpadach, polegające na transporcie odpadów, zobowiązane do uzyskania wpisu w rejestrze, o którym mowa w art. 49 ust. 1 ustawy z dnia 14 grudnia 2012 r. o odpadach, z wyłączeniem przedsiębiorstw, dla których usługi te nie stanowią podstawowej działalności gospodarczej określonej zgodnie z przepisami wydаныmi na podstawie art. 40 ust. 2 ustawy z dnia 29 czerwca 1995 r. o statystyce publicznej.

3.3 Podsektor Przetwarzanie odpadów, w tym sortowanie, wraz z nadzorem nad wymienionymi działaniami, a także późniejsze postępowanie z miejscami unieszkodliwiania odpadów obejmuje:

- Przedsiębiorstwa świadczące usługi w rozumieniu ustawy z dnia 14 grudnia 2012 r. o odpadach, polegające na przetwarzaniu odpadów w tym sortowaniu, wraz z nadzorem nad wymienionymi działaniami, a także podmioty świadczące usługi z późniejszym postępowaniem z miejscami unieszkodliwiania odpadów, zobowiązane do uzyskania wpisu w rejestrze, o którym mowa w art. 49 ust. 1 ustawy z dnia 14 grudnia 2012 r. o odpadach, z wyłączeniem przedsiębiorstw, dla których usługi te nie stanowią podstawowej działalności gospodarczej określonej zgodnie z przepisami wydanyymi na podstawie art. 40 ust. 2 ustawy z dnia 29 czerwca 1995 r. o statystyce publicznej.

3.4 Podsektor działania wykonywane w charakterze sprzedawcy odpadów lub pośrednika w obrocie odpadami obejmuje:

- Przedsiębiorstwa świadczące usługi w rozumieniu ustawy z dnia 14 grudnia 2012 r. o odpadach, polegające na działaniach wykonywanych w charakterze sprzedawcy odpadów lub pośrednika w obrocie odpadami, zobowiązane do uzyskania wpisu w rejestrze, o którym mowa w art. 49 ust. 1 ustawy z dnia 14 grudnia 2012 r. o odpadach, z wyłączeniem przedsiębiorstw, dla których usługi te nie stanowią podstawowej działalności gospodarczej określonej zgodnie z przepisami wydanyymi na podstawie art. 40 ust. 2 ustawy z dnia 29 czerwca 1995 r. o statystyce publicznej.

Zalegające śmieci są istotnym problemem. Wraz z rozwojem gospodarczym powstaje ich coraz więcej, co stanowi realne zagrożenie dla środowiska oraz dla naszego zdrowia. W szczególności część odpadów ma szczególnie negatywny wpływ na zdrowie czy środowisko w związku z czym konieczne jest zabezpieczenie tego sektora.

4. Produkcja, wytwarzanie i dystrybucja chemikaliów

Chemikalia są wykorzystywane przez wiele sektorów gospodarki oraz społeczeństwo. W tym kontekście ważne jest zapewnienie ciągłości łańcuchów dostaw chemikaliów. Incydent w fabryce chemikaliów może spowodować utrudnienia w dostawach, co będzie szczególnie dotkliwe, jeżeli dana fabryka jest jedyna w określonym regionie, a sprowadzenie zamienników może zająć dużo czasu. Incydent związany z chemikaliami może również doprowadzić do zanieczyszczenia środowiska oraz zdrowia i życia ludzi, jeżeli wskutek zdarzenia w systemie sterującym produkcją (np. wskutek błędu ludzkiego lub celowego ataku) dojdzie do wycieku chemikaliów. Naruszenie poufności systemów informacyjnych sterujących produkcją chemikaliów może z kolei spowodować naruszenie praw własności intelektualnej – takie zdarzenie może być efektem działań wywiadu przemysłowego.

W ramach tego sektora wyróżniony następujące rodzaje podmiotów:

- Przedsiębiorstwa zajmujące się produkcją substancji oraz dystrybucją substancji lub mieszanin, o których mowa w art. 3 pkt 9 i 14 rozporządzenia (WE) nr 1907/2006 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2006 r. w sprawie rejestracji, oceny, udzielania zezwoleń i stosowanych ograniczeń w zakresie chemikaliów (REACH) i utworzenia Europejskiej Agencji Chemikaliów, zmieniające dyrektywę 1999/45/WE oraz uchylające rozporządzenie Rady (EWG) nr 793/93 i rozporządzenie Komisji (WE) nr 1488/94, jak również dyrektywę Rady 76/769/EWG i dyrektywy Komisji 91/155/EWG, 93/67/EWG, 93/105/WE i 2000/21/WE (Dz. Urz. UE L 396 z 30.12.2006, str. 1, z późn. zm.).
 - W tym przypadku sformułowanie „Przedsiębiorstwa zajmujące się produkcją substancji oraz dystrybucją substancji lub mieszanin” należy rozumieć alternatywnie, tzn. dotyczy ono przedsiębiorstw które zarówno produkują i dystrybuują substancję i mieszaniny jak również tylko te, które wyłącznie produkują albo wyłącznie dystrybuują”. Dzięki temu zostanie uchwycony łańcuch dostaw w sektorze chemicznym.

- Przedsiębiorstwa zajmujące się wytwarzaniem z substancji lub mieszanin wyrobów o których mowa w art. 3 pkt 3 rozporządzenia (WE) nr 1907/2006 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2006 r. w sprawie rejestracji, oceny, udzielania zezwoleń i stosowanych ograniczeń w zakresie chemikaliów (REACH) i utworzenia Europejskiej Agencji Chemikaliów, zmieniające dyrektywę 1999/45/WE oraz uchylające rozporządzenie Rady (EWG) nr 793/93 i rozporządzenie Komisji (WE) nr 1488/94, jak również dyrektywę Rady 76/769/EWG i dyrektywy Komisji 91/155/EWG, 93/67/EWG, 93/105/WE i 2000/21/WE.
 - Określając, czy coś jest wyrobem w rozumieniu REACH, należy przeanalizować czy stanowi przedmiot, który podczas produkcji otrzymuje określony kształt, powierzchnię, konstrukcję lub wygląd zewnętrzny, co decyduje o jego funkcji w stopniu większym niż jego skład chemiczny. Taka sytuacja zachodzi na przykład w przypadku produkcji ubrań, podłóg, mebli, biżuterii, gazet czy plastikowych opakowań.

Wskazać należy, że sama dyrektywa NIS 2 wymienia powyższe rodzaje podmiotów jako należące do sektora ważnego i jedynie w zakresie definicyjnym odwołuje się do REACH nie wskazując na to, czy podmiot ten objęty jest wskazanymi w tym rozporządzeniu obowiązkami. Ani dyrektywa, ani ustawa, nie uzależnia zatem przynależności do sektora od objęcia obowiązkami na podstawie innych przepisów. Identyfikacja podmiotu jako podmiotu ważnego powinna zatem opierać się wyłącznie na badaniu przesłanek wynikających z ustawy.

5. Produkcja, przetwarzanie i dystrybucja żywności

Incydent związany z produkcją i dystrybucją żywności może doprowadzić do zaburzenia łańcuchów dostaw żywności, stąd też sektor ten został ujęty w dyrektywie NIS 2.

W ramach tego sektora wyróżniono:

- Przedsiębiorstwa spożywcze w rozumieniu art. 3 pkt 2 rozporządzenia (WE) nr 178/2002 Parlamentu Europejskiego i Rady z dnia 28 stycznia 2002 r. ustanawiające ogólne zasady i wymagania prawa żywnościowego, powołujące Europejski Urząd ds. Bezpieczeństwa Żywności oraz ustanawiające procedury w zakresie bezpieczeństwa żywności, zajmujące się dystrybucją hurtową oraz przemysłowymi produkcją i przetwarzaniem (Dz. Urz. UE L 31 z 01.02.2002, str. 1, z późn. zm.).

- Analogicznie jak w sektorze produkcji, wytwarzania i dystrybucji chemikaliów, do niniejszego sektora zaliczają się rozłącznie zarówno przedsiębiorstwa zajmujące się dystrybucją, produkcją jak i przetwarzaniem. Aby podlegać pod przepisy niniejszej ustawy nie zachodzi konieczność zajmowania się powyższą działalnością łącznie.

6. Sektor Produkcja

Zaburzenie ciągłości łańcuchów dostaw towarów może doprowadzić do poważnego utrudnienia funkcjonowania gospodarki.

Sektor produkcji mierzy z różnymi zagrożeniami, takimi jak:

- ataki poprzez łańcuch dostaw – brak odpowiednich środków technicznych i organizacyjnych w relacjach z dostawcami może spowodować, że złośliwi „aktorzy” będą próbowali zdobyć dostęp do kluczowych danych i systemów poprzez systemy dostawcy
- kradzież własności intelektualnej, naruszenie tajemnicy przedsiębiorstwa
- ataki na niezabezpieczone przemysłowe urządzenia Internetu Rzeczy, dzięki czemu atakujący mogą monitorować i kontrolować procesy w fabryce
- ataki phishingowe nakierowane na pracowników fabryki
- ataki ransomware prowadzące do zaszyfrowania danych oraz utrudniające produkcję
- ataki prowadzące do fizycznego uszkodzenia urządzeń produkcyjnych.

6.1 Podsektor Produkcja wyrobów medycznych i wyrobów medycznych do diagnostyki in vitro.

W ramach tego podsektora wskazano dwa rodzaje podmiotów:

- Podmioty produkujące wyroby medyczne w rozumieniu art. 2 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2017/745 z dnia 5 kwietnia 2017 r. w sprawie wyrobów medycznych, zmiany dyrektywy 2001/83/WE, rozporządzenia (WE) nr 178/2002 i rozporządzenia (WE) nr 1223/2009 oraz uchylecia dyrektyw Rady 90/385/EWG i 93/42/EWG (Dz. Urz. UE L 117 z 05.05.2017, str. 1, z późn. zm.).
- Podmioty produkujące wyroby medyczne do diagnostyki in vitro w rozumieniu art. 2 ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2017/746 z dnia 5 kwietnia 2017 r. w sprawie wyrobów medycznych do diagnostyki in vitro oraz uchylecia dyrektywy 98/79/WE i decyzji Komisji 2010/227/UE (Dz. Urz. UE L 117

z 05.05.2017, str. 176, z późn. zm.), z wyjątkiem podmiotów produkujących wyroby medyczne uznane za mające krytyczne znaczenie podczas danego stanu zagrożenia zdrowia publicznego.

6.2 Podsektor Produkcja komputerów, wyrobów elektronicznych i optycznych

Przedsiębiorca prowadzący którykolwiek z rodzajów działalności gospodarczej, o których mowa w sekcji C dział 26 klasyfikacji NACE Rev. 2, ujętej w załączniku I do rozporządzenia (WE) nr 1893/2006 Parlamentu Europejskiego i Rady z dnia 20 grudnia 2006 r. w sprawie statystycznej klasyfikacji działalności gospodarczej NACE Rev. 2 i zmieniającego rozporządzenie Rady (EWG) nr 3037/90 oraz niektóre rozporządzenia WE w sprawie określonych dziedzin statystycznych (Dz. Urz. UE L 393 z 30.12.2006, str. 1, z późn. zm.).

NACE	nazwa Nace	PKD 2025
26.11	Produkcja elementów elektronicznych	26.11.Z
26.12	Produkcja elektronicznych obwodów drukowanych	26.12.Z
26.20	Produkcja komputerów i urządzeń peryferyjnych	26.20.Z
26.30	Produkcja sprzętu (tele)komunikacyjnego	26.30.Z
26.40	Produkcja elektronicznego sprzętu powszechnego użytku	26.40.Z
26.51	Produkcja instrumentów i przyrządów pomiarowych, kontrolnych i nawigacyjnych	26.51.Z
26.52	Produkcja zegarków i zegarów	26.52.Z
26.60	Produkcja urządzeń napromieniowujących,	26.60.Z

	sprzętu elektromedycznego i elektroterapeutycznego	
26.70	Produkcja instrumentów optycznych i sprzętu fotograficznego	26.70.Z
26.80	Produkcja magnetycznych i optycznych niezapisanych nośników informacji	

6.3 Podsektor Produkcja urządzeń elektrycznych

Przedsiębiorca prowadzący którykolwiek z rodzajów działalności gospodarczej, o których mowa w sekcji C dział 27 klasyfikacji NACE Rev. 2.

NACE	nazwa Nace	PKD 2025
27.11	Produkcja elektrycznych silników, prądnic i transformatorów	27.11.Z
27.12	Produkcja aparatury rozdzielczej i sterowniczej energii elektrycznej	27.12.Z
27.20	Produkcja baterii i akumulatorów	27.20.Z
27.31	Produkcja kabli światłowodowych	27.31.Z
27.32	Produkcja pozostałych elektronicznych i elektrycznych przewodów i kabli	27.32.Z
27.33	Produkcja sprzętu instalacyjnego	27.33.Z
27.40	Produkcja elektrycznego sprzętu oświetleniowego	27.40.Z
27.51	Produkcja elektrycznego sprzętu gospodarstwa domowego	27.51.Z

27.52	Produkcja nonelektrycznego sprzętu gospodarstwa domowego	27.52.Z
27.90	Produkcja pozostałego sprzętu elektrycznego	27.90.Z

6.4 Podsektor Produkcja maszyn i urządzeń, gdzie indziej niesklasyfikowana

Przedsiębiorca prowadzący którykolwiek z rodzajów działalności gospodarczej, o których mowa w sekcji C dział 28 klasyfikacji NACE Rev. 2.

NACE	nazwa Nace	PKD 2025
28.11	Produkcja silników i turbin, z wyłączeniem silników lotniczych, samochodowych i motocyklowych	28.11.Z
28.12	Produkcja sprzętu i wyposażenia do napędu hydraulicznego i pneumatycznego	28.12.Z
28.13	Produkcja pozostałych pomp i sprężarek	28.13.Z
28.14	Produkcja pozostałych kurków i zaworów	28.14.Z
28.15	Produkcja łożysk, kół zębatach, przekładni zębatach i elementów napędowych	28.15.Z
28.21	Produkcja pieców, palenisk i palników piecowych	28.21.Z
28.22	Produkcja urządzeń dźwigowych i chwytaków	28.22.Z
28.23	Produkcja maszyn i sprzętu biurowego (z wyłączeniem	28.23.Z

	komputerów i urządzeń peryferyjnych)	
28.24	Produkcja narzędzi ręcznych mechanicznych	28.24.Z
28.25	Produkcja przemysłowych urządzeń chłodniczych i wentylacyjnych	28.25.Z
28.29	Produkcja pozostałych maszyn ogólnego przeznaczenia, gdzie indziej niesklasyfikowana	28.29.Z
28.30	Produkcja maszyn dla rolnictwa i leśnictwa	28.30.Z
28.41	Produkcja maszyn do obróbki metalu	28.41.Z
28.49	Produkcja pozostałych narzędzi mechanicznych	28.42.Z
28.91	Produkcja maszyn dla metalurgii	28.91.Z.
28.92	Produkcja maszyn dla górnictwa, kopalnictwa i budownictwa	28.92.Z
28.93	Produkcja maszyn stosowanych w przetwórstwie żywności, tytoniu i produkcji napojów	28.93.Z.
28.94	Produkcja maszyn dla przemysłu tekstylnego, odzieżowego i skórzanego	28.94.Z
28.95	Produkcja maszyn dla przemysłu papierniczego	28.95.Z
28.96	Produkcja maszyn do obróbki gumy lub tworzyw sztucznych	28.96.Z

	oraz wytwarzania wyrobów z tych materiałów	
28.99	Produkcja pozostałych maszyn specjalnego przeznaczenia, gdzie indziej niesklasyfikowana	28.99.Z

6.5 Podsektor Produkcja pojazdów samochodowych, przyczep i naczep

Przedsiębiorca prowadzący którykolwiek z rodzajów działalności gospodarczej, o których mowa w sekcji C dział 29 klasyfikacji NACE Rev. 2.

NACE	nazwa Nace	PKD 2025
29.10	Produkcja pojazdów samochodowych	29.10
29.20	Produkcja nadwozi do pojazdów silnikowych; produkcja przyczep i naczep	29.20.Z
29.31	Produkcja wyposażenia elektrycznego i elektronicznego do pojazdów silnikowych	29.31.Z
29.32	Produkcja pozostałych części i akcesoriów do pojazdów silnikowych	29.32.Z

6.6 Podsektor Produkcja pozostałego sprzętu transportowego

Przedsiębiorca prowadzący którykolwiek z rodzajów działalności gospodarczej, o których mowa w sekcji C dział 30 klasyfikacji NACE Rev. 2.30.11

	Produkcja statków i konstrukcji pływających	30.11.Z 30.13.Z
30.12	Produkcja łodzi wycieczkowych i sportowych	30.12.Z

30.20	Produkcja lokomotyw kolejowych oraz taboru szynowego	30.20.Z
30.30	Produkcja statków powietrznych, statków kosmicznych i podobnych maszyn	30.31.Z 30.32.Z
30.40	Produkcja wojskowych pojazdów bojowych	30.40.Z
30.91	Produkcja motocykli	30.91.Z
30.92	Produkcja rowerów i wózków inwalidzkich	30.92.Z
30.99	Produkcja pozostałego sprzętu transportowego, gdzie indziej niesklasyfikowana	30.99.Z

7. Dostawcy usług cyfrowych

Dostawcy usług cyfrowych występowali już na gruncie dyrektywy NIS. W dyrektywie NIS 2 zmieniono zakres podmiotowy tego zbioru podmiotów. Należy przy tym pamiętać, że jest to pojęcie specyficzne dla dyrektywy NIS 2 i nie można tego pojęcia ze wszystkimi podmiotami świadczącymi usługi drogą elektroniczną.

W ramach tego sektora wyodrębnia się:

- Dostawcę internetowej platformy handlowej – ten rodzaj podmiotu już występował na gruncie dyrektywy NIS,
- Dostawcę wyszukiwarki internetowej – ten rodzaj podmiotu już występował na gruncie dyrektywy NIS,
- Dostawcę platformy sieci usług społecznościowych.

Do tych podmiotów będą stosowały się szczególne regulacje dotyczące jurysdykcji państwa członkowskiego Unii Europejskiej – podlegają one właściwości państwa członkowskiego w którym podmiot ma główną siedzibę działalności.

8. *Badania naukowe*

W tym sektorze występują następujące rodzaje podmiotów:

- Organizacja badawcza,
- Podmioty, o których mowa w art. 7 ust. 1 pkt 1–4, 6–7 ustawy z dnia z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce.

Działania badawcze odgrywają kluczową rolę w rozwoju nowych produktów i procesów. Wiele z tych działań jest prowadzonych przez podmioty, które udostępniają, rozpowszechniają lub wykorzystują wyniki swoich badań do celów handlowych. Podmioty te mogą zatem być ważnymi uczestnikami łańcuchów wartości, co sprawia, że bezpieczeństwo ich sieci i systemów informatycznych stanowi integralną część ogólnego cyberbezpieczeństwa rynku wewnętrznego.

Dyrektywa NIS 2 nałożyła na organizacje badawcze obowiązki z zakresu zarządzania ryzykiem i zgłaszania incydentów. Do tej pory organizacje badawcze nie miały takich wymogów prawnych.

W projekcie ustawy o zmianie ustawy o KSC oraz niektórych innych ustaw definicja organizacji badawczej odwołuje się do osoby prawnej albo ułamnej osoby prawnej prowadzącej działalność wskazaną w ustawie z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce, tj. badania aplikacyjne oraz prace rozwojowe. Definicja organizacji badawczej wyłącza spod jej zakresu inne podmioty szkolnictwa wyższego, co jest zgodne z definicją z dyrektywy NIS 2.

Sektor badania naukowe jest sektorem ważnym. Oznacza to że, podmioty te mają mniejsze wymogi nadzorcze, nie mają obowiązku przeprowadzania cyklicznych audytów oraz maksymalna wysokość kary jest niższa niż w przypadku podmiotów kluczowych. Obowiązki z zakresu systemu zarządzania bezpieczeństwem informacji oraz zgłaszania incydentów są takie same jak dla podmiotów kluczowych. Podmioty z sektora organizacji badawczych będą obowiązane wdrożyć system zarządzania bezpieczeństwem informacji w systemie informacyjnym służącym w procesie świadczenia usług. Środki te mają być proporcjonalne do wielkości podmiotu i charakteru świadczonych usług. Podmioty te mają zgłaszać incydenty poważne do CSIRT sektorowego.

Organem właściwym do spraw cyberbezpieczeństwa dla tej grupy podmiotów będzie minister właściwy do spraw szkolnictwa wyższego i nauki. Zgodnie z projektem ustawy będzie

utworzony dla tej grupy podmiotów CSIRT sektorowy do którego podmioty te będą zgłaszały incydenty poważne za pomocą systemu teleinformatycznego S46.

Sektor badania naukowe tworzą:

- Organizacja badawcza:
 - osoba prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej jeżeli prowadzi działalność:
 - badania aplikacyjne rozumiane jako prace mające na celu zdobycie nowej wiedzy oraz umiejętności, nastawione na opracowywanie nowych produktów, procesów lub usług lub wprowadzanie do nich znaczących ulepszeń,
 - prace rozwojowe, które są działalnością obejmującą nabywanie, łączenie, kształtowanie i wykorzystywanie dostępnej aktualnie wiedzy i umiejętności, w tym w zakresie narzędzi informatycznych lub oprogramowania, do planowania produkcji oraz projektowania i tworzenia zmienionych, ulepszonych lub nowych produktów, procesów lub usług, z wyłączeniem działalności obejmującej rutynowe i okresowe zmiany wprowadzane do nich, nawet jeżeli takie zmiany mają charakter ulepszeń.
- Podmioty, o których mowa w art. 7 ust. 1 pkt 1–4, 6–7 ustawy z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce, tj.:
 - uczelnie,
 - federacje podmiotów systemu szkolnictwa wyższego i nauki, zwane dalej „federacjami”,
 - Polska Akademia Nauk, działająca na podstawie ustawy z dnia 30 kwietnia 2010 r. o Polskiej Akademii Nauk (Dz. U. z 2020 r. poz. 1796 oraz z 2025 r. poz. 621), zwana dalej „PAN”,
 - instytuty naukowe PAN, działające na podstawie ustawy, o której mowa w pkt 3, zwane dalej „instytutami PAN”,
 - międzynarodowe instytuty naukowe utworzone na podstawie odrębnych ustaw działające na terytorium Rzeczypospolitej Polskiej, zwane dalej „instytutami międzynarodowymi”,
 - Centrum Łukasiewicz, działające na podstawie ustawy z dnia 21 lutego 2019 r. o Sieci Badawczej Łukasiewicz (Dz. U. z 2024 r. poz. 925 i 1089),
 - instytuty działające w ramach Sieci Badawczej Łukasiewicz, zwane dalej „instytutami Sieci Łukasiewicz”,

- Centrum Medycznego Kształcenia Podyplomowego, działające na podstawie ustawy z dnia 13 września 2018 r. o Centrum Medycznego Kształcenia Podyplomowego (Dz. U. z 2025 r. poz. 269), zwane dalej „CMKP”,
- Polska Akademia Umiejętności, zwana dalej „PAU”.

Organizacje badawcze połączono w ramach sektora z pozostałymi podmiotami systemu szkolnictwa wyższego, ponieważ te podmioty również często prowadzą badania naukowe. Ponadto uczelnie już w chwili obecnej podlegały wymaganiom rozporządzenia Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych w zakresie wymogów cyberbezpieczeństwa oraz zgłaszania incydentów w podmiocie publicznym co z kolei wynika z rozdziału 5 obecnej ustawy o KSC.

Instytuty badawcze znajdują się w sektorze podmioty publiczne i mają status podmiotów kluczowych, ponieważ mogą otrzymać status państwowego instytutu badawczego, który to instytut może realizować zadania z zakresu bezpieczeństwa państwa i obronności.

9. Podmioty publiczne będące podmiotami ważnymi

W tym sektorze występują następujące rodzaje podmiotów:

- samorządowe jednostki budżetowe,
- samorządowe zakłady budżetowe,
- samorządowe instytucje kultury,
- spółki prawa handlowego wykonujące zadania o charakterze użyteczności publicznej w rozumieniu art. 1 ust. 2 ustawy z dnia 20 grudnia 1996 r. o gospodarce komunalnej.

Znajdujące się w tym sektorze podmioty będą objęte zmniejszonymi wymaganiami z zakresu cyberbezpieczeństwa. Wprowadzono tę zmianę po uwagach przedstawicieli samorządu terytorialnego, którzy wskazali, że te podmioty będą dużo mniejsze niż inne podmioty kluczowe i ważne i w związku z tym konieczne jest uwzględnienie ich specyfiki w przepisach.

Załącznik nr 3 do projektu ustawy określa funkcje krytyczne. Jest on oparty na rozwiązaniach z innych państw europejskich, zwłaszcza francuskiej liście funkcji krytycznych. Załącznik ten wskazuje funkcje których narażenie szczególnie zagroziłoby systemowi czy sieci w ramach której funkcjonują. Produkty, usługi lub procesy pochodzące od dostawcy wysokiego ryzyka

muszą być wycofane w pierwszej kolejności co odzwierciedla krótszy termin na wykonanie tego obowiązku.

Załącznik nr 4 obejmuje uproszczone wymagania dla samorządowych podmiotów publicznych, które są podmiotami ważnymi. Mają one charakter listy kontrolnej minimalnych wymogów takich jak inwentaryzacja zasobów informatycznych, weryfikacja uprawnień personelu, stosowanie oprogramowania antywirusowego czy stosowanie zasad cyberhigieny. Zrezygnowane więc z podejścia opartego na ryzyku, ponieważ wymagałoby to najpierw posiadania odpowiedniego personelu przez mniejsze jednostki samorządowe, który potrafiłby przeprowadzić szacowanie ryzyka i na podstawie tego wprowadzić odpowiednie środki techniczne i organizacyjne. Mniejsze jednostki samorządowe nie posiadają takich zasobów osobowych, stąd obniżono wymagania z zakresu cyberbezpieczeństwa.

W załączniku nr 4 określono, że system zarządzania bezpieczeństwem informacji dla podmiotu ważnego będącego podmiotem publicznym może dodatkowo obejmować określanie i kontrolowanie zasad korzystania przez podmiot publiczny będący podmiotem ważnym z ogólnodostępnych usług dostawców chmury obliczeniowej. Należy podkreślić, że obecnie żaden akt prawa powszechnie obowiązującego nie reguluje w pełni zasad korzystania z usług dostawców chmury obliczeniowej. Zagadnienia te najszerzej regulowane są obecnie w uchwale Rady Ministrów w sprawie Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa” (WIIP) oraz Standardach Cyberbezpieczeństwa Chmur Obliczeniowych (SCCO). Z uwagi na charakter tych dokumentów wiążą one jedynie podmioty wymienione w § 6 ust. 1 WIIP. Uchwała WIIP stanowi również podstawę dla systemu zapewnienia usług chmurowych (ZUCH), z którego korzystają także inne podmioty, nieobjęte uchwałą, w tym jednostki samorządu terytorialnego.

Mając powyższe na uwadze, a także cel wydania SCCO, tj. stworzenie dokumentu mającego stanowić pomoc dla jednostek administracji publicznej planujących skorzystanie z modelu przetwarzania danych w chmurach obliczeniowych, wprowadzającego jednolite standardy, upraszczającego proces wyboru dostawcy, zakresu usług i oceny cyberbezpieczeństwa środowiska przetwarzania, podmioty ważne będące podmiotami publicznymi (jako odbiorcy SCCO) powinny przy określaniu systemu zarządzania bezpieczeństwem informacji zgodnie z załącznikiem nr 4, uwzględniać zarówno uchwałę WIIP jak i SCCO, a także inne akty takie jak RODO czy ustawa o ochronie informacji niejawnych. Wynika to z potrzeby zapewnienia wysokiego poziomu bezpieczeństwa przetwarzanych danych w chmurze obliczeniowej,

spójnego podejścia administracji publicznej oraz dalszej niezakłóconej możliwości korzystania z usług oferowanych w systemie ZUCH.

10. Informacja o projektach aktów wykonawczych

Zgodnie z projektem ustawy obowiązkowo muszą zostać wydane następujące akty wykonawcze:

1. Rozporządzenie Rady Ministrów wydane na podstawie art. 11 ust. 4 określające progi uznania incydentu za poważny według rodzaju zdarzenia w poszczególnych sektorach i podsektorach określonych w załączniku nr 1 i 2 do ustawy.
2. Rozporządzenie Rady Ministrów wydane na podstawie art. 36d, które określi:
 - 1) tryb przeprowadzania oceny bezpieczeństwa,
 - 2) szczegółowe informacje przekazywane do zespołów CSIRT przy uzgadnianiu sposobu przeprowadzenia oceny bezpieczeństwa,
 - 3) rodzaje przeprowadzanych testów bezpieczeństwa w ramach oceny bezpieczeństwa,
 - 4) sposób niszczenia materiałów zawierających informacje, o których mowa w art. 36b ust. 10,
 - 5) tryb działania komisji, o której mowa w art. 36b ust. 11 zdanie pierwsze,
 - 6) wzór protokołu zniszczenia materiałów zawierających informacje, o których mowa w art. 36b ust. 10.
3. Rozporządzenie Rady Ministrów, określające szczegółowy zakres działania oraz tryb pracy Kolegium do spraw Cyberbezpieczeństwa – jest to konieczne, ze względu na zmianę przepisów materialnych dotyczących samego Kolegium.

Pozostałe rozporządzenia mają charakter fakultatywny.

11. Pozostałe informacje

Projektowana ustawa wejdzie w życie po upływie miesiąca od dnia jej ogłoszenia. Taki termin gwarantuje, że wszystkie podmioty, których dotyczą projektowane przepisy, będą miały czas na zapoznanie się z nimi. Termin ten jest też konieczny z uwagi na konieczność pilnego wdrożenia dyrektywy NIS 2, ponieważ termin jej wdrożenia – wypadający 17 października 2024 r. – został już przekroczony. Zauważyć przy tym należy, że ustawa przewiduje 6-miesięczny okres dostosowawczy dla podmiotów kluczowych i podmiotów ważnych. Takie rozwiązanie zapewni wdrożenie dyrektywy w terminie, a z drugiej strony pozwoli podmiotom przygotować się do jej wdrożenia.

Projekt ustawy nie zawiera przepisów technicznych w rozumieniu przepisów rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. poz. 2039 oraz z 2004 r. poz. 597) i w związku z tym nie podlega procedurze notyfikacji.

Projekt ustawy jest zgodny z przepisami prawa Unii Europejskiej i służy ich stosowaniu.

Projekt ustawy został przesłany do Europejskiego Banku Centralnego, w celu uzyskania opinii, natomiast nie podlegał przedstawieniu innym właściwym organom i instytucjom Unii Europejskiej, w celu uzyskania opinii, dokonania powiadomienia, konsultacji albo uzgodnienia. Opinia Europejskiego Banku Centralnego została sporządzona 20 stycznia 2025 r. a następnie opublikowana w portalu EUR-Lex¹⁰²⁾.

Projekt ustawy stosownie do wymogów art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingsowej w procesie stanowienia prawa (Dz. U. z 2025 r. poz. 677) oraz zgodnie z § 52 ust. 1 uchwały nr 190 Rady Ministrów z dnia 29 października 2013 r. – Regulamin pracy Rady Ministrów (M.P. z 2024 r. poz. 806 oraz z 2025 r. poz. 408) został udostępniony w BIP na stronie podmiotowej Rządowego Centrum Legislacji, w serwisie Rządowy Proces Legislacyjny, oraz w BIP na stronie podmiotowej Ministra Cyfryzacji.

¹⁰²⁾ <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52025AB0002&qid=1742257266264>.

Nazwa projektu Ustawa o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw Ministerstwo wiodące i ministerstwa współpracujące Ministerstwo Cyfryzacji Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu Paweł Olszewski, Sekretarz Stanu w Ministerstwie Cyfryzacji Kontakt do opiekuna merytorycznego projektu Łukasz Wojewoda, dyrektor Departamentu Cyberbezpieczeństwa w Ministerstwie Cyfryzacji Marcin Wysocki, zastępca dyrektora Departamentu Cyberbezpieczeństwa w Ministerstwie Cyfryzacji email: sekretariat.DC@cyfra.gov.pl tel. + 48 22 245 59 22	Data sporządzenia 30.10.2025 Źródło: Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz. Urz. UE L 333 z 27.12.2022, str. 80). Rozporządzenie delegowane Komisji (UE) 2024/1366 z dnia 11 marca 2024 r. uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/943 poprzez ustanowienie kodeksu sieci dotyczącego zasad sektorowych w zakresie aspektów cyberbezpieczeństwa w transgranicznych przepływach energii elektrycznej Kamień milowy reformy C3.1. Krajowego Planu Odbudowy i Zwiększania Odporności Inwestycja C3.1.1. Cyberbezpieczeństwo – CyberPL, infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo Nr w Wykazie prac legislacyjnych i programowych Rady Ministrów: UC32

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

Projektowana ustawa ma na celu wdrożenie dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz. Urz. UE L 333 z 27.12.2022 str. 80), zwanej dalej „dyrektywą NIS 2”.

Pojawianie się nowych cyberzagrożeń, jak również szybki wzrost katalogu usług publicznych dostępnych online powodują, że instytucje publiczne jak i podmioty prywatne odpowiedzialne za cyberbezpieczeństwo będą zmuszone poświęcać coraz więcej środków na zapewnienie cyberbezpieczeństwa. Zmieniająca się sytuacja międzynarodowa oraz konieczność dostarczenia usług dużej grupie nowych klientów sprawia, że niezbędne jest dalsze wzmacnianie podmiotów krajowego systemu cyberbezpieczeństwa. Tą sytuację uwiadamniają statystyki zespołu CSIRT NASK. W 2022 r. do zespołu CSIRT NASK zgłoszono ponad 39 000 incydentów cyberbezpieczeństwa, a w 2023 r. ponad 75 000 incydentów cyberbezpieczeństwa. Dyrektywa NIS 2 i przepisy ją implementujące są odpowiedzią na dynamicznie zmieniającą się sytuację w cyberprzestrzeni.

Dyrektywa NIS 2 zastąpiła dotychczasowy podział na operatorów usług kluczowych i dostawców usług cyfrowych określony w dyrektywie Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. Urz. UE L 194 z 19.07.2016, str. 1), zwanej dalej „dyrektywą NIS 1”, na podmioty kluczowe i podmioty ważne. Ponadto rozszerzeniu uległ katalog sektorów objętych dyrektywą. Dyrektywa NIS 2 nakłada również szereg obowiązków na podmioty kluczowe i podmioty ważne. Jako podstawowy obowiązek należy wskazać stosowanie odpowiednich i proporcjonalnych środków technicznych, operacyjnych i organizacyjnych w celu zarządzania ryzykiem dla bezpieczeństwa sieci i systemów informatycznych wykorzystywanych przez te podmioty do prowadzenia działalności lub świadczenia usług oraz w celu zapobiegania wpływowi incydentów na odbiorców ich usług lub na inne usługi bądź minimalizowania takiego wpływu.

Zauważono również, że uprawnienia Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa są niewystarczające w stosunku do zadań, które organ ten musi wypełniać. Pełnomocnikowi Rządu do Spraw Cyberbezpieczeństwa brakuje skutecznych środków oddziaływania na podmioty krajowego systemu cyberbezpieczeństwa. W przeciwieństwie do innych Pełnomocników Rządu nie ma on uprawnień do żądania niezbędnych informacji od

organów administracji rządowej, możliwości powoływania zespołów problemowych czy zlecania badań. Pełnomocnikowi Rządu do Spraw Cyberbezpieczeństwa brakuje również środka prawnego, który umożliwiłby wydawanie rekomendacji o charakterze technicznym (w tym zakresie – Narodowych Standardów Cyberbezpieczeństwa, o których mowa w już nieobowiązującej Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024, zwaną dalej, „Strategią”) i jednocześnie obowiązku uwzględnienia tych rekomendacji przez podmioty krajowego systemu cyberbezpieczeństwa, w trakcie procesu zarządzania ryzykiem.

Do tej pory zostały utworzone tylko dwa sektorowe zespoły cyberbezpieczeństwa – CSIRT KNF i CSIRT Centrum e-Zdrowie. W pozostałych sektorach gospodarki brakuje zespołów wspierających przedsiębiorców w reagowaniu na incydenty. Utworzenie tych zespołów przewiduje Inwestycja C3.1.1 Krajowego Planu Odbudowy i Zwiększania Odporności, zwanego dalej „KPO”, *Cyberbezpieczeństwo – CyberPL, infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo*. Planowana jest realizacja projektu pod nazwą „utworzenie lub rozwój przynajmniej 5 sektorowych Zespołów Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT)”.

Komisja Europejska wielokrotnie, m.in. w opublikowanych w marcu 2019 r. zaleceniach dot. cyberbezpieczeństwa sieci 5G podkreślała, że kwestia zapewnienia bezpieczeństwa wdrażanej technologii 5G jest priorytetem. Potwierdzenie tego znajduje swój wymiar w opublikowanym w styczniu 2020 r. zestawie środków dot. minimalnej harmonizacji i standaryzacji na poziomie Unii Europejskiej rozwiązań cyberbezpieczeństwa sieci 5G, określanego jako 5G Toolbox¹⁾. Zestaw obejmuje zarówno narzędzia o charakterze strategicznym i technicznym, jak i te o charakterze wspierającym. Cele są dwa: po pierwsze bezpieczeństwo sieci 5G, po drugie uspołnienie polityk państw członkowskich w obszarze bezpieczeństwa technologii 5G. 5G Toolbox zawiera także definicje zestawu środków zabezpieczających na poziomie strategicznym i technicznym oraz wskazuje działania wspierające stosowanie tych środków dla ograniczenia ryzyk cyberbezpieczeństwa w sieciach 5G, które będą kręgosłupem Jednolitego Rynku Cyfrowego (JRC) UE. Wyróżnione są m.in. środki o charakterze:

- 1) strategicznym – m.in. większe uprawnienia dla organów właściwych, w tym ocena ryzyka dostawców sprzętu lub oprogramowania (środek strategiczny SM03);
- 2) technicznym – m.in. badanie bezpieczeństwa oprogramowania i urządzeń – uprawnienia Pełnomocnika Rządu ds. Cyberbezpieczeństwa oraz zespołów CSIRT poziomu krajowego: CSIRT MON, CSIRT NASK, CSIRT GOV – wynikające z art. 33 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077 i 1222 oraz z 2025 r. poz. 1017 i 1069), zwanej dalej „KSC”;
- 3) wspierającym – m.in. dotyczące prac nad europejskim programem standaryzacji i certyfikacji cyberbezpieczeństwa.

Obecnie brakuje także podstawy prawnej do przeprowadzenia identyfikacji dostawców sprzętu lub oprogramowania, którzy stwarzają zagrożenie dla bezpieczeństwa narodowego, tym samym nie jest wdrożony środek SM03 z Toolboxa 5G.

Podsumowując, aby wdrożyć dyrektywę NIS 2 oraz postanowienia Toolboxa 5G konieczne jest wprowadzenie zmian na poziomie ustawowym.

Aby zapewnić stosowanie rozporządzenia delegowanego Komisji (UE) 2024/1366 z dnia 11 marca 2024 r. uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/943 poprzez ustanowienie kodeksu sieci dotyczącego zasad sektorowych w zakresie aspektów cyberbezpieczeństwa w transgranicznych przepływach energii elektrycznej należy wyznaczyć organ, który będzie realizował zadania nadzorcze wynikające z tego rozporządzenia.

2. Rekomendowane rozwiązanie, w tym planowane narzędzia interwencji, i oczekiwany efekt

Zmiany wprowadzone przez dyrektywę NIS 2 oraz pojawiające się nowe cyberzagrożenia powodują konieczność wprowadzenia stosownych zmian w KSC. Jest to podstawowy akt dotyczący cyberbezpieczeństwa w Polsce, który poprzednio wdrożył dyrektywę NIS 1. Istotne jest uspołnienie krajowego systemu cyberbezpieczeństwa z rozwiązaniami europejskimi. Poprzez zmianę KSC wdrożone zostaną także postanowienia Toolboxa 5G. Natomiast część zmian wprowadzanych do KSC wykracza poza obszar dyrektywy NIS 2 i są to zmiany niezbędne do zapewnienia kompleksowego stosowania dyrektywy NIS 2, które mają na uwadze obecną sytuację geopolityczną i stan rozwoju zmian technologicznych w cyberbezpieczeństwie.

Nowelizacja KSC polega w szczególności na:

- 1) rozszerzeniu katalogu podmiotów krajowego systemu cyberbezpieczeństwa o nowe sektory gospodarki (ścieki, zarządzanie ICT, przestrzeń kosmiczna, poczta, produkcja, produkcja i dystrybucja chemikaliów, produkcja i dystrybucja żywności);

¹⁾ *Cybersecurity of 5G networks. EU Toolbox of risk mitigating measures*, <https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures>.

- 2) nałożeniu obowiązków z zakresu środków zarządzania ryzykiem na podmioty kluczowe lub podmioty ważne w cyberbezpieczeństwie, dotyczące w szczególności stosowania odpowiednich i proporcjonalnych środków technicznych, operacyjnych i organizacyjnych w celu zarządzania ryzykiem dla bezpieczeństwa sieci i systemów informatycznych, zgodne z dyrektywą NIS 2;
- 3) wprowadzeniu odpowiedzialności kierownika podmiotu kluczowego lub podmiotu ważnego za realizację zadań z zakresu cyberbezpieczeństwa – kierownik takiego podmiotu będzie odpowiedzialny za realizację tych zadań przez dany podmiot; w przypadku niewywiązania się z tych zadań na kierownika będą mogły być nałożone kary; kierownik będzie obowiązany również do przejścia stosownego szkolenia z zakresu cyberbezpieczeństwa;
- 4) wprowadzeniu możliwości zgłaszania incydentów przez podmioty kluczowe i podmioty ważne, za pomocą systemu teleinformatycznego ministra właściwego do spraw informatyzacji, zwanego dalej „ministrem”, do właściwych zespołów CSIRT sektorowych i CSIRT poziomu krajowego;
- 5) utworzeniu zespołów CSIRT sektorowych w poszczególnych sektorach gospodarki, które będą wspierać podmioty kluczowe i podmioty ważne w obsłudze incydentów cyberbezpieczeństwa;
- 6) wzmocnieniu kompetencji nadzorczych organów właściwych do spraw cyberbezpieczeństwa, polegających na możliwości wydawania ostrzeżeń, wyznaczania urzędnika monitorującego wykonywanie obowiązków przez dany podmiot kluczowy, nakazywanie przeprowadzenia oceny bezpieczeństwa systemu informacyjnego, nakazywanie przeprowadzenia audytu bezpieczeństwa;
- 7) wprowadzeniu nowych kar pieniężnych za niewykonanie obowiązków ustawowych przez podmioty kluczowe lub podmioty ważne, m.in. za niewdrożenie systemu zarządzania bezpieczeństwem informacji czy niezarejestrowanie się w wykazie podmiotów kluczowych i podmiotów ważnych;
- 8) wprowadzeniu Krajowego Planu reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę;
- 9) rozszerzeniu kompetencji ministra (organ ten będzie mógł dokonać, w drodze decyzji, prawnej identyfikacji dostawcy wysokiego ryzyka, będzie mógł też wydać polecenie zabezpieczające ze wskazaniem zachowania, które ograniczy skutki trwającego incydentu krytycznego);
- 10) wzmocnieniu pozycji Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa poprzez wyposażenie go w konkretne uprawnienia w zakresie wydawania rekomendacji mających na celu wzmocnienie poziomu cyberbezpieczeństwa systemów informacyjnych podmiotów krajowego systemu cyberbezpieczeństwa; Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa będzie mógł także żądać informacji niezbędnych do wykonywania jego zadań od organów administracji rządowej oraz zlecać wykonanie badań niezbędnych do realizacji jego zadań; Pełnomocnikowi Rządu do Spraw Cyberbezpieczeństwa umożliwi się także zakupy oprogramowania z zakresu cyberbezpieczeństwa dla uczestników posiedzeń Połączonego Centrum Operacyjnego Cyberbezpieczeństwa;
- 11) rozszerzeniu kompetencji zespołów CSIRT poziomu krajowego, w tym CSIRT NASK, co jest związane ze zwiększoną liczbą podmiotów kluczowych i podmiotów ważnych, którym CSIRT NASK będzie udzielał wsparcia w reagowaniu na incydenty;
- 12) rozwijaniu kompetencji ministra w zakresie edukacji cyberbezpieczeństwa – przewiduje się środki na prowadzenie kampanii edukacyjnych i programów z zakresu cyberbezpieczeństwa.

Projekt ustawy służy również realizacji celów (już nieobowiązującej) Strategii, jakimi są podniesienie poziomu odporności na cyberzagrożenia oraz poziomu ochrony informacji w sektorach: publicznym, militarnym i prywatnym. Projekt realizuje także cel szczegółowy Strategii, odnoszący się do rozwoju krajowego systemu cyberbezpieczeństwa poprzez ewaluację przepisów prawa dotyczących cyberbezpieczeństwa. Ponadto, projekt realizuje cele Strategii w odniesieniu do zapewnienia bezpieczeństwa łańcucha dostaw sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa.

Jednocześnie wprowadzenie w życie projektowanych zmian w KSC zrealizuje kamień milowy reformy C3.1.1 KPO *Cyberbezpieczeństwo – CyberPL, infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo*.

W projekcie nałożono obowiązki na podmioty kluczowe i podmioty ważne zgodne z wykazem tych podmiotów wskazanych w załączniku nr 1 i 2 do dyrektywy NIS 2. Będą one obowiązane dokonać samorejestracji w wykazie podmiotów kluczowych lub podmiotów ważnych, co umożliwi ich identyfikację, aktywne wsparcie ich przez zespoły CSIRT sektorowe i zespoły CSIRT poziomu krajowego oraz wykonywanie czynności nadzorczych przez organy właściwe do spraw cyberbezpieczeństwa. Umożliwi to także przekazywanie danych o liczbie tych podmiotów do Komisji Europejskiej i Agencji Unii Europejskiej do spraw Cyberbezpieczeństwa.

Podmioty kluczowe i podmioty ważne będą obowiązane wprowadzić system zarządzania bezpieczeństwem informacji w procesach służących świadczeniu usług przez te podmioty. Odpowiada to zakresowi wymogów co do środków zarządzania ryzykiem wskazanych w art. 21 dyrektywy NIS 2. Podmioty kluczowe obowiązane będą przeprowadzać audyty bezpieczeństwa co trzy lata. Możliwe będzie także zlecenie podmiotowi przeprowadzenie audytu doraźnego.

Dyrektywa NIS 2 wprowadziła nowe rozwiązania w zakresie zgłaszania incydentów poważnych. Zmiany te polegają na m.in. dwuetapowym zgłaszaniu incydu, tj. w pierwszej kolejności podmiot kluczowy lub podmiot ważny będzie zgłaszał do CSIRT sektorowego wczesne ostrzeżenie o incydencie poważnym (24 godziny od momentu wykrycia), kolejnym krokiem będzie zgłoszenie incydu poważnego (72 godziny od momentu wykrycia). Zgłoszenie wczesnego ostrzeżenia może zawierać wniosek o wskazanie wytycznych dotyczących możliwych do wdrożenia środków ograniczających skutki incydu poważnego lub o wsparcie techniczne przy obsłudze incydu. CSIRT sektorowy zobowiązany będzie w terminie 24 godzin udzielić wsparcia zgodnie z treścią wniosku.

W trakcie obsługi incydu poważnego podmiot zgłaszający incydu, na wniosek CSIRT sektorowego, przekazuje sprawozdanie okresowe z obsługi tego incydu. Natomiast sprawozdanie końcowe z obsługi incydu poważnego przekazywane będzie nie później niż w ciągu miesiąca od dnia zgłoszenia incydu. Jeżeli jednak obsługa incydu poważnego nie zakończy się w terminie miesiąca podmiot zgłaszający incydu poważny przesyła sprawozdanie z postępu obsługi incydu, a sprawozdanie końcowe w terminie miesiąca od zakończenia obsługi tego incydu.

Progi uznania incydu za incydu poważny zostaną określone przez Radę Ministrów, w drodze rozporządzenia.

Zgłoszenie incydu będzie dokonywane za pośrednictwem systemu S46. Zgodnie z projektem ustawy system S46 zostanie dostosowany do tego, by stać się głównym środkiem komunikacji pomiędzy podmiotami krajowego systemu cyberbezpieczeństwa. W związku z koniecznością dodania do tego systemu bardzo dużej liczby podmiotów zrezygnowano z zawierania porozumienia o dołączeniu do systemu. Ponadto dołączenie do systemu nie będzie już wymagało zakupu specjalnych urządzeń, ale będzie odbywało się za pomocą rozwiązań chmurowych. Podmioty kluczowe i podmioty ważne są obowiązane zapewnić zgodność swoich systemów informacyjnych z minimalnymi wymaganiami technicznymi i funkcjonalnymi podłączenia do systemu.

Projektowane rozwiązania zapewnią szybkie reagowanie na pojawiające się incydenty.

Krajowy Plan reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę będzie nowym dokumentem strategicznym przyjmowanym w drodze uchwały Rady Ministrów. Dokument ten będzie określał zasady postępowania w przypadku wystąpienia takiego incydu oraz zasady współpracy między organami realizującymi zadania z zakresu cyberbezpieczeństwa oraz organami właściwymi do spraw zarządzania kryzysowego. Pozwoli to na zwiększenie efektywności działania współpracujących organów. Przyjęcie takiego dokumentu jest wymagane przez dyrektywę NIS 2.

Minister, w drodze postępowania administracyjnego, może uznać dostawcę produktów ICT, usług ICT lub procesów ICT za dostawcę wysokiego ryzyka. Sprzęt takiego dostawcy będzie musiał być wycofany z systemów podmiotów kluczowych lub podmiotów ważnych, a nowy nie będzie mógł być wprowadzany do użytku. Pozwoli to wyeliminować potencjalnie niebezpieczny sprzęt z systemów teleinformatycznych podmiotów, których działalność jest szczególnie istotna dla funkcjonowania społeczeństwa. Wycofanie produktów ICT, usług ICT i procesów ICT dostarczanych przez dostawcę wysokiego ryzyka wiązać się może z kosztami, które będą musiały ponieść podmioty kluczowe lub podmioty ważne. Nie jest jednak możliwe w tej chwili wskazanie tych kosztów, ponieważ nie można obecnie przewidzieć jaką decyzję wyda minister właściwy do spraw informatyzacji, a w związku z tym jakie koszty poniosą podmioty zobowiązane do wycofania sprzętu. Należy podkreślić, że w projektowanych przepisach nie ma mechanizmu nakazującego natychmiastowe wycofanie sprzętu lub oprogramowania wskazanego w ocenie ryzyka dostawców. Podmioty kluczowe i podmioty ważne zostaną zobowiązane do wycofania danego sprzętu lub oprogramowania w określonym czasie.

Należy podkreślić, że przyjęcie przepisów adresujących zagrożenie wynikające z działania dostawców wysokiego ryzyka wynika z przyjętego przez państwa członkowskie Toolboxa 5G, który to dokument wymaga wprowadzenia takich środków. To podejście potwierdza także Komisja Europejska w swoim komunikacie z dnia 29 stycznia 2020 r., który stanowi, że państwa członkowskie zgodziły się co do konieczności oceny profilu ryzyka poszczególnych dostawców i w konsekwencji stosowania odpowiednich ograniczeń wobec dostawców uznanych za stwarzających wysokie ryzyko, w tym niezbędnych wyłączeń, aby skutecznie łagodzić ryzyko w odniesieniu do kluczowych aktywów, jak wskazano w Toolboxie²⁾.

Minister będzie mógł wydać, w drodze decyzji administracyjnej, polecenie zabezpieczające w przypadku wystąpienia incydu krytycznego. Zawarte w nim będzie wskazanie określonego zachowania, które zmniejszy skutki incydu lub zapobiegnie jego rozprzestrzenianiu się. Może to być m.in. nakaz zastosowania określonej poprawki bezpieczeństwa, nakaz szczególnej konfiguracji sprzętu lub oprogramowania, zakaz korzystania z określonego sprzętu lub oprogramowania. Jednocześnie należy wskazać, że zakaz korzystania z konkretnych usług i oprogramowania będzie dotyczył wyłącznie rozwiązań mających związek z trwającym incydem krytycznym. Takie rozwiązanie jest

²⁾ https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=COM:2020:0050:FIN&_sm_au_=iVVZRW54FHZ10n2PVkFHNKt0jRsMJ.

niezbędne, aby zapewnić skuteczną odpowiedź na wystąpienie najbardziej niebezpiecznego incydentu. W szczególności celem tego rozwiązania jest zapobiegnięcie scenariuszowi rozlewania się incydentu na kolejne sektory, np. w przypadku wystąpienia incydentu u operatora telekomunikacyjnego napastnicy mogą potencjalnie uzyskać dostęp do systemów jego klientów, wśród których mogą znajdować się szpitale czy elektrownie. Administracja musi posiadać narzędzia, które pozwolą zapobiec realizacji takiego scenariusza.

Zmiany wprowadzane projektem obejmą w dużym zakresie przepisy dotyczące nadzoru i egzekwowania przepisów. Widoczne to jest m.in. na przykładzie obecnych Operatorów Usług Kluczowych, których wyznaczono ok. 397. Dyrektywa NIS 2 obejmować będzie swoim zakresem zdecydowanie więcej podmiotów, głównie z powodu objęcia tą regulacją większej ilości sektorów. Obecnie KSC nadzór nad podmiotami krajowego systemu cyberbezpieczeństwa statuuje w art. 53, który określa organy nadzoru właściwe dla poszczególnych podmiotów oraz doprecyzowuje zakres tego nadzoru. Określone zostały również sposoby nadzoru, które w głównej mierze sprowadzają się do prowadzenia kontroli oraz nakładania kar pieniężnych na operatorów usług kluczowych i dostawców usług cyfrowych. Projektowane regulacje znacznie rozbudowują ten obszar wyposażając organy właściwe do spraw cyberbezpieczeństwa w szerokie kompetencje nadzoru i egzekwowania przepisów takie jak wydawanie ostrzeżeń, nakazów, decyzji administracyjnych nakazujących podjęcie lub zaniechanie określonego działania. Organy te zostaną również wyposażone w środki, które znajdą zastosowanie w sytuacji, w której podmiot kluczowy lub podmiot ważny nie wykonał w terminie postanowień określonych w ostrzeżeniu, nakazie czy decyzji. Wprowadza się również katalog kryteriów, które organ właściwy do spraw cyberbezpieczeństwa będzie musiał przeanalizować w celu podjęcia działań nadzorczych i egzekwowania przepisów, w tym także nakładania kar pieniężnych.

W związku z rozbudowanymi kompetencjami w powyższym zakresie, wprowadza się także możliwość stworzenia przez organ właściwy do spraw cyberbezpieczeństwa metodyki nadzoru oraz określenie hierarchii priorytetów działań nadzorczych w oparciu o metodykę i analizę ryzyka. Pozwoli to na właściwe zarządzanie swoimi obowiązkami i kompetencjami, a także prawidłowe i efektywne prowadzenie nadzoru co w konsekwencji przełoży się na wysoki poziom cyberbezpieczeństwa kraju. Powyższe zmiany związane są z kompleksowym podejściem dyrektywy NIS 2 do nadzoru, ale również są wynikiem przeprowadzonej analizy obecnie obowiązujących przepisów i doświadczeń zebranych w toku ich funkcjonowania.

Nadzór wobec podmiotów kluczowych będzie miał charakter *ex ante*, a wobec podmiotów ważnych *ex post*.

Zmiana przepisów merytorycznych, w szczególności nałożenie na podmioty kluczowe i podmioty ważne nowych obowiązków i wyposażenie organów właściwych do spraw cyberbezpieczeństwa w nowe kompetencje nadzorcze, implikuje konieczność wprowadzenia szeregu zmian w przepisach o karach pieniężnych, w tym rozbudowany katalog przypadków określających, kiedy podmioty kluczowe lub podmioty ważne podlegają karze pieniężnej, fakultatywne kary pieniężne nakładane na podmiot kluczowy lub podmiot ważny lub na kierownika podmiotu kluczowego lub podmiotu ważnego, zmianę wysokości kar pieniężnych, określenie formy i procedury wymierzania kar pieniężnych oraz termin jej płatności. Wprowadzona zostanie również okresowa kara pieniężna w celu przymuszenia podmiotu kluczowego lub podmiotu ważnego do realizacji nałożonych na niego obowiązków.

Oczekiwanym skutkiem wejścia w życie zaproponowanych przepisów będzie prawidłowe implementowanie do porządku krajowego przepisów dyrektywy NIS 2 oraz zapewnienie sprawnego i skutecznego nadzoru nad podmiotami kluczowymi i podmiotami ważnymi, a przede wszystkim podniesienie poziomu krajowego poziomu cyberbezpieczeństwa.

Minister właściwy do spraw energii będzie organem właściwym w rozumieniu rozporządzenia delegowanego Komisji (UE) 2024/1366 z dnia 11 marca 2024 r. uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/943 poprzez ustanowienie kodeksu sieci dotyczącego zasad sektorowych w zakresie aspektów cyberbezpieczeństwa w transgranicznych przepływach energii elektrycznej.

3. Jak problem został rozwiązany w innych krajach, w szczególności krajach członkowskich OECD/UE?

W celu porównania zaproponowanych w projekcie regulacji z rozwiązaniami z innych krajów wybrane zostały trzy kraje o odmiennych warunkach i położeniu geograficznym. Pierwszym z analizowanych krajów były Niemcy, duży kraj, w którym szczególnie dużo podmiotów będzie podlegało przepisom dyrektywy NIS 2. Jest to również kraj o znacznych zasobach i zdolnościach w zakresie działania w cyberprzestrzeni. Kolejnym wybranym krajem jest Belgia, która również posiada znaczne zasoby, ale jest znacznie mniejsza, co oznacza, że liczba podmiotów dotkniętych nowymi regulacjami będzie znacznie mniejsza niż w przypadku Niemiec. Wobec tego możliwa jest ocena, jak państwa o innych uwarunkowaniach podchodzą do kwestii systemu cyberbezpieczeństwa. Zdecydowano się również przeanalizować rozwiązania z innego kraju Europy Środkowo-Wschodniej, tak aby móc przeanalizować, czy inna sytuacja tego regionu w polityce międzynarodowej wpływa na przyjmowane rozwiązania. Ze względu na to, że żaden z krajów tego regionu nie implementował jeszcze przepisów dotyczących NIS 2 podjęto decyzję

o przeanalizowaniu rozwiązania zawartego w czeskim projekcie ustawy, który jest na zaawansowanym etapie prac legislacyjnych.

W zakresie reagowania na incydenty krytyczne przeanalizowane zostały 3 kraje – Czechy, Niemcy i Włochy. Są to stosunkowo duże kraje, posiadające rozległe rynki, które często mierzą się z podobnymi problemami. Czechy, pomimo różnic wielkościowych, są z kolei krajem z Europy Środkowo-Wschodniej, co daje nam możliwość zapoznania się z perspektywą innego kraju narażonego na podobne zagrożenia jak Polska.

Niemcy

W Niemczech model nadzoru nad cyberbezpieczeństwem ma charakter scentralizowany, a zadania, w tym zakresie wykonywane są przez Federalny Urząd ds. Bezpieczeństwa Informacji (BSI), który będzie m.in. sprawował nadzór nad wszystkimi podmiotami kluczowymi i podmiotami ważnymi.

Obowiązki nałożone na podmioty kluczowe i podmioty ważne w zakresie środków mających zapewnić cyberbezpieczeństwo zostały wskazane w sposób ogólny. Mają one być zgodne z aktualnym stanem wiedzy oraz uwzględniać odpowiednie normy europejskie i międzynarodowe, koszty wdrożenia poszczególnych rozwiązań, mają także być adekwatne do oszacowanego ryzyka. Minimalne środki jakie powinny być zastosowane zostały wskazane wprost w ustawie. Status podmiotów kluczowych i podmiotów ważnych będzie nadawany z mocy samej ustawy. Podmioty spełniające wymogi ustawowe będą musiały zarejestrować się w BSI, w ciągu 3 miesięcy od wejścia w życie ustawy. Urząd może sam zarejestrować taki podmiot, jeśli nie wykona on swojego obowiązku.

Ustawa przewiduje również specjalną procedurę zwolnienia z wykonywania obowiązków określonych w ustawie dla podmiotów wykonujących zadania związane z bezpieczeństwem narodowym lub bezpieczeństwem publicznym.

Urzędy federalne muszą przeznaczać co najmniej 20% wydatków informatycznych na cyberbezpieczeństwo.

W rozporządzeniu do ustawy może być wprowadzony obowiązek korzystania z certyfikowanych produktów i usług.

Belgia

W Belgii przygotowany został projekt ustawy implementującej dyrektywę NIS 2. Przygotowana ustawa ma zastąpić dotychczasową ustawę regulującą kwestie cyberbezpieczeństwa.

Zgodnie z nową ustawą status podmiotu kluczowego i podmiotu ważnego będą posiadać z mocy prawa podmioty, które spełniają warunki określone w ustawie, będące bezpośrednim przeniesieniem przepisów dyrektywy NIS 2. Do podmiotów, które nie spełniają tych warunków, ale z innych powodów powinny być objęte regulacją, np. są jedynym dostawcą danej usługi w Belgii, pomimo niespełniania kryteriów z dyrektywy NIS 2, mogą być wydane decyzje o uznaniu ich za taki podmiot. Decyzje te wydaje krajowy organ ds. cyberbezpieczeństwa, po zasięgnięciu opinii sektorowego organu cyberbezpieczeństwa. W przypadku gdy opinia ta jest negatywna, sprawa jest kierowana do Rady Bezpieczeństwa Narodowego. Krajowy organ co dwa lata dokonuje przeglądu wydanych decyzji.

Od momentu wejścia w życie przepisów implementujących dyrektywę NIS 2 podmioty kluczowe i podmioty ważne będą miały 5 miesięcy na zarejestrowanie się w odpowiedniej bazie danych. W przypadku zmiany określonych danych, podmioty te będą miały dwa tygodnie na ich aktualizację.

Dużą rolę w ramach nowej legislacji będą miały akty wykonawcze wydawane przez króla. W takiej formie będzie przyjęty m.in. krajowy plan reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę.

Ustawa przewiduje również formułę dobrowolnego zgłaszania incydentów w przypadku gdy prawo nie wymaga, aby dany incydent zgłaszać, m.in. gdy podmiot, u którego incydent wystąpił nie jest podmiotem kluczowym ani podmiotem ważnym.

Ustawa określiła minimalne środki zarządzania ryzykiem w cyberbezpieczeństwie, ale to jakie dokładnie środki mają być zastosowane zależą od analizy ryzyka w konkretnym podmiocie. Odpowiedzialność za prawidłowe jej sporządzenie spoczywa na danym podmiocie.

Ustawa wyraźnie wskazuje także ogólną odpowiedzialność kierownictwa za działania, w tym zakresie i nakłada obowiązek odpowiedniego przeszkolenia wszystkich osób z kierownictwa w zakresie cyberbezpieczeństwa.

Czechy

Czeski projekt ustawy implementującej dyrektywę NIS 2 jest bardzo obszerny i zawiera rozwiązania wykraczające poza wąsko rozumiane wprowadzenie przepisów Unii Europejskiej do krajowego porządku prawnego. Projekt przewiduje utworzenie Agencji Cyberbezpieczeństwa na wzór niemieckiego BSI czy francuskiego ANSSI, która będzie zajmować się szerokim spektrum zadań z tego obszaru.

Projekt określa ogólne warunki do uznania danego podmiotu za dostawcę usług regulowanych. W zależności od rodzaju działalności dostawca usług regulowanych może być obowiązany do stosowania wysokiego reżimu cyberbezpieczeństwa albo niskiego reżimu cyberbezpieczeństwa. Jeśli dany podmiot wykonuje działalność z obu grup to wszystkie jego usługi są objęte wysokim reżimem. Na podmioty spełniające te warunki ustawa nakłada obowiązek zgłoszenia się do Agencji Cyberbezpieczeństwa w ciągu 30 dni od uzyskania wiedzy o tym. Agencja może również wpisać do wykazu tych podmiotów, te z nich o których wie, że spełniają wymagania. Projekt przewiduje również

odrębny tryb wpisu do wykazu dla podmiotów spełniających odrębnie uregulowane warunki. Ten wpis będzie odbywał się na podstawie decyzji administracyjnej Prezesa Agencji. Z obowiązkiem zgłoszenia się do Agencji powiązana została sankcja karnoadministracyjna.

Dostawcy usług regulowanych mają obowiązek wdrożyć wymagane prawem rozwiązania w ciągu roku od wpisu do wykazu. Obowiązki te ujęte są bardzo ogólnie w samej ustawie, a uszczegółowione zostaną w aktach wykonawczych. Bardziej szczegółowo niż w samej dyrektywie NIS 2 zostały w nich określone środki techniczne i organizacyjne jakie mają stosować dostawcy usług regulowanych. W szczególności należy zwrócić uwagę na uregulowanie obowiązków i zadań kierownictwa podmiotów kluczowych i podmiotów ważnych. Do ich zadań należy np. informowanie pracowników o znaczeniu cyberbezpieczeństwa czy zapewniania odpowiednich zasobów do realizacji zadań z tego obszaru. Akty wykonawcze nakazują też dokonanie określonych zmian w strukturze tych podmiotów poprzez utworzenie Komitetu Zarządzania Cyberbezpieczeństwem, w którym będzie musiał zasiadać przedstawiciel kierownictwa danego podmiotu. Ponadto w akcie wykonawczym określono zakres zadań: – menadżera ds. cyberbezpieczeństwa, – architekta cyberbezpieczeństwa, – audytora cyberbezpieczeństwa i – osoby odpowiedzialnej za bezpieczeństwo zasobów i nakazano utworzyć takie stanowiska u dostawców usług regulowanych.

Agencja Cyberbezpieczeństwa może stosować środki zaradcze w postaci różnego rodzaju ostrzeżeń i środków reaktywnych. W ramach środków reaktywnych Agencja może nakazać dostawcy usług zastosowanie określonych środków, określonych w sposób ogólny, w drodze decyzji. Taki środek jest podawany do wiadomości publicznej, a ponadto Agencja informuje o nim podmioty, do których jest skierowany. Środek obowiązuje od chwili jego ogłoszenia.

Projekt przewiduje również wyłączenie stosowania przepisów o dostępie do informacji publicznej do informacji, których ujawnienie mogłoby utrudnić zapewnianie cyberbezpieczeństwa lub zmniejszać efektywność środków zaradczych.

Ustawa definiuje strategicznie ważne sektory. W odniesieniu do podmiotów, w tych sektorach, Agencja może ustanowić dodatkowe warunki dotyczące dostawców sprzętu i usług oraz zakazać stosowania sprzętu określonego dostawcy, jeśli stwierdzono, że w oparciu o kryteria ryzyka dostawców występuje znaczne zagrożenie dla bezpieczeństwa państwa, porządku wewnętrznego lub porządku publicznego.

Przewidziany został również specyficzny stan nadzwyczajny – stan cyberzagrożenia. W czasie jego trwania Agencja może wydawać rozstrzygnięcia z pominięciem przepisów o postępowaniu administracyjnym. W ramach tych rozstrzygnięć może np. zakazać stosowania określonego sprzętu przez organy administracji czy zobowiązać określone podmioty publiczne do udzielenia pomocy.

Należy zauważyć, że wszystkie projekty przewidują pewną formę samoidentyfikacji podmiotów kluczowych i podmiotów ważnych, o których mówi dyrektywa NIS 2.

Analiza w zakresie środków reagowania na incydenty krytyczne

Czechy

Czeska Agencja ds. cyberbezpieczeństwa NUKIB na podstawie sekcji 12 (1) ustawy o cyberbezpieczeństwie³⁾, może wydawać ostrzeżenia do podmiotów. Ostrzeżenia wydawane są w przypadku wysokiego prawdopodobieństwa wystąpienia sytuacji kryzysowej, która może mieć krytyczne znaczenie dla bezpieczeństwa państwa. Ostrzeżenie zawiera także listę rekomendowanych działań, które podmioty powinny wdrożyć celem ograniczenia ryzyk związanych z sytuacją kryzysową. Przykłady rekomendacji: zwrócenie uwagi na określony typ cyberataków np. spear-phishingów, potrzebie zablokowania dostępu do swojej infrastruktury IT, pilnej konieczności dokonania aktualizacji oprogramowania, czy też zwrócenie szczególnej uwagi na wskazane w ostrzeżeniu domeny. Przykładem takiego ostrzeżenia jest dokument wydany dnia 16 kwietnia 2020 r. znak 2066/2020-NÚKIB-E/350. Na podstawie analizy możliwych zagrożeń NUKIB wydał ostrzeżenie dla całego państwa, ze szczególnym naciskiem na sektor ochrony zdrowia⁴⁾. Innym przykładem jest ostrzeżenie NUKIB z dnia 25 lutego 2022 r. znak 2384/2022-NÚKIB-E/350 wskazujące na cyberzagrożenia o charakterze krytycznym, którego wystąpienie w systemach czeskiej administracji publicznej czy innych organizacji strategicznych jest bardzo prawdopodobne⁵⁾.

Niemcy

Niemiecki Federalny Urząd Bezpieczeństwa Teleinformatycznego (Bundesamt für Sicherheit in der Informationstechnik – BSI) może, na podstawie § 7 BSI-Gesetz⁶⁾ ogłaszać ostrzeżenia o: podatnościach w produktach

³⁾ Zákon č. 181/2014 Sb. Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) <https://www.zakonyprolidi.cz/cs/2014-181>.

⁴⁾ https://www.nukib.cz/download/publications_en/Warning-NUKIB-2020-04-16.pdf.

⁵⁾ https://nukib.cz/download/aktuality/2021-01-17_varovani_v.1.7_EN.pdf.

⁶⁾ Gesetz über das Bundesamt für Sicherheit in der Informationstechnik https://www.gesetze-im-internet.de/bsig_2009/BJNR282110009.html.

i usługach informatycznych, złośliwym oprogramowaniu, utracie lub nieautoryzowanym dostępie do danych, a także zalecać środki bezpieczeństwa.

Włochy

We Włoszech dekret nr 105 z dnia 21 września 2019 r.⁷⁾ uprawnia Prezesa Rady Ministrów do nakazania całkowitego lub częściowego wycofania z eksploatacji jednego lub więcej urządzeń lub produktów, w sytuacji poważnego i bezpośredniego zagrożenia bezpieczeństwa narodowego związanego z podatnościami występującymi w sieciach, systemach i usługach. Środek ten może być stosowany, jeżeli zagrożenia nie można uniknąć w inny sposób i tylko przez czas ściśle niezbędny do wyeliminowania lub ograniczenia konkretnego ryzyka.

Analiza w zakresie dostawców wysokiego ryzyka

Projektodawca przy projektowaniu przepisów prawa dotyczących uznania dostawców sprzętu lub oprogramowania za dostawców wysokiego ryzyka – czyli wdrożenia zaleceń z tzw. 5G Toolbox, dokonał analizy porównawczej rozwiązań prawno-organizacyjnych zaimplementowanych lub zaproponowanych mechanizmów. Wyniki analizy zostały zaprezentowane w załączniku nr 1 do OSR *Dostawca wysokiego ryzyka (high risk vendor) i bezpieczeństwo sieci 5G w Europie*.

W większości państw Unii Europejskiej wprowadzone zostały przepisy umożliwiające wyłączenie z budowy sieci 5G dostawcy uznanego za potencjalne zagrożenie dla bezpieczeństwa narodowego. Obowiązujące regulacje przewidują dokonanie takiego wyłączenia w drodze władczego rozstrzygnięcia dokonywanego przez jeden z organów władzy wykonawczej np. w drodze decyzji administracyjnej. W wielu państwach w tego rodzaju postępowaniach istotną rolę odgrywa również organ doradczy składający się z przedstawicieli administracji, wojska oraz służb specjalnych.

4. Podmioty, na które oddziałuje projekt

W przypadku liczby podmiotów kluczowych lub podmiotów ważnych źródłem danych jest *Kwartalna informacja o podmiotach gospodarki narodowej w rejestrze REGON rok 2024*⁸⁾ (stan na dzień 30 września 2024 r.), chyba że wskazano inne źródło. Korzystając z REGON przyjęto dane o liczbie podmiotów, które zatrudniają co najmniej 50 pracowników, nie brano przy tym pod uwagę danych o obrocie i bilansie. Ze względu na brak dokładnych danych, a także niewystarczającą dokładność kodów Polskiej Klasyfikacji Działalności, zwanej dalej „PKD”, m.in. w sektorze infrastruktury cyfrowej, zarządzania ICT czy dostawców usług cyfrowych należy traktować te dane jako dane szacunkowe. Część podmiotów świadczy zróżnicowane usługi, przekraczające zakres pojedynczego sektora z dyrektywy NIS 2. Ponadto z uwagi na bieżące życie gospodarcze liczba podmiotów w poszczególnych sektorach ciągle się zmienia, tworzone są nowe podmioty, a dotychczasowe są przekształcane oraz likwidowane. Liczba podmiotów w OSR będzie podlegała aktualizacji w toku procesu legislacyjnego, stosownie do posiadanych danych.

Grupa	Wielkość	Źródło danych	Oddziaływanie
Centrum e-Zdrowie	1	informacja ogólnodostępna	Z dniem wejścia w życie ustawy stanie się zespołem CSIRT sektorowym.
CSIRT KNF	1	informacja ogólnodostępna	Z dniem wejścia w życie ustawy stanie się zespołem CSIRT sektorowym.
CSIRT NASK	1	informacja ogólnodostępna	Z dniem wejścia w życie ustawy stanie się zespołem CSIRT sektorowym.
Kolegium do Spraw Cyberbezpieczeństwa	1	informacja ogólnodostępna	Kolegium otrzyma nowe kompetencje w postaci wydawania opinii o dostawcy sprzętu lub oprogramowania dla podmiotów krajowego

⁷⁾ Decreto-legge 21 settembre 2019, n. 105 Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica. <https://www.gazzettaufficiale.it/eli/id/2019/09/21/19G00111/sg>.

⁸⁾ <https://stat.gov.pl/obszary-tematyczne/podmioty-gospodarcze-wyniki-finansowe/zmiany-strukturalne-grup-podmiotow/kwartalna-informacja-o-podmiotach-gospodarki-narodowej-w-rejestrze-regon-rok-2024,7,14.html>.

			systemu cyberbezpieczeństwa.
Minister Obrony Narodowej	1	informacja ogólnodostępna	Będzie pełnił rolę organu ds. zarządzania kryzysowego w cyberbezpieczeństwie na dużą skalę w zakresie w jakim dotyczy to obronności i Sił Zbrojnych.
minister właściwy do spraw informatyzacji	1	informacja ogólnodostępna	Będzie pełnił rolę organu ds. zarządzania kryzysowego w cyberbezpieczeństwie na dużą skalę. Obowiązek utworzenia wykazu podmiotów kluczowych i podmiotów ważnych.
organy właściwe do spraw cyberbezpieczeństwa: Komisja Nadzoru Finansowego Minister Obrony Narodowej minister właściwy do spraw energii minister właściwy do spraw finansów publicznych minister właściwy do spraw gospodarki minister właściwy do spraw gospodarki morskiej minister właściwy do spraw gospodarki wodnej minister właściwy do spraw informatyzacji minister właściwy do spraw klimatu minister właściwy do spraw nauki i szkolnictwa wyższego minister właściwy do spraw rolnictwa minister właściwy do spraw transportu minister właściwy do spraw zdrowia Prezes Urzędu Komunikacji Elektronicznej	15	informacja ogólnodostępna	Wypożyczenie w uprawnienia i nałożenie obowiązków w związku ze sprawowaniem nadzoru nad podmiotami kluczowymi i podmiotami ważnymi.
Agencja Bezpieczeństwa Wewnętrznego	1		Uprawnienie do żądania dostępu do danych zawartych w wykazie

			podmiotów kluczowych i podmiotów ważnych.
Agencji Wywiadu	1		Uprawnienie do żądania dostępu do danych zawartych w wykazie podmiotów kluczowych i podmiotów ważnych.
dyrektor Rządowego Centrum Bezpieczeństwa	1		Uprawnienie do żądania dostępu do danych zawartych w wykazie podmiotów kluczowych i podmiotów ważnych. Przekazuje informacje do ministra właściwego do spraw informatyzacji o uznaniu podmiotu za podmiot krytyczny.
organy Krajowej Administracji Skarbowej	151		Uprawnienie do żądania dostępu do danych zawartych w wykazie podmiotów kluczowych i podmiotów ważnych.
Najwyższa Izba Kontroli	1		Uprawnienie do żądania dostępu do danych zawartych w wykazie podmiotów kluczowych i podmiotów ważnych.
Policja	1		Uprawnienie do żądania dostępu do danych zawartych w wykazie podmiotów kluczowych i podmiotów ważnych. Uprawnienie do żądania danych dotyczących rejestracji nazw domen od rejestru nazw domen najwyższego poziomu oraz podmiotów świadczących usługi rejestracji nazw domen.
Prezes Urzędu Lotnictwa Cywilnego	1		Uprawnienie do żądania dostępu do danych zawartych w wykazie podmiotów kluczowych i podmiotów ważnych.
Prezes Urzędu Ochrony Danych Osobowych	1		Uprawnienie do żądania dostępu do danych zawartych w wykazie podmiotów kluczowych i podmiotów ważnych.
Prezes Urzędu Transportu Kolejowego	1		Uprawnienie do żądania dostępu do danych zawartych w wykazie

			podmiotów kluczowych i podmiotów ważnych.
Prokuratoria Generalna Rzeczypospolitej Polskiej	1		Uprawnienie do żądania dostępu do danych zawartych w wykazie podmiotów kluczowych i podmiotów ważnych.
Prokurator			Uprawnienie do żądania dostępu do danych zawartych w wykazie podmiotów kluczowych i podmiotów ważnych.
Służba Kontrwywiadu Wojskowego	1		Uprawnienie do żądania dostępu do danych zawartych w wykazie podmiotów kluczowych i podmiotów ważnych.
Służba Ochrony Państwa	1		Uprawnienie do żądania dostępu do danych zawartych w wykazie podmiotów kluczowych i podmiotów ważnych.
Służba Wywiadu Wojskowego	1		Uprawnienie do żądania dostępu do danych zawartych w wykazie podmiotów kluczowych i podmiotów ważnych.
Straż Graniczna	1		Uprawnienie do żądania dostępu do danych zawartych w wykazie podmiotów kluczowych i podmiotów ważnych.
Żandarmeria Wojskowa	1		Uprawnienie do żądania dostępu do danych zawartych w wykazie podmiotów kluczowych i podmiotów ważnych.
Szef Krajowej Administracji Skarbowej	1	informacja ogólnodostępna	Na żądanie organu właściwego do spraw cyberbezpieczeństwa będzie przekazywał informacje niezbędne do ustalenia wielkości przedsiębiorcy – podmiotu kluczowego/ważnego.
Zakład Ubezpieczeń Społecznych	1	informacja ogólnodostępna	Na żądanie organu właściwego do spraw cyberbezpieczeństwa będzie przekazywał informacje niezbędne do ustalenia wielkości przedsiębiorcy – podmiotu kluczowego/ważnego.

Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa	1	informacja ogólnodostępna	Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa będzie mógł wydawać rekomendacje, nakazywać CSIRT poziomu krajowego wsparcie w obsłudze incydentów konkretnym podmiotom krajowego systemu cyberbezpieczeństwa. Będzie mógł także żądać od administracji rządowej informacji i dokumentów niezbędnych do wykonywania jego zadań, a także otrzyma możliwość zlecania niezbędnych badań. Pełnomocnikiem z mocy ustawy będzie minister właściwy do spraw informatyzacji, sekretarz stanu albo podsekretarz stanu w urzędzie obsługującym ministra właściwego do spraw informatyzacji.
podmioty kluczowe lub podmioty ważne z podsektora produkcji wyrobów medycznych i wyrobów medycznych do diagnostyki in vitro	44	REGON PKD sekcja C dział 32 podklasa 3250z	Nowe obowiązki w zakresie zarządzania ryzykiem cyberbezpieczeństwa oraz obowiązki zgłaszania incydentów do właściwych CSIRT sektorowych. Obowiązek wycofania produktów ICT, usług ICT i procesów ICT w przypadku uznania dostawcy za dostawcę wysokiego ryzyka.
podmioty kluczowe lub podmioty ważne z sektora podmiotów publicznych	Co najmniej 27905 ⁹⁾	REGON	Nowe obowiązki w zakresie zarządzania ryzykiem cyberbezpieczeństwa oraz obowiązki zgłaszania incydentów do właściwych CSIRT sektorowych. Obowiązek wycofania produktów ICT, usług ICT i procesów ICT w przypadku uznania dostawcy za dostawcę wysokiego ryzyka.
podmioty ważne z sektora badań naukowych	169	REGON	Nowe obowiązki w zakresie zarządzania

⁹⁾ Przy obliczaniu wzięto pod uwagę następujące rodzaje podmiotów.

		PKD sekcja M dział 72 podklasa: 7219Z Badania naukowe i prace rozwojowe w dziedzinie pozostałych nauk przyrodniczych i technicznych 7220Z Badania naukowe i prace rozwojowe w dziedzinie nauk społecznych i humanistycznych	ryzykiem cyberbezpieczeństwa oraz obowiązki zgłaszania incydentów do właściwych CSIRT sektorowych. Obowiązek wycofania produktów ICT, usług ICT i procesów ICT w przypadku uznania dostawcy za dostawcę wysokiego ryzyka.
podmioty kluczowe lub podmioty ważne z sektora bankowości i infrastruktury rynków finansowych	55	szacunki KNF	Nowe obowiązki w zakresie zarządzania ryzykiem cyberbezpieczeństwa oraz obowiązki zgłaszania incydentów do właściwych CSIRT sektorowych. Obowiązek wycofania produktów ICT, usług ICT i procesów ICT w przypadku uznania dostawcy za dostawcę wysokiego ryzyka.
podmioty kluczowe lub podmioty ważne z sektora dostawców usług cyfrowych	ok. 40	szacunki Ministerstwa Cyfryzacji	Nowe obowiązki w zakresie zarządzania ryzykiem cyberbezpieczeństwa oraz obowiązki zgłaszania incydentów do właściwych CSIRT sektorowych. Obowiązek wycofania produktów ICT, usług ICT i procesów ICT w przypadku uznania dostawcy za dostawcę wysokiego ryzyka.
podmioty kluczowe lub podmioty ważne z sektora energii	365	szacunki Ministerstwa Klimatu i Środowiska, obecnie Ministerstwo Energii	Nowe obowiązki w zakresie zarządzania ryzykiem cyberbezpieczeństwa oraz obowiązki zgłaszania incydentów do właściwych CSIRT sektorowych. Obowiązek wycofania produktów ICT, usług ICT i procesów ICT w przypadku uznania dostawcy za dostawcę wysokiego ryzyka.
podmioty ważne z sektora gospodarowania odpadami	276	REGON PKD: sekcja E dział 38 podklasa 3811Z Zbieranie odpadów innych niż niebezpieczne	Nowe obowiązki w zakresie zarządzania ryzykiem cyberbezpieczeństwa oraz obowiązki zgłaszania incydentów do właściwych CSIRT sektorowych.

		sekcja E dział 38 podklasa 3812Z Zbieranie odpadów niebezpiecznych sekcja E dział 38 podklasa 3821Z Obróbka i usuwanie odpadów innych niż niebezpieczne sekcja E dział 38 podklasa 3822Z Przetwarzanie i unieszkodliwianie odpadów niebezpiecznych sekcja E dział 38 podklasa 3831Z Demontaż wyrobów zużytych sekcja E dział 38 podklasa 3832Z Odzysk surowców z materiałów segregowanych sekcja E dział 38 podklasa 3900Z Działalność związana z rekultywacją i pozostała działalność usługowa związana z gospodarką odpadami	Obowiązek wycofania produktów ICT, usług ICT i procesów ICT w przypadku uznania dostawcy za dostawcę wysokiego ryzyka.
podmioty kluczowe i podmioty ważne z sektora infrastruktury cyfrowej z wyłączeniem podsektora komunikacji elektronicznej	462	szacunki Ministerstwa Cyfryzacji	Nowe obowiązki w zakresie zarządzania ryzykiem cyberbezpieczeństwa oraz obowiązki zgłaszania incydentów do właściwych CSIRT sektorowych. Obowiązek wycofania produktów ICT, usług ICT i procesów ICT w przypadku uznania dostawcy za dostawcę wysokiego ryzyka.
podmioty kluczowe lub podmioty ważne z podsektora komunikacji elektronicznej	3332 w zakresie podmiotów świadczących usługę komunikacji interpersonalnej niewykorzystującej numerów (OTT-1) brak danych	Rejestr przedsiębiorców telekomunikacyjnych	Nowe obowiązki w zakresie zarządzania ryzykiem cyberbezpieczeństwa oraz obowiązki zgłaszania incydentów do właściwych CSIRT sektorowych. Obowiązek wycofania produktów ICT, usług ICT i procesów ICT w przypadku uznania dostawcy za dostawcę wysokiego ryzyka.
podmioty ważne z sektora poczty	280	Rejestr operatorów pocztowych	Nowe obowiązki w zakresie zarządzania ryzykiem cyberbezpieczeństwa oraz obowiązki zgłaszania incydentów do właściwych CSIRT sektorowych.

			Obowiązek wycofania produktów ICT, usług ICT i procesów ICT w przypadku uznania dostawcy za dostawcę wysokiego ryzyka.
podmioty kluczowe lub podmioty ważne z sektora produkcja, przetwarzanie i dystrybucja żywności	1204	REGON PKD: sekcja C dział 10 Produkcja artykułów spożywczych sekcja H dział 46 podklasa 4631Z Sprzedaż hurtowa owoców i warzyw sekcja H dział 46 podklasa 4632Z Sprzedaż hurtowa mięsa i wyrobów z mięsa sekcja H dział 46 podklasa 4633Z Sprzedaż hurtowa mleka, wyrobów mleczarskich, jaj, olejów i tłuszczów jadalnych sekcja H dział 46 podklasa 4634A Sprzedaż hurtowa napojów alkoholowych sekcja H dział 46 podklasa 4634B Sprzedaż hurtowa napojów bezalkoholowych	Nowe obowiązki w zakresie zarządzania ryzykiem cyberbezpieczeństwa oraz obowiązki zgłaszania incydentów do właściwych CSIRT sektorowych. Obowiązek wycofania produktów ICT, usług ICT i procesów ICT w przypadku uznania dostawcy za dostawcę wysokiego ryzyka.
podmioty kluczowe lub podmioty ważne z sektora produkcja, wytwarzanie i dystrybucja chemikaliów	214	REGON PKD sekcja C dział 20 Produkcja chemikaliów i wyrobów chemicznych	Nowe obowiązki w zakresie zarządzania ryzykiem cyberbezpieczeństwa oraz obowiązki zgłaszania incydentów do właściwych CSIRT sektorowych. Obowiązek wycofania produktów ICT, usług ICT i procesów ICT w przypadku uznania dostawcy za dostawcę wysokiego ryzyka.
podmioty kluczowe lub podmioty ważne z sektora produkcji, z wyłączeniem wyrobów medycznych	1120	REGON PKD sekcja C dział 26 Produkcja komputerów, wyrobów elektronicznych i optycznych PKD sekcja C dział 27 Produkcja urządzeń elektrycznych PKD sekcja C dział 28 Produkcja maszyn i urządzeń, gdzie indziej niesklasyfikowana	Nowe obowiązki w zakresie zarządzania ryzykiem cyberbezpieczeństwa oraz obowiązki zgłaszania incydentów do właściwych CSIRT sektorowych. Obowiązek wycofania produktów ICT, usług ICT i procesów ICT w przypadku uznania dostawcy za dostawcę wysokiego ryzyka.

		PKD sekcja C dział 29 Produkcja pojazdów samochodowych, przyczep i naczep, z wyłączeniem motocykli PKD sekcja C dział 30 Produkcja pozostałego sprzętu transportowego	
podmioty kluczowe lub podmioty ważne z sektora ścieków	102	REGON PKD sekcja E dział 37 podklasa 3700z Odprowadzanie i oczyszczanie ścieków	Nowe obowiązki w zakresie zarządzania ryzykiem cyberbezpieczeństwa oraz obowiązki zgłaszania incydentów do właściwych CSIRT sektorowych. Obowiązek wycofania produktów ICT, usług ICT i procesów ICT w przypadku uznania dostawcy za dostawcę wysokiego ryzyka.
podmioty kluczowe lub podmioty ważne z sektora transportu	co najmniej 450	szacunki Ministerstwa Infrastruktury	Nowe obowiązki w zakresie zarządzania ryzykiem cyberbezpieczeństwa oraz obowiązki zgłaszania incydentów do właściwych CSIRT sektorowych. Obowiązek wycofania produktów ICT, usług ICT i procesów ICT w przypadku uznania dostawcy za dostawcę wysokiego ryzyka.
podmioty kluczowe lub podmioty ważne z sektora transportu wodnego	11	REGON	Nowe obowiązki w zakresie zarządzania ryzykiem cyberbezpieczeństwa oraz obowiązki zgłaszania incydentów do właściwych CSIRT sektorowych. Obowiązek wycofania produktów ICT, usług ICT i procesów ICT w przypadku uznania dostawcy za dostawcę wysokiego ryzyka.
podmioty kluczowe lub podmioty ważne z sektora zaopatrzenia w wodę i jej dystrybucji	268	REGON PKD Sekcja E dział 36 podklasa 3600Z Pobór, uzdatnianie i dostarczanie wody	Nowe obowiązki w zakresie zarządzania ryzykiem cyberbezpieczeństwa oraz obowiązki zgłaszania incydentów do właściwych CSIRT sektorowych. Obowiązek wycofania produktów ICT, usług ICT i procesów ICT

			w przypadku uznania dostawcy za dostawcę wysokiego ryzyka.
podmioty kluczowe lub podmioty ważne z sektora zarządzania ICT	43	REGON PKD sekcja J dział 62 podklasa 6203z Działalność związana z zarządzaniem urządzeniami informatycznymi W zakresie dostawców usług zarządzanych w zakresie cyberbezpieczeństwa źródłem informacji są dane ENISA ¹⁰⁾	Nowe obowiązki w zakresie zarządzania ryzykiem cyberbezpieczeństwa oraz obowiązki zgłaszania incydentów do właściwych CSIRT sektorowych. Obowiązek wycofania produktów ICT, usług ICT i procesów ICT w przypadku uznania dostawcy za dostawcę wysokiego ryzyka.
podmioty kluczowe lub podmioty ważne z sektora ochrony zdrowia	1248	REGON PKD Dział 21 Produkcja podstawowych substancji farmaceutycznych oraz leków i pozostałych wyrobów farmaceutycznych PKD Dział 86 Opieka zdrowotna PKD sekcja M dział 72 podklasa 7211Z Badania naukowe i prace rozwojowe w dziedzinie biotechnologii rozporządzenie Ministra Zdrowia z dnia 19 czerwca 2012 r. w sprawie wykazu laboratoriów referencyjnych	Nowe obowiązki w zakresie zarządzania ryzykiem cyberbezpieczeństwa oraz obowiązki zgłaszania incydentów do właściwych CSIRT sektorowych. Obowiązek wycofania produktów ICT, usług ICT i procesów ICT w przypadku uznania dostawcy za dostawcę wysokiego ryzyka.
sądy administracyjne	17	Dane o podmiotach świadczących usługi publiczne z Katalogu Podmiotów Publicznych czerwiec 2025 r. ¹¹⁾	Rozpatrywanie skarg na decyzje o nałożeniu administracyjnej kary pieniężnej na podmiot kluczowy lub podmiot ważny.
Szef Agencji Wywiadu	1	informacja ogólnodostępna	Pozytywne. Szef Agencji Wywiadu będzie mógł uczestniczyć w posiedzeniach Kolegium do Spraw Cyberbezpieczeństwa, a tym samym współtworzyć opinie Kolegium, dzięki czemu będą uwzględnione wszystkie aspekty cyberbezpieczeństwa

¹⁰⁾ <https://www.enisa.europa.eu/topics/incident-response/csirt-inventory/certs-by-country-interactive-map>.

¹¹⁾ <https://dane.gov.pl/pl/dataset/3520,dane-podmiotow-swiadczacych-uslugi-publiczne-z-kat/resource/68039/table>

			i bezpieczeństwa narodowego.
Szef Służby Wywiadu Wojskowego	1	informacja ogólnodostępna	Pozytywne. Szef Służby Wywiadu Wojskowego będzie mógł uczestniczyć w posiedzeniach Kolegium do Spraw Cyberbezpieczeństwa, a tym samym współtworzyć opinie Kolegium, dzięki czemu będą uwzględnione wszystkie aspekty cyberbezpieczeństwa i bezpieczeństwa narodowego.
Szef Agencji Bezpieczeństwa Wewnętrznego	1	informacja ogólnodostępna	Będzie pełnił rolę organu właściwego do spraw cyberbezpieczeństwa w sektorze administracji publicznej.
konsumenci			Większy poziom bezpieczeństwa dostarczanych produktów i usług.
Urząd Dozoru Technicznego	1	informacja ogólnodostępna	Urząd Dozoru Technicznego będzie pełnił funkcję CSIRT sektorowego dla sektorów produkcji, produkcji chemikaliów i przestrzeni kosmicznej.
Państwowa Straż Pożarna	351	Dane o podmiotach świadczących usługi publiczne z Katalogu Podmiotów Publicznych czerwiec 2025 r.	Strażacy i pracownicy Państwowej Straży Pożarnej zajmujący się cyberbezpieczeństwem jednostek organizacyjnych PSP będą mogli otrzymać świadczenie teleinformatyczne z Funduszu Cyberbezpieczeństwa.
Urząd Ochrony Danych Osobowych	1	informacja ogólnodostępna	Pracownicy Urzędu Ochrony Danych Osobowych realizujący zadania związanych z cyberbezpieczeństwem będą mogli otrzymać świadczenie teleinformatyczne ze środków przekazanych z Funduszu Cyberbezpieczeństwa do Urzędu Ochrony Danych Osobowych.

jednostki organizacyjne Krajowej Administracji Skarbowej	303	Dane o podmiotach świadczących usługi publiczne z Katalogu Podmiotów Publicznych czerwiec 2025 r.	Pracownicy i funkcjonariusze Krajowej Administracji Skarbowej realizujący zadania związanych z cyberbezpieczeństwem będą mogli otrzymać świadczenie teleinformatyczne ze środków przekazanych z Funduszu Cyberbezpieczeństwa do Krajowej Administracji Skarbowej.
sądy powszechne	379	Dane o podmiotach świadczących usługi publiczne z Katalogu Podmiotów Publicznych czerwiec 2025 r.	Pracownicy sądów powszechnych realizujący zadania związanych z cyberbezpieczeństwem będą mogli otrzymać świadczenie teleinformatyczne ze środków przekazanych z Funduszu Cyberbezpieczeństwa do sądów powszechnych.
Generalna Dyrekcja Dróg Krajowych i Autostrad	1		Pracownicy Generalnej Dyrekcji Dróg Krajowych i Autostrad będą mogli otrzymać świadczenie teleinformatyczne ze środków przekazanych z Funduszu Cyberbezpieczeństwa do Generalnej Dyrekcji Dróg Krajowych i Autostrad.
Główny Inspektorat Transportu Drogowego	1		Pracownicy Głównego Inspektoratu Transportu Drogowego będą mogli otrzymać świadczenie teleinformatyczne ze środków przekazanych z Funduszu Cyberbezpieczeństwa do Głównego Inspektoratu Transportu Drogowego.
instytutach badawczych nadzorowanych przez ministra właściwego do spraw: -gospodarki morskiej, -gospodarki wodnej, -transportu, -żeglugi śródlądowej.	4		Pracownicy tych 4 instytutów badawczych będą mogli otrzymać świadczenie teleinformatyczne ze środków przekazanych z Funduszu Cyberbezpieczeństwa.
Urząd Lotnictwa Cywilnego	1		Pracownicy Urzędu Lotnictwa Cywilnego będą mogli otrzymać świadczenie

			teleinformatyczne ze środków przekazanych z Funduszu Cyberbezpieczeństwa do Urzędu Lotnictwa Cywilnego.
Państwowe Gospodarstwo Wodne Wody Polskie	1		Pracownicy Państwowego Gospodarstwa Wodnego Wody Polskie będą mogli otrzymać świadczenie teleinformatyczne ze środków przekazanych z Funduszu Cyberbezpieczeństwa do Państwowego Gospodarstwa Wodnego Wody Polskie.
Transportowy Dozór Techniczny	1		Pracownicy Transportowego Dozoru Technicznego będą mogli otrzymać świadczenie teleinformatyczne ze środków przekazanych z Funduszu Cyberbezpieczeństwa do Transportowego Dozoru Technicznego.
Urząd do Spraw Cudzoziemców	1		Pracownicy Urzędu do Spraw Cudzoziemców będą mogli otrzymać świadczenie teleinformatyczne ze środków przekazanych z Funduszu Cyberbezpieczeństwa do Urzędu do spraw Cudzoziemców.
Urzędy morskie	2		Pracownicy urzędów morskich będą mogli otrzymać świadczenie teleinformatyczne ze środków przekazanych z Funduszu Cyberbezpieczeństwa do urzędów morskich.
Urzędy żeglugi śródlądowej	3		Pracownicy urzędów żeglugi śródlądowej będą mogli otrzymać świadczenie teleinformatyczne ze środków przekazanych z Funduszu Cyberbezpieczeństwa do urzędów żeglugi śródlądowej.

Jednostki samorządu terytorialnego	16 województw 314 powiatów 66 miast na prawach powiatu 2479 gmin	Rejestr TERYT	Uprawnienie do wyznaczenia wspólnej jednostki realizującej zadania w zakresie cyberbezpieczeństwa w jednostkach organizacyjnych JST. Uprawnienie do wyznaczenia jako jednostki obsługującej jak również obsługiwanej spółki komunalnej.
minister kierujący działem administracji rządowej	19 ministerstw		Uprawnienie do wyznaczenia wspólnej jednostki realizującej zadania w zakresie cyberbezpieczeństwa w jednostkach organizacyjnych podległych i nadzorowanych przez tego ministra.
centralny organ administracji rządowej			Uprawnienie do wyznaczenia wspólnej jednostki realizującej zadania w zakresie cyberbezpieczeństwa w jednostkach organizacyjnych podległych temu organowi.
Wojewoda	16		Uprawnienie do wyznaczenia wspólnej jednostki realizującej zadania w zakresie cyberbezpieczeństwa w jednostkach organizacyjnych podległych wojewodzie.
Prokurator Generalny	1	informacja ogólnodostępna	Uprawnienie do wyznaczenia wspólnej jednostki realizującej zadania w zakresie cyberbezpieczeństwa w jednostkach organizacyjnych prokuratury.
Połączone Centrum Operacyjne Cyberbezpieczeństwa	1	informacja ogólnodostępna	Umocowanie de facto istniejącego centrum na poziomie ustawy.

5. Informacje na temat zakresu, czasu trwania i podsumowanie wyników konsultacji

Stosownie do postanowień art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingsowej w procesie stanowienia prawa (Dz. U. z 2025 r. poz. 677), projekt ustawy został udostępniony w Biuletynie Informacji Publicznej Ministerstwa Cyfryzacji.

Ponadto zgodnie z § 52 ust. 1 uchwały nr 190 Rady Ministrów z dnia 29 października 2013 r. – Regulamin pracy Rady Ministrów (M.P. z 2024 r. poz. 806 oraz z 2025 r. poz. 408), projekt ustawy został udostępniony również w Biuletynie

Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji, w serwisie Rządowy Proces Legislacyjny.

W ramach 30-dniowych konsultacji publicznych projekt ustawy został skierowany do następujących podmiotów:

- 1) Amerykańskiej Izby Handlowej;
- 2) Business Centre Club;
- 3) Federacji Konsumentów;
- 4) Fundacji Bezpieczna Cyberprzestrzeń;
- 5) Fundacji ePaństwo;
- 6) Fundacji im. Stefana Batorego;
- 7) Fundacji Instytut Mikromakro;
- 8) Fundacji My Pacjenci;
- 9) Fundacji Nowoczesna Polska;
- 10) Fundacji Panoptikon;
- 11) Fundacji Projekt Polska;
- 12) Fundacji Przedsiębiorców Polskich Archiwizjoner;
- 13) Fundacji Pułaskiego;
- 14) Green Rev Institute;
- 15) Internet Society Poland Chapter;
- 16) Internet Society Poland;
- 17) ISAC-GIG;
- 18) ISAC-Kolej;
- 19) ISAC-Lotniczy;
- 20) Izby Domów Maklerskich;
- 21) Izby Gospodarczej Towarzystw Emerytalnych;
- 22) Izby Gospodarki Elektronicznej;
- 23) Konfederacji Lewiatan;
- 24) Krajowego Związku Banków Spółdzielczych;
- 25) Krajowej Izby Gospodarczej Elektroniki i Telekomunikacji;
- 26) Krajowej Izby Gospodarczej;
- 27) Krajowej Izby Gospodarki Cyfrowej;
- 28) Krajowej Izby Gospodarki Morskiej;
- 29) Krajowej Izby Komunikacji Ethernetowej;
- 30) Krajowej Izby Rozliczeniowej;
- 31) Krajowej Spółdzielczej Kasy Oszczędnościowo-Kredytowej;
- 32) Naczelnej Organizacji Technicznej;
- 33) Naczelnej Rady Zrzeszeń Handlu i Usług;
- 34) Ogólnopolskiego Porozumienia Organizacji Radioamatorskich;
- 35) Polskiego Centrum Badań i Certyfikacji S.A.;
- 36) Polskiego Stowarzyszenia Marketingu SMB;
- 37) Polskiego Towarzystwa Informatycznego;
- 38) Polskiego Związku Krótkofalowców;
- 39) Polskiej Izby Brokerów Ubezpieczeniowych i Reasekuracyjnych;
- 40) Polskiej Izby Handlu;
- 41) Polskiej Izby Informatyki i Telekomunikacji;
- 42) Polskiej Izby Komunikacji Elektronicznej;
- 43) Polskiej Izby Producentów Urządzeń i Usług na rzecz Kolei;
- 44) Polskiej Izby Radiodifuzji Cyfrowej;
- 45) Polskiej Izby Ubezpieczeń;
- 46) Polskiej Organizacji Handlu i Dystrybucji;
- 47) Polskiej Organizacji Niebankowych Instytucji Płatności;
- 48) Polskiej Rady Biznesu;
- 49) Polskiej Wytwórni Papierów Wartościowych;
- 50) Sektorowej Rady ds. Kompetencji – Telekomunikacja i Cyberbezpieczeństwo;
- 51) Stowarzyszenia Inżynierów Telekomunikacji;
- 52) Stowarzyszenia Polskich Brokerów Ubezpieczeniowych i Reasekuracyjnych;
- 53) Towarzystwa Gospodarczego Polskie Elektrownie;
- 54) Związku Banków Polskich;
- 55) Związku Importerów i Producentów Sprzętu Elektrycznego i Elektronicznego Branży RTV i IT – ZIPSEE „Cyfrowa Polska”;

- 56) Związku Pracodawców Branży Internetowej IAB Polska;
- 57) Związku Pracodawców Mediów Elektronicznych i Telekomunikacji Mediakom;
- 58) Związku Pracodawców Mediów Publicznych;
- 59) Związku Przemysłu Motoryzacyjnego;
- 60) Związku Telewizji Kablowych w Polsce Izba Gospodarcza.

W ramach 30-dniowego opiniowania projekt ustawy został skierowany do następujących podmiotów:

- 1) Agencji Bezpieczeństwa Wewnętrznego;
- 2) Agencji Wywiadu;
- 3) Biura Bezpieczeństwa Narodowego;
- 4) Centralnego Biura Antykorupcyjnego;
- 5) Komisji Nadzoru Finansowego;
- 6) Krajowej Rady Radiofonii i Telewizji;
- 7) Najwyższej Izby Kontroli;
- 8) Polskiego Komitetu Normalizacyjnego;
- 9) Prezesa Głównego Urzędu Statystycznego;
- 10) Prezesa Urzędu Komunikacji Elektronicznej;
- 11) Prezesa Urzędu Ochrony Danych Osobowych;
- 12) Prezesa Urzędu Ochrony Konkurencji i Konsumentów;
- 13) Prokuratury Generalnej Rzeczypospolitej Polskiej;
- 14) Rady Dialogu Społecznego;
- 15) Rządowego Centrum Bezpieczeństwa;
- 16) Rzecznika Małych i Średnich Przedsiębiorców;
- 17) Rzecznika Praw Obywatelskich;
- 18) Służby Kontrwywiadu Wojskowego;
- 19) Służby Ochrony Państwa;
- 20) Służby Wywiadu Wojskowego;
- 21) Urzędu Zamówień Publicznych;
- 22) Wojskowego Biura Zarządzania Częstotliwościami.

Wyniki przeprowadzonych konsultacji publicznych i opiniowania zostały omówione w raporcie z konsultacji.

Projekt ustawy uzyskał w dniu 14 stycznia 2025 r. pozytywną wiążącą opinię Komisji Wspólnej Rządu i Samorządu Terytorialnego (opinię wydał Zespół do Spraw Społeczeństwa Informacyjnego, który został w tym celu upoważniony przez Komisję).

Minister Cyfryzacji przyjął propozycję strony samorządowej Komisji Wspólnej Rządu i Samorządu Terytorialnego, aby wprowadzić obniżone wymagania z zakresu cyberbezpieczeństwa dla samorządowych jednostek budżetowych, samorządowych zakładów budżetowych, samorządowych instytucji kultury oraz spółek prawa handlowego wykonujących zadania o charakterze użyteczności publicznej w rozumieniu art. 1 ust. 2 ustawy z dnia 20 grudnia 1996 r. o gospodarce komunalnej (Dz. U. z 2021 r. poz. 679) oraz wprowadzić obniżone wymagania w zakresie zgłaszania incydentów.

6. Wpływ na sektor finansów publicznych

(ceny stałe z 2025 r.)	Skutki w okresie 10 lat od wejścia w życie zmian [mln zł]											
	0	1	2	3	4	5	6	7	8	9	10	Łącznie (0–10)
Dochody ogółem	0	23,578	26,014	28,621	31,411	34,176	37,240	40,398	44,013	47,498	17,797	330,747
budżet państwa	0	3,884	4,822	5,826	6,901	8,051	9,281	10,598	12,007	13,514	15,128	90,011
JST	0	0,685	0,851	1,028	1,218	1,421	1,638	1,870	2,119	2,385	2,670	15,884
Fundusz Pracy	0	0,492	0,527	0,563	0,603	0,645	0,691	0,739	0,791	0,846	0,000	5,897
FS	0	0,714	0,764	0,817	0,874	0,936	1,001	1,071	1,146	1,227	0,000	8,550
FUS	0	13,981	14,961	16,010	17,132	18,333	19,618	20,993	22,465	24,039	0,000	167,531
NFZ	0	3,82	4,09	4,38	4,68	4,79	5,01	5,13	5,49	5,49	0,00	42,87
Fundusz Cyberbezpieczeństwa	0	101,51	101,51	101,51	101,51	101,51	101,51	101,51	101,51	101,51	101,51	1015,11
Wydatki ogółem	0	301,000	305,654	318,661	342,259	368,763	400,126	409,875	443,118	482,981	533,329	3905,764
budżet państwa	0	301,000	305,654	318,661	342,259	368,763	400,126	409,875	443,118	482,981	533,329	3905,764
JST	0	0	0	0	0	0	0	0	0	0	0	0

Fundusz Pracy	0	0	0	0	0	0	0	0	0	0	0	0
Fundusz Solidarnościowy	0	0	0	0	0	0	0	0	0	0	0	0
Fundusz Ubezpieczeń Społecznych	0	0	0	0	0	0	0	0	0	0	0	0
Narodowy Fundusz Zdrowia	0	0	0	0	0	0	0	0	0	0	0	0
Fundusz Cyberbezpieczeństwa	0	0	0	0	0	0	0	0	0	0	0	0
Saldo ogółem	0	-277,422	-279,640	-290,040	-310,848	-334,587	-362,886	-369,477	-399,105	-435,482	-515,532	-3575,018
budżet państwa	0	-297,116	-300,831	-312,834	-335,358	-360,713	-390,845	-399,277	-431,111	-469,466	-518,202	-3815,753
IST	0	0,685	0,851	1,028	1,218	1,421	1,638	1,870	2,119	2,385	2,670	15,884
Fundusz Pracy	0	0,492	0,527	0,563	0,603	0,645	0,691	0,739	0,791	0,846	0,000	5,897
Fundusz Solidarnościowy	0	0,714	0,764	0,817	0,874	0,936	1,001	1,071	1,146	1,227	0,000	8,550
Fundusz Ubezpieczeń Społecznych	0	13,981	14,961	16,010	17,132	18,333	19,618	20,993	22,465	24,039	0,000	167,531
Narodowy Fundusz Zdrowia	0	3,822	4,090	4,376	4,683	4,791	5,011	5,127	5,486	5,486	0,000	42,873
Fundusz Cyberbezpieczeństwa	0	101,51	101,51	101,51	101,51	101,51	101,51	101,51	101,51	101,51	101,51	1015,11
Źródła finansowania	Budżet państwa w częściach: • 20 gospodarka • 21 gospodarka morską • 22 gospodarka wodna • 27 informatyzacja • 28 szkolnictwo wyższe i nauka • 32 rolnictwo • 39 transport • 47 energia • 51 klimat • 57 Agencja Bezpieczeństwa Wewnętrznego • 76 Urząd Komunikacji Elektronicznej Jako rok 1 przyjęto rok 2026 – pierwszy rok funkcjonowania ustawy. Zadania przewidziane w projekcie są zadaniami nowymi, które do tej pory nie były planowane w budżecie państwa, stąd też jest zasadne zwiększenie limitów wydatków w poszczególnych częściach budżetowych. Przykładowo zadania ministra ds. gospodarki, wynikające z nowelizacji KSC, będą finansowane w ramach części 20 (od 2026 r.) ze zwiększonego limitu wydatków dla tej części, a nie w ramach dostępnych limitów. Ewentualne skutki dla części 05 – <i>Naczelny Sąd Administracyjny</i> wynikające z wejścia w życie projektowanej ustawy zostaną sfinansowane w ramach dotychczasowych środków finansowych i nie będą stanowić podstawy do planowania oraz ubiegania się o dodatkowe środki z budżetu państwa w roku wejścia w życie ustawy oraz w latach kolejnych. Wszystkie skutki finansowe z tytułu realizacji projektowanej ustawy w części 46 – <i>Zdrowie</i> sfinansowane zostaną w ramach środków na ochronę zdrowia, w tym w ramach ustalonego funduszu wynagrodzeń (niezwiększonego z tytułu tej ustawy), określonych zgodnie z art. 131c ustawy z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (Dz. U. z 2025 r. poz. 1461), bez możliwości ubiegania się o dodatkowe środki ponad te kwoty.											

	W tabeli powyżej przedstawiono dochody i wydatki w milionach zł zaokrąglone do 3 miejsc po przecinku. Szczegółowe wykazanie wydatków bez zaokrąglenia znajduje się w załączniku nr 4 do OSR.
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	Wsparcie kadrowe organów właściwych do spraw cyberbezpieczeństwa w realizacji zadań nadzorczych nad podmiotami kluczowymi i podmiotami ważnymi Projektowane zmiany mają zapewnić odpowiedni poziom finansowania działalności organów właściwych ds. cyberbezpieczeństwa. Wspomniany poziom musi być adekwatny do zadań nałożonych na te organy wymaganiami procedowanej ustawy oraz dyrektywy NIS 2. Obecny poziom finansowania nie pozwala na zatrudnienie wystarczającej liczby specjalistów w stosunku do liczby obowiązków, a także liczby podmiotów, jakie będą objęte nadzorem organów właściwych do spraw cyberbezpieczeństwa wraz z wejściem w życie przedmiotowej regulacji. Dodatkowo poprzez zwiększanie finansowania zostanie zapewniona nie tylko większa liczba etatów niezbędnych do efektywnej realizacji zadań organu właściwego ds. cyberbezpieczeństwa, ale także zostanie zapewniona możliwość zaoferowania wynagrodzeń, które będą adekwatne i proporcjonalne do realiów panujących w sektorze prywatnym oraz do wymaganej wiedzy i umiejętności. Obecnie obowiązująca KSC zapewnia finansowanie na poziomie 789 000,00 zł rocznie, co na dzień wejścia ustawy w życie miało zapewnić – stworzenie 8 stanowisk pracy (dla organu właściwego do spraw energii) przy założeniach, że dla 1 etatu przyjęto mnożnik kwoty bazowej w wysokości 3,20, przy maksymalnym 20% dodatku stażowym. Dodatkowo, założenie obejmowało również trzynaste wynagrodzenie roczne. Jednakże powyższe obliczenia były realizowane dla kwoty bazowej wynoszącej 1 874,00 zł. Przez ostatnie lata kwota bazowa ulegała zwiększeniu i obecnie wynosi ona 2 759,97 zł, co powoduje, że pierwotne założenia dotyczące maksymalnego wynagrodzenia oraz liczby stanowisk pracy, jakie miały być zapewnione – są nieaktualne. W dotychczasowej kwocie nie założono wzrostu kwoty bazowej przy zapewnieniu finansowania, co powinno zostać zmienione w powstającej regulacji. Dodatkowo dyrektywa NIS 2 w sposób diametralny zmienia metodę wyznaczania podmiotów, które zostaną objęte nadzorem organów właściwych do spraw cyberbezpieczeństwa oraz zakres podmiotowy regulacji, powodujący znaczny wzrost liczby tych podmiotów czy też znacznie zwiększa zakres obowiązków realizowanych przez organy właściwe, co również przekłada się na konieczność zapewnienia odpowiednich zasobów kadrowych. Zgodnie z przepisami zawartymi w dyrektywie NIS 2 pojawia się zasada, która wskazuje, że przedsiębiorstwa automatycznie zostaną uznane za kluczowe lub podmioty ważne w procesie samoidentyfikacji, po spełnieniu kryteriów dla średniego przedsiębiorstwa wskazanych w art. 2 załącznika do zalecenia 2003/361/WE, w związku z tym, podmiotami kluczowymi będą podmioty z sektorów, o których mowa w załączniku nr I KSC, przekraczające pułapy dla średnich przedsiębiorców. Natomiast, podmioty ważne to podmioty z sektorów wymienionych w załączniku nr I lub nr II, które nie kwalifikują się jako podmioty kluczowe. W związku z tym, że główne zadania organu właściwego ds. cyberbezpieczeństwa skupiają się na czynnościach nadzorczych, w tym zadaniach kontrolnych, przyjęto następujące założenia do obliczenia wymaganej liczby pracowników, którzy będą realizować te zadania. Założono, że rocznie należy przeprowadzić kontrolę około 10% nadzorowanych podmiotów (kontrola o charakterze <i>ex-ante</i> lub <i>ex-post</i>). Zespół kontrolny liczący 3 osoby jest w stanie przeprowadzić około 6 kontroli rocznie. W przypadku sektorów, gdzie jest znikoma liczba podmiotów, może to być mniejsza liczba osób. Założono przy tym, że niezależnie od wielkości sektora, maksymalna liczba nowych etatów nadzorujących sektor to 40 etatów. Należy podkreślić, że działania kontrolne są jednymi z wielu zadań wynikających z dyrektywy NIS 2, a co za tym idzie, wymienione wyżej zespoły kontrolne będą okresowo wyłączane z czynności kontrolnych, na rzecz innych działań. Oprócz czynności kontrolnych, niektóre inne kompetencje organu właściwego ds. cyberbezpieczeństwa to: 1) prowadzenie bieżącej analizy podmiotów w danym sektorze lub podsektorze pod kątem uznania ich za podmiot kluczowy lub podmiot ważny; 2) wpisywanie z urzędu podmiotów kluczowych lub podmiotów ważnych do wykazu podmiotów kluczowych i podmiotów ważnych; 3) monitorowanie stosowania przepisów ustawy przez podmioty kluczowe i podmioty ważne; 4) wzywanie na wnioski CSIRT MON, CSIRT NASK lub CSIRT GOV podmiotów kluczowych lub podmiotów ważnych do usunięcia w wyznaczonym terminie podatności, które doprowadziły lub mogły doprowadzić do incydentu poważnego lub krytycznego;

- 5) w uzasadnionych przypadkach współpraca z organami ścigania i organem właściwym do spraw ochrony danych osobowych;
- 6) przygotowywanie we współpracy z CSIRT MON, CSIRT NASK, CSIRT GOV i sektorowymi zespołami cyberbezpieczeństwa rekomendacji dotyczących działań mających na celu wzmocnienie cyberbezpieczeństwa, w tym wytyczne sektorowe dotyczące zgłaszania incydentów;
- 7) nakładanie administracyjnych kar pieniężnych.

W związku z powyższym należy zapewnić finansowanie działania organu właściwego ds. cyberbezpieczeństwa na poziomie wystarczającym do niezakłóconego i efektywnego realizowania zadań, które bezpośrednio przełożą się na cyberbezpieczeństwo sektorów. Kwota powinna być systematycznie zwiększana w kolejnych latach.

Dla 1 etatu przyjęto wynagrodzenie w wysokości 6 308,50 zł.

Dodatkowo rekomenduje się rozwiązanie, które pozwoli zniwelować problem niewystarczającego poziomu finansowania w przypadku wzrostu kosztów zatrudnienia związanego z m.in. wzrostem kwoty bazowej czy wzrostem średniego wynagrodzenia w gospodarce w kolejnych 10 latach. Takiego mechanizmu zabrakło w obowiązującej KSC, co spowodowało część opisanych wyżej problemów.

Określenie tego, w jaki sposób będzie kształtowała się kwota bazowa lub średnie wynagrodzenie w kolejnych 10 latach, jest bardzo trudne. Wobec powyższego przyjęto mechanizm, który pozwoli oszacować wspomniany wzrost, bazując na danych historycznych.

Do prognozowania skutków finansowych projektowanej ustawy dla kolejnych 10 lat wraz z uwzględnieniem konieczności wzrostu tego finansowania bazowano na danych historycznych z Zakładu Ubezpieczeń Społecznych.

ROK	ŚREDNIE WYNAGRODZENIE w GOSPODARCE KRAJOWEJ	PROCENT WZROSTU
2013	3650,06	
2014	3783,46	3,65 %
2015	3899,78	3,07%
2016	4047,21	3,78 %
2017	4271,51	5,54%
2018	4585,03	7,34%
2019	4918,17	7,27%
2020	5167,47	5,07%
2021	5662,53	9,58%
2022	6346,15	12,07%
2023	7155,48	12,75%
2024	8181,72	14,34%

Na podstawie powyższych danych można ustalić, że wzrost przeciętnego wynagrodzenia w gospodarce krajowej w ciągu ostatnich 10 lat wyniósł średnio 7,01%. W związku z tym proponuje się przyjąć prognozę analogicznego wzrostu przeciętnego wynagrodzenia w gospodarce w prognozie na kolejne 10 lat.

O wartość 7,01% w każdym kolejnym roku zostanie powiększona kwota finansowania organu właściwego ds. cyberbezpieczeństwa, co powinno zapewnić wystarczające środki finansowe w obliczu powiększania się kwoty bazowej w administracji, ale także pozwoli na zapewnienie konkurencyjności wynagrodzeń w stosunku do zwiększającego się przeciętnego wynagrodzenia w gospodarce krajowej w sektorze prywatnym.

Wzrost finansowania organów właściwych do spraw cyberbezpieczeństwa o 7,0% w każdym roku jest zasadny i konieczny, aby zapewnić odpowiedni poziom kadry, bowiem dyrektywa NIS 2 nakazuje państwom członkowskim wprowadzenie efektywnego nadzoru nad podmiotami kluczowymi i podmiotami ważnymi – aby to zrealizować organy właściwe do spraw cyberbezpieczeństwa potrzebują niezbędnej kadry. Obniżenie poziomu finansowania może spowodować ryzyko odpływu doświadczonych pracowników do sektora prywatnego, ponieważ nie zostaną zapewnione dla nich odpowiednie warunki finansowe. Ponadto, nieadekwatne wynagrodzenie nie przyciągnie kandydatów z rynku, co spowoduje nieskuteczność kadry organów właściwych do spraw cyberbezpieczeństwa.

Podsumowanie nowych etatów		
Sektor/podsektor	Organ właściwy do spraw cyberbezpieczeństwa	Nowe etaty
Energia	minister właściwy do spraw energii	10
Transport wodny	minister właściwy do spraw gospodarki morskiej	1
Transport	minister właściwy do spraw transportu	12
Ochrona zdrowia	minister właściwy do spraw zdrowia	20
Zaopatrzenie w wodę i jej dystrybucja	minister właściwy do spraw gospodarki wodnej	7
Ścieki	minister właściwy do spraw gospodarki wodnej	3
Infrastruktura Cyfrowa	minister właściwy do spraw informatyzacji	15
Komunikacja elektroniczna	Prezes UKE	20
Zarządzanie ICT	minister właściwy do spraw informatyzacji	2
Podmioty publiczne, z wyłączeniem MON, służb specjalnych i jednostek podległych lub nadzorowanych przez ministra właściwego ds. finansów publicznych	minister właściwy do spraw informatyzacji	20
Przestrzeń kosmiczna	minister właściwy do spraw gospodarki	0
Poczta	Prezes UKE	7
Gospodarowanie odpadami	minister właściwy do spraw klimatu	7
Produkcja, wytwarzanie i dystrybucja chemikaliów	minister właściwy do spraw gospodarki	6
Produkcja, przetwarzanie i dystrybucja żywności	minister właściwy do spraw rolnictwa	20
Produkcja wyrobów medycznych i wyrobów medycznych do diagnostyki in vitro	minister właściwy do spraw zdrowia	2
Produkcja ogółem	minister właściwy do spraw gospodarki	20

z wyłączeniem wyrobów medycznych		
Dostawcy usług cyfrowych	minister właściwy do spraw informatyzacji	1
Badania naukowe	minister właściwy do spraw nauki i szkolnictwa wyższego	5
SUMA		178

Minister właściwy do spraw finansów publicznych będzie organem właściwym do spraw cyberbezpieczeństwa dla podległych i nadzorowanych przez niego jednostek organizacyjnych oraz dla spółki, o której mowa w art. 2 ust. 1 ustawy z dnia 29 kwietnia 2016 r. o szczególnych zasadach wykonywania niektórych zadań dotyczących informatyzacji w zakresie działań administracji rządowej budżet i finanse publiczne (Dz. U. z 2021 r. poz. 186 oraz z 2025 r. poz. 1158).

Przyjęto następujące koszty utworzenia 1 stanowiska pracy:

Nazwa składnika	Koszt w zł
komputer osobisty (laptop)	7 500,00
stacja dokująca	800,00
telefon komórkowy	1 000,00
licencja MS Office	1 730,00
Suma:	11 030,00

Koszty te zostaną poniesione w 2026 r.

Utworzenie CSIRT sektorowych

Projekt ustawy przewiduje utworzenie zespołów CSIRT sektorowych, które będą wspierać podmioty kluczowe i podmioty ważne w reagowaniu na incydenty.

Koszty utworzenia i funkcjonowania CSIRT sektorowego będą różnić się od sektora (podsektora), dla którego realizuje zadania. Pod uwagę należy wziąć liczbę podmiotów w danym sektorze (podsektorze) oraz charakter świadczonych przez nich usług. Te czynniki będą determinowały jaki personel jest niezbędny w CSIRT sektorowym do realizacji zadań oraz jakie jest niezbędne oprogramowanie i sprzęt. To z kolei będzie miało wpływ na koszty funkcjonowania CSIRT sektorowych.

Wydatki na utworzenie i funkcjonowanie CSIRT sektorowych zostaną poniesione z budżetu państwa, z poszczególnych części budżetowych organów właściwych do spraw cyberbezpieczeństwa w wysokości ok. 47 mln zł.

Jednakże w ramach Inwestycji C3.1.1 KPO Cyberbezpieczeństwo – CyberPL, infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo planowana jest realizacja projektu, pn. „utworzenie lub rozwój przynajmniej 5 sektorowych Zespołów Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT)”. Z KPO przeznaczono na utworzenie lub rozwój tych zespołów kwotę ok. 50 mln zł <https://www.kpo.gov.pl/strony/aktualnosci/zespoły-reagowania-wzmacniają-cyberbezpieczeństwo-kluczowych-sektorów-w-polsce/>.

Przepisy nie określają formy prawnej podmiotu realizującego zadania CSIRT sektorowego, pozostawiając organowi właściwemu decyzję co do wyboru podmiotu, który stanie się takim CSIRT. Mogą to być zarówno jednostki budżetowe, jak i państwowe instytuty badawcze.

Planuje się, że zostaną utworzone następujące zespoły CSIRT sektorowe:

Część budżetowa	Nazwa części budżetowej	CSIRT sektorowy
20	Gospodarka	CSIRT produkcja, produkcja chemikaliów i przestrzeń kosmiczna
22	Gospodarka wodna	CSIRT woda pitna i ścieki
27	Informatyzacja	CSIRT infrastruktura cyfrowa, usługi cyfrowe oraz zarządzanie ICT
28	Szkolnictwo wyższe i nauka	CSIRT badania naukowe
32	Rolnictwo	CSIRT produkcja żywności
39	Transport	CSIRT transport

46	Zdrowie	CSIRT zdrowie, produkcja i urzędów medycznych
47	Energia	CSIRT energia oraz inwestycje energetyki jądrowej
51	Klimat	CSIRT gospodarowanie odpadami
76	Urząd Komunikacji Elektronicznej	CSIRT komunikacja elektroniczna i poczta

CSIRT KNF, będący obecnie sektorowym zespołem cyberbezpieczeństwa, stanie się CSIRT sektorowym z dniem wejścia w życie ustawy.

Centrum e-Zdrowie, będące obecnie sektorowym zespołem cyberbezpieczeństwa, stanie się CSIRT sektorowym z dniem wejścia w życie ustawy i będzie finansowane z części 46 budżetu państwa zgodnie z art. 131c ustawy z 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych.

CSIRT NASK oraz CSIRT GOV będą pełnić funkcję CSIRT sektorowych dla podmiotów publicznych w zakresie dotychczasowego *constituency*. Pozwoli to na zachowanie ciągłości działań w tym obszarze oraz ułatwi podmiotom publicznym dostosowanie się do nowej sytuacji prawnej.

Minister właściwy do spraw finansów publicznych utworzy CSIRT sektorowy dla swoich jednostek podległych i nadzorowanych oraz dla spółki, o której mowa w art. 2 ust. 1 ustawy z dnia 29 kwietnia 2016 r. o szczególnych zasadach wykonywania niektórych zadań dotyczących informatyzacji w zakresie działów administracji rządowej budżet i finanse publiczne.

Urząd Dozoru Technicznego będzie pełnił rolę CSIRT sektorowego dla sektorów CSIRT produkcja, produkcja chemikaliów i przestrzeń kosmiczna. Urząd Dozoru Technicznego będzie finansował zadania wynikające z projektowanej ustawy z przychodów po podwyższeniu stawek za czynności dozoru technicznego.

Dyrektywa NIS 2 określiła podmioty w ramach, których będą funkcjonować podmioty kluczowe lub podmioty ważne. Sektory te są dla nas wiążące przy tworzeniu CSIRT sektorowych i na ich podstawie przygotowane zostało powyższe zestawienie. Nazwy CSIRT sektorowych ani ich dokładne zakresy nie są na obecnym etapie prac przesądzone. To na organach właściwych będzie spoczywał obowiązek ich organizacji. W przypadku, gdy dwa lub więcej organów właściwych wyrazi zgodę, możliwe będzie utworzenie jednego CSIRT sektorowego dla kilku sektorów. Powyższe zestawienie stanowi więc plan, który może ulegać zmianie. Przynależność sektora do poszczególnej części budżetowej ustalono na podstawie przepisów określających zakres poszczególnych działów administracji rządowej i funkcjonujących w nich organów.

Nie przewiduje się odrębnego CSIRT sektorowego dla podsektora transportu wodnego z uwagi na niewielką liczbę podmiotów w tym podsektorze. Zakłada się, że w ramach porozumienia dwóch organów do spraw cyberbezpieczeństwa podsektor ten będzie obsługiwany przez CSIRT transport.

Przyjęto kwotę 10 833,00 zł miesięcznego wynagrodzenia w CSIRT sektorowym (bez składek). Przyjęto rocznie wzrost tej kwoty o 7,01%.

Za planem finansowym Centrum Cyberbezpieczeństwa przyjęto per CSIRT w 2026 r.:

- 1) koszt usług obcych w wysokości 1 650 000,00 zł;
- 2) koszt materiałów i energii w wysokości 277 000,00 zł;
- 3) koszty amortyzacji w wysokości 280 000,00 zł;
- 4) pozostałe koszty funkcjonowania w wysokości 695 000,00 zł.

W kolejnych latach doliczono do tych kosztów wzrost wskaźnika CPI w oparciu o *Wytyczne dotyczące stosowania jednolitych wskaźników makroekonomicznych będących podstawą oszacowania skutków finansowych projektowanych ustaw Aktualizacja – październik 2023 r.*¹²⁾.

Zestawienie kosztów pojedynczego zespołu CSIRT sektorowego zawiera załącznik nr 2 do OSR.

¹²⁾ <https://www.gov.pl/web/finanse/wytyczne-sytuacja-makroekonomiczna>

Wzrost kwoty dotacji podmiotowej na CSIRT NASK

W związku z nowymi zadaniami zespołu CSIRT NASK przewiduje się zwiększenie kwoty dotacji podmiotowej na ten zespół. Zadanie będzie finansowane z części 27 budżetu państwa. Koszty przedstawiono w załączniku nr 3 do OSR.

Wzrost kwoty dotacji celowej na S46

System S46 utrzymywany i rozwijany jest przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy będzie pełnił rolę wykazu podmiotów kluczowych i podmiotów ważnych, a także będzie podstawowym sposobem zgłaszania incydentów przez podmioty kluczowe i podmioty ważne. Stąd też konieczne jest zapewnienie odpowiedniego wzrostu dotacji celowej na rozwój tego systemu. Zadanie będzie finansowane z części 27 budżetu państwa. Koszty przedstawiono w załączniku nr 3 do OSR.

Zwiększenie nakładów na utrzymanie i rozwój S46 jest związane z czynnikami wymienionymi poniżej:

1. Zwiększona o dwa rzędy wielkości liczba uczestników systemu S46 przekłada się na koszty obsługi systemu, zarówno jeśli chodzi o wsparcie oferowane przez poszczególne linie wsparcia, jak również w zakresie wsparcia merytorycznego.
2. Nowelizacja ustawy przewiduje uruchomienie rejestru podmiotów KSC zapewniającego podmiotom mechanizm samorejestracji za pośrednictwem sieci internet i mechanizmów węzła krajowego. Uruchomienie bezpiecznego mechanizmu samorejestracji oraz wsparcie podmiotów podłączanych do S46 wymaga zwiększonych nakładów w stosunku do planowanych w obowiązującej ustawie.
3. W trakcie realizacji zadań związanych z utrzymaniem, okazało się konieczne powołanie zespołu analitycznego zdolnego do zauważania zależności, analizowania spójności modeli i ryzyk itp. W związku z nowelizacją powstanie większe zapotrzebowanie na tego rodzaju analizy. Należy wziąć pod uwagę również zatrudnienie specjalistów specjalizujących się w nowych technologiach, takich jak AI. Podniesienie nakładów umożliwi organizację zespołu analitycznego, który będzie mógł realizować funkcje wspomagające procesy analityczne zespołów CSIRT krajowych, zespołów CSIRT sektorowych oraz organów właściwych do spraw cyberbezpieczeństwa na poziomie systemu S46.
4. Doświadczenia dotyczące utrzymania i rozwoju systemu wskazują, że konieczne jest zapewnienie ciągłego doskonalenia funkcjonalności S46. Nowelizacja ustawy spowoduje wzrost liczby użytkowników co oznacza, że konieczne staje się utrzymanie stałego zespołu deweloperskiego, dedykowanego do ciągłego doskonalenia systemu, oraz wprowadzania poprawek. Zwiększenie liczby personelu dedykowanego do rozwoju systemu S46, umożliwi obsługę zwiększającej się skali i poziomu złożoności systemu. Brak dodatkowych nakładów w obszarze zespołów rozwojowych mógłby spowodować drastyczne wydłużenie okresu wprowadzania poprawek i dostosowywania systemu do wymagań zwiększonej w wyniku nowelizacji liczby użytkowników. Działania związane z utrzymaniem i rozwojem wymagają również inwestycji w narzędzia do analizy danych. Brak inwestycji w ww. narzędzia może wydłużyć czas reakcji na zagrożenia w obszarze cyberbezpieczeństwa.

Wsparcie kadrowe ministra właściwego do spraw informatyzacji w związku z nowymi zadaniami

Nowe zadania ministra właściwego do spraw informatyzacji w obszarze zarządzania kryzysowego w cyberprzestrzeni wymagają wsparcia kadrowego. Przewiduje się na to 4 etaty w urzędzie obsługującym ministra właściwego do spraw informatyzacji. Koszty zostaną poniesione z cz. 27 budżetu państwa.

Celem realizacji zadań w obszarze zarządzania kryzysowego niezbędny jest zakup sprzętu i oprogramowania umożliwiającego przetwarzanie informacji niejawnych.

- 1) zestaw komputerowy stacjonarny – stacja robocza + monitor + klawiatura + mysz + słuchawki – spełniający wymagania norm NATO serii SDIP- 27 LEVEL A – 4 szt.
- 2) drukarka laserowa A4 monochromatyczna – spełniająca wymagania norm NATO serii SDIP- 27 LEVEL A – 2 szt.
- 3) urządzenie wielofunkcyjne laserowe A4 kolor – spełniająca wymagania norm NATO serii SDIP- 27 LEVEL A – 3 szt.
- 4) zewnętrzny moduł portów USB + czytnik kart 14 w 1 – spełniająca wymagania norm NATO serii SDIP- 27 LEVEL A – 6 szt.
- 5) słuchawki USB na złączu DB9 – spełniające wymagania norm NATO serii SDIP- 27 LEVEL A – 1 szt.
- 6) zasilacz awaryjny UPS – 4 szt.

Koszty tego sprzętu oszacowano na 489810,6 zł¹³⁾. Będzie to zakup jednorazowy w 2026 r. z części 27 budżetu państwa.

Aby zapewnić efektywność postępowań administracyjnych w sprawie uznania za dostawcę wysokiego ryzyka oraz postępowań w sprawach nałożenia administracyjnych kar pieniężnych za nie wycofanie produktów ICT, usług ICT i procesów ICT pochodzących od dostawcy wysokiego ryzyka przewiduje się wzmocnienie urzędu obsługującego ministra do spraw informatyzacji o 3 etaty. Zadanie będzie finansowane z części 27 budżetu państwa.

Powyższe 7 etatów przewiduje się od stycznia 2026 r. Kalkulacje przyjęto jak dla osób pełniących funkcje nadzorcze w organie właściwym do spraw cyberbezpieczeństwa.

Podnoszenie zdolności instytucji zapewniających cyberbezpieczeństwo

Przewiduje się możliwość, aby Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa mógł dokonywać zakupów sprzętu/oprogramowania dla uczestników posiedzeń Połączonego Centrum Operacyjnego Cyberbezpieczeństwa. Przewiduje się na to zadanie 31 772 800,00zł rocznie począwszy od 2026 r.

Rodzaj	kwota
platforma CTI poziomu operacyjnego	18 920 000,00
platforma CTI z zakresu złośliwego oprogramowania dla 8 instytucji KSC	7 852 800,00
platforma CTI dla poziomu strategicznego	5 000 000,00
Suma	31 772 800,00zł

Platforma CTI poziomu operacyjnego – platforma Cyber Threat Intelligence służąca do dostarczania i analizy w czasie rzeczywistym informacji o zagrożeniach w cyberprzestrzeni. Rozwiązanie wspiera organizację w identyfikacji, ocenie i zarządzaniu ryzykiem związanym z cyberprzestępczością. Kwotę określono na podstawie zrealizowanego postępowania przetargowego na zakup dostępu do platformy na rzecz 8 podmiotów Krajowego Systemu Cyberbezpieczeństwa. Numer ogłoszenia o zamówieniu lub o zamiarze zawarcia umowy Dz. Urz. UE: 2023/S 186-581359. Numer referencyjny postępowania: PN-17/C/2023.

Platforma CTI z zakresu złośliwego oprogramowania – platforma dla 8 podmiotów krajowego systemu cyberbezpieczeństwa (np. CSIRT sektorowych, CSIRT poziomu krajowego, służb specjalnych) służąca do dostarczania i analizy informacji o złośliwym oprogramowaniu. Założono kwotę 250 000 \$ rocznie per podmiot, co przy kursie \$ 3,9264 daje łącznie 7 852 800,00 zł.

Platforma CTI poziomu strategicznego – Platforma/System służąca do dostarczania informacji z zakresu Cyber Threat Intelligence o poziomie strategicznym na rzecz podmiotów zapewniających bezpieczeństwo teleinformatyczne w ramach funkcjonowania Krajowego Systemu Cyberbezpieczeństwa. Dostarcza dane o zagrożeniach w cyberprzestrzeni za pomocą algorytmów lub programów typu crawler i dedykowanych zespołów analityków cyberbezpieczeństwa (zespół minimalnie 200 osób, praca w reżimie 24/7/365) przynajmniej z otwartych oraz zamkniętych źródeł. Kwota zamówienia określona na podstawie szacowania rynkowego.

Działalność edukacyjna

Przewiduje się także zapewnienie środków na działalność edukacyjną ministra właściwego do spraw informatyzacji. Działalność ta polega na wspieraniu świadomości co do cyberzagrożeń. Przewidziano na to zadanie 6 630 000,00 zł rocznie od 2026 r. Będą to programy edukacyjne, szkolenia z zakresu cyberbezpieczeństwa, a także zakupy usług i oprogramowania wspierające te programy, np. platformy szkoleniowe. Koszty Programów opracowano na podstawie dotychczasowych działań Ministra Cyfryzacji – programów SecureV, Bezpieczni w Sieci i CyberLekcji.

Badania lub ekspertyzy na rzecz Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa

Projekt ustawy przewiduje możliwość zlecenia przez Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa badań, które mają na celu wsparcie realizacji jego zadań. Przewiduje się na to zadanie 100 000,00 zł rocznie począwszy od 2026 r.

Koszt zakupu licencji do norm technicznych i innych dokumentów standaryzacyjnych z zakresu Cyberbezpieczeństwa

¹³⁾ <https://zamowienia.gov.pl/mp-client/search/list/ocds-148610-64efbcf6-5d1a-11ee-9aa3-96d3b4440790>

Aby wykonywać czynności nadzorcze organ właściwy do spraw cyberbezpieczeństwa musi mieć dostęp do niezbędnej wiedzy. W tym celu zasadne jest, aby rokrocznie organy mogły zakupić normy techniczne i inne dokumenty normalizacyjne z zakresu cyberbezpieczeństwa. Przewiduje się, że w 2026 r. koszt wyniesie 7 000 zł per organ właściwy do spraw cyberbezpieczeństwa, a od 2027 r. 8 000 zł.

Badanie sprzętu lub oprogramowania

Przewiduje się rocznie 3 mln zł dla Agencji Bezpieczeństwa Wewnętrznego na prowadzenie badań sprzętu lub oprogramowania pod kątem identyfikacji podatności zagrażającej bezpieczeństwu narodowemu.

Koszty budżetu państwa związane ze zmianami w ustawie z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa

Przewiduje się od 2026 r. wzrost kwoty dotacji przeznaczonej na zasilenie Funduszu Cyberbezpieczeństwa z budżetu państwa – kwota ta wzrośnie do 351,511 mln zł rocznie. Dzieje się tak z uwagi na wzrost liczby podmiotów uprawnionych do otrzymywania tego wsparcia. Koszty te będą poniesione z cz. 27 budżetu państwa.

Ponadto do obsługi Funduszu Cyberbezpieczeństwa dodaje się 4 etaty w urzędzie obsługującym ministra właściwego do spraw informatyzacji. Dzieje się tak z uwagi na konieczność obsługi dużej liczby wniosków o udzielenie wsparcia z Funduszu Cyberbezpieczeństwa również wynikającej z dodania nowych rodzajów podmiotów uprawnionych do wnioskowania o środki z tego Funduszu.

Koszty te wykazano w Zał. 5 Koszty budżetu państwa związane ze zmianami w ustawie z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa w tys. zł. Koszty te będą poniesione z cz. 27 budżetu państwa.

W związku z tym skorygowano regułę wydatkową w tej ustawie dodając do obecnej kwoty – 250 mln zł – koszty zwiększenia wydatków.

Wpływ finansowy projektu na podmioty publiczne

Podmioty publiczne w tym jednostki samorządu terytorialnego już obecnie są obowiązane do zgłaszania incydentów w podmiocie publicznym oraz do zarządzania incydentami, co wynika z art. 22 KSC. Ponadto podmioty publiczne mają obowiązek wdrożenia systemu zarządzania bezpieczeństwem informacji i przeprowadzania m.in. audytów (co wynika z § 19 rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, Dz. U. poz. 773). Podsumowując już obecnie jednostki samorządu terytorialnego mają obowiązki z zakresu cyberbezpieczeństwa i na to powinny mieć przeznaczone środki finansowe w budżecie. Dostosowanie się podmiotów publicznych, w tym jednostek samorządu terytorialnego, do wymogów dyrektywy NIS2 będzie polegało na przeglądzie już wdrożonych systemów zarządzania bezpieczeństwem informacji i uzupełnienia dokumentacji oraz środków technicznych i organizacyjnych. Skala zmian będzie zależna od obecnej dojrzałości organizacyjnej poszczególnych podmiotów publicznych. Oszacowanie kosztów dostosowawczych nie jest możliwe.

W ramach Inwestycji C3.1.1. KPO Cyberbezpieczeństwo – CyberPL, infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo przewiduje się m.in. realizację projektu pn. „Wsparcie 500 podmiotów krajowego systemu cyberbezpieczeństwa w modernizacji i rozbudowie infrastruktury cyberbezpieczeństwa w sieciach IT, w tym wsparcie podmiotów wykorzystujących technologie informacyjne (IT) oraz operacyjne (OT) stosowane w przemysłowych systemach sterowania (ICS)”. Projekt ten zakłada udzielenie wsparcia o wartości – ok. 700,5 mln zł m.in. dla ok. 70 urzędów administracji centralnej i rządowej. W ramach tego projektu urzędy administracji centralnej i rządowej będą mogły uzyskać wsparcie finansowe na dostosowanie się do projektowanej ustawy.

Ponad 2 500 samorządów (blisko 90%) otrzyma w bieżącym roku wsparcie finansowe w postaci grantów finansowanych ze środków budżetu państwa oraz programu Fundusze Europejskie na Rozwój Cyfrowy 2021–2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa. Wsparcie to jednostki samorządu

terytorialnego będą mogły wykorzystać na modernizację rozwiązań w obszarze cyberbezpieczeństwa. Łączna wartość wsparcia jaka zostanie przekazana wyniesie ok. 1,5 mld zł.

Poniższa tabela przedstawia projekty wsparcia przygotowane przez Ministerstwo Cyfryzacji i wspierające podmioty publiczne w realizacji wymogów regulacyjnych w obszarze cyberbezpieczeństwa:

Źródło	Nazwa	Skrót	Opis	Budżet	Okres realizacji
FERC	Cyberbezpieczny Samorząd	CS	Wsparcie grantowe dla JST na: - sprzęt i usługi cyberbezpieczeństwa, - wdrożenie procedur i audyty SZBI, - szkolenia z cyberbezpieczeństwa. Wysokość wsparcia dla pojedynczego podmiotu - 200 tys. zł - 850 tys. zł Wsparcie otrzymało 2495 JST	1.474 mln zł	07.2023 - 31.12.2027
FERC	Utworzenie lub rozwój Lokalnych Centrów Cyberbezpieczeństwa	LCC	Budowa centrów obsługujących lokalnie wiele JST w obszarze cyberbezpieczeństwa - wsparcie centralizacji mikroregionalnej w ramach ścisłej współpracy między samorządami w tym obszarze. Średnia wysokość wsparcia dla pojedynczego podmiotu - 9 mln zł	270 mln zł	W przygotowaniu 2025–2029
FERC	Wsparcie finansowe na rzecz cyberbezpieczeństwa – NIS 2	NIS 2	Doposażenie jednostek administracji publicznej w zw. ze wzrostem wymagań dot. zapewnienia cyberbezpieczeństwa w instytucjach administracji publicznej, w wyniku nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa, wprowadzającej do prawodawstwa krajowego wymagania dyrektywy NIS 2, zgodnie z którą staną się one podmiotami kluczowymi. Średnia wysokość wsparcia dla pojedynczego podmiotu - 5 mln zł	500 mln zł	W przygotowaniu 2025–2029

7. Wpływ na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców, oraz na rodzinę, obywateli i gospodarstwa domowe

Skutki							
Czas w latach od wejścia w życie zmian	0	1	2	3	5	10	<i>Łącznie (0-10)</i>
W ujęciu pieniężnym (w mln zł, ceny stałe z r.)	duże przedsiębiorstwa						
	sektor mikro-, małych i średnich przedsiębiorstw						
	rodzina, obywatele oraz gospodarstwa domowe						
	(dodaj/usuń)						
W ujęciu niepieniężnym	duże przedsiębiorstwa	Celem dostosowania się do wymogów projektu przedsiębiorstwa będą musiały wdrożyć środki techniczne i organizacyjne proporcjonalne do wielkości podmiotu. W przypadku dużych przedsiębiorstw może to zająć pewien czas. Niezbędne będzie dokonanie inwentaryzacji infrastruktury, przeglądu procesów i wewnętrznych procedur, przeprowadzenie wewnętrznych szkoleń. Każdy z podmiotów będzie musiał zbudować system zarządzania bezpieczeństwem uwzględniający kwestie takie jak np.: 1) prowadzenie systematycznego szacowania ryzyka wystąpienia incydentu oraz zarządzanie tym ryzykiem; 2) wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, uwzględniających najnowszy stan wiedzy, koszty wdrożenia, wielkość podmiotu, prawdopodobieństwo wystąpienia incydentów, narażenie podmiotu na ryzyka, w szczególności utrzymanie i bezpieczną eksploatację systemu informacyjnego; 3) zbieranie informacji o cyberzagrożeniach i podatnościach na incydenty systemu informacyjnego wykorzystywanego do świadczenia usługi; 4) zarządzanie incydentami; 5) stosowanie środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego wykorzystywanego do świadczenia usługi. Dyrektywa NIS 2 odeszła od wprowadzania konkretnych wymogów bezpieczeństwa na rzecz podejścia opartego na ryzyku. W związku z tym każdy podmiot objęty jej postanowieniami musi sam przeprowadzić analizę ryzyka oraz dostosować stosowane zabezpieczenia do wykrytego ryzyka. Takie rozwiązanie zapewnia elastyczność jak również proporcjonalność wprowadzanych zabezpieczeń do charakteru danej organizacji. Na tym etapie nie jest możliwe oszacowanie kosztów dostosowawczych po stronie przedsiębiorców w zależności od ich rodzajów z uwagi na brak danych. Projekt oddziałuje na podmioty o zróżnicowanej wielkości – od małych do dużych. Koszty audytów bezpieczeństwa, zatrudnienia specjalistów z zakresu cyberbezpieczeństwa, wdrożenia systemu zarządzania bezpieczeństwem informacji itd., będą się znacząco różnić od wielkości i charakteru usług świadczonych przez podmiot.					

		Zasadne będzie poniesienie kosztów na sprzęt, oprogramowanie oraz zatrudnienie nowego personelu. Konieczny może być zakup zewnętrznych usług konsultingowych z zakresu cyberbezpieczeństwa. Warto zauważyć, że już obecnie duże przedsiębiorstwa mają działy zajmujące się cyberbezpieczeństwem, co powinno im ułatwić dostosowanie się do projektu ustawy. Należy zauważyć, że wymogi te stosowane będą jednolicie w całej Unii Europejskiej w związku z czym nie powinno dojść do zaburzeń konkurencyjności. Sama ustawa przewiduje jednakowe dla wszystkich podmiotów kluczowych. Również wymogi dla podmiotów ważnych nie będą różnicowane. Podmioty krajowego systemu cyberbezpieczeństwa będą obowiązane wycofać produkty ICT, usługi ICT i procesy ICT dostawcy uznanego za dostawcę wysokiego ryzyka. Będzie to generowało koszty związane z wycofaniem tego tych produktów, usług i procesów oraz zastąpienie innymi. W tym momencie nie jest jednak możliwe oszacowanie tych kosztów.
sektor mikro-, małych i średnich przedsiębiorstw		Projekt ma wpływ na co najmniej średnie przedsiębiorstwa, z wyjątkami takimi jak przedsiębiorcy komunikacji elektronicznej czy dostawcy usług zaufania – ci będą podlegać ustawie niezależnie od wielkości. Projekt przewiduje, że podmioty kluczowe i podmioty ważne będą wdrażać środki techniczne i organizacyjne proporcjonalne do wielkości podmiotu – uwzględniona została więc sytuacja podmiotów z sektora MŚP. Na tym etapie nie jest możliwe oszacowanie kosztów dostosowawczych po stronie przedsiębiorców w zależności od ich rodzajów z uwagi na brak danych. Projekt oddziałuje na podmioty o zróżnicowanej wielkości – od małych do dużych. Koszty audytów bezpieczeństwa, zatrudnienia specjalistów z zakresu cyberbezpieczeństwa, wdrożenia systemu zarządzania bezpieczeństwem informacji itd., będą się znacząco różnić od wielkości i charakteru usług świadczonych przez podmiot. Projekt może być uzupełniony w tym zakresie, jeżeli w toku konsultacji publicznych zostaną przedstawione dane dotyczące kosztów wdrożenia. W przypadku mikro- i małych przedsiębiorców podlegających ustawie wprowadzono wymóg wyznaczenia co najmniej jednej osoby odpowiedzialnej za utrzymywanie kontaktów z innymi podmiotami kluczowymi lub podmiotami ważnymi – jest to obniżenie wymagań, gdyż regułą jest wyznaczenie 2 osób. Podmioty krajowego systemu cyberbezpieczeństwa będą obowiązane wycofać produkty ICT, usługi ICT i procesy ICT dostawcy uznanego za dostawcę wysokiego ryzyka. Będzie to generowało koszty związane z wycofaniem tego tych produktów, usług i procesów oraz zastąpienie innymi. W tym momencie nie jest jednak możliwe oszacowanie tych kosztów.
rodzina, obywatele oraz gospodarstwa domowe		Rodziny, obywatele, gospodarstwa domowe – regulacje ustawowe przyczynią się do zwiększenia bezpieczeństwa usług, z których korzystają wszyscy obywatele. Zwiększą pewność ciągłości usług. Polepszy się ochrona danych

		osobowych przetwarzanych przez podmioty ważne i podmioty kluczowe. Kierownik podmiotu kluczowego lub podmiotu ważnego będzie podlegał odpowiedzialności karno-administracyjnej za niewykonywanie zadań z zakresu cyberbezpieczeństwa w podmiocie. Tylko osoby niekarane za przestępstwa przeciwko ochronie informacji będą mogły realizować w podmiocie kluczowym lub podmiocie ważnym zadania związane z zarządzaniem ryzykiem cyberbezpieczeństwa oraz obsługi i zgłaszania incydentów. Organy właściwe do spraw cyberbezpieczeństwa, zespoły CSIRT sektorowe, zespoły CSIRT poziomu krajowego i minister właściwy do spraw informatyzacji będą przetwarzały dane osobowe osób do kontaktu wskazanych przez podmioty kluczowe i podmioty ważne. Odbywać to się będzie z zachowaniem właściwości poszczególnych organów czy zespołów. Dane te będą znajdowały się w wykazie podmiotów kluczowych i podmiotów ważnych. Dane te nie będą dostępne publicznie. Obecnie istnieje podobny obowiązek wskazania po 1 osobie do kontaktu przez podmioty publiczne i operatorów usług kluczowych.
Niemierzalne	Koszty związane z wycofaniem sprzętu lub oprogramowania od dostawców wysokiego ryzyka	Nowelizacja ustawy przewiduje kompetencję dla ministra właściwego do spraw informatyzacji do wydania decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Nie jest możliwe w tej chwili wskazanie kosztów jakie poniosą podmioty kluczowe i podmioty ważne w związku z wycofaniem produktów ICT, usług ICT i procesów ICT pochodzących od dostawców wysokiego ryzyka, ponieważ nie można w tej chwili przewidzieć jaką decyzję wyda minister właściwy do spraw informatyzacji i w związku z tym jakie koszty poniosą podmioty zobowiązane do wycofania sprzętu. Należy podkreślić, że w zaproponowanych przepisach prawa nie ma mechanizmu nakazującego natychmiastowe wycofanie sprzętu lub oprogramowania wskazanego w ocenie ryzyka dostawców. Podmioty kluczowe i podmioty ważne zostaną zobowiązane do wycofania danego sprzętu lub oprogramowania w określonym czasie. W przekazanym projekcie jest mowa o 5–7 latach – termin ten jest często uznawany za średni okres użytkowania sprzętu lub oprogramowania, czyli tzw. cykl życia urządzenia. Z uwagi na wskazanie tak długiego okresu na wdrożenie decyzji o ocenie ryzyka, nie są planowane rekompensaty dla przedsiębiorców z uwagi na konieczność wycofania sprzętu lub oprogramowania od dostawców uznanych za dostawców wysokiego ryzyka.
	Koszty związane z wykonaniem polecenia zabezpieczającego	Nowelizacja przewiduje nowe kompetencje dla ministra właściwego do spraw informatyzacji do wydania polecenia zabezpieczającego w drodze decyzji administracyjnej. Nie jest możliwe w tej chwili wskazanie kosztów jakie poniosą podmioty krajowego systemu cyberbezpieczeństwa, ponieważ polecenie zabezpieczające będzie wydawane po wystąpieniu incydentu krytycznego. Podkreślić przy tym należy, że polecenie zabezpieczające ma być adekwatne do cyberzagrożenia.

Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	Wpływ na konkurencyjność gospodarki i przedsiębiorczość będzie różnił się w zależności od typu podmiotu i sektora. Nie jest możliwe oszacowanie kosztów dostosowania się przedsiębiorców do wymogów określonych w nowelizacji. Wynika to z faktu, że konkretne środki techniczne i organizacyjne stosowane przez przedsiębiorców będą zależne od przeprowadzonego szacowania ryzyka. Innego rodzaju środki będą stosować operatorzy zarządzający własną infrastrukturą telekomunikacyjną, a inne dostawcy usług komunikacji elektronicznej, którzy swoją działalność opierają o infrastrukturę innego operatora. Ponadto nie są znane konkretne środki już teraz stosowane przez przedsiębiorców – często z powodów bezpieczeństwa informacja o tych środkach stanowi tajemnicę przedsiębiorstwa. Podkreślić należy, że nakładane obowiązki z zakresu zarządzania ryzykiem cyberbezpieczeństwa pokrywają się z normami technicznymi i innymi standardami stosowanymi dobrowolnie przez przedsiębiorców. Wielu przedsiębiorców już teraz wdraża systemy zarządzania bezpieczeństwem informacji zgodne z normą ISO 27001 oraz systemy zarządzania ciągłością działania zgodne z normą ISO 22301. Część z tych przedsiębiorców uzyskuje nawet certyfikację zgodności z tymi normami. Nie są to oczywiście jedyne sposoby zapewnienia zgodności z projektowanymi przepisami. Niemniej część obowiązków proponowanych w projekcie jest już obecnie stosowana przez przedsiębiorców. Zakłada się, że nowo powstałe zespoły CSIRT sektorowe będą aktywnie wspierać przedsiębiorców w reagowaniu na incydenty, ale także w przekazywaniu informacji o cyberzagrożeniach i podatnościach. CSIRT sektorowe będą także prowadzić działalność szkoleniową. Ideałem jest osiągnięcie wzajemnego zaufania między podmiotami kluczowymi i podmiotami ważnymi z danego sektora a CSIRT sektorowym. Projekt nakłada jedynie konieczne i niezbędne obowiązki, aby osiągnąć cele ustawy. Projekt nie wprowadza regulacji dot. zakazu wykonywania określonej działalności gospodarczej. Z tych powodów uznaje się, że projekt jest zgodny z ustawą z dnia 6 marca 2018 r. – Prawo przedsiębiorców (Dz. U. z 2024 r. poz. 236, z późn. zm.). Projekt zakłada przetwarzanie danych osobowych w minimalnym zakresie – niezbędnym do realizacji czynności nadzorczych organów właściwych do spraw cyberbezpieczeństwa, realizacji zadań zespołów CSIRT w zakresie reagowania na incydenty czy wykonywania obowiązków wynikających z prawa unijnego.

8. Zmiana obciążeń regulacyjnych (w tym obowiązków informacyjnych) wynikających z projektu

☐ nie dotyczy

Wprowadzane są obciążenia poza bezwzględnie wymaganymi przez UE (szczegóły w odwróconej tabeli zgodności).

☒ tak

☐ nie

☐ nie dotyczy

☐ zmniejszenie liczby dokumentów

☒ zwiększenie liczby dokumentów

☐ zmniejszenie liczby procedur

☒ zwiększenie liczby procedur

☐ skrócenie czasu na załatwienie sprawy

☐ wydłużenie czasu na załatwienie sprawy

☐ inne:

☐ inne:

Wprowadzane obciążenia są przystosowane do ich elektronizacji.

☒ tak

☐ nie

☐ nie dotyczy

Komentarz:

Nałożono obowiązki na podmioty kluczowe i podmioty ważne zgodne z wykazem tych podmiotów wskazanych w załączniku nr 1 i 2 do dyrektywy NIS 2. Będą one obowiązane dokonać samorejestracji w wykazie podmiotów kluczowych i ważnych, co umożliwi ich identyfikację, aktywne wsparcie ich przez zespoły CSIRT sektorowe i zespoły CSIRT poziomu krajowego oraz wykonywanie czynności nadzorczych przez organy właściwe do spraw

cyberbezpieczeństwa. Umożliwi to także przekazywanie danych o liczbie tych podmiotów do Komisji Europejskiej i Agencji Unii Europejskiej do spraw Cyberbezpieczeństwa.

Podmioty kluczowe i podmioty ważne będą obowiązane wprowadzić system zarządzania bezpieczeństwem informacji w procesach służących świadczeniu usług przez te podmioty. Odpowiada to zakresowi wymogów co do środków zarządzania ryzykiem wskazanych w art. 21 dyrektywy NIS 2.

Podmioty kluczowe lub podmioty ważne będą obowiązane: wyznaczyć co najmniej 2 osoby odpowiedzialne za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa, zapewnić użytkownikowi usługi dostęp do wiedzy dotyczących cyberzagrożeń, zapewnić możliwość zgłoszenia cyberzagrożenia, incydentu lub podatności związanych ze świadczoną usługą.

Określono wymogi dla podmiotów kluczowych i podmiotów ważnych co do prowadzenia dokumentacji dotyczącej systemu zarządzania bezpieczeństwem informacji.

Kierownik podmiotu kluczowego lub podmiotu ważnego będzie odpowiedzialny za realizację tych zadań przez podmiot – i będą mogły być nałożone na niego kary. Będzie miał też obowiązek przejścia stosownego szkolenia z zakresu cyberbezpieczeństwa.

Tak jak do tej pory operatorzy usług kluczowych tak i inne podmioty kluczowe będą obowiązane przeprowadzać audyty bezpieczeństwa swoich systemów informacyjnych. Audyty będą przeprowadzane co trzy lata. W przypadku podmiotów ważnych audyt będzie przeprowadzany na podstawie decyzji organu właściwego do spraw cyberbezpieczeństwa.

Projektowana ustawa w zakresie zgłaszania incydentów zwiększa liczbę obowiązków nakładanych na podmioty objęte jej regulacją. Podmioty kluczowe i podmioty ważne będą w pierwszej kolejności zgłaszać wczesne ostrzeżenie o incydencie poważnym. Zgłoszenia będą kierowane do CSIRT sektorowego. Wczesne ostrzeżenie będzie mogło zawierać wniosek o wskazanie wytycznych dotyczących możliwych do wdrożenia środków ograniczających skutki incydentu poważnego lub o wsparcie techniczne przy obsłudze incydentu. Po otrzymaniu takiego wniosku CSIRT sektorowy zobowiązany będzie do udzielenia stosownego wsparcia podmiotowi zgłaszającemu taki wniosek. Następnie dokonywane będzie zgłoszenie incydentu. W trakcie obsługi incydentu, na wniosek właściwego CSIRT sektorowego, przekazywane będzie sprawozdanie okresowe, a po zakończeniu obsługi incydentu – sprawozdanie końcowe.

Dostawcy usług zarządzanych w zakresie cyberbezpieczeństwa świadczący usługę obsługi incydentów będą obowiązani udostępniać na swojej stronie internetowej informacje na temat świadczonych usług.

CSIRT sektorowe będą przedstawiały Pełnomocnikowi Rządu do Spraw Cyberbezpieczeństwa sprawozdanie z działalności za poprzedni rok.

Podmioty, które mogą spełniać kryteria uznania za podmioty kluczowe lub podmioty ważne będą mogły być „odpytywane” przez organy właściwe do spraw cyberbezpieczeństwa o informacje, które pozwolą ustalić ich status. Brak udzielenia odpowiedzi będzie skutkował nałożeniem administracyjnej kary pieniężnej.

Nowym zadaniem ministra właściwego do spraw informatyzacji będzie przygotowanie Krajowego Planu reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę. Dokument ten będzie określał zasady postępowania w przypadku wystąpienia takiego incydentu oraz zasady współpracy między organami realizującymi zadania z zakresu cyberbezpieczeństwa oraz organami właściwymi do spraw zarządzania kryzysowego i będzie przyjmowany w drodze uchwały Rady Ministrów. Minister właściwy do spraw informatyzacji będzie również prosił o wkłady inne organy, zwłaszcza te działające w obszarze zarządzania kryzysowego.

Minister właściwy do spraw informatyzacji będzie również dalej realizował zadania pojedynczego punktu kontaktowego oraz przygotowywał i aktualizował krajową strategię cyberbezpieczeństwa. Dalej będzie również działał w ciałach kolegialnych Unii Europejskiej zajmujących się cyberbezpieczeństwem.

CSIRT NASK będzie pełnił rolę koordynatora na potrzeby skoordynowanego ujawniania podatności. W związku z powyższym konieczne będzie przygotowanie procedur w tym zakresie, w szczególności w obszarze komunikacji z producentami sprzętu i oprogramowania, u których będą wykrywane podatności.

Projektowane przepisy przewidują również udział polskich organów ds. cyberbezpieczeństwa w procedurze wzajemnej oceny z organami z innych krajów Unii Europejskiej. Wymaga to przygotowania procedur związanych z ich wyjazdami zagranicznymi oraz przyjmowaniem przedstawicieli innych państw w Polsce.

Minister Obrony Narodowej będzie udostępniał CSIRT NASK listę przedsiębiorców, wobec których wydano decyzję w sprawie realizacji zadań na rzecz Sił Zbrojnych.

CSIRT NASK będzie prowadził usługę online umożliwiającą sprawdzenie przez osobę fizyczną, czy jej dane osobowe nie zostały ujawnione w sieci internet w sposób nieuprawniony, na skutek incydentu lub cyberzagrożenia.

Zespoły CSIRT poziomu krajowego oraz CSIRT sektorowe otrzymają możliwość weryfikacji niekaralności swojego personelu.

Producent badanego produktu ICT lub dostawca badanej usługi ICT w trybie art. 33 KSC będą obowiązani przekazać dokumentację dotyczącą badanego produktu ICT lub badanej usługi ICT na żądanie CSIRT poziomu krajowego prowadzącego badanie.

Minister Obrony Narodowej będzie obowiązany do udzielenia wsparcia CSIRT koordynującemu obsługę incydentu krytycznego przez właściwe jednostki organizacyjne podległe Ministrowi Obrony Narodowej lub przez niego nadzorowane, jeżeli został zobowiązany przez Prezesa Rady Ministrów.

Minister właściwy do spraw zagranicznych będzie prowadził i koordynował działalność dyplomatyczną w zakresie cyberbezpieczeństwa w stosunkach z państwami trzecimi i organizacjami międzynarodowymi.

W związku z nałożeniem na podmioty krajowego systemu cyberbezpieczeństwa szeregu obowiązków istotne zmiany zachodzą w przepisach dotyczących nadzoru i egzekwowania przepisów, a także nakładania kar administracyjnych. Projektowane regulacje wyposażają organy właściwe do spraw cyberbezpieczeństwa w szerokie kompetencje nadzoru i egzekwowania przepisów takie jak wydawanie ostrzeżeń, nakazów, decyzji administracyjnych nakazujących podjęcie lub zaniechanie określonego działania. Organy te zostaną również wyposażone w środki, które znajdą zastosowanie w sytuacji, w której podmiot kluczowy lub podmiot ważny nie wykonał w terminie postanowień określonych w ostrzeżeniu, nakazie czy decyzji. Wśród obowiązków nakładanych na organy właściwe do spraw cyberbezpieczeństwa należy wymienić w szczególności obowiązek brania pod uwagę określonych kryteriów, które należy przeanalizować w celu podjęcia działań nadzorczych i egzekwowania przepisów, a także wymierzając karę pieniężną.

Rozbudowany został również katalog przypadków określających kiedy podmioty kluczowe lub podmioty ważne podlegają karze pieniężnej. Oznacza to co do zasady zwiększenie zadań dla organów właściwych do spraw cyberbezpieczeństwa, które będą musiały nakładać kary pieniężne za określone działania lub zaniechania, których dopuszczać się będą podmioty kluczowe lub podmioty ważne. Ponownie należy podkreślić, że wymierzając karę pieniężną organy właściwe do spraw cyberbezpieczeństwa obligatoryjnie będą musiały dokonywać analizy określonych w projektowanych przepisach przesłanek.

Ustawa nakłada nowe obowiązki na podmioty świadczące usługi rejestracji nazw domen oraz rejestrowi nazw domen najwyższego poziomu. Przede wszystkim podmioty te muszą prowadzić bazy danych dotyczących rejestrowanych domen zawierające informacje o domenach, kto i kiedy je zarejestrował. Na żądanie uprawnionych podmiotów takich jak organy ścigania, sądy, prokuratura, ale również Prezesa UKE podmioty te będą obowiązane udzielać informacji o zarejestrowanych domenach, w tym także danych osobowych.

Względem dyrektywy NIS 2 wskazano dodatkowe obowiązki dla podmiotów kluczowych i podmiotów ważnych:

- Dostawcy usług zarządzanych w zakresie cyberbezpieczeństwa świadczący usługę obsługi incydentów są obowiązani publikować na swojej stronie internetowej informacje o zakresie swoich usług – jest to zgodne z przyjętą rynkową praktyką.
- Dostawcy usług zarządzanych w zakresie cyberbezpieczeństwa, którzy są małymi lub średnimi przedsiębiorcami są traktowani jako podmioty kluczowe – istotą jest włączenie do krajowego systemu cyberbezpieczeństwa także mniejszych zespołów typu SOC/CSIRT/CERT, które ze względu na wrażliwe informacje o swoich klientach powinny spełniać wymogi z zakresu cyberbezpieczeństwa.
- Dodano nowe rodzaje podmiotów podlegających krajowym regulacjom:
 - podmiot będący operatorem obiektu energetyki jądrowej – jako podmiot kluczowy;
 - inwestor obiektu energetyki jądrowej – jako podmiot ważny.

Celem jest objęcie wymogami z zakresu cyberbezpieczeństwa również budowanych elektrowni jądrowych, co zmniejszy ryzyko wystąpienia incydentów cyberbezpieczeństwa związanych z energią jądrową.

- Podmioty kluczowe i podmioty ważne są obowiązane zapewnić użytkownikom swoich usług możliwość zgłaszania im incydentów, podatności i cyberzagrożeń związanych z usługami świadczonymi przez te podmioty – celem jest zapewnienie wymiany informacji między użytkownikiem usługi, który mógł doświadczyć incydentu, a podmiotem świadczącym usługę.
- Dostawcy sprzętu i oprogramowania są obowiązani przekazać na żądanie zespołu CSIRT przeprowadzającego badanie z art. 33 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa dokumentację badanego produktu ICT lub usługi ICT. – rozwiązanie to ma na celu umożliwić efektywne badanie pod kątem identyfikacji podatności, które zagrażają bezpieczeństwu narodowemu.

- Zespoły CSIRT poziomu krajowego otrzymają również licencję ustawową m.in. na analizę kodu źródłowego badanego produktu ICT lub usługi ICT.
- Podmioty kluczowe oraz podmioty ważne będą obowiązane podać w wykazie podmiotów kluczowych i podmiotów ważnych domeny internetowe wykorzystywane przez podmiot kluczowy lub podmiot ważny w sposób ciągły – umożliwi to zespołom CSIRT informowanie zwrotnie podmiotów o cyberzagrożeniach oraz podatnościach, które dotyczą tych domen.

Dyrektywa NIS 2 wprowadza na podmioty kluczowe i podmioty ważne obowiązek zapewnienia bezpieczeństwa łańcuchów dostaw i mitygacji podatności związanych z dostawcami sprzętu lub oprogramowania. Projekt nowelizacji wprowadza postępowanie w sprawie uznania za dostawcę wysokiego ryzyka – skutkiem identyfikacji jest obowiązek wycofania sprzętu i oprogramowania przez podmioty kluczowe i podmioty ważne w terminach od 4 do 7 lat. Jest to wdrożenie Toolboxa 5G, natomiast zdaniem projektodawcy jest to rozwiązanie spójne z dyrektywą.

9. Wpływ na rynek pracy

Implementacja dyrektywy NIS 2 wprowadza regulacje, które obejmują wiele nowych podmiotów prawnych i prywatnych. Oprócz tradycyjnych sektorów infrastruktury krytycznej nowelizacja KSC dotyczyć będzie również m.in.: usługi pocztowe i kurierskie, produkcję żywności, farmaceutykę, sektor IT, gospodarkę odpadami, czy sektor cyfrowy. Zwiększy to zapotrzebowanie na usługi oraz ekspertów z zakresu cyberbezpieczeństwa w nowych sektorach gospodarki.

Nowe zadania i obowiązki podmiotów kluczowych lub podmiotów ważnych przyczynią się do zwiększenia popytu na usługi z zakresu m.in.: zarządzania ryzykiem, raportowania o incydentach, testowania zabezpieczeń, szyfrowania danych czy prowadzenia szkoleń o tej tematyce. Obecnie na rynku działają przedsiębiorstwa świadczące tego rodzaju usługi, jednak wprowadzone przepisy zwiększą popyt na ich działalność, skutkiem czego będzie zatrudnienie dodatkowych osób.

Ponadto w związku z tym, że wiele podmiotów z nowych sektorów, które obejmuje dyrektywa NIS 2 będzie musiało po raz pierwszy wdrożyć procedury cyberbezpieczeństwa, zapotrzebowanie na rynku usług z tego zakresu w danych obszarach gospodarki wzrośnie. W wyniku tego należy spodziewać się nowych ofert pracy dla osób będących specjalistami w dziedzinie cyberbezpieczeństwa, ale również znających się na funkcjonowaniu podmiotów z sektorów wymienionych w NIS 2.

Warto podkreślić, że większy nacisk, jaki będzie kładziony na cyberbezpieczeństwo, może wpłynąć pozytywnie również na inne zawody związane z informatyką. Dyrektywa NIS 2 promuje podejście „security by design”, które zakłada uwzględnienie wymagań bezpieczeństwa już na etapie projektowania rozwiązań informatycznych. Tworzenie takich rozwiązań oraz większa dbałość o bezpieczeństwo systemów w ramach codziennej działalności również będzie wymagało zatrudnienia dodatkowych osób.

Zgodnie z raportem „NIS Investments 2024” Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) wynika, że organizacje przeznaczają obecnie średnio 9,0% budżetu IT na bezpieczeństwo informacji (wzrost o 1,9 punktów procentowych w stosunku do roku poprzedniego). Udział etatów związanych z bezpieczeństwem w całkowitej liczbie pracowników IT spadł do 11,1%, co świadczy o utrzymujących się trudnościach w pozyskiwaniu wykwalifikowanych kadr. Aż 89% badanych podmiotów deklaruje potrzebę zwiększenia zasobów ludzkich w obszarze cyberbezpieczeństwa, aby sprostać wymogom NIS 2, przy czym największe potrzeby dotyczą architektury i inżynierii bezpieczeństwa – 46% oraz operacji bezpieczeństwa – 40%. Jednocześnie 59% małych i średnich przedsiębiorstw wskazuje, że napotyka trudności w rekrutacji we wszystkich dziedzinach bezpieczeństwa, a 76% pracowników zespołów cyberbezpieczeństwa nie posiada formalnych certyfikatów branżowych, co pokazuje skalę luki kompetencyjnej.

Komisja Europejska szacowała, że w 2024 roku deficyt specjalistów ds. cyberbezpieczeństwa w Unii Europejskiej wyniósł około 299 tys. osób¹⁴⁾. Potwierdza to analiza OECD¹⁵⁾ z 2024 r., wskazująca na niedobór ok. 347 tys. ekspertów w Europie.

W 2024 r. Grant Thornton, organizacja audytorsko-doradcza, zauważyła, że 45% ankietowanych uważa, że dużym wyzwaniem na drodze do wdrożenia NIS 2 jest brak odpowiedniej liczby specjalistów w tym obszarze¹⁶⁾.

¹⁴⁾ <https://digital-skills-jobs.europa.eu/en/cybersecurity-skills-academy> (dostęp: 25.9.2025 r.)

¹⁵⁾ Building a Skilled Cyber Security Workforce in Europe - Insights from France, Germany and Poland z 6 lutego 2024 roku. Dostępne do pobrania pod adresem: https://www.oecd.org/en/publications/building-a-skilled-cyber-security-workforce-in-europe_3673cd60-en/full-report.html (dostęp: 25.9.2025 r.)

¹⁶⁾ Dyrektywa NIS-2: Czym jest, kogo dotyczy i kiedy wchodzi w życie? - Grant Thornton (dostęp: 26.9.2025 r.)

W efekcie projekt zwiększy zapotrzebowanie na specjalistów z zakresu cyberbezpieczeństwa – operatorów 1, 2, 3 linii operacyjnego centrum bezpieczeństwa, analityków cyberzagrożeń, podatności, specjalistów ds. świadomości cyberbezpieczeństwa (awareness), menedżerów z zakresu cyberbezpieczeństwa. Ponadto będzie zapotrzebowanie na audytorów przeprowadzających audyty bezpieczeństwa.

Warto zauważyć, że w związku z zapotrzebowaniem na specjalistów w zakresie omawianym w nowelizacji, zaistnieje również zapotrzebowanie na nauczycieli akademickich, gdyż uczelnie wyższe coraz częściej oferują w swojej ofercie kierunki związane z cyberbezpieczeństwem.

Mapowaniem ról i zawodów na obowiązki związane z dyrektywą NIS 2 przeprowadziła ENISA <https://www.enisa.europa.eu/publications/cybersecurity-roles-and-skills-for-nis2-essential-and-important-entities>.

Z powyższych względów wpływ projektu na rynek pracy należy uznać za pozytywny, zarówno z perspektywy wzrostu zatrudnienia, jak i rozwoju kompetencji cyfrowych.

10. Wpływ na pozostałe obszary

☐ środowisko naturalne	☐ demografia	☒ informatyzacja
☐ sytuacja i rozwój regionalny	☐ mienie państwowe	☐ zdrowie
☒ sądy powszechne, administracyjne lub wojskowe	☐ inne:	

Omówienie wpływu	Znaczne zwiększenie nacisku na cyberbezpieczeństwo będzie miało pozytywny wpływ na informatyzację. Nowe wymogi sprawią, że wzrośnie znaczenie rynkowe produktów, które zapewniają odpowiedni poziom cyberbezpieczeństwa. Wzrost popytu na takie rozwiązania będzie powodował, że producenci będą musieli dostarczyć produkty i usługi dostosowane do klientów. Przy projektowaniu i tworzeniu tych produktów będą brane pod uwagę kwestie cyberbezpieczeństwa. Będzie to miało pozytywny wpływ na cały rynek ICT, gdyż zwiększy dostępność bezpiecznych rozwiązań ICT. Projekt ustawy przewiduje nowe administracyjne kary pieniężne. Skargi na decyzje administracyjne w sprawie nałożenia kary będą rozpatrywały sądy administracyjne. Utworzony zostanie nowy wykaz – wykaz podmiotów kluczowych i podmiotów ważnych. Za jego funkcjonowanie będzie odpowiedzialny minister właściwy do spraw informatyzacji. Przewiduje się powierzenie realizacji tego zadania Naukowej i Akademickiej Sieci Komputerowej – Państwowemu Instytutowi Badawczemu, z uwagi na to, że wykaz będzie funkcjonował w systemie S46, który już obecnie jest prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy. Proponowane przepisy ustanowią spójne wymogi cyberbezpieczeństwa także dla systemów informacyjnych wykorzystywanych przez podmioty publiczne. Przepisy kolejnych, nowych ustaw, tworzące nowe systemy informacyjne czy rejestry publiczne powinny być spójne z przepisami nowelizowanej KSC.

11. Planowane wykonanie przepisów aktu prawnego

Projektowana ustawa wejdzie w życie w terminie miesiąca od dnia ogłoszenia.

Pierwszym krokiem będzie utworzenie przez ministra właściwego do spraw informatyzacji wykazu podmiotów kluczowych i podmiotów ważnych. Podmioty, które w dniu wejścia w życie projektowanej ustawy spełniają kryteria dla podmiotu kluczowego lub podmiotu ważnego będą obowiązane zarejestrować się w wykazie. Minister właściwy do spraw informatyzacji udostępni w Biuletynie Informacji Publicznej harmonogram rejestracji, aby przeciwdziałać obciążeniu systemu.

Podmioty kluczowe i podmioty ważne otrzymają 6 miesięcy okresu dostosowawczego do nowych obowiązków.

W zakresie utworzenia CSIRT sektorowych pierwszym krokiem będzie zaplanowanie budowy takiej instytucji – wybranie podmiotu, który będzie realizował to zadanie, zaplanowanie budżetu, określenie liczby etatów, zaplanowanie struktury zespołu. Następnie konieczne będzie zapewnienie lokalizacji, sprzętu, oprogramowania, rekrutacja kadr. Po uzyskaniu zdolności operacyjnej nastąpi ogłoszenie tej informacji w dzienniku urzędowym organu właściwego do spraw cyberbezpieczeństwa – od tego momentu podmioty kluczowe lub podmioty ważne będą zgłaszać incydenty do danego CSIRT sektorowego. Niezależnie od tego powinna być przeprowadzona akcja informacyjna w ramach sektora – spotkania, konferencje mające przybliżyć zespół CSIRT, a także budować zaufanie między podmiotami a zespołem.

Polecenie zabezpieczające oraz postępowanie w sprawie uznania za dostawcę wysokiego ryzyka będą stosowane w razie zaistnienia potrzeby.

12. W jaki sposób i kiedy nastąpi ewaluacja efektów projektu oraz jakie mierniki zostaną zastosowane?

Zastosowane będą następujące mierniki:

- 1) liczba podmiotów wpisanych do wykazu podmiotów kluczowych i podmiotów ważnych;
- 2) liczba zgłoszonych incydentów poważnych w danym roku kalendarzowym;
- 3) liczba przeprowadzonych audytów przez podmioty kluczowe;
- 4) liczba incydentów krytycznych w danym roku kalendarzowym;
- 5) liczba przeprowadzonych ocen bezpieczeństwa;
- 6) liczba przeprowadzonych badań produktów i usług ICT z art. 33;
- 7) liczba wydanych rekomendacji Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa;
- 8) liczba i rodzaj przeprowadzonych czynności nadzorczych;
- 9) liczba nałożonych administracyjnych kar pieniężnych.

Mierniki te dadzą odpowiedź na pytanie, czy i w jaki sposób przepisy ustawy są stosowane. Zostanie też przeprowadzona analiza orzecznictwa sądów w sprawach dot. odpowiedzialności administracyjnej wynikającej z nowych przepisów. Analiza ta wykaże istotne kwestie w wykładni przepisów ustawy przez sądy. Będzie ona stanowiła podstawę do ustalenia, czy konieczna jest interwencja prawodawcy celem doprecyzowania przepisów ustawy.

Dzięki obowiązkowi sprawozdawania się przez CSIRT sektorowe Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa będzie w stanie dokonać oceny ich funkcjonowania, w ramach jego kompetencji do oceny funkcjonowania krajowego systemu cyberbezpieczeństwa, w szczególności wzięte pod uwagę zostaną takie kwestie jak: liczba zgłoszonych incydentów do danego CSIRT, w tym liczba zgłoszonych incydentów poważnych, czas reagowania na incydenty, a także pozostała działalność CSIRT sektorowego, liczba przeprowadzonych działań edukacyjnych wśród podmiotów kluczowych/ podmiotów ważnych.

Monitorowana będzie liczba incydentów poważnych, a także przyczyny ich wystąpienia oraz ich skutki dla cyberbezpieczeństwa kraju.

Dużo informacji przyniosą pierwsze miesiące stosowania ustawy – będzie to czas samorejestracji podmiotów w wykazie podmiotów kluczowych i podmiotów ważnych. Będzie można wtedy zidentyfikować, jak rozumiana jest kwalifikacja podmiotu jako podmiot kluczowy lub podmiot ważny. Dużą rolę odegra tutaj działalność organów właściwych do spraw cyberbezpieczeństwa, które powinny edukować swoje sektory w tym zakresie. Ministerstwo Cyfryzacji będzie monitorować szczególnie ten okres – i w razie potrzeby podejmować adekwatne działania takie jak publikowanie wyjaśnień co do stosowania przepisów ustawy czy kwalifikacji podmiotu jako podmiotu kluczowego lub podmiotu ważny. W skrajnym przypadku dopuszcza się możliwość nowelizacji ustawy, jeżeli okaże się, że obowiązujące przepisy w praktyce są zbyt niejasne, aby je stosować.

Zgodnie z § 152 ust. 1 pkt 2 uchwały nr 190 Rady Ministrów z dnia 29 października 2013 r. – Regulamin pracy Rady Ministrów, po 3 latach od wejścia w życie nowelizacji zostanie sporządzony OSR ex-post, który zostanie skonsultowany z Komisją Wspólną Rządu i Samorządu Terytorialnego.

13. Załączniki (istotne dokumenty źródłowe, badania, analizy itp.)

Załącznik nr 1 do OSR – Dostawca wysokiego ryzyka (high risk vendor) i bezpieczeństwo sieci 5G w Europie;

Załącznik nr 2 do OSR – Koszty pojedynczego zespołu CSIRT sektorowego w zł;

Załącznik nr 3 do OSR – Ocena skutków regulacji KSC 2.0 dla NASK-PIB w latach 2025–2035 Estymacja kosztów;

Załącznik nr 4 do OSR – podsumowanie wydatków dla poszczególnych części budżetowych w zł;

Załącznik nr 5 do OSR – Koszty budżetu państwa związane ze zmianami w ustawie z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa w tys. zł.

Dostawca wysokiego ryzyka (high risk vendor) i bezpieczeństwo sieci 5G w Europie

Austria.....	2
Belgia	3
Bułgaria.....	3
Chorwacja	4
Cypr.....	4
Czechy.....	4
Dania	5
Estonia.....	6
Finlandia	7
Francja.....	8
Grecja.....	9
Hiszpania.....	9
Irlandia	10
Litwa	11
Luksemburg	12
Łotwa	12
Malta	13
Niderlandy.....	13
Niemcy	14
Portugalia	17
Rumunia	18
Słowacja.....	18
Słowenia.....	19
Szwecja	20
Wielka Brytania	21
Węgry.....	21
Włochy.....	21

Austria

W zakresie bezpieczeństwa sieci 5G kluczowym aktem prawnym jest austriackie rozporządzenie w sprawie bezpieczeństwa sieci¹⁾ z 2020 r. Zgodnie z tym rozporządzeniem na operatorów telekomunikacyjnych, posiadających ponad 100 000 abonentów, nałożono liczne obowiązki informacyjne, w tym obowiązek przedstawiania na uzasadnione żądanie organu regulacyjnego wykazu funkcji i producentów urządzeń wykorzystywanych do obsługi sieci 5G oraz, w stosownych przypadkach, innych komponentów przez nich wykorzystywanych.

Ponadto, operatorzy muszą:

- 1) prowadzić Sieciowe Centra Operacyjne (NOC), jak również Centra Operacyjne Bezpieczeństwa (SOC) we własnych obiektach na terenie Unii Europejskiej;
- 2) skutecznie monitorować przez NOC/SOC wszystkie krytyczne elementy sieci 5G, w celu wykrywania anomalii oraz identyfikacji i zapobiegania zagrożeniom;
- 3) zarządzać ruchem sieciowym lub usługami komunikacyjnymi, w celu zapobiegania nieuprawnionym nieautoryzowanym zmianom w komponentach sieci lub usług;
- 4) zapewniać ochronę fizyczną krytycznych komponentów sieci i sieci 5G, z zastosowaniem podejścia opartego na analizie ryzyka w przypadku wielodostępowych komputerów brzegowych (MEC) i stacji bazowych;
- 5) zapewnić, aby dostęp do sieci miał wyłącznie wykwalifikowany personel, który przeszedł kontrolę bezpieczeństwa, a dostęp osób trzecich był ograniczony i monitorowany;
- 6) stosować odpowiednie narzędzia i procesy w celu zapewnienia integralności oprogramowania, w szczególności aktualizować oprogramowanie oraz likwidować wykryte podatności;
- 7) posiadać strategię wielu dostawców uwzględniającą ograniczenia techniczne i wymogi interoperacyjności różnych części sieci 5G.

W załączniku do tego rozporządzenia została określona lista funkcji komponentów sieci 5G²⁾. Federalny Minister Rolnictwa, Regionów i Turystyki może ze względów bezpieczeństwa narodowego zakwalifikować, w drodze decyzji, producentów elementów sieci łączności elektronicznej lub dostawców usług dla takich sieci, w każdym przypadku, z wyjątkiem sieci nadawczych w rozumieniu federalnej ustawy o radiofonii i telewizji (BVG-Rundfunk), jako dostawców wysokiego ryzyka.

Taki dostawca jest wykluczony:

¹⁾ https://www.rtr.at/TKP/aktuelles/veroeffentlichungen/veroeffentlichungen/Verordnungen/TKNSiV-Text-BGBLA_2020_II_301.pdf.

²⁾ <https://www.rtr.at/TKP/aktuelles/veroeffentlichungen/veroeffentlichungen/Verordnungen/TKNSiV-Anhang2.pdf>.

- 1) z dostaw składników istotnych dla bezpieczeństwa lub składników sieciowych dla sieci oraz
- 2) ze świadczenia usług związanych z bezpieczeństwem sieci.

Tego typu decyzja może obowiązywać maksymalnie 2 lata.

Prawo austriackie w zakresie czynników wpływających na uznanie za dostawcę wysokiego ryzyka nie odnosi się wprost do kwestii wpływu państw trzecich na dostawcę.

Belgia

W dniu 11 marca 2022 r. opublikowano w Dzienniku Ustaw Belgii ustawę o zmianie niektórych przepisów dotyczących łączności elektronicznej w celu wprowadzenia dodatkowych środków bezpieczeństwa w odniesieniu do świadczenia usług telefonii komórkowej 5G³⁾. Przewidziano w niej procedurę autoryzacji dla sprzętu wykorzystywanego w sieci 5G. Wnioski w tym zakresie zgłasza się do ministra, który będzie wydawał decyzje przy autoryzacji.

Będą przy tym brane pod uwagę czynniki związane z dostawcą takie jak:

- 1) powiązania z rządami państw trzecich;
- 2) prawo lub sytuacja w kraju dostawcy, w szczególności w przypadku braku nadzoru demokratycznego lub legislacyjnego;
- 3) funkcjonowanie konwencji o ochronie danych lub bezpieczeństwa między Unią Europejską a danym państwem;
- 4) zdolność danego państwa do wywierania jakiegokolwiek formy nacisku, w tym w odniesieniu do miejsca produkcji sprzętu;
- 5) zdolność dostawcy do zabezpieczenia dostaw;
- 6) ogólna jakość produktów lub usług oraz praktyki bezpieczeństwa dostawcy, w tym stopień kontroli nad jego własnym łańcuchem dostaw oraz czy praktyki bezpieczeństwa są odpowiednio traktowane priorytetowo.

Bulgaria

Obecne przepisy prawa komunikacji elektronicznej w Bułgarii nakładają jedynie ogólny obowiązek zapewniania bezpieczeństwa sieci telekomunikacyjnych oraz szacowania ryzyka⁴⁾. Od dnia 9 czerwca 2023 r. w Bułgarii obowiązuje akt określający minimalne wymagania w zakresie bezpieczeństwa publicznych sieci i usług łączności elektronicznej oraz sposobów zarządzania ryzykiem bezpieczeństwa⁵⁾. Kwestie dostawcy wysokiego ryzyka są na razie na

³⁾ <http://reflex.raadvst-consetat.be/reflex/pdf/Mbbs/2022/03/11/149027.pdf>.

⁴⁾ <https://www.lex.bg/laws/ldoc/2135553187>.

⁵⁾ https://cnc.bg/files/Pravna/Pravila_minimalni_iziskvania.pdf.

etapie opracowywania przepisów w ramach planowanych zmian w prawie komunikacji elektronicznej. Proponowane zasady nie zostały jeszcze opublikowane.

Chorwacja

Na razie nie wprowadziła żadnych regulacji w zakresie HRV. Nie ujawniono też informacji o planowanej legislacji.

Cypr

Funkcjonuje tam regulacja dotycząca oceny ryzyka dostawców. Podstawą dla niej jest decyzja cypryjskiego organu ds. cyberbezpieczeństwa, która reguluje szczegóły związane z oceną ryzyka dostawców – przypomina ona rozporządzenie z polskiego porządku prawnego⁶⁾. W ramach cypryjskiej ustawy o bezpieczeństwie sieci i systemów informacyjnych⁷⁾ implementowano przepisy Europejskiego Kodeksu Łączności Elektronicznej dotyczące bezpieczeństwa sieci.

W ramach kryteriów branych pod uwagę przy ocenie dostawców są również czynniki strategiczne.

Czechy

W ramach ustawy implementującej dyrektywę NIS 2, przyjętej w 2025 r., Czechy wprowadziły do swojego porządku prawnego instytucję dostawcy wysokiego ryzyka. W ramach tej ustawy administracja może zakazać korzystania z usług lub produktów określonego podmiotu jeżeli Urząd ds. Cyberbezpieczeństwa uzna, że taki ogólny środek jest niezbędny dla ochrony bezpieczeństwa Republiki Czeskiej lub porządku wewnętrznego. Termin na jaki przyjęty jest środek określa decyzja podawana jest do publicznej wiadomości. Zakaz kierowany jest do wszystkich dostawców strategicznie istotnych usług, czyli usług, których zakłócenie mogłoby mieć znaczny wpływ na bezpieczeństwo lub porządek publiczny w państwie. Instytucja ta nie jest więc ograniczona tylko do sektora telekomunikacji. Ponadto, w przedmiotowej ustawie, Czechy wprowadziły również instytucję polecenia zabezpieczającego.

W lutym 2022 r. czeski CSIRT wystosował rekomendacje dotyczące oceny wiarygodności dostawców technologii dla sieci 5G w Republice Czeskiej⁸⁾. Nie są one wiążące, ale podmioty, na które nałożone są ogólne obowiązki zapewniania cyberbezpieczeństwa, powinny brać je pod uwagę.

⁶⁾ <https://dsa.cy/images/pdf-upload/Decision-408-2020.pdf>.

⁷⁾ <https://dsa.cy/images/pdf-upload/DSA-Law-89-I-2020.pdf>.

⁸⁾ https://nukib.cz/download/aktuality/5G-Recommendation_EN.pdf.

W tym dokumencie wskazane zostało, że na wiarygodność dostawców wpływają następujące czynniki:

- 1) rezydowanie lub podleganie prawu w demokratycznym państwie;
- 2) naruszanie prawa międzynarodowego, w szczególności jeśli zostały przeciwko nim skierowane rezolucje Rady Bezpieczeństwa Organizacji Narodów Zjednoczonych lub restrykcyjne środki wspólnej polityki zagranicznej i bezpieczeństwa Unii Europejskiej;
- 3) prowadzenie działań sprzecznych z podstawowymi interesami Republiki Czeskiej lub jej państw sprzymierzonych;
- 4) nieznajdowanie się pod niewłaściwym wpływem obcego rządu lub organu administracji państwowej i możliwość zapewnienia dostępności, integralności i wiarygodności danych w dostarczanych rozwiązaniach technologicznych z odpowiednim stopniem autonomii;
- 5) spełnianie norm bezpieczeństwa, które są powszechne na rynku w momencie dostawy i jest skłonny zobowiązać się do ich spełniania w przyszłości;
- 6) prowadzenie działalności gospodarczej zgodnie z międzynarodowymi praktykami handlowymi oraz to, że nie czerpie nieproporcjonalnych korzyści od państwa, w którym zamieszkuje lub pod którego wpływy podlega.

Dania

Kwestie dostawcy wysokiego ryzyka zostały uregulowane w ustawie o bezpieczeństwie dostawców w krytycznej infrastrukturze telekomunikacyjnej⁹⁾. Zgodnie z tą ustawą Centrum Cyberbezpieczeństwa może zakazać dostawcy publicznych usług telekomunikacyjnych zawarcie umowy lub nakazać odstąpienie od umowy, która stwarza zagrożenie dla bezpieczeństwa narodowego.

Przy ocenie czy umowa stwarza takie zagrożenie, Centrum bierze pod uwagę cechy kontrahenta takie, jak:

- 1) wpływ jego poddostawców i podmiotów mogących wywierać kontrolę na danego przedsiębiorcę;
- 2) pochodzenie z kraju, który nie ma zawartej umowy związanej z bezpieczeństwem z Danią, bądź nie gwarantuje współpracy w obszarze bezpieczeństwa;
- 3) bycie kontrolowanym, pośrednio lub bezpośrednio, przez obcy rząd;

⁹⁾ <https://www.retsinformation.dk/api/pdf/223450>.

- 4) historia zaangażowania w działania w Danii lub innych krajach, które spowodowały zagrożenie dla bezpieczeństwa narodowego, bezpieczeństwa informacji lub porządku publicznego.

Centrum może nakazać ww. środki tylko, gdy bezpieczeństwa narodowego nie da się zapewnić w inny sposób. Decyzja Centrum może prowadzić do wywłaszczenia własności prywatnej za odszkodowaniem.

Taka decyzja może być zaskarżona do sądu. W ramach procesu sądowego powoływany jest specjalny adwokat, który ma mieć dostęp do dokumentów będących podstawą ww. decyzji. Te dokumenty nie są ujawniane bezpośrednio stronie. Jednakże minister obrony może wskazać, że niektóre dokumenty nie będą przedstawione temu specjalnemu przedstawicielowi.

Estonia

Estonia wprowadziła kwestie bezpieczeństwa sieci 5G do swojego porządku prawnego w ramach wdrażania Europejskiego Kodeksu Łączności Elektronicznej¹⁰⁾. Akt ten zobowiązuje operatorów telekomunikacyjnych do stosowania odpowiednich środków technicznych i organizacyjnych w celu zapewnienia bezpieczeństwa swoim sieciom oraz do szacowania ryzyka w tym obszarze. Zgodnie z art. 87³ ww. aktu sprzęt lub oprogramowanie używane w sieci telekomunikacyjnej nie może powodować zagrożenia dla bezpieczeństwa narodowego¹¹⁾. Przy ocenie sprzętu lub oprogramowania wysokiego ryzyka bierze się pod uwagę m.in. informacje o tym czy:

- 1) lokalizacja lub siedziba znajduje się w państwie (dalej: państwo lokalizacji), które nie jest członkiem Unii Europejskiej, Organizacji Traktatu Północnoatlantyckiego (dalej: NATO) lub państwem członkowskim Organizacji Współpracy Gospodarczej i Rozwoju (dalej: OECD);
- 2) w państwie pochodzenia nie są przestrzegane zasady demokratycznego państwa prawa lub nie są przestrzegane prawa człowieka;
- 3) w państwie przyjmującym nie jest chroniona własność intelektualna, dane osobowe lub tajemnice handlowe osób z innego państwa;
- 4) państwo pochodzenia zachowuje się agresywnie w cyberprzestrzeni;
- 5) państwa członkowskie Unii Europejskiej, NATO lub OECD przypisały cyberataki państwu pochodzenia;

¹⁰⁾ <https://www.riigiteataja.ee/en/eli/501042015003/consolide>.

¹¹⁾ riigiteataja.ee/akt/ESS.

- 6) podlega władzy rządowej lub państwowej państwa pochodzenia lub innego obcego państwa bez niezależnej kontroli sądowej;
- 7) państwo pochodzenia lub inne obce państwo może zobowiązać go do działania w sposób zagrażający bezpieczeństwu państwa estońskiego;
- 8) działalność gospodarcza nie jest oparta na konkurencji rynkowej lub w kraju pochodzenia nie stworzono do tego celu wystarczających warunków;
- 9) struktura własności, struktura organizacyjna lub struktura zarządzania nie jest przejrzysta;
- 10) finansowanie nie jest przejrzyste;
- 11) produkty lub usługi zawierają słabe punkty bezpieczeństwa i nie wdrożono odpowiednich środków bezpieczeństwa w celu ich wyeliminowania;
- 12) nie jest konsekwentnie w stanie zapewnić dostaw produktów lub usług, z wyjątkiem przypadków spowodowanych siłą wyższą.

Sprzęt, który zostanie uznany za stanowiący zagrożenie będzie mógł być wykorzystywany tylko po uzyskaniu zgody odpowiedniego organu. W przypadku obecnie wykorzystywanych urządzeń wprowadzono kilka kategorii sprzętu w zależności od jego funkcji. Danym kategoriom wyznaczono terminy w jakich mogą być użytkowane bez potrzeby uzyskania pozwolenia.

Przepisy te weszły w życie w dniu 3 września 2022 r.

Finlandia

Kluczowymi fińskimi aktami prawnymi w tym obszarze są Prawo Komunikacji Elektronicznej¹²⁾ oraz Rozporządzenie Agencji Transportu i Komunikacji w sprawie krytycznych części sieci łączności¹³⁾. Rozporządzenie to zawiera listę funkcji krytycznych w sieci 5G. Z kolei Prawo Komunikacji Elektronicznej przewiduje, że urządzenie sieci komunikacyjnej nie może być używane w krytycznych częściach publicznej sieci komunikacyjnej, jeżeli istnieją poważne podstawy do podejrzeń, że użycie urządzenia zagrażałoby bezpieczeństwu narodowemu lub obronie narodowej w taki sposób, że użycie to umożliwiłoby działania obcego wywiadu lub działania, które zakłóciłyby, sparaliżowały lub w inny sposób negatywnie wpłynęły na ważne interesy Finlandii, podstawowe funkcje społeczeństwa lub demokratyczny porządek społeczny. Agencja Transportu i Łączności może

¹²⁾ <https://www.finlex.fi/fi/laki/ajantasa/2014/20140917#O9L29P244a>.

¹³⁾ https://finlex.fi/data/normit/47015/Regulation_on_critical_parts_of_a_communications_network.pdf.

zobowiązać właściciela lub innego posiadacza sieci łączności do usunięcia urządzenia sieci łączności z krytycznych części jego sieci.

Powołana została również Rada doradcza ds. bezpieczeństwa sieci, w której zasiadają zarówno przedstawiciele administracji publicznej, jak i biznesu, która będzie prezentować rekomendacje organom rządowym.

Francja

1. W celu zagwarantowania bezpieczeństwa i obrony narodowej w ustawie „LOI n° 2019-810” wprowadza się przepis o wcześniejszej kontroli wszelkiej działalności polegającej na eksploatacji niektórych urządzeń radioelektrycznych w sieciach 5G. Operatorzy będą musieli składać wnioski o zezwolenie do premiera. Premier udzieli odpowiedzi w terminie dwóch miesięcy od dnia otrzymania pełnej dokumentacji wniosku.

Ustali, czy istnieje poważne ryzyko naruszenia interesów w obszarze obrony i bezpieczeństwa narodowego na podstawie kryteriów określonych w ustawie, a zwłaszcza w świetle gwarancji, jakie dają urządzenia co do integralności, bezpieczeństwa, dostępności sieci lub poufności przekazywanych wiadomości i informacji powiązanych z komunikacją.

W razie niespełniania jednego z tych kryteriów wnioski o zezwolenie może zostać odrzucony przez premiera. Aby ocenić ryzyko, uwzględnia się zasady budowy i eksploatacji wprowadzone przez operatora, poziom bezpieczeństwa urządzenia i fakt, czy operator lub jego usługodawcy, w tym podwykonawcy, podlegają lub nie podlegają kontroli lub ingerencji państwa niebędącego członkiem Unii Europejskiej.

2. Budowa sieci 5G zwiększa ryzyko w obszarze cyberbezpieczeństwa związane z urządzeniami sieci ze względu na:

- 1) szczególny charakter techniczny sieci 5G (dynamiczne zarządzanie siecią dostępu, wprowadzenie jednostek przetwarzania informacji na końcówkach sieci – edge computing), oraz
- 2) przypadki używania sieci 5G w dziedzinach przemysłowych, w niektórych gałęziach o znaczeniu krytycznym (np. pojazd podłączony/pojazd autonomiczny, przemysł przyszłości, sieć elektroenergetyczna itp.).

To zwiększone ryzyko wpływa na nowe wymogi w obszarze bezpieczeństwa w odniesieniu do urządzeń, które będą wspierać przyszłe sieci 5G, dotyczące zarówno ich cech technicznych, jak i zobowiązań prawnych, które mogą zmuszać dostawców do współpracy z obcymi organami w gromadzeniu informacji.

Mając na uwadze te nowe obawy dotyczące bezpieczeństwa i najnowsze zmiany w planach budowy sieci 5G niektórych francuskich operatorów telekomunikacyjnych, które mogą zagrażać bezpieczeństwu narodowemu Francji, przyjęto ustawę o bezpieczeństwie sieci. Celem jest ustanowienie wcześniejszego systemu zezwoleń na urządzenia sieci radioelektrycznych. Przepisy francuskie wpisują się również w skoordynowane działania na szczeblu Unii Europejskiej zainicjowane przez Komisję Europejską. Ustawa ta zapewnia ochronę ruchomych sieci radiowych przed zagrożeniami szpiegostwa, piractwa i sabotażu.

Grecja

Nie zostały wprowadzone przepisy odnoszące się bezpośrednio do HRV.

Hiszpania

Od dnia 31 marca 2022 r. obowiązuje w Hiszpanii dekret królewski z mocą ustawy w sprawie wymogów mających na celu zagwarantowanie bezpieczeństwa sieci i usług łączności elektronicznej piątej generacji¹⁴⁾. Dekret nakłada na operatorów telekomunikacyjnych m.in. obowiązek szacowania i zarządzania ryzykiem w obszarze 5G oraz stosowania odpowiednich środków technicznych i organizacyjnych w celu zabezpieczenia sieci. Ustawa przewiduje, że rząd będzie mógł dokonywać oceny dostawców. Przy dokonywaniu takiej oceny mają być brane pod uwagę następujące czynniki:

- 1) powiązania dostawców i ich łańcucha dostaw z rządami państw trzecich;
- 2) skład kapitału zakładowego i struktura organów dostawcy;
- 3) uprawnienie państwa trzeciego do wywierania nacisku na wyniki lub lokalizację przedsiębiorstwa;
- 4) cechy reżimu politycznego państwa pochodzenia dostawcy i jego polityki w zakresie cyberbezpieczeństwa, takie jak:
 - a) charakterystyka reżimu politycznego państwa trzeciego i jego polityki cyberbezpieczeństwa,
 - b) umowy o współpracy w dziedzinie bezpieczeństwa, umowy o współpracy w zakresie cyberbezpieczeństwa, cyberprzestępczości lub ochrony danych podpisane z danym państwem trzecim, jak również traktaty międzynarodowe dotyczące tych dziedzin, których stroną jest to państwo,

¹⁴⁾ [BOE-A-2022-4973 Dekret królewski z mocą ustawy nr 7/2022 z dnia 29 marca 2022 r. w sprawie wymogów mających na celu zagwarantowanie bezpieczeństwa sieci i usług łączności elektronicznej piątej generacji.](#)

- c) stopień zgodności jego przepisów o ochronie danych osobowych z przepisami unijnymi w tym zakresie.

Ustawa przewiduje trzy poziomy ryzyka jakie można przypisać dostawcy.

Szczegółowe obowiązki mają być nakładane na operatorów telekomunikacyjnych w drodze aktów wykonawczych (schematów bezpieczeństwa sieci i usług 5G), które szczegółowo będą określały środki techniczne i organizacyjne jakie będą musieli przyjąć. W takim schemacie może być nałożony obowiązek zmiany dostawcy oraz inne obowiązki związane z bezpieczeństwem łańcucha dostaw.

Irlandia

W dniu 2 marca 2023 r. uchwalona została ustawa Communications Regulation and Digital Hub Development Agency Act 2023¹⁵⁾, która częściowo wdraża dyrektywę 2018/1972 ustanawiającą Europejski Kodeks Łączności Elektronicznej. Ustawa ma na celu zapewnienie, że podmioty udostępniające publiczne sieci łączności elektronicznej i podmioty świadczące publicznie dostępne usługi łączności elektronicznej będą podejmowały odpowiednie, proporcjonalne środki w celu zarządzania zagrożeniami dla bezpieczeństwa sieci i usług, w szczególności łańcuchów dostaw.

Ustawa wyposaża Ministra Środowiska, Klimatu i Komunikacji w uprawnienie do określania, czy dostawcę należy uznać za dostawcę wysokiego ryzyka. Minister może dokonać oceny czy dany dostawca kwalifikuje się do określenia go mianem dostawcy wysokiego ryzyka w każdym czasie. Bierze przy tym pod uwagę poniższe kryteria:

- 1) istnieje prawdopodobieństwo, że dostawca pozostaje pod wpływem państwa trzeciego;
- 2) istnieje znaczące ryzyko, że dostawca nie będzie w stanie zabezpieczyć dostaw krytycznych komponentów;
- 3) ogólna jakość krytycznych komponentów dostarczanych przez dostawcę jest nieodpowiednia lub praktyki w zakresie cyberbezpieczeństwa stosowane przez dostawcę są nieodpowiednie.

Określając prawdopodobieństwo dla pozostawiania dostawcy pod wpływem państwa trzeciego Minister rozważa czy istnieje silny związek między dostawcą a rządem jakiegokolwiek państwa trzeciego, stan praworządności i sytuację polityczną w danym państwie trzecim, w szczególności czy istnieje nadzór demokratyczny i legislacyjny, niezależne sądownictwo, umowy o ochronie danych lub bezpieczeństwie pomiędzy UE a danym państwem trzecim oraz

¹⁵⁾ <https://data.oireachtas.ie/ie/oireachtas/act/2023/4/eng/enacted/a0423.pdf>.

czy państwo trzecie z którego pochodzi dostawca prowadzi ofensywną politykę cyberbezpieczeństwa lub jest z nią powiązany. Minister bada również charakterystykę praktyk biznesowych dostawcy, w szczególności czy jego struktura i źródła finansowania są przejrzyste. Istotne znaczenie ma także zdolność danego państwa trzeciego do wywierania jakiegokolwiek formy nacisku na dostawcę, w tym w odniesieniu do wpływania na to, gdzie sprzęt się znajduje.

Minister może m.in. zakazać instalowania krytycznych komponentów wyprodukowanych lub dostarczonych przez dostawcę wysokiego ryzyka, zakazać lub ograniczyć stosowanie tych komponentów, nałożyć konkretne warunki związane z instalacją lub używaniem tego rodzaju komponentów, wymagać usunięcia, wyłączenia lub modyfikacji krytycznych komponentów wyprodukowanych lub dostarczonych przez dostawcę wysokiego ryzyka. Usługodawca, który nie zastosuje się do postanowienia Ministra popełnia przestępstwo i podlega w związku z tym karze grzywny nieprzekraczającej 250 000 euro lub pozbawienia wolności nawet do 5 lat.

Litwa

Rząd lub upoważniony przez niego organ określa kryteria, zgodnie z którymi uznaje się, że przedsiębiorstwo świadczy usługi mobilne piątej generacji (5G) lub zarządza infrastrukturą niezbędną do świadczenia takich usług.

Na Litwie zobowiązanie do wyeliminowania niezaufanych dostawców oprogramowania i sprzętu z sieci 5G zostało ujęte jako jeden ze strategicznych celów nowego programu rządowego, zatwierdzonego w marcu 2021 r. W dniu 25 maja 2021 r. litewski parlament jasno zadeklarował, że Litwa nie chce należeć do technosfery kontrolowanej przez Chiny i wprowadził zmiany do istniejących ram prawnych, które umożliwiają rządowi uniemożliwienie udziału nierzetelnych dostawców w rynku komunikacji elektronicznej. Jednym z głównych kryteriów przy definiowaniu zaufanego producenta jest to, czy jest on (lub jego beneficjent) zarejestrowany w kraju NATO, Unii Europejskiej lub EOG i/lub Organizacji Współpracy Gospodarczej i Rozwoju (OECD). Kryterium to dotyczy firmy telekomunikacyjnej, dostawcy sprzętu oraz dostawcy usług utrzymania sprzętu, co oznacza, że na rynku komunikacji elektronicznej nie mogą uczestniczyć tzw. firmy z krajów trzecich. Litewskie Narodowe Centrum Cyberbezpieczeństwa¹⁶⁾ (NCSC) będzie odgrywać główną rolę w procesie weryfikacji zaufania do urządzeń, gdzie jedną z funkcji NCSC jest zapewnienie oceny bezpieczeństwa cybernetycznego konkretnych urządzeń i aplikacji w oparciu o potrzeby

¹⁶⁾ <https://www.nksc.lt/en/>.

sektora prywatnego i publicznego. Między innymi na podstawie jego opinii litewski rząd będzie mógł wydać decyzję stwierdzającą, że inwestor stanowi potencjalne zagrożenie dla bezpieczeństwa narodowego. W przypadku wydania takiej decyzji inwestor nie może zawierać decyzji dotyczących obszarów, w których stanowi to zagrożenie do czasu aż ustanie powód, dla którego uznano go za zagrożenie. Decyzje w tej sprawie podejmuje Komisja Bezpieczeństwa Narodowego, w której skład wchodzi przedstawiciele administracji oraz służb specjalnych.

Ww. środki mogą być przedsięwzięte wobec producentów i dostawców sprzętu komputerowego, urządzeń lub oprogramowania wykorzystywanego w działalności związanej z łącznością elektroniczną i/lub dostawcy usług konserwacyjnych lub pomocniczych.

Luksemburg

Luksemburg nie zdefiniował w swoim prawie pojęcia dostawcy wysokiego ryzyka. Wprowadzone jednak zostały regulacje związane z ochroną sieci 5G w ramach ustawy implementującej Europejski Kodeks Łączności Elektronicznej¹⁷⁾. Zgodnie z tą ustawą w przypadku poważnego zagrożenia dla bezpieczeństwa sieci i usług, wpływającego na bezpieczeństwo narodowe, które jest spowodowane wykorzystywanym sprzętem lub oprogramowaniem, na wniosek ministra właściwego do spraw komunikacji elektronicznej i poczty, rząd może wprowadzić środki odnoszące się do tych urządzeń lub programów, w tym zakaz ich stosowania. W ustawie wpisano wprost, że zastosowanie tych środków nie rodzi uprawnień do jakichkolwiek roszczeń odszkodowawczych od rządu.

Powołany został również narodowy komitet telekomunikacji składający się z 20 przedstawicieli ministerstw i innych organów państw, który ma doradzać rządowi w zakresie środków opisanych powyżej.

Łotwa

Funkcjonują zasady związane z zawieraniem umów dotyczących systemów wysokiego ryzyka.

Umowy ich dotyczące mogą zawierać tylko:

- 1) osoby prawne:
 - a) mające siedzibę w państwie członkowskim NATO, Unii Europejskiej lub Europejskiego Obszaru Gospodarczego,

¹⁷⁾ <https://legilux.public.lu/eli/etat/leg/loi/2021/12/17/a927/jo>.

- b) których rzeczywisty właściciel jest obywatelem państwa członkowskiego NATO, Unii Europejskiej lub Europejskiego Obszaru Gospodarczego lub jest obywatelem Republiki Łotewskiej,
 - c) producentem oprogramowania lub sprzętu wykorzystywanego przez nich do świadczenia usługi jest osoba prawna mająca siedzibę w państwie członkowskim NATO, Unii Europejskiej lub Europejskiego Obszaru Gospodarczego lub osoba fizyczna będąca obywatelem Republiki Łotewskiej lub obywatelem państwa NATO, Unii Europejskiej lub Europejskiego Obszaru Gospodarczego;
- 2) osoby fizyczne będące obywatelami Republiki Łotewskiej lub obywatelami państwa należącego do NATO, Unii Europejskiej lub Europejskiego Obszaru Gospodarczego.
- Podmiot, który nie spełnia tych wymagań musi uzyskać zgodę organu odpowiedzialnego za bezpieczeństwo narodowe.

Malta

Malta stoi na stanowisku, że ryzyka związane z dostawcą wysokiego ryzyka, a zwłaszcza powiązane ze środkiem strategicznym SM03, nie stanowią realnego zagrożenia dla ich systemu. Na Malcie została wydana decyzja w sprawie przyznania częstotliwości¹⁸⁾, zgodnie z którą operatorzy telekomunikacyjni muszą szacować ryzyko i stosować adekwatne środki. Nie ma tam jednak bezpośrednich odniesień do dostawcy wysokiego ryzyka.

Niderlandy

W Niderlandach funkcjonuje kategoria dostawcy wysokiego ryzyka¹⁹⁾. Minister Sprawiedliwości i Bezpieczeństwa, nałożył na dostawcę publicznej sieci lub usługi łączności elektronicznej obowiązek wyłącznego korzystania, w wyznaczonych częściach jego sieci lub urządzeń towarzyszących, z produktów lub usług podmiotów innych niż podmiot wyznaczony przez Ministra.

Dostawcą Wysokiego Ryzyka jest podmiot, który:

- 1) jest państwem, podmiotem lub osobą, o której wiadomo lub co do której istnieją podstawy do podejrzeń, że zamierza ona niewłaściwie korzystać z sieci łączności elektronicznej lub usług oferowanych w Niderlandach lub zakłócać ich działanie, lub

¹⁸⁾ <https://www.mca.org.mt/sites/default/files/Assignment%20process%20for%20additional%20spectrum%20for%20wireless%20broadband%20electronic%20communications%20service.pdf>.

¹⁹⁾ <https://wetten.overheid.nl/BWBR0042843/2020-03-01>.

- 2) ma bliskie powiązania z państwem, podmiotem lub osobą, o których mowa w pkt 1, lub jest podmiotem lub osobą, co do których istnieją podstawy do podejrzeń, że mają takie powiązania lub wpływ.

W przypadku, gdy produkty danego dostawcy są już wykorzystywane w funkcjonujących sieciach, minister wyznaczy termin na ich wymianę biorąc pod uwagę konieczność zapewnienia ciągłości świadczenia usług.

Niemcy

W Niemczech zaprezentowano aktualizację modelu dotyczącego cyberbezpieczeństwa z uwzględnieniem funkcjonowania sieci 5G. Podstawowe zasady funkcjonowania systemu zostały przedstawione w kwietniu 2020 r. w opracowaniu zatytułowanym „Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten nach § 109 Telekommunikationsgesetz (TKG)”²⁰⁾. Publikację przygotowały podmioty zajmujące się cyberbezpieczeństwem oraz rynkiem telekomunikacyjnym, w tym m.in. Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahn.

Wśród uwzględnionych kwestii wskazano np.: katalog wymagań z zakresu cyberbezpieczeństwa, składniki infrastruktury telekomunikacyjnej dla 5G, komponenty systemu odpowiedzialne za realizację funkcji krytycznych, a także stworzono listę funkcji krytycznych odnoszących się m.in. do infrastruktury zapewniającej przekazywanie i przechwytywanie danych telekomunikacyjnych. Wiele uwagi poświęcono również procesowi certyfikacji gwarantującej, że dany komponent systemu spełnia określone wymagania z zakresu bezpieczeństwa, odwołując się w tym przypadku do obowiązujących już przepisów Unii Europejskiej oraz regulacji niemieckich. Ważnym aspektem jest ponadto wprowadzenie zasad odnoszących się bezpośrednio do dostawców, takich jak choćby ich różnorodność, wiarygodność, weryfikacja technologiczna czy zobowiązanie do wczesnego informowania o nowych produktach i usługach.

1. Nowe regulacje bezpieczeństwa zostały opublikowane przez niemiecki urząd Bundesnetzagentur (BNetzA), regulujący funkcjonowanie sektora telekomunikacyjnego. Według serwisu Tech Radar wprowadzają one dodatkowe wymagania wobec wszystkich firm, które będą chciały brać udział w budowie niemieckiej sieci łączności 5G. Według

²⁰⁾ https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/KatalogSicherheitsanforderungen/KatalogSicherheitsanforderungen.pdf?__blob=publicationFile&v=6.

nowych przepisów producenci sprzętu zobowiązani są do certyfikowania krytycznych komponentów zgodnie z wymogami bezpieczeństwa ustalonymi przez niemieckie organy państwowe. Zobowiązani są również do zatrudniania w obszarach związanych z bezpieczeństwem jedynie kwalifikowanych pracowników, a także do ciągłego monitorowania procedur bezpieczeństwa. Niemiecka administracja wezwała również działające w kraju firmy telekomunikacyjne do dywersyfikacji dostawców sprzętu i „unikania monokultury”.

2. Niemiecki rząd uchwalił projekt nowej ustawy dotyczącej bezpieczeństwa informatycznego. Ma ona umożliwić dokładne sprawdzenie wiarygodności dostawców komponentów dla systemów infrastrukturalnych o krytycznym znaczeniu, takich jak sieć 5G. Kwestia ta była przedmiotem ożywionych publicznych dyskusji w związku z ewentualnym uczestnictwem chińskich koncernów w budowaniu niemieckiej sieci 5G. W ustawie tej chodzi o zdecydowanie o zagrożenia bezpieczeństwa informatycznego, a nie o poszczególnych producentów.

Zgodnie z brzmieniem ustawy producenci mają składać oświadczenia, w których będą musieli między innymi zadeklarować, czy i jak mogą zapewnić, by komponenty o krytycznym znaczeniu nie posiadały żadnych technicznych właściwości pozwalających na ich nadużywanie, „w szczególności na potrzeby sabotażu, szpiegowania lub terroryzmu poprzez wpływanie na bezpieczeństwo, integralność, dostępność lub zdolność funkcjonowania krytycznie ważnej infrastruktury”. Minimalne wymogi bezpieczeństwa, jakie ma spełniać producent, określi federalne ministerstwo spraw wewnętrznych.

Gdyby okazał się on nie w pełni wiarygodny, na przykład nie zgłaszając użytkownikowi znanych sobie niedociągnięć systemu, będzie można jemu wycofać współpracę. W razie utrzymującego się braku dowodów wiarygodności resortowi spraw wewnętrznych wolno będzie w porozumieniu z innymi zainteresowanymi ministerstwami zabronić dalszego użytkowania wszystkich pochodzących od tego producenta komponentów.

Projekt ustawy zawiera również nakaz zgłaszania przez zarządców krytycznej infrastruktury kierowanych przeciwko niej cyberataków. Wprowadza ponadto jednolitą formę wystawianych przez Federalny Urząd Bezpieczeństwa Techniki Informacyjnej (BSI) certyfikatów bezpieczeństwa dla sprzętu - <https://cyberdefence24.pl/polityka-i-prawo/niemcy-wzmacniają-cyberbezpieczenstwo>

3. W Niemczech Federalna Agencja ds. Sieci (Bundesnetzagentur – BnetzA) określiła bardzo konkretny katalog wymagań w zakresie bezpieczeństwa. Według zaostrzonych kryteriów, w szczególności pod lupę będą brane te elementy infrastruktury, które realizują

tw. funkcje krytyczne. Będą one musiały przejść przez proces certyfikacji, tj. po przeprowadzeniu odpowiedniej procedury technicznej zdobyć świadectwo, że dany komponent spełnia wymagania w zakresie bezpieczeństwa –https://biznes.interia.pl/gospodarka/news-bezpieczenstwo-sieci-5g-kluczowe-dla-funkcjonowania-panstwa,nId,4732854#utm_source=paste&utm_medium=paste&utm_campaign=firefox.

4. W dniu 11 sierpnia 2020 r. Federalna Agencja ds. Sieci opublikowała aktualny projekt katalogu wymagań bezpieczeństwa dla obsługi systemów telekomunikacyjnych i przetwarzania danych oraz przetwarzania danych osobowych. Katalog został opracowany w porozumieniu z Federalnym Urzędem Bezpieczeństwa Informacji (BSI) oraz Federalnym Komisarzem ds. Ochrony Danych i Wolności Informacji (BfDI).

Katalog wymagań bezpieczeństwa dotyczy operatorów sieci telekomunikacyjnych i systemów przetwarzania danych oraz przetwarzania danych osobowych. Jest podstawą koncepcji bezpieczeństwa, uzgodnień technicznych i innych środków zwiększających bezpieczeństwo sieci i usług.

Katalog zawiera w szczególności krytyczne komponenty do certyfikacji:

- 1) deklaracje wiarygodności do uzyskania od producentów i dostawców systemów;
- 2) zapewnienie integralności produktu;
- 3) wprowadzenie monitoringu bezpieczeństwa;
- 4) zatrudnianie wyłącznie przeszkolonego i wykwalifikowanego personelu do pracy w obszarach związanych z bezpieczeństwem;
- 5) dostępność wystarczającej refundacji;
- 6) unikanie monokultur.

Katalog zawiera dodatkowe wymagania bezpieczeństwa dla publicznych sieci i usług telekomunikacyjnych o wysokim poziomie ryzyka. W związku z tym należy stworzyć listę funkcji krytycznych dla infrastruktur o wysokim poziomie ryzyka. Te krytyczne funkcje zostaną wymienione w dokumencie sporządzonym wspólnie z BSI.

W przyszłości lista funkcji krytycznych ma być stale aktualizowana i poprawiana. Uwzględniono i są brane pod uwagę wyniki międzynarodowych analiz, np. Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) czy Organu Europejskich Regulatorów Łączności Elektronicznej (BEREC).

Następujące funkcje są uważane za krytyczne:

- 1) zarządzanie abonentami i mechanizmami kryptograficznymi (jeśli jest to element sieci);
- 2) interfejsy międzysieciowe;

- 3) zarządzane usługi sieciowe;
- 4) zarządzanie wirtualizacją funkcji sieciowych i orkiestracja sieci (MANO), a także wirtualizacja;
- 5) systemy zarządzania i inne systemy wsparcia;
- 6) kontrola transportu i przepływu informacji.

Portugalia

Portugalia wdrożyła przepisy Toolboxa 5G w ramach Prawa Komunikacji Elektronicznej z dnia 16 sierpnia 2022 r.²¹⁾ Nowe przepisy nałożyły na przedsiębiorców komunikacji elektronicznej obowiązki związane z obsługą incydentów jak również uregulowały postępowanie w sprawie potencjalnie niebezpiecznego sprzętu. Organy państwa mogą nałożyć na przedsiębiorców komunikacji elektronicznej dodatkowe obowiązki takie jak:

- 1) obowiązek stosowania produktów, usług i procesów certyfikowanych w ramach systemów certyfikacji cyberbezpieczeństwa, tj. na podstawie przepisów rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych;
- 2) obowiązek zapewnienia zgodności ze szczególnymi warunkami wirtualizacji funkcji sieciowych w zakresie eksploatacji i bezpieczeństwa sieci i usług;
- 3) obowiązek zapewnienia zgodności ze szczegółowymi warunkami podwykonawstwa funkcji w zakresie eksploatacji i bezpieczeństwa sieci i usług lub ich zakaz;
- 4) obowiązek przyjęcia strategii dywersyfikacji dostawców w zakresie eksploatacji i bezpieczeństwa sieci i usług;
- 5) obowiązek lokalizacji centrum operacyjnego sieci i centrum operacyjnego bezpieczeństwa na terytorium krajowym lub na terytorium państwa członkowskiego.

Ponadto, korzystanie z urządzeń w sieciach łączności elektronicznej może podlegać ocenie bezpieczeństwa, przeprowadzanej z inicjatywy dowolnego członka Komitetu Oceny Bezpieczeństwa. Ocenę tą przeprowadza ww. Komitet w którego skład wchodzi wysocy przedstawiciele administracji. W wyniku oceny bezpieczeństwa Komitet może nakazać wykluczenie, zastosowanie ograniczeń w użytkowaniu lub zaprzestanie użytkowania sprzętu lub usług i musi ustanowić, w stosownych przypadkach, rozsądny termin na dostosowanie się. Wydana została jedna decyzja w tym trybie dotycząca firmy Huawei²²⁾.

²¹⁾ <https://diariodarepublica.pt/dr/detalhe/lei/16-2022-187481298>

²²⁾ <https://www.gns.gov.pt/docs/cas-1-2023.pdf>

W ramach warunków aukcji 5G wskazano, że posiadacze nabytych częstotliwości będą podlegali obowiązkom wynikającym z implementacji Europejskiego Kodeksu Łączności Elektronicznej oraz Toolboxa 5G.

Rumunia

W Rumunii funkcjonuje ustawa nr 163/2021 o przyjęciu środków dotyczących infrastruktury informacyjnych i komunikacyjnych o znaczeniu krajowym oraz warunków wdrażania sieci 5G²³⁾. Zgodnie z nią producent sprzętu, który miałby być wykorzystany do budowy sieci 5G musi uzyskać autoryzację w formie decyzji Premiera, wydanej na podstawie zgody Najwyższej Rady Obrony Narodowej. W procesie oceny dostawcy brane pod uwagę są kwestie, takie jak:

- 1) kontrola obcego rządu nad producentem przy braku niezależnego systemu prawnego;
- 2) brak przejrzystej struktury akcjonariatu producenta;
- 3) brak historii etycznego postępowania korporacyjnego producenta;
- 4) funkcjonowanie producenta w systemie prawnym, który nie narzuca przejrzystych praktyk korporacyjnych.

W Najwyższej Radzie Obrony Narodowej zasiadają przedstawiciele rządu, wojska oraz służb specjalnych²⁴⁾. Decyzją nr 35 z dnia 21 lutego 2024 r. Rumunia odmówiła firmie Huawei zezwolenia na dostarczanie sprzętu do sieci 5G.

Słowacja

Słowacja nie posiada ściśle określonych zasad dotyczących bezpieczeństwa sieci 5G. W niektórych ustawach pojawiają się ogólne obowiązki związane z zarządzaniem bezpieczeństwem w łańcuchu dostaw.

Ponadto, przewidywana jest procedura oceny ryzyka dostawcy produktów do działań bezpośrednio związanych z eksploatacją sieci i systemów informatycznych dla operatora usługi podstawowej (zwanego dalej „osobą trzecią”) na rzecz cyberbezpieczeństwa Republiki Słowackiej.

W 2020 r. podpisane zostało przez Słowację i USA memorandum²⁵⁾ dotyczące sieci 5G, które podkreśla znaczenie zachęcania do udziału rzetelnych i godnych zaufania dostawców sprzętu sieciowego i oprogramowania na rynkach 5G, uwzględniania oceny profilu ryzyka oraz

²³⁾ <https://lege5.ro/gratuit/haydomrygy2q/legea-nr-163-2021-privind-adoptarea-unor-masuri-referitoare-la-infrastructuri-informatice-si-de-comunicatii-de-interes-national-si-conditiile-implementarii-retelelor-5g>.

²⁴⁾ <https://csat.presidency.ro/ro/prima-pagina/componenta-csat>.

²⁵⁾ <https://2017-2021.state.gov/united-states-slovak-republic-joint-declaration-on-5g-security/index.html>.

promowania ram, które skutecznie chronią sieć 5G przed nieautoryzowanym dostępem i zakłóceniami.

Wskazano, że w szczególności, oceny bezpieczeństwa powinny być staranne i kompletne oraz obejmować zwłaszcza następujące elementy:

- 1) czy dostawcy sprzętu sieciowego i oprogramowania podlegają kontroli ze strony obcego rządu;
- 2) czy dostawcy sprzętu sieciowego i oprogramowania mają przejrzyste struktury własności, partnerstwa i ładu korporacyjnego;
- 3) czy dostawcy sprzętu sieciowego i oprogramowania są zaangażowani w działalność innowacyjną i poszanowanie praw własności intelektualnej;
- 4) czy dostawcy sprzętu sieciowego i oprogramowania mają na koncie etyczne zachowania korporacyjne i podlegają systemowi prawnemu, który wymusza przejrzyste praktyki korporacyjne.

Słowenia

Przepisy rangi ustawowej dotyczące bezpieczeństwa sieci 5G nie zostały jeszcze wprowadzone. Zgodnie z projektem ustawy rząd będzie mógł zabronić stosowania urządzeń dostarczanych przez dostawcę wysokiego ryzyka w niektórych częściach sieci. Istniejące urządzenia HRV w tych częściach należy wymienić. Jego produkty będą mogły być również zakazane w niektórych innych obszarach takich jak infrastruktura krytyczna, systemy rządowe, obrona narodowa czy systemy ratownicze. Decyzja w sprawie HRV będzie miała charakter niejawny. Rząd, na podstawie opinii Rady Bezpieczeństwa Narodowego, będzie określać dostawców wysokiego ryzyka w drodze decyzji.

Będą przy tym brane pod uwagę następujące kryteria, z których będą musiały wystąpić przynajmniej trzy:

- 1) powiązanie dostawcy z rządem państwa trzeciego;
- 2) ustawodawstwo państwa trzeciego, szczególnie w przypadku braku demokratycznej kontroli i trójpodziału władz, oraz zawarte umowy o bezpieczeństwie lub ochronie danych między UE a danym państwem trzecim;
- 3) cechy własności korporacyjnej dostawcy;
- 4) zdolność państwa trzeciego do wywierania jakiegokolwiek formy nacisku, w tym w odniesieniu do miejsca produkcji sprzętu;
- 5) zdolność dostawcy do zapewnienia dostaw;

- 6) ogólna jakość produktów i praktyk dostawcy w zakresie bezpieczeństwa cybernetycznego, w tym stopień kontroli nad własnym łańcuchem dostaw oraz to, czy praktykom w zakresie bezpieczeństwa nadano odpowiedni priorytet.

Nie rzadziej jednak niż raz na dwa lata będzie przeprowadzany przegląd wydanych decyzji.

W tym momencie kwestia bezpieczeństwa sieci 5G jest regulowana przez rozporządzenie w sprawie środków ograniczających ryzyko dla sieci 5G, które zostało znowelizowane w 2023 r. Jego przepisy odnoszą się do kwestii związanych z dostawcą wysokiego ryzyka.

Szwecja

Szwedzkie prawo komunikacji elektronicznej zawiera jedynie ogólne obowiązki będące implementacją Europejskiego Kodeksu Łączności Elektronicznej²⁶⁾. Implementacja przepisów Toolboxa 5G nastąpiła poprzez określenie warunków aukcji sieci 5G.

W październiku 2020 r. szwedzki krajowy regulacyjny organ telekomunikacyjny (PTS) nałożył następujące warunki udziału w aukcji widma 5G:

- 1) nowe instalacje i wdrożenie funkcji centralnych dla radia w pasmach częstotliwości nie mogą korzystać z produktów pochodzących od chińskich sprzedawców;
oraz
- 2) wszelka istniejąca infrastruktura pochodząca od takich dostawców musi zostać wycofana najpóźniej do dnia 1 stycznia 2025 r.

Ponadto w 2020 r., na podstawie ogólnych przepisów dotyczących aukcji 5G, wykluczył z udziału w aukcji firmę Huawei²⁷⁾. Zakaz został podtrzymany przez szwedzkie sądy.

Wielka Brytania

*Telecommunications (Security) Act 2021*²⁸⁾ znowelizował *The Communications Act 2003*. Właściwy sekretarz stanu może wydać „*designated vendor directions*”, jeśli uważa, że są one niezbędne ze względu na interes bezpieczeństwa narodowego i jeśli nałożone przez ten środek wymagania są proporcjonalne. Do tych aktów muszą stosować się przedsiębiorcy telekomunikacyjni.

Designated vendor direction zawierają zakazy lub ograniczenia dotyczące używania produktów, usług dostarczanych przez dostawcę.

²⁶⁾ https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2022482-om-elektronisk-kommunikation_sfs-2022-482#K8.

²⁷⁾ <https://perma.cc/645J-YLKL>

²⁸⁾ *Telecommunications (Security) Act 2021* chapter 31 <https://www.legislation.gov.uk/ukpga/2021/31/enacted>.

Designated vendor directions mają być przeglądane, co jakiś czas. Sekretarz stanu może wymagać od dostawców usług telekomunikacyjnych przygotowania i przedstawienia planu wdrożenia wymagań określonych w *designated vendor directions*.

Dostawca zostaje określony w *designation notice*. Przy wydawaniu tego aktu sekretarz stanu bierze pod uwagę zarówno czynniki techniczne (jakość, niezawodność, bezpieczeństwo produktów), jak i nietechniczne (związki między dostawcą a krajem pochodzenia, tożsamość osób uczestniczących w rozwoju lub produkcji produktów).

Węgry

Węgry nie wprowadziły przepisów związanych z dostawcą wysokiego ryzyka. Art. 156 węgierskiego Prawa telekomunikacyjnego²⁹⁾ nakłada na operatorów telekomunikacyjnych ogólne obowiązki związane z zapewnianiem bezpieczeństwa, nie odnosi się jednak do kwestii bezpieczeństwa łańcucha dostaw czy oceny wysokiego ryzyka.

W tym obszarze funkcjonuje jeszcze rozporządzenie 41/2015 Ministra Spraw Wewnętrznych, które wprowadza ogólne wymogi bezpieczeństwa informacji dla podmiotów węgierskiego systemu cyberbezpieczeństwa³⁰⁾.

Włochy

Włochy implementowały przepisy Toolboxa 5G w zakresie dostawcy wysokiego ryzyka poprzez zastosowanie do operatorów w tej sieci zasad zawartych w ustawie z dnia 15 marca 2012 r. o specjalnych uprawnieniach dotyczących struktur korporacyjnych w sektorach obronności i bezpieczeństwa narodowego, a także dla działalności o znaczeniu strategicznym w sektorach energii, transportu i komunikacji³¹⁾. Do 2022 r. środki z tej ustawy, takie jak możliwość zablokowania zawarcia umowy bądź nałożenia określonych obowiązków, miały zastosowanie do umów z podmiotami spoza UE dotyczących:

- 1) zakupu towarów i usług związanych z projektowaniem, wdrażaniem, utrzymaniem i obsługą sieci 5G; i/lub
- 2) nabycia powiązanych komponentów zaawansowanych technologicznie.

Ustawa nakłada obowiązek notyfikacji takich transakcji. Krajowy Urząd Oceny i Certyfikacji (Centro di valutazione e certificazione nazionale – CVCN) ocenia ewentualne czynniki

²⁹⁾ <https://net.jogtar.hu/jogszabaly?docid=a0300100.tv>.

³⁰⁾ <https://njt.hu/jogszabaly/2015-41-20-0A>.

³¹⁾ <https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legge:2012-03-15;21>.

podatności, które mogłyby zagrozić integralności i bezpieczeństwu sieci 5G i przesyłanych danych poprzez wstępne dochodzenie³²⁾.

W 2022 r. Włochy rozszerzyły tę regulację także na te dotyczące cyberbezpieczeństwa i usługi chmurowe, które zostaną wskazane szczegółowo w aktach wykonawczych. Zmieniono także procedurę, wprowadzając że obowiązek zgłoszenia nie dotyczy już zamiaru zawarcia konkretnej umowy z dostawcą spoza UE na dostawę towarów lub usług ale, rocznego planu dotyczącego zamiaru zakupu przez cały rok, od dowolnego dostawcy (niezależnie od jego narodowości), towarów lub usług związanych z danymi usługami. Realizacja planu następuje po otrzymaniu zezwolenia. W ramach postępowania administracja może proponować wprowadzenia określonych zmian w planie.

³²⁾ <https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legge:2019-09-21;105>.

Załącznik nr 2 do OSR: koszty pojedynczego zespołu CSIRT sektorowego w zł

Kalkulacje w oparciu o plan finansowy Centrum Cyberbezpieczeństwa w Zamościu na 2024 r.

	2025	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035	2036
nazwa	0	1	2	3	4	5	6	7	8	9	10	11
wynagrodzenia osobowe CSIRT- 14 osób	0	1 819 873	1 948 000	2 083 963	2 230 048	2 386 375	2 553 660	2 732 671	2 924 231	3 129 220	3 348 578	5 119 020
dodatkowe wynagrodzenie roczne	0	0	220 980	236 480	253 060	270 800	289 780	310 080	331 820	355 080	379 980	406 620
składki na ubezpieczenie społeczne finansowane przez pracodawcę	0	446 900	516 220	552 420	591 140	632 580	676 920	724 360	775 140	829 480	887 640	949 860
składki na Fundusz Pracy	0	26 000	30 040	32 140	34 380	36 800	39 380	42 140	45 100	48 260	51 640	55 260
składki na Fundusz Solidarnościowy	0	37 700	43 540	46 600	49 860	53 360	57 100	61 100	65 380	69 960	74 880	80 120
usługi obce	0	1 650 000	1 701 150	1 743 679	1 787 271	1 831 952	1 877 751	1 924 695	1 972 812	2 022 133	2 072 686	2 124 503
materiały i energia	0	277 000	285 587	292 727	300 045	307 546	315 235	323 115	331 193	339 473	347 960	356 659
amortyzacja	0	280 000	288 680	295 897	303 294	310 877	318 649	326 615	334 780	343 150	351 729	360 522
pozostałe koszty funkcjonowania	0	695 000	716 545	734 459	752 820	771 641	790 932	810 705	830 973	851 747	873 041	894 867
SUMA	0	5 232 473	5 750 742	6 018 364	6 301 918	6 601 931	6 919 406	7 255 482	7 611 430	7 988 503	8 388 134	10 347 430

Ocena skutków regulacji KSC 2.0 dla NASK-PIB w latach 2025–2035

Estymacja kosztów

1. Cel dokumentu

Niniejszy dokument ma na celu zaprezentowanie estymacji dodatkowych kosztów, jakie będzie ponosił NASK-PIB w latach 2025 – 2035 w związku z realizacją ustawowych obowiązków wynikających z projektu nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw, zwaną dalej „uKSC”, w tym przepisów implementujących dyrektywę Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniającą rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającą dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz. Urz. UE L 333 z 27.12.2022, str. 80), zwaną dalej „NIS2”.

Na potrzeby estymacji kosztów przyjęto, że dotychczasowe i nowe obowiązki ustawowe będą podlegać ciągłemu procesowi rozwoju i doskonalenia. Zważywszy na ciągle rosnącą liczbę form cyberzagrożeń oraz faktycznych ataków, zapewnienie rozwoju i doskonalenia ww. procesów jest kluczowe dla istotnej poprawy cyberbezpieczeństwa w Polsce.

Estymacja kosztów przygotowana została w podziale na:

1. Zadania CSIRT NASK finansowane z dotacji podmiotowej (KSC)
2. Zadania w ramach projektu S46, finansowane z dotacji celowej.

2. Założenia ogólne

Podczas szacowania kosztów przyjęto następujące założenia:

1. Rok bazowy – 2025.
2. Perspektywa kalkulacji – lata 2025 – 2035.
3. Wysokość kosztów ogólnych od sumy kosztów bezpośrednich – 25%.
4. Średni narzut na inflację w ujęciu rocznym – 6%.
5. Średni narzut na rozwój (współczynnik rozwoju) w ujęciu rocznym – 10%.

3. Estymacja kosztów dla KSC

3.1. Założenia

Podczas szacowania kosztów przyjęto następujące założenia:

1. Rok bazowy – 2025.
2. Perspektywa kalkulacji – lata 2025 – 2035.
3. Wysokość kosztów ogólnych od sumy kosztów bezpośrednich – 25%.
4. Średni narzut na inflację w ujęciu rocznym – 6%.
5. Średni narzut na rozwój (współczynnik rozwoju) w ujęciu rocznym – 10%.

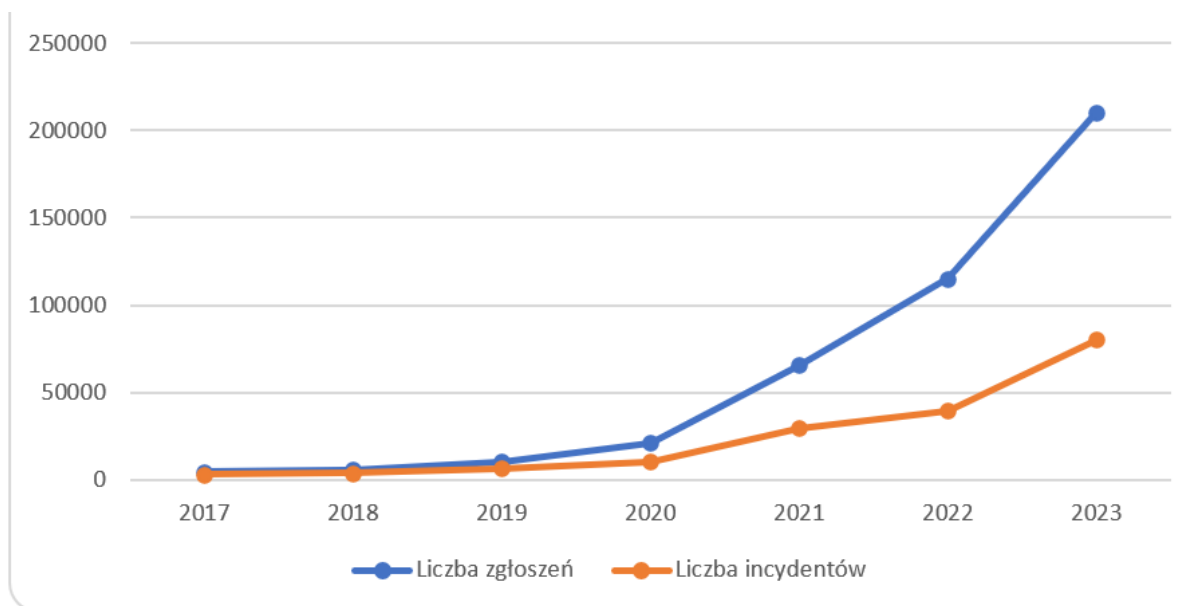
3.2. Opis zadań

W ramach szacowania skutków regulacji na funkcjonowanie CSIRT NASK poza nowymi zadaniami trzeba również wziąć pod uwagę szerszy zakres sektorów gospodarki, które będą objęte krajowym systemem cyberbezpieczeństwa. Zgodnie z aktualnie obowiązującą ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077, z późn. zm.), zwaną dalej „KSC”, przybliżona liczba operatorów usług kluczowych i dostawców usług cyfrowych wynosi 400, natomiast przybliżona liczba podmiotów kluczowych i ważnych – 38 000. W projekcie nowelizacji uKSC liczba sektorów wzrasta z 7 do 18, co bezpośrednio wpłynie na zwiększenie liczby podmiotów kluczowych i ważnych oraz liczbę operatorów usług kluczowych i dostawców usług cyfrowych.

Rosnące zapotrzebowanie na dodatkowe etaty do realizacji dotychczasowych zadań obrazują też poniższe wykresy liczby incydentów oraz zgłoszeń. W skali rocznej można zaobserwować podwojenie liczby zgłoszeń incydentów (rys. 1), a od wejścia KSC w 2018 r. widać wzrost liczby zgłoszeń i incydentów odpowiednio: 44 krotnie i 25 krotnie (rys. 2). Jest to istotne również w kontekście obowiązku wypełniania przez CSIRT poziomu krajowego obowiązków CSIRTów sektorowych przez okres przejściowy trwający do 18 miesięcy od wejścia w życie projektowanej ustawy.



rys. 1. Liczba zgłoszeń i incydentów obsługiwanych przez CERT Polska w okresie IV 2023 – IV 2024 z podziałem na miesiące.



rys. 2. Liczba zgłoszeń i incydentów obsługiwanych przez CERT Polska w latach 2017–2023.

Kalkulacja dotyczy realizacji zadań wynikających z projektu nowelizacji KSC, które nie są ujęte w aktualnie obowiązującej KSC i obejmuje realizację następujących zadań:

ID	Zakres zadania	Podstawa prawna
N.1	Zapewnienie wsparcia w obsłudze incydentów na zlecenie Pełnomocnika	art. 26 ust. 2a nowelizacji
N.2	a) współpraca z sektorowymi i międzysektorowymi społecznościami podmiotów kluczowych i podmiotów ważnych oraz, w odpowiednich przypadkach, wymieniają z nimi stosowne informacje, b) współpraca z krajowymi zespołami reagowania na incydenty bezpieczeństwa komputerowego z państw trzecich, w ramach której mogą wymieniać informacje w tym dane osobowe zgodnie z unijnymi przepisami o ochronie danych,	art. 26 ust. 3 pkt 18–22 nowelizacji

ID	Zakres zadania	Podstawa prawna
	c) udział we wdrażaniu bezpiecznych narzędzi wymiany informacji zgodnie z podmiotami kluczowymi i podmiotami ważnymi oraz innymi podmiotami, d) prowadzenie działań na rzecz podnoszenia poziomu bezpieczeństwa systemów informacyjnych podmiotów krajowego systemu cyberbezpieczeństwa, przez: – wykonywanie oceny bezpieczeństwa, – identyfikowanie podatności systemów dostępnych w otwartych sieciach teleinformatycznych, a także powiadamianie właścicieli tych systemów o wykrytych podatnościach oraz cyberzagrożeniach, e) promowanie, przyjmowanie i stosowanie wspólnych lub znormalizowanych praktyk, systemów klasyfikacji i systematyki związanych z: – procedurami obsługi incydentu, – zarządzaniem kryzysowym w obszarze cyberbezpieczeństwa, – ujawnianiem podatności.	
N.3	udział w procesie wzajemnej oceny państw członkowskich, o którym mowa w art. 19 dyrektywy NIS 2, jako ekspertów ds. cyberbezpieczeństwa (tu mogą być koszty delegacji, analiz, sprawozdań, itp.)	art. 26 ust. 12 nowelizacji
N.4	pełnienie funkcji koordynatora na potrzeby skoordynowanego ujawniania podatności	art. 26a ust. 1 nowelizacji
N.5	współpraca z Prezesem Urzędu Lotnictwa Cywilnego, Prezesem Urzędu Komunikacji Elektronicznej oraz Komisją Nadzoru Finansowego	art. 34 ust. 3 nowelizacji
N.6	dokonywanie ocen bezpieczeństwa systemów informacyjnych wykorzystywanych przez podmioty krajowego systemu cyberbezpieczeństwa	Rozdział 6 – Ocena bezpieczeństwa – art. 36a–36d nowelizacji
N.7	wykonywanie ocen bezpieczeństwa w stosunku do podmiotów kluczowych na podstawie szacowania ryzyka na zlecenie organu właściwego do spraw cyberbezpieczeństwa	art. 53 ust. 2 pkt 3 nowelizacji
N.8	pozyskiwanie oraz analizowanie danych na potrzeby zasilania usługi online polegającej na możliwości sprawdzenia przez użytkownika czy jego dane zostały upublicznione w sieci internet w sposób nieuprawniony.	art. 26c nowelizacji
N.9	na wniosek Przewodniczącego Kolegium przeprowadzanie analiz dotyczących wpływu konkretnych produktów ICT, usług ICT lub procesów ICT na bezpieczeństwo usług świadczonych	art. 65a nowelizacji

Tabela poniżej przedstawia opis/zakres działań w odniesieniu do przepisów z projektu nowelizacji. Projekt nowelizacji, oprócz nowych zadań, rozszerza również zakres zadań już realizowanych, stąd niektóre obowiązki wynikające z nowelizacji KSC zostały w całości lub częściowo przypisane do tych zadań (zadania 1 do 10). Pozostałe zadania (od 11 do 13) są zadaniami nowymi.

Lp.	Zadanie	ID zad. z nowelizacji	Opis zadania/Uwagi	Ilość planowanych etatów
1.	Prowadzenie zespołu reagowania na incydenty	N1, N2, N.8, N.9	Zadanie obejmuje ogół czynności polegających na przyjmowaniu, analizie, klasyfikacji i reagowaniu na zgłoszone incydenty. Udzielanie pomocy w obsłudze incydentów na zlecenie Pełnomocnika, Rządu do Spraw Cyberbezpieczeństwa, współpraca z krajowymi zespołami reagowania na incydenty oraz większa liczba zgłoszeń od podmiotów zobowiązanych (wynikająca z rozszerzenia zakresu podmiotów zobowiązanych do wykonywania obowiązków w ramach uKSC) zwiększy nakład pracy. Wynika z tego konieczność zwiększenia liczby etatów w zespołach zajmujących się obsługą zgłoszeń w ramach CSIRT NASK oraz potrzeba automatyzacji możliwych elementów procesu.	23 etaty
2.	Monitorowanie zagrożeń cyberbezpieczeństwa	N.1, N.8, N.9	Działanie będzie realizowane w znacznie większym stopniu niż obecnie. Celem bardziej efektywnego wykorzystania gromadzonej wiedzy i danych konieczne jest zadbanie o ich właściwą analizę i jakość danych. Zwiększenie zasobów na to zadanie pozwoli na lepsze wykorzystanie wskaźników zbieranych przez podmioty KSC (dane systemów CERT Polska, IoC itp.). Zagregowane dane mogą być istotne podczas nowego zadania „dokonywanie ocen bezpieczeństwa systemów informacyjnych wykorzystywanych przez podmioty krajowego systemu cyberbezpieczeństwa”. Dodatkowe zadania pojawią się w związku z rosnącą liczbą podmiotów kluczowych i ważnych, obowiązkiem zapewnienia wsparcia w obsłudze incydentów na zlecenie Pełnomocnika, Rządu do Spraw Cyberbezpieczeństwa np. monitorowanie zagrożeń cyberbezpieczeństwa dla udzielenia wsparcia osobom będącym w zasięgu zainteresowań aktywnie działających grup APT.	21 etatów
3.	Przekazywanie inf. dot. zagrożeń podmiotom KSC	N.2	W związku ze zwiększającą się liczbą podmiotów kluczowych i ważnych większe będzie zapotrzebowanie na etaty osób z kompetencjami technicznymi, odpowiedzialnych za ostrzeganie użytkowników o zagrożeniach. Dodatkowo	2 etaty

Lp.	Zadanie	ID zad. z nowelizacji	Opis zadania/Uwagi	Ilość planowanych etatów
			zacieśniona współpraca z sektorowymi i międzysektorowymi społecznościami podmiotów kluczowych i podmiotów ważnych będzie powodować zwiększenie częstotliwości przekazywanie informacji dotyczących zagrożeń podmiotom KSC.	
4.	Wydawanie komunikatów o zidentyfikowanych zagrożeniach	N.1 N.2, N.8, N.9	Komunikacja zewnętrzna dotycząca zagrożeń odbywa się wieloma kanałami. W bieżącej pracy operacyjnej najskuteczniejszym kanałem komunikacji są media społecznościowe. Stosowne komunikaty opracowywane są przez ekspertów Zespołu Analiz Bieżących Zagrożeń oraz Zespół Obsługi Podatności i Poszukiwania Zagrożeń we współpracy ze specjalistami odpowiedzialnymi za popularyzację (recenzja pod kątem językowym i poziomem „trudności” przekazu dla wybranej grupy odbiorców). Konieczność wydawania komunikatów może wynikać ze zlecenia Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa lub współpracy z sektorowymi i międzysektorowymi społecznościami podmiotów kluczowych i ważnych.	5 etatów
5.	Współpraca z OW, SZC, CSIRTs, podmiotami kluczowymi i ważnymi oraz innymi z KSC	N.2, N.5	Poszerza się katalog podmiotów, które będą uznane za kluczowe albo ważne, więc konieczne będzie utrzymanie aktywnej współpracy z całą grupą podmiotów w celu utrzymania wysokiej świadomości i bezpieczeństwa. Dodatkowo ważne jest uwzględnienie wsparcia specjalistów merytorycznych, którzy będą mogli tworzyć ostrzeżenia, prezentacje edukacyjne czy wypełniać inne tego typu zapotrzebowanie. Taką rolę w większym niż do tej pory stopniu będzie spełniał m.in. Program Partnerstwo dla Cyberbezpieczeństwa, który wspiera efektywną komunikację z podmiotami KSC.	6 etatów
6.	Prowadzenie zaawansowanych analiz szkodliwego oprogramowania i podatności	N.1	Zaawansowana analiza oprogramowania i poszukiwanie podatności są realizowane zarówno w procesie obsługi incydentów, kiedy oczekiwana jest szybka analiza i rekomendacje, jak i w trybie projektowym, kiedy urządzenia lub oprogramowanie poddawane są kompleksowej systematycznej analizie w celu poszukiwania podatności, które mogłyby spowodować istotne zagrożenie w przypadku użycia danego rozwiązania. Dodatkowe zadania wymagają zwiększenia ilości etatów w celu możliwości zapewnienia ich realizacji, zwłaszcza ze względu na bardzo szerokie constituency CSIRT NASK oraz rosnącą liczbę podmiotów, które będą	15 etatów

Lp.	Zadanie	ID zad. z nowelizacji	Opis zadania/Uwagi	Ilość planowanych etatów
			uznane ze kluczowe albo ważne.	
7.	Współpraca międzynarodowa	N.2, N.3	Realizacja zadania ma na celu rozwinięcie relacji międzynarodowych dla lepszej współpracy zarówno na poziomie techniczno-operacyjnym, jak i strategicznym. Efektem tych działań jest, z jednej strony, wzmocnienie istniejących kanałów wymiany informacji technicznych, a z drugiej wykorzystanie i udostępnianie materiałów budujących świadomość, tak aby dzielić się i korzystać z dorobku i doświadczeń innych państw.	5 etatów
8.	Współpraca z organami ścigania i wymiary sprawiedliwości	N.1, N.2, N.6, N.9	Działania w ramach tego zadania mają na celu częstsze i szersze zakresowo wsparcie organów ścigania, wymiaru sprawiedliwości i służb specjalnych w realizacji ich ustawowych obowiązków. Wsparcie to udzielane jest zarówno na etapie operacyjno-rozpoznawczym, jak i procesowym. Współpraca z organami ścigania jest stałym elementem obsługi incydentów, zwłaszcza typu ransomware. Nowe obowiązki wynikające z konieczności wspierania podmiotów KSC w obsłudze incydentów czy dokonywania ocen bezpieczeństwa systemów informacyjnych wykorzystywanych przez podmioty krajowego systemu cyberbezpieczeństwa będą wymagały również utrzymania aktywnej współpracy z organami ścigania i wymiarem sprawiedliwości.	2 etaty
9.	Testy aktywne	N.1, N.6	Realizacja zadania polega na aktywnej analizie bezpieczeństwa poszczególnych sektorów oraz dokonywanie ocen bezpieczeństwa systemów informacyjnych wykorzystywanych przez podmioty krajowego systemu cyberbezpieczeństwa. Analizie poddawane mogą być różnego rodzaju usługi IT udostępniane przez podmioty danego sektora, począwszy od stron informacyjnych, poprzez udostępniane publicznie usługi web lub API po interfejsy urządzeń przemysłowych. Działania te przeprowadzane są w systemie projektowym, a każdy projekt kończy się raportem i, jeśli jest to uzasadnione, zestawem rekomendacji dla danego sektora/podsektora. Zadanie należy do kluczowych zarówno w kontekście zapewnienia wsparcia w obsłudze incydentów na zlecenie Pełnomocnika, jak i dokonywania ocen bezpieczeństwa systemów informacyjnych wykorzystywanych przez podmioty krajowego systemu cyberbezpieczeństwa.	12 etatów

Lp.	Zadanie	ID zad. z nowelizacji	Opis zadania/Uwagi	Ilość planowanych etatów
10.	Utrzymanie systemów i ciągłości funkcjonowania	N.2, N.6	Realizacja zadania ma na celu wzmocnienie procesu utrzymania i rozwoju systemów CSIRT używanych przez wszystkie linie wsparcia, w tym wzmocnienie zarządzania procesem ciągłości działania (BCM). Wymaga to zaangażowania nowych zasobów.	4 etaty
11.	Identyfikowanie podatności systemów dostępnych w otwartych sieciach teleinformatycznych, a także powiadamianie właścicieli tych systemów o wykrytych podatnościach oraz cyberzagrożeniach	N.1, N.2, N.6, N.9	Zadanie nowe Zadanie obejmuje działania polegające na wykonywaniu ocen bezpieczeństwa w stosunku do podmiotów kluczowych, dokonywanie ocen bezpieczeństwa systemów informacyjnych wykorzystywanych przez podmioty krajowego systemu cyberbezpieczeństwa oraz prowadzenie i zarządzanie, procesem komunikacji z podmiotami. Ze względu na konieczność cyklicznego skanowania kilkudziesięciu tysięcy podmiotów w ramach constituency CSIRT NASK konieczne jest zwiększenie zasobów osobowych dedykowanych do rozwoju i obsługi stosownych narzędzi oraz procesu komunikacji.	9 etatów
12.	Pełnienie funkcji koordynatora na potrzeby skoordynowanego ujawniania podatności	N.4	Zadanie nowe Zadanie polegające na pełnieniu funkcji koordynatora na potrzeby skoordynowanego ujawniania podatności. W ramach wypełnienia tego obowiązku, konieczne będzie techniczne weryfikowanie zgłaszanych podatności oraz komunikacja i ewentualne mediacje między zgłaszającym a podmiotem (producentem), którego produktu dotyczy podatność. Wraz z rosnącą skalą zgłoszeń konieczne będzie rozwijanie narzędzi, które usprawnią proces obsługi zgłoszeń podatności oraz rozbudowa i podniesienie poziomu roli takiej jak CNA.	8 etatów
13.	Wykonywanie ocen bezpieczeństwa w stosunku do podmiotów kluczowych na podstawie szacowania ryzyka na zlecenie	N.7	Zadanie nowe Zadanie polegające na wykonywaniu ocen bezpieczeństwa w stosunku do podmiotów kluczowych na podstawie szacowania ryzyka na zlecenie organu właściwego do spraw cyberbezpieczeństwa. Zależnie od sytuacji może to m.in. polegać na technicznym badaniu i ocenie infrastruktury podmiotu jak również na ocenie istniejących procedur reagowania na incydenty.	2 etaty

Lp.	Zadanie	ID zad. z nowelizacji	Opis zadania/Uwagi	Ilość planowanych etatów
	organu właściwego do spraw cyberbezpieczeństwa			

3.3. Analityka kosztowa

Estymację kosztów na lata 2025–2035 w podziale na poszczególne rodzaje kosztów przedstawia tabela poniżej. W pozycji *Koszty inne* uwzględniono inne wydatki niezbędne do realizacji zadań nie ujęte w pozostałych pozycjach w szczególności koszty organizacji wydarzeń.

Rodzaj kosztu	2025	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035
Koszty osobowe	0	27 907 200,00	32 372 352,00	37 551 928,32	43 560 236,85	50 529 874,75	58 614 654,71	67 992 999,46	78 871 879,37	91 491 380,07	106 130 000,89
Delegacje	0	984 000,00	1 141 440,00	1 324 070,40	1 535 921,66	1 781 669,13	2 066 736,19	2 397 413,98	2 781 000,22	3 225 960,25	3 742 113,89
Usługi, koszty pośrednie, materiały i wydatki nisko cenne	0	492 000,00	570 720,00	662 035,20	767 960,83	890 834,57	1 033 368,10	1 198 706,99	1 390 500,11	1 612 980,13	1 871 056,95
Szkolenia personelu	0	9 802 050,00	11 370 378,00	13 189 638,48	15 299 980,64	17 747 977,54	20 587 653,94	23 881 678,58	27 702 747,15	32 135 186,69	37 276 816,56
RAZEM	0	39 185 250,00	45 454 890,00	52 727 672,40	61 164 099,98	70 950 355,98	82 302 412,94	95 470 799,01	110 746 126,85	128 465 507,15	149 019 988,29

Do celów wyliczenia kosztów osobowych przyjęto wartość średniej pensji na poziomie 20 400 złotych miesięcznie brutto przy szacowanej ilości etatów na poziomie 114 dla roku bazowego (2025). Należy zaznaczyć, że dotacja podmiotowa nie pokrywa kosztów inwestycyjnych powyżej

10 tys. zł kosztu jednostkowego. Oznacza to, że inwestycje infrastrukturalne, a także wydatki na systemy czy narzędzia, przekraczające 10 tys. zł kosztu jednostkowego, wymagają finansowania z projektów celowych lub dofinansowania unijnego.

3.4. Realizacja zadań nadzorczych na zlecenie Ministra właściwego ds. informatyzacji

Zgodnie z art. 41a ust. 5 nowelizacji KSC minister właściwy do spraw informatyzacji może powierzyć realizację zadań nadzorczych nad podmiotami kluczowymi w sektorze administracji publicznej CSIRT NASK, ale środki na te czynności muszą się znaleźć w dotacji podmiotowej.

Z założeń zawartych w dokumencie z OSR nowelizacji KSC liczba podmiotów kluczowych i podmiotów ważnych z sektora administracji publicznej to 27905. Założenia sugerują prowadzenie kontroli w około 10% podmiotów rocznie, każda kontrola powinna być prowadzona przez zespół 3 osób, które mogą przeprowadzić 6 kontroli rocznie. Wynika z tego, że do wypełnienia założenia kontroli w 2790 podmiotach konieczne byłoby zatrudnienie 465 zespołów po trzy osoby, co przekłada się na 1395 etatów. Jednocześnie w założeniach wpisano, że maksymalna liczba etatów nadzorujących sektor to 40.

W związku z powyższym przyjęto założenie, że NASK-PIB zapewni 40 etatów, w ramach których będzie realizował powierzone zadania nadzorcze. Tabela poniżej przedstawia estymacje kosztów dla 40 etatów. Na potrzeby wyliczenia kosztów dla roku bazowego (2025) przyjęto następujące założenia:

1. Stawka miesięcznego wynagrodzenia – 20 400 zł.
2. Dzienna stawka delegacyjna – 500 zł.
3. Liczba dni delegacyjnych w skali miesiąca dla jednego etatu – 15.
4. Roczna kwota przeznaczona na szkolenia w ramach jednego etatu – 3 600 zł.
5. Inflacja rok do roku – 6%.

Rodzaj kosztu	Rok										
	2025	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035
Koszty osobowe	0 9 792 000,00	10 379 520,00	11 002 291,20	11 662 428,67	12 362 174,39	13 103 904,86	13 890 139,15	14 723 547,50	15 606 960,35	16 543 377,97	
Delegacje	0 3 600 000,00	3 816 000,00	4 044 960,00	4 287 657,60	4 544 917,06	4 817 612,08	5 106 668,80	5 413 068,93	5 737 853,07	6 082 124,25	
Szkolenia	0 144 000,00	167 040,00	193 766,40	224 769,02	260 732,07	302 449,20	350 841,07	406 975,64	472 091,74	547 626,42	
Razem	0 13 536 000,00	14 362 560,00	15 241 017,60	16 174 855,30	17 167 823,52	18 223 966,13	19 347 649,02	20 543 592,07	21 816 905,16	23 173 128,64	

Koszty projektu [Bezpiecznedane.gov.pl](https://bezpiecznedane.gov.pl)

W ramach dotacji podmiotowej przewiduje się sfinansowanie projektu <https://bezpiecznedane.gov.pl/>.

Rodzaj kosztu	Od 2026
Bezpieczne dane – Wynagrodzenia osobowe	1 696 962
Bezpieczne dane – Usługi obce	129 900
Bezpieczne dane – Licencje/oprogramowanie	104 000
Bezpieczne dane – Razem koszty	1 930 862
Bezpieczne dane - Koszty pośrednie	482 716
SUMA	4 344 440,09 zł

4. Estymacja dla projektu S46

4.1. Utrzymanie i rozwój systemu S46

4.1.1. Wprowadzenie

System S46, dalej określany również jako „S46”, jest systemem teleinformatycznym, o którym mowa w art. 46 KSC. System został uruchomiony zgodnie ze wskazanym terminem ustawowym w dniu 1 stycznia 2021 r. Realizacja S64 bazowała na dorobku projektów NPC i NPCNet, które były dofinansowane przez NCBiR. Dostosowanie produktów ww. projektów, do przepisów KSC, zostało zrealizowane przez NASK-PIB w wyniku realizacji zadania publicznego „Rozwój systemu teleinformatycznego S46”.

W kolejnych latach NASK-PIB realizował zadania publiczne, których celem było utrzymanie i rozwój systemu teleinformatycznego S46. W obszarze utrzymania finansowane były elementy takie jak obsługa administratorska, linie wsparcia, korekty błędów oraz niezbędne do działania systemu zakupy. Obszar rozwoju obejmował ulepszanie funkcjonalności systemu, niezbędną rozbudowę infrastruktury oraz podłączanie nowych użytkowników. Zwiększenie skali połączeń instytucji do systemu S46 zostało również osiągnięte przy wykorzystaniu środków z Unii Europejskiej finansowanego z inicjatywy REACT-EU. Środki pozyskane z Unii Europejskiej pozwoliły również na zwiększenie odporności S46 na katastrofy.

Ze względu na wzrastającą rolę systemu S46, wynikającą w nowelizacji ustawy o KSC, konieczne jest zapewnienie dalszego finansowania zarówno w obszarze utrzymania, jak i rozwoju systemu S46.

4.1.2. Streszczenie managerskie

Aktualnie obowiązująca KSC przewiduje w ramach OSR kwoty na utrzymanie i rozwój systemu o którym jest mowa w art. 46 KSC.

Analiza wykazała, że do rozwoju i utrzymania systemu jest konieczne przeznaczenie większych środków od tych, które zostały uwzględnione w ramach OSR dla KSC.

Poniższa tabela ilustruje potrzeby w zakresie zwiększania kwot na utrzymanie i rozwój systemu S46.

rok	Bieżące	majątkowe	Suma	OSR2018	zwiększenie kosztów
2025	0 zł	0 zł	0 zł	9 500 000,00 zł	0 zł
2026	22 624 317,00 zł	12 214 576,50 zł	34 838 893,50 zł	9 500 000,00 zł	25 338 893,50 zł
2027	25 660 615,68 zł	2 344 995,00 zł	28 005 610,68 zł	9 500 000,00 zł	18 505 610,68 zł
2028	22 436 552,14 zł	6 571 680,90 zł	29 008 233,04 zł	9 500 000,00 zł	19 508 233,04 zł
2029	30 246 145,93 zł	8 893 638,00 zł	39 139 783,93 zł	9 500 000,00 zł	29 639 783,93 zł
2030	32 063 937,62 zł	18 450 000,00 zł	50 513 937,62 zł	9 500 000,00 zł	41 013 937,62 zł

2031	37 095 769,70 zł	27 749 230,50 zł	64 845 000,20 zł	9 500 000,00 zł	55 345 000,20 zł
2032	44 076 677,03 zł	1 815 480,00 zł	45 892 157,03 zł		45 892 157,03 zł
2033	49 566 936,42 zł	7 876 932,30 zł	57 443 868,72 zł		57 443 868,72 zł
2034	59 889 994,58 zł	12 874 410,00 zł	72 764 404,58 zł		72 764 404,58 zł
2035	68 007 369,59 zł	27 675 000,00 zł	95 682 369,59 zł		95 682 369,59 zł

Tabela 1 Potrzeby w zakresie finansowania utrzymania i rozwoju S46

Zwiększenie nakładów na utrzymanie i rozwój S46 jest związane z czynnikami wymienionymi poniżej:

1. W szacunkach do OSR KSC z 2018 r., uwzględniono koszty wynikające z sukcesywnego podłączania podmiotów krajowego systemu cyberbezpieczeństwa. Założono dynamikę połączeń na poziomie około stu uczestników rocznie. Nowelizacja KSC w znaczący sposób zwiększa liczbę podmiotów, które będą korzystać z systemu S46, aż do poziomu ponad 10 tysięcy. Zwiększona o dwa rzędy wielkości liczba uczestników przekłada się na koszty obsługi systemu, zarówno jeśli chodzi o wsparcie oferowane przez poszczególne linie wsparcia, jak również w zakresie wsparcia merytorycznego. Brak zwiększenia środków wygeneruje problemy z wykorzystaniem systemu, który w projekcie nowelizacji jest systemem obowiązkowym.
2. Projektowana nowelizacja KSC przewiduje uruchomienie rejestru podmiotów krajowego systemu cyberbezpieczeństwa zapewniającego podmiotom mechanizm samorejestracji za pośrednictwem sieci internet i mechanizmów węzła krajowego. Uruchomienie bezpiecznego mechanizmu samorejestracji, oraz wsparcie podmiotów podłączanych do S46, wymaga nakładów w stosunku do planowanych w OSR z 2018
3. W zestawie założeń przyjętych w OSR KSC z 2018 r. założono dostęp do S46 dla kilkuset podmiotów poprzez sieć wydzieloną. Powodowało to konieczność finansowania urządzenia końcowego dedykowanego dla danego partnera. Takie podejście nie jest możliwe do dalszego stosowania przy konieczności obsługi kilkudziesięciu tysięcy podmiotów. W związku z tym została podjęta decyzja o uruchomieniu dostępu do S46 w trybie SaaS. Jedynie w przypadku szczególnie istotnych podmiotów (CSiRTy, OW itp.) oraz już podłączonych jednostek, pozostawiony zostanie dostęp przez sieć wydzieloną. Dzięki takiemu podejściu, nie będzie konieczne zapewnienie dodatkowych urządzeń końcowych użytkownikom S46. Konieczne jest natomiast utrzymanie i zapewnienie wsparcia dla aktualnie użytkowanych końcówek.
4. W trakcie realizacji zadań związanych z utrzymaniem, okazało się konieczne powołanie zespołu analitycznego zdolnego do zauważania zależności, analizowania spójności modeli i ryzyk itp. W założeniach do KSC z 2018 r. funkcje takie nie były znane i przewidywane, a zatem nie mogły być też wycenione. Należy wziąć pod uwagę również zatrudnienie specjalistów specjalizujących się w nowych technologiach, takich jak AI. Podniesienie nakładów umożliwi organizację zespołu analitycznego, który będzie mógł realizować analizy wspomagając działanie wszystkich CSRIT-ów.

5. Doświadczenia dotyczące utrzymania i rozwoju systemu wskazują, że konieczne jest zapewnienie ciągłego doskonalenia funkcjonalności S46. Planowany wzrost liczby użytkowników powoduje, że konieczne staje się utrzymanie stałego zespołu deweloperskiego, dedykowanego do ciągłego doskonalenia systemu, oraz wprowadzania poprawek. Zwiększenie liczby personelu dedykowanego do rozwoju systemu S46, umożliwi obsługę zwiększającej się skali i poziomu złożoności systemu. Brak dodatkowych nakładów w obszarze zespołów rozwojowych mógłby spowodować drastyczne wydłużenie okresu wprowadzania poprawek i dostosowywania systemu do wymagań użytkowników.
6. Doświadczenia z eksploatacji systemu S46 wskazują, że należy przewidzieć intensywny rozwój w zakresie technologii do analizy danych. Przewidując zapotrzebowanie w tym zakresie, zaplanowano w okresie 10-cio letnim wykorzystanie stosownych narzędzi, w tym narzędzi opartych o sztuczną inteligencję. Brak inwestycji w narzędzia do analizy danych może wydłużyć czas reakcji na zagrożenia w obszarze cyberbezpieczeństwa.

4.1.3. Założenia

Podczas szacowania kosztów przyjęto następujące założenia, które adresują zagadnienia opisane w ramach streszczenia managerskiego:

1. Perspektywa kalkulacji – lata 2025–2035.
2. Wysokość kosztów ogólnych od sumy kosztów bezpośrednich – 20% (z wyłączeniem usług obcych).
3. Narzut na inflację w ujęciu rocznym – 6%.
4. Współczynnik rozwoju – 10%.
5. Koszty zakupów liczono z uwzględnieniem 23% VAT.
6. Nie przewiduje się zakupu dedykowanych końcówek dla systemu S46. Uczestnicy mogą korzystać z już zakupionych urządzeń będących w dyspozycji Operatora S46, lub mogą zakupić urządzenia we własnym zakresie.
7. Koszty transmisji już podłączonych uczestników, za pomocą dedykowanych urządzeń końcowych są refundowane przez skarb państwa.

4.1.4. Metodyka kalkulacji

Podczas szacowania kosztów przyjęto założenia przedstawione w rozdziale 1.3. Szacowanie przeprowadzono osobno w rozbiciu na:

1. Koszty osobowe.
2. Koszty inwestycji.

Wyniki kalkulacji przedstawiono w podziale na lata i następujące kategorie kosztowe:

1. Sprzęt.
2. Materiały.
3. Usługi obce.
4. Wynagrodzenia.
5. Delegacje.
6. Koszty pośrednie.

Koszty osobowe

Koszty oszacowano w głównych obszarach: utrzymania i rozwoju.

W obszarze **utrzymania** rozróżniono działania związane z utrzymaniem na poziomie aplikacyjnym oraz działaniami na poziomie sieci i zasobów obliczeniowych. Ze względu na prognozowane zwiększenie liczby podmiotów korzystających z systemu, przewiduje się, że monitorowanie, reagowanie na awarie oraz rozwiązywanie zgłoszeń użytkowników będzie wymagać zwiększonego wysiłku. Ze względu na czas życia systemu konieczne będzie również zaangażowanie zespołów w zadania związane z modernizacją systemu.

W pierwszych latach, od wejścia w życie uKSC szacuje się zwiększone obciążenie związane z przyjmowaniem użytkowników do systemu, oraz związanych ze wsparciem w zakresie korzystania systemu ale przede wszystkim w zakresie operacyjnym i szkoleń.

W obszarze **rozwoju** oszacowano potrzeby związane z utrzymaniem i rozwojem aplikacji oraz utrzymaniem i rozwojem zasobów obliczeniowych. Spodziewany jest duży nacisk na dostosowywanie systemu i rozwój nowych funkcjonalności. Działania w obszarze rozwoju będą wymagać dużego zaangażowania zespołów deweloperskich i skrócenia czasu realizacji wydań, stąd konieczność zwiększenia zasobów.

Lata	2026	2027	2028	2029	2030	2031
rozwój	18	18	19	19	19	19
utrzymanie i rozwój aplikacji	12,5	12,5	18	18	18	18
utrzymanie i rozwój sieci i zasobów obliczeniowych	5,5	5,5	1	1	1	1
utrzymanie	48,23	51,45	33,63	33,63	29,63	33,63
onboarding	12,4	12,19	3,09	3,09	3,09	3,09
szkolenia	3,21	5,67	4,54	4,54	4,54	4,54
utrzymanie i rozwój aplikacji	2	2	2	2	2	2
wspólne	1	1	1,54	1,54	1,54	1,54
analizy między CSIRT	19,62	20,59	8,46	8,46	8,46	8,46
utrzymanie i rozwój sieci i zasobów obliczeniowych	10	10	14	14	10	14
Suma końcowa	66,23	69,45	52,63	52,63	48,63	52,63

Po przyjęciu szacunkowych stawek kosztów osobowych, z uwzględnieniem narzutów koszty osobowe rozkładają się w następujący sposób:

Lata	2026	2027	2028	2029	2030	2031
	19 077 120,00	23 222 736,00	19 707 011,71	24 658 285,78	28 603 612,02	33 180 192,00
	zł	zł	zł	zł	zł	zł
rozwój	5 652 000,00	6 556 320,00	8 525 721,60	9 889 837,06	11 472 210,58	13 307 765,18
	zł	zł	zł	zł	zł	zł
utrzymanie i rozwój aplikacji	4 068 000,00	4 718 880,00	8 138 188,80	9 440 299,01	10 950 746,40	12 702 866,69
utrzymanie i rozwój sieci i zasobów obliczeniowych	1 584 000,00	1 837 440,00				
	zł	zł	387 532,80 zł	449 538,05 zł	521 464,18 zł	604 898,50 zł
utrzymanie	13 425 120,00	16 666 416,00	11 181 290,11	14 768 448,72	17 131 401,44	19 872 426,82
	zł	zł	zł	zł	zł	zł
analizy między CSIRT	5 650 560,00	6 878 707,20	3 278 527,49	3 803 091,89	4 411 586,93	5 117 441,28
	zł	zł	zł	zł	zł	zł
adaptacja pracowników	3 250 080,00	3 717 475,20	1 089 936,00	1 264 325,76	1 466 617,96	1 701 276,86
	zł	zł	zł	zł	zł	zł
szkolenia		1 894 233,60	1 759 398,91	2 040 902,74	2 367 447,36	2 746 239,17
	924 480,00 zł	zł	zł	zł	zł	zł
utrzymanie i rozwój aplikacji				1 123 845,12	1 303 660,22	1 512 245,95
	720 000,00 zł	835 200,00 zł	968 832,00 zł	zł	zł	zł
utrzymanie i rozwój sieci i zasobów obliczeniowych	2 592 000,00	3 006 720,00	3 487 795,20	5 843 994,62	6 779 034,14	7 863 679,87
	zł	zł	zł	zł	zł	zł
wspólne	288 000,00 zł	334 080,00 zł	596 800,51 zł	692 288,59 zł	803 054,83 zł	931 543,68 zł
	zł	zł	zł	zł	zł	zł
Suma końcowa	19 077 120,00	23 222 736,00	19 707 011,71	24 658 285,78	28 603 612,02	33 180 192,00
	zł	zł	zł	zł	zł	zł

Oraz w kolejnych latach:

Lata	2032	2033	2034	2035
o	38 489 021,38 zł	44 647 266,24 zł	51 790 827,17 zł	60 077 360,68 zł
rozwój	15 437 007,79 zł	17 906 929,92 zł	20 772 038,30 zł	24 095 564,50 zł
utrzymanie i rozwój aplikacji	14 735 325,60 zł	17 092 978,56 zł	19 827 854,78 zł	23 000 311,58 zł

utrzymanie i rozwój sieci i zasobów obliczeniowych	701 682,19 zł	813 951,36 zł	944 183,52 zł	1 095 252,91 zł
utrzymanie	23 052 013,59 zł	26 740 336,32 zł	31 018 788,87 zł	35 981 796,18 zł
analizy między CSIRT	5 936 231,34 zł	6 886 028,51 zł	7 987 792,58 zł	9 265 839,64 zł
adaptacja pracowników	1 973 481,05 zł	2 289 238,04 zł	2 655 516,07 zł	3 080 398,78 zł
szkolenia	3 185 637,15 zł	3 695 339,17 zł	4 286 593,18 zł	4 972 448,22 zł
utrzymanie i rozwój aplikacji	1 754 205,41 zł	2 034 878,40 zł	2 360 458,94 zł	2 738 132,35 zł
utrzymanie i rozwój sieci i zasobów obliczeniowych	9 121 868,06 zł	10 581 367,10 zł	12 274 385,47 zł	14 238 287,71 zł
wspólne	1 080 590,58 zł	1 253 485,09 zł	1 454 042,62 zł	1 686 689,48 zł
Suma końcowa	38 489 021,38 zł	44 647 266,24 zł	51 790 827,17 zł	60 077 360,68 zł

Należy również zauważyć, iż założono że w latach, w których przewidziano finansowanie zgodne z OSR do uKSC (do roku 2030), odpowiednia część z oszacowanych wydatków będzie uwzględniona w kwotach aktualnie wpisanych do OSR projektu nowelizacji KSC. Zestawienie rozbitcia poszczególnych kosztów na koszty majątkowe i bieżące, z uwzględnieniem poszczególnych kwot, zostały wskazane w rozdziale „koszty całościowe”.

Koszty całościowe

Podczas szacowania kosztów utrzymania rozwoju i działania systemu S46 oprócz kosztów osobowych, uwzględniono również koszty inwestycyjne ponoszone w związku z zakupem sprzętu oraz oprogramowania, koszty usług obcych, materiałów i przedmiotów niskocennych oraz delegacji. Koszty te są ponoszone zarówno w związku z rozbudową, modernizacją jak i utrzymaniem infrastruktury, aplikacji i zdolności analitycznych.

Podsumowanie kosztów w poszczególnych kategoriach z podziałem na koszty inwestycyjne i koszty bieżące przedstawia poniższa tabela:

Lata	2026	2027	2028	2029	2030	2031
Bieżące	22 624 317,00 zł	25 660 615,68 zł	22 436 552,14 zł	30 246 145,93 zł	32 063 937,62 zł	37 095 769,70 zł
Rozwój	5 652 000,00 zł	6 556 320,00 zł	8 525 721,60 zł	9 889 837,06 zł	11 472 210,58 zł	13 307 765,18 zł
Osobowe	5 652 000,00 zł	6 556 320,00 zł	8 525 721,60 zł	9 889 837,06 zł	11 472 210,58 zł	13 307 765,18 zł
Utrzymanie	16 972 317,00 zł	19 104 295,68 zł	13 910 830,54 zł	20 356 308,87 zł	20 591 727,04 zł	23 788 004,51 zł
Delegacje	71 340,00 zł	82 754,40 zł	95 995,10 zł	111 354,32 zł	129 171,01 zł	149 838,37 zł
Materiały	170 970,00 zł	162 655,20 zł	188 680,03 zł	813 297,09 zł	253 887,85 zł	294 509,91 zł
Osobowe	13 425 120,00 zł	16 666 416,00 zł	11 181 290,11 zł	14 768 448,72 zł	17 131 401,44 zł	19 872 426,82 zł
Usługi obce	3 304 887,00 zł	2 192 470,08 zł	2 444 865,29 zł	4 663 208,74 zł	3 077 266,74 zł	3 471 229,42 zł
Inwestycje	12 214 576,50 zł	2 344 995,00 zł	6 571 680,90 zł	8 893 638,00 zł	18 450 000,00 zł	27 749 230,50 zł

Rozwój					18 450 000,00 zł	
Sprzęt					18 450 000,00 zł	
Utrzymanie	12 214 576,50 zł	2 344 995,00 zł	6 571 680,90 zł	8 893 638,00 zł	0,00 zł	27 749 230,50 zł
Sprzęt	10 787 776,50 zł	2 344 995,00 zł	6 571 680,90 zł	8 893 638,00 zł	0,00 zł	25 609 030,50 zł
Oprogramowanie	1 426 800,00 zł		0,00 zł	0,00 zł	0,00 zł	2 140 200,00 zł
Suma końcowa	34 838 893,50 zł	28 005 610,68 zł	29 008 233,04 zł	39 139 783,93 zł	50 513 937,62 zł	64 845 000,20 zł

W kolejnych latach koszty rozkładają się następująco:

Lata	2032	2033	2034	2035
Bieżące	44 076 677,03 zł	49 566 936,42 zł	59 889 994,58 zł	68 007 369,59 zł
Rozwój	15 437 007,79 zł	17 906 929,92 zł	20 772 038,30 zł	24 095 564,50 zł
Osobowe	15 437 007,79 zł	17 906 929,92 zł	20 772 038,30 zł	24 095 564,50 zł
Utrzymanie	28 639 669,23 zł	31 660 006,50 zł	39 117 956,27 zł	43 911 805,09 zł
Delegacje	173 812,51 zł	201 622,52 zł	233 882,12 zł	271 303,26 zł
Materiały	396 106,99 zł	259 705,36 zł	1 131 508,22 zł	421 966,42 zł
Osobowe	23 052 013,59 zł	26 740 336,32 zł	31 018 788,87 zł	35 981 796,18 zł
Usługi obce	5 017 736,14 zł	4 458 342,30 zł	6 733 777,07 zł	7 236 739,23 zł
Inwestycje	1 815 480,00 zł	7 876 932,30 zł	12 874 410,00 zł	27 675 000,00 zł
Rozwój				27 675 000,00 zł
Sprzęt				27 675 000,00 zł
Utrzymanie	1 815 480,00 zł	7 876 932,30 zł	12 874 410,00 zł	0,00 zł
Sprzęt	1 815 480,00 zł	7 876 932,30 zł	12 874 410,00 zł	0,00 zł
Oprogramowanie	0,00 zł	0,00 zł	0,00 zł	0,00 zł
Suma końcowa	45 892 157,03 zł	57 443 868,72 zł	72 764 404,58 zł	95 682 369,59 zł

Koszty inwestycyjne w obszarze utrzymania są związane z wymianą aktualnie użytkowanej infrastruktury. Usługi obce w tym obszarze obejmują przedłużanie subskrypcji na oprogramowanie, opłaty za kolokację i łączność, opłaty serwisowe oraz opłaty za usługi chmurowe. W przypadku rozwoju planuje się poniesienie kosztów związanych z uruchomieniem części niejawnej S46.

Należy zwrócić uwagę, że koszty wdrożenia nowych usług w ramach nowelizacji uKSC w latach 2025–2026 roku ponoszone będą w dużej części z dofinansowaniem z funduszy Krajowego Planu Odbudowy i Rozwoju, w ramach projektu S46-KPO. Te wydatki rozwojowe są ujęte w przedstawionych tu kalkulacjach w latach 2025 i 2026.

Ich podsumowanie wygląda następująco (wydatki poniższe są częścią wydatków przedstawionych wyżej):

Lata	KPO
	23 375 236,19
2025	zł
2026	8 223 208,10 zł

nr części budżetowej	nazwa części budżetowej	nazwa zadania	0	1	2	3	4	5	6	7	8	9	10	suma
20	gospodarka	Działalność edukacyjna skierowana do podmiotów gospodarczych		1 000 000	1 000 000	1 000 000	1 000 000	1 000 000	1 000 000	1 000 000	1 000 000	1 000 000	1 000 000	10 000 000
20	gospodarka	Wynagrodzenie roczne dla pracowników nadzorujących sektor produkcji i przestrzeni kosmicznej		1 514 039	1 620 173	1 733 747	1 855 283	1 985 338	2 124 510	2 273 438	2 432 806	2 603 346	2 785 841	20 928 521
20	gospodarka	Dodatkowe wynagrodzenie roczne dla pracowników nadzorujących sektor produkcji i przestrzeni kosmicznej		0	128 700	137 720	147 360	157 700	168 760	180 580	193 240	206 780	221 280	1 542 120
20	gospodarka	Składka na ubezpieczenia społeczne dla pracowników nadzorujących sektor produkcji i przestrzeni kosmicznej finansowana przez pracodawcę		260 260	300 640	321 700	344 260	368 380	394 220	421 840	451 420	483 060	516 920	3 862 700
20	gospodarka	Składka na Fundusz Pracy dla pracowników nadzorujących sektor produkcji i przestrzeni kosmicznej		15 140	17 480	18 720	20 020	21 440	22 940	24 540	26 260	28 100	30 080	224 720
20	gospodarka	Składka na Fundusz Solidarnościowy dla pracowników nadzorujących sektor produkcji i przestrzeni kosmicznej		21 960	25 360	27 140	29 040	31 080	33 260	35 580	38 080	40 740	43 600	325 840
20	gospodarka	Składka na PPK dla pracowników nadzorujących sektor produkcji i przestrzeni kosmicznej		22 720	26 240	28 080	30 040	32 140	34 400	36 820	39 400	42 160	45 100	337 100
20	gospodarka	Wynagrodzenie dla pracowników nadzorujących sektor produkcji chemikaliów		454 212	486 052	520 124	556 585	595 601	637 353	682 032	729 842	781 004	835 752	6 278 556
20	gospodarka	Dodatkowe wynagrodzenie roczne dla pracowników nadzorujących sektor produkcji chemikaliów		0	38 610	41 316	44 208	47 310	50 628	54 174	57 972	62 034	66 384	462 636
20	gospodarka	Składka na ubezpieczenia społeczne dla pracowników nadzorujących sektor produkcji chemikaliów		78 078	90 192	96 510	103 278	110 514	118 266	126 552	135 426	144 918	155 076	1 158 810
20	gospodarka	Składka na Fundusz Pracy dla pracowników nadzorujących sektor produkcji chemikaliów		4 542	5 244	5 616	6 006	6 432	6 882	7 362	7 878	8 430	9 024	67 416
20	gospodarka	Składka na Fundusz Solidarnościowy dla pracowników nadzorujących sektor produkcji chemikaliów		6 588	7 608	8 142	8 712	9 324	9 978	10 674	11 424	12 222	13 080	97 752
20	gospodarka	Składka na PPK dla pracowników nadzorujących sektor produkcji chemikaliów		6 816	7 872	8 424	9 012	9 642	10 320	11 046	11 820	12 648	13 530	101 130
20	gospodarka	Koszt stanowisk pracy dla osób nadzorujących sektor produkcji chemikaliów		66 180	0	0	0	0	0	0	0	0	0	66 180
20	gospodarka	Koszty najmu powierzchni biurowej i stanowisk pracy dla osób nadzorujących sektory produkcji i przestrzeni kosmicznej		1 983 360	1 589 967	1 631 212	1 673 840	1 717 593	1 763 499	1 808 586	1 855 890	1 904 441	1 572 730	17 501 118
20	gospodarka	koszty stanowisk pracy dla osób nadzorujących sektory produkcji i przestrzeni kosmicznej		220 600	0	0	0	0	0	0	0	0	0	220 600
20	gospodarka	Koszt zakupu licencji do norm technicznych i innych dokumentów standaryzacyjnych z zakresu cyberbezpieczeństwa		7 426	8 000	8 000	8 000	8 000	8 000	8 000	8 000	8 000	8 000	79 426
		suma	0	5 661 921	5 352 138	5 586 451	5 835 644	6 100 494	6 383 016	6 681 224	6 999 458	7 337 883	7 316 397	63 254 626

nr części budżetowej	nazwa części budżetowej	nazwa zadania	0	1	2	3	4	5	6	7	8	9	10	suma
21	gospodarka morska	Wynagrodzenie roczne dla pracowników nadzorujących podsektor transportu wodnego		75 702	81 009	86 687	92 764	99 267	106 226	113 672	121 640	130 167	139 292	1 046 426
21	gospodarka morska	Dodatkowe Wynagrodzenie roczne dla pracowników nadzorujących podsektor transportu wodnego		0	6 435	6 886	7 368	7 885	8 438	9 029	9 662	10 339	11 064	77 106
21	gospodarka morska	Składka na ubezpieczenia społeczne dla pracowników nadzorujących podsektor transportu wodnego		13 013	15 032	16 085	17 213	18 419	19 711	21 092	22 571	24 153	25 846	193 135
21	gospodarka morska	Składka na Fundusz Pracy dla pracowników nadzorujących podsektor transportu wodnego		757	874	936	1 001	1 072	1 147	1 227	1 313	1 405	1 504	11 236
21	gospodarka morska	Składka na Fundusz Solidarnościowy dla pracowników nadzorujących podsektor transportu wodnego		1 098	1 268	1 357	1 452	1 554	1 663	1 779	1 904	2 037	2 180	16 292
21	gospodarka morska	Składka na PPK dla pracowników nadzorujących podsektor transportu wodnego		1 136	1 312	1 404	1 502	1 607	1 720	1 841	1 970	2 108	2 255	16 855
21	gospodarka morska	Koszt stanowisk pracy dla osób nadzorujących podsektor transportu wodnego		11 030	0	0	0	0	0	0	0	0	0	11 030
21	gospodarka morska	Koszt zakupu licencji do norm technicznych i innych dokumentów standaryzacyjnych z zakresu cyberbezpieczeństwa		7 426	8 000	8 000	8 000	8 000	8 000	8 000	8 000	8 000	8 000	79 426
		suma		110 162	113 930	121 355	129 300	137 804	146 905	156 640	167 060	178 209	190 141	1 451 506

nr części budżetowej	nazwa części budżetowej	nazwa zadania	0	1	2	3	4	5	6	7	8	9	10	suma
22	gospodarka wodna	CSIRT zaopatrzenie w wodę i jej dystrybucja i ścieki	0	5 232 473	5 750 742	6 018 364	6 301 918	6 601 931	6 919 406	7 255 482	7 611 430	7 988 503	8 388 134	68 068 382
22	gospodarka wodna	Wynagrodzenie dla pracowników nadzorujących sektor zaopatrzenie w wodę i jej dystrybucja	0	529 914	567 061	606 811	649 349	694 868	743 579	795 703	851 482	911 171	975 044	7 324 982
22	gospodarka wodna	Dodatkowe wynagrodzenie roczne dla pracowników nadzorujących sektor zaopatrzenie w wodę i jej dystrybucja	0	0	45 045	48 202	51 576	55 195	59 066	63 203	67 634	72 373	77 448	539 742

22	gospodarka wodna	Składka na ubezpieczenia społeczne dla pracowników nadzorujących sektor zaopatrzenie w wodę i jej dystrybucja	0	91 091	105 224	112 595	120 491	128 933	137 977	147 644	157 997	169 071	180 922	1 351 945
22	gospodarka wodna	Składka na Fundusz Pracy dla pracowników nadzorujących sektor zaopatrzenie w wodę i jej dystrybucja	0	5 299	6 118	6 552	7 007	7 504	8 029	8 589	9 191	9 835	10 528	78 652
22	gospodarka wodna	Składka na Fundusz Solidarnościowy dla pracowników nadzorujących sektor zaopatrzenie w wodę i jej dystrybucja	0	7 686	8 876	9 499	10 164	10 878	11 641	12 453	13 328	14 259	15 260	114 044
22	gospodarka wodna	Składka na PPK dla pracowników nadzorujących sektor zaopatrzenie w wodę i jej dystrybucja	0	7 952	9 184	9 828	10 514	11 249	12 040	12 887	13 790	14 756	15 785	117 985
22	gospodarka wodna	Koszt stanowisk pracy dla osób nadzorujących sektor zaopatrzenie w wodę	0	77 210	0	0	0	0	0	0	0	0	0	77 210
22	gospodarka wodna	Wynagrodzenie dla pracowników nadzorujących sektor ścieki	0	227 106	243 026	260 062	278 292	297 801	318 677	341 016	364 921	390 502	417 876	3 139 278
22	gospodarka wodna	Dodatkowe wynagrodzenie roczne dla pracowników nadzorujących sektor ścieków	0	0	19 305	20 658	22 104	23 655	25 314	27 087	28 986	31 017	33 192	231 318
22	gospodarka wodna	Składka na ubezpieczenia społeczne dla pracowników nadzorujących sektor ścieków	0	39 039	45 096	48 255	51 639	55 257	59 133	63 276	67 713	72 459	77 538	579 405
22	gospodarka wodna	Składka na Fundusz Pracy dla pracowników nadzorujących sektor ścieków	0	2 271	2 622	2 808	3 003	3 216	3 441	3 681	3 939	4 215	4 512	33 708
22	gospodarka wodna	Składka na Fundusz Solidarnościowy dla pracowników nadzorujących sektor ścieków	0	3 294	3 804	4 071	4 356	4 662	4 989	5 337	5 712	6 111	6 540	48 876
22	gospodarka wodna	Składka na PPK dla pracowników nadzorujących sektor ścieków	0	3 408	3 936	4 212	4 506	4 821	5 160	5 523	5 910	6 324	6 765	50 565
22	gospodarka wodna	Koszt stanowisk pracy dla osób nadzorujących sektor ścieków	0	33 090	0	0	0	0	0	0	0	0	0	33 090
22	gospodarka wodna	Koszt zakupu licencji do norm technicznych i innych dokumentów standaryzacyjnych z zakresu cyberbezpieczeństwa	0	7 426	8 000	8 000	8 000	8 000	8 000	8 000	8 000	8 000	8 000	79 426
		suma	0	6 267 259	6 818 038	7 159 917	7 522 920	7 907 970	8 316 451	8 749 881	9 210 033	9 698 596	10 217 544	81 868 609

nr części budżetowej	nazwa części budżetowej	nazwa zadania	0	1	2	3	4	5	6	7	8	9	10	suma
27	informatyzacja	Wynagrodzenie dla pracowników realizujących zadania ministra właściwego do spraw informatyzacji w zakresie zarządzania kryzysowego w cyberprzestrzeni	0	302 808	324 035	346 749	371 057	397 068	424 902	454 688	486 561	520 669	557 168	4 185 704
27	informatyzacja	Dodatkowe wynagrodzenie roczne dla pracowników realizujących zadania ministra właściwego do spraw informatyzacji w zakresie zarządzania kryzysowego w cyberprzestrzeni	0	0	25 740	27 544	29 472	31 540	33 752	36 116	38 648	41 356	44 256	308 424
27	informatyzacja	Składka na ubezpieczenia społeczne dla pracowników realizujących zadania ministra właściwego do spraw informatyzacji w zakresie zarządzania kryzysowego w cyberprzestrzeni	0	52 052	60 128	64 340	68 852	73 676	78 844	84 368	90 284	96 612	103 384	772 540
27	informatyzacja	Składka na Fundusz Pracy dla pracowników realizujących zadania ministra właściwego do spraw informatyzacji w zakresie zarządzania kryzysowego w cyberprzestrzeni	0	3 028	3 496	3 744	4 004	4 288	4 588	4 908	5 252	5 620	6 016	44 944
27	informatyzacja	Składka na Fundusz Solidarnościowy dla pracowników realizujących zadania ministra właściwego do spraw informatyzacji w zakresie zarządzania kryzysowego w cyberprzestrzeni	0	4 392	5 072	5 428	5 808	6 216	6 652	7 116	7 616	8 148	8 720	65 168
27	informatyzacja	Składka na PPK dla pracowników realizujących zadania ministra właściwego do spraw informatyzacji w zakresie zarządzania kryzysowego w cyberprzestrzeni	0	4 544	5 248	5 616	6 008	6 428	6 880	7 364	7 880	8 432	9 020	67 420
27	informatyzacja	Koszt stanowisk pracy dla osób realizujących zadania ministra wł. ds. informatyzacji w zakresie zarządzania kryzysowego w cyberprzestrzeni	0	44 120	0	0	0	0	0	0	0	0	0	44 120
27	informatyzacja	wzrost dotacji podmiotowej dla CSIRT NASK	0	57 065 690	64 161 890	72 313 130	81 683 395	92 462 620	104 870 819	119 162 888	135 634 159	154 626 852	176 537 557	1 058 519 001
27	informatyzacja	Wzrost dotacji celowej dla Naukowej i Akademickiej Sieci Komputerowej- Państwowego Instytutu Badawczego na utrzymanie i rozwój systemu S46	0	25 338 894	18 505 611	19 508 233	29 639 784	41 013 938	55 345 000	45 892 157	57 443 869	72 764 405	95 682 370	461 134 259
27	informatyzacja	Badania/ekspertyzy dla Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa	0	100 000	100 000	100 000	100 000	100 000	100 000	100 000	100 000	100 000	100 000	1 000 000
27	informatyzacja	Działania edukacyjne Ministra Cyfryzacji	0	6 630 000	6 630 000	6 630 000	6 630 000	6 630 000	6 630 000	6 630 000	6 630 000	6 630 000	6 630 000	66 300 000
27	informatyzacja	Podnoszenie zdolności instytucji zapewniających cyberbezpieczeństwo	0	31 772 800	31 772 800	31 772 800	31 772 800	31 772 800	31 772 800	31 772 800	31 772 800	31 772 800	31 772 800	317 728 000
27	informatyzacja	Wynagrodzenie dla pracowników prowadzących postępowania w sprawie uznania za dostawcę wysokiego ryzyka	0	227 106	243 026	260 062	278 292	297 801	318 677	341 016	364 921	390 502	417 876	3 139 278
27	informatyzacja	Dodatkowe wynagrodzenie roczne dla pracowników prowadzących postępowania w sprawie uznania za dostawcę wysokiego ryzyka	0	0	19 305	20 658	22 104	23 655	25 314	27 087	28 986	31 017	33 192	231 318
27	informatyzacja	Składka na ubezpieczenia społeczne dla pracowników prowadzących postępowania w sprawie uznania za dostawcę wysokiego ryzyka	0	39 039	45 096	48 255	51 639	55 257	59 133	63 276	67 713	72 459	77 538	579 405

		suma	0	6 472 731	7 029 898	7 386 628	7 765 520	8 167 577	8 594 260	9 047 161	9 528 154	10 039 014	10 581 826	84 612 769
nr części budżetowej	nazwa części budżetowej	nazwa zadania	0	1	2	3	4	5	6	7	8	9	10	suma
46	zdrowie	CSIRT zdrowie, produkcja urządzeń medycznych	0	5 232 473	5 750 742	6 018 364	6 301 918	6 601 931	6 919 406	7 255 482	7 611 430	7 988 503	8 388 134	68 068 382
46	zdrowie	Wynagrodzenie dla pracowników nadzorujących sektor ochrony zdrowia	0	1 514 039	1 620 173	1 733 747	1 855 283	1 985 338	2 124 510	2 273 438	2 432 806	2 603 346	2 785 841	20 928 521
46	zdrowie	Dodatkowe wynagrodzenie roczne dla pracowników nadzorujących sektor ochrony zdrowia	0	0	128 700	137 720	147 360	157 700	168 760	180 580	193 240	206 780	221 280	1 542 120
46	zdrowie	Składka na ubezpieczenia społeczne dla pracowników nadzorujących sektor ochrony zdrowia	0	260 260	300 640	321 700	344 260	368 380	394 220	421 840	451 420	483 060	516 920	3 862 700
46	zdrowie	Składka na Fundusz Pracy dla pracowników nadzorujących sektor ochrony zdrowia	0	15 140	17 480	18 720	20 020	21 440	22 940	24 540	26 260	28 100	30 080	224 720
46	zdrowie	Składka na Fundusz Solidarnościowy dla pracowników nadzorujących sektor ochrony zdrowia	0	21 960	25 360	27 140	29 040	31 080	33 260	35 580	38 080	40 740	43 600	325 840
46	zdrowie	Składka na PPK dla pracowników nadzorujących sektor ochrony zdrowia	0	22 720	26 240	28 080	30 040	32 140	34 400	36 820	39 400	42 160	45 100	337 100
46	zdrowie	Koszt stanowisk pracy dla osób nadzorujących sektor ochrony zdrowia	0	220 600	0	0	0	0	0	0	0	0	0	220 600
46	zdrowie	Wynagrodzenie dla pracowników nadzorujących sektor produkcji urządzeń medycznych	0	151 404	162 017	173 375	185 528	198 534	212 451	227 344	243 281	260 335	278 584	2 092 852
46	zdrowie	Dodatkowe wynagrodzenie roczne dla pracowników nadzorujących sektor produkcji urządzeń medycznych	0	0	12 870	13 772	14 736	15 770	16 876	18 058	19 324	20 678	22 128	154 212
46	zdrowie	Składka na ubezpieczenia społeczne dla pracowników nadzorujących sektor produkcji urządzeń medycznych	0	26 026	30 064	32 170	34 426	36 838	39 422	42 184	45 142	48 306	51 692	386 270
46	zdrowie	Składka na Fundusz Pracy dla pracowników nadzorujących sektor produkcji urządzeń medycznych	0	1 514	1 748	1 872	2 002	2 144	2 294	2 454	2 626	2 810	3 008	22 472
46	zdrowie	Składka na Fundusz Solidarnościowy dla pracowników nadzorujących sektor produkcji urządzeń medycznych	0	2 196	2 536	2 714	2 904	3 108	3 326	3 558	3 808	4 074	4 360	32 584
46	zdrowie	Składka na PPK dla pracowników nadzorujących sektor produkcji wyrobów medycznych	0	2 272	2 624	2 808	3 004	3 214	3 440	3 682	3 940	4 216	4 510	33 710
46	zdrowie	Koszt stanowisk pracy dla osób nadzorujących sektor produkcji urządzeń medycznych	0	22 060	0	0	0	0	0	0	0	0	0	22 060
46	zdrowie	Koszt zakupu licencji do norm technicznych i innych dokumentów standaryzacyjnych z zakresu cyberbezpieczeństwa	0	7 426	8 000	8 000	8 000	8 000	8 000	8 000	8 000	8 000	8 000	79 426
		suma	0	7 500 090	8 089 194	8 520 181	8 978 521	9 465 616	9 983 305	10 533 560	11 118 757	11 741 107	12 403 236	98 333 569

nr części budżetowej	nazwa części budżetowej	nazwa zadania	0	1	2	3	4	5	6	7	8	9	10	suma
47	energia	CSIRT energia	0	5 232 473	5 750 742	6 018 364	6 301 918	6 601 931	6 919 406	7 255 482	7 611 430	7 988 503	8 388 134	68 068 382
47	energia	Wynagrodzenie dla pracowników nadzorujących sektor energii	0	757 019	810 086	866 874	927 641	992 669	1 062 255	1 136 719	1 216 403	1 301 673	1 392 920	10 464 261
47	energia	Dodatkowe wynagrodzenie roczne dla pracowników nadzorujących sektor energii	0	0	64 350	68 860	73 680	78 850	84 380	90 290	96 620	103 390	110 640	771 060
47	energia	Składka na ubezpieczenia społeczne dla pracowników nadzorujących sektor energii	0	130 130	150 320	160 850	172 130	184 190	197 110	210 920	225 710	241 530	258 460	1 931 350
47	energia	Składka na Fundusz Pracy dla pracowników nadzorujących sektor energii	0	7 570	8 740	9 360	10 010	10 720	11 470	12 270	13 130	14 050	15 040	112 360
47	energia	Składka na Fundusz Solidarnościowy dla pracowników nadzorujących sektor energii	0	10 980	12 680	13 570	14 520	15 540	16 630	17 790	19 040	20 370	21 800	162 920
47	energia	Składka na PPK dla pracowników nadzorujących sektor energia	0	11 360	13 120	14 040	15 020	16 070	17 200	18 410	19 700	21 080	22 550	168 550
47	energia	Koszt stanowisk pracy dla osób nadzorujących sektor energii	0	110 300	0	0	0	0	0	0	0	0	0	110 300
47	energia	Koszt zakupu licencji do norm technicznych i innych dokumentów standaryzacyjnych z zakresu cyberbezpieczeństwa	0	7 426	8 000	8 000	8 000	8 000	8 000	8 000	8 000	8 000	8 000	79 426
		suma	0	6 267 259	6 818 038	7 159 917	7 522 920	7 907 970	8 316 451	8 749 881	9 210 033	9 698 596	10 217 544	81 868 609

nr części budżetowej	nazwa części budżetowej	nazwa zadania	0	1	2	3	4	5	6	7	8	9	10	suma
51	klimat	CSIRT gospodarowanie odpadami	0	5 232 473	5 750 742	6 018 364	6 301 918	6 601 931	6 919 406	7 255 482	7 611 430	7 988 503	8 388 134	68 068 382
51	klimat	Wynagrodzenie dla pracowników nadzorujących sektor gospodarowania odpadami	0	529 914	567 061	606 811	649 349	694 868	743 579	795 703	851 482	911 171	975 044	7 324 982
51	klimat	Dodatkowe wynagrodzenie roczne dla pracowników nadzorujących sektor gospodarowania odpadami	0	0	45 045	48 202	51 576	55 195	59 066	63 203	67 634	72 373	77 448	539 742
51	klimat	Składka na ubezpieczenia społeczne dla pracowników nadzorujących sektor gospodarowania odpadami	0	91 091	105 224	112 595	120 491	128 933	137 977	147 644	157 997	169 071	180 922	1 351 945
51	klimat	Składka na Fundusz Pracy dla pracowników nadzorujących sektor gospodarowania odpadami	0	5 299	6 118	6 552	7 007	7 504	8 029	8 589	9 191	9 835	10 528	78 652
51	klimat	Składka na Fundusz Solidarnościowy dla pracowników nadzorujących sektor gospodarowania odpadami	0	7 686	8 876	9 499	10 164	10 878	11 641	12 453	13 328	14 259	15 260	114 044
51	klimat	Składka na PPK dla pracowników nadzorujących sektor gospodarowania odpadami	0	7 952	9 184	9 828	10 514	11 249	12 040	12 887	13 790	14 756	15 785	117 985

51	klimat	Koszt stanowisk pracy dla osób nadzorujących sektor gospodarowania odpadami	0	77 210	0	0	0	0	0	0	0	0	0	77 210
51	klimat	Koszt zakupu licencji do norm technicznych i innych dokumentów standaryzacyjnych z zakresu cyberbezpieczeństwa	0	7 426	8 000	8 000	8 000	8 000	8 000	8 000	8 000	8 000	8 000	79 426
		suma	0	5 959 051	6 500 250	6 819 851	7 159 019	7 518 558	7 899 737	8 303 961	8 732 852	9 187 968	9 671 121	77 752 368

nr części budżetowej	nazwa części budżetowej	nazwa zadania	0	1	2	3	4	5	6	7	8	9	10	suma
57	Agencja Bezpieczeństwa Wewnętrznego	Koszty prowadzenia badań produktu lub usługi ICT z art.. 33	0	3 000 000	3 000 000	3 000 000	3 000 000	3 000 000	3 000 000	3 000 000	3 000 000	3 000 000	3 000 000	30 000 000
		suma	0	3 000 000	3 000 000	3 000 000	3 000 000	3 000 000	3 000 000	3 000 000	3 000 000	3 000 000	3 000 000	30 000 000

nr części budżetowej	nazwa części budżetowej	nazwa zadania	0	1	2	3	4	5	6	7	8	9	10	suma
76	Urząd Komunikacji Elektronicznej	CSIRT komunikacja elektroniczna i poczta	0	5 232 473	5 750 742	6 018 364	6 301 918	6 601 931	6 919 406	7 255 482	7 611 430	7 988 503	8 388 134	68 068 382
76	Urząd Komunikacji Elektronicznej	Wynagrodzenie dla pracowników nadzorujących podsektor komunikacji elektronicznej	0	1 514 039	1 620 173	1 733 747	1 855 283	1 985 338	2 124 510	2 273 438	2 432 806	2 603 346	2 785 841	20 928 521
76	Urząd Komunikacji Elektronicznej	Dodatkowe wynagrodzenie roczne dla pracowników nadzorujących sektor komunikacji elektronicznej	0	0	128 700	137 720	147 360	157 700	168 760	180 580	193 240	206 780	221 280	1 542 120
76	Urząd Komunikacji Elektronicznej	Składka na ubezpieczenia społeczne dla pracowników nadzorujących sektor komunikacji elektronicznej	0	260 260	300 640	321 700	344 260	368 380	394 220	421 840	451 420	483 060	516 920	3 862 700
76	Urząd Komunikacji Elektronicznej	Składka na Fundusz Pracy dla pracowników nadzorujących sektor komunikacji elektronicznej	0	15 140	17 480	18 720	20 020	21 440	22 940	24 540	26 260	28 100	30 080	224 720
76	Urząd Komunikacji Elektronicznej	Składka na Fundusz Solidarnościowy dla pracowników nadzorujących sektor komunikacji elektronicznej	0	21 960	25 360	27 140	29 040	31 080	33 260	35 580	38 080	40 740	43 600	325 840
76	Urząd Komunikacji Elektronicznej	Składka na PPK dla pracowników nadzorujących podsektor komunikacji elektronicznej	0	22 720	26 240	28 080	30 040	32 140	34 400	36 820	39 400	42 160	45 100	337 100
76	Urząd Komunikacji Elektronicznej	Koszt stanowisk pracy dla osób nadzorujących sektor komunikacji elektronicznej	0	220 600	0	0	0	0	0	0	0	0	0	220 600
76	Urząd Komunikacji Elektronicznej	Wynagrodzenie dla pracowników nadzorujących sektor poczty	0	529 914	567 061	606 811	649 349	694 868	743 579	795 703	851 482	911 171	975 044	7 324 982
76	Urząd Komunikacji Elektronicznej	Dodatkowe wynagrodzenie roczne dla pracowników nadzorujących sektor poczty	0	0	45 045	48 202	51 576	55 195	59 066	63 203	67 634	72 373	77 448	539 742
76	Urząd Komunikacji Elektronicznej	Składka na ubezpieczenia społeczne dla pracowników nadzorujących sektor poczty	0	91 091	105 224	112 595	120 491	128 933	137 977	147 644	157 997	169 071	180 922	1 351 945
76	Urząd Komunikacji Elektronicznej	Składka na Fundusz Pracy dla pracowników nadzorujących sektor poczty	0	5 299	6 118	6 552	7 007	7 504	8 029	8 589	9 191	9 835	10 528	78 652
76	Urząd Komunikacji Elektronicznej	Składka na Fundusz Solidarnościowy dla pracowników nadzorujących sektor poczty	0	7 686	8 876	9 499	10 164	10 878	11 641	12 453	13 328	14 259	15 260	114 044
76	Urząd Komunikacji Elektronicznej	Składka na PPK dla pracowników nadzorujących sektor poczty	0	7 952	9 184	9 828	10 514	11 249	12 040	12 887	13 790	14 756	15 785	117 985
76	Urząd Komunikacji Elektronicznej	Koszt stanowisk pracy dla osób nadzorujących sektor poczty	0	77 210	0	0	0	0	0	0	0	0	0	77 210
76	Urząd Komunikacji Elektronicznej	Koszt zakupu licencji do norm technicznych i innych dokumentów standaryzacyjnych z zakresu cyberbezpieczeństwa	0	7 426	8 000	8 000	8 000	8 000	8 000	8 000	8 000	8 000	8 000	79 426
		suma	0	8 013 770	8 618 842	9 086 958	9 585 022	10 114 636	10 677 828	11 276 759	11 914 059	12 592 154	13 313 941	105 193 970

Załącznik 5 Koszty budżetu państwa związane ze zmianami w ustawie z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa w tys. zł

			2025	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035
cz. Budż.	nazwa cz. Budż.	opis zadania	0	1	2	3	4	5	6	7	8	9	10
27	informatyzacja	Wynagrodzenie dla 4 pracowników obsługujących Fundusz Cyberbezpieczeństwa	0	303	324	347	371	397	425	455	487	521	557
27	informatyzacja	Dodatkowe wynagrodzenie roczne dla 4 pracowników obsługujących Fundusz Cyberbezpieczeństwa	0	0	26	28	29	32	34	36	39	41	44
27	informatyzacja	Składka na ubezpieczenia społeczne dla 4 pracowników obsługujących Fundusz Cyberbezpieczeństwa	0	52	60	64	69	74	79	84	90	97	103
27	informatyzacja	Składka na Fundusz Pracy dla 4 pracowników obsługujących Fundusz Cyberbezpieczeństwa	0	3	3	4	4	4	5	5	5	6	6
27	informatyzacja	Składka na Fundusz Solidarnościowy dla 4 pracowników obsługujących Fundusz Cyberbezpieczeństwa	0	4	5	5	6	6	7	7	8	8	9
27	informatyzacja	Składka na PPK dla 4 pracowników obsługujących Fundusz Cyberbezpieczeństwa	0	5	5	6	6	6	7	7	8	8	9
27	informatyzacja	Koszt stanowisk pracy dla 4 pracowników obsługujących Fundusz Cyberbezpieczeństwa	0	44	0	0	0	0	0	0	0	0	0
27	informatyzacja	Wzrost dotacji z budżetu państwa dla Funduszu Cyberbezpieczeństwa	0	101 511	101 511	101 511	101 511	101 511	101 511	101 511	101 511	101 511	101 511
		SUMA	0	101 922	101 935	101 964	101 996	102 030	102 067	102 106	102 147	102 192	102 240

RAPORT Z KONSULTACJI

projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

Niniejszy raport został sporządzony na podstawie § 51 ust. 1 uchwały nr 190 Rady Ministrów z dnia 29 października 2013 r. – Regulamin pracy Rady Ministrów (M.P. z 2024 r. poz. 806 oraz z 2025 r. poz. 408). Zawiera on podsumowanie konsultacji publicznych i opiniowania ww. projektu ustawy.

1. Omówienie wyników przeprowadzonych konsultacji publicznych i opiniowania oraz informacje o okresie ich przeprowadzenia i terminie wyznaczonym do zajęcia stanowiska

Projekt został udostępniony w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji, w serwisie Rządowy Proces Legislacyjny, oraz w Biuletynie Informacji Publicznej na stronie podmiotowej Ministra Cyfryzacji.

W ramach konsultacji publicznych projekt (z terminem 30 dni na przedstawienie uwag), otrzymały następujące podmioty:

- 1) Amerykańska Izba Handlowa;
- 2) Business Centre Club;
- 3) Federacja Konsumentów;
- 4) Fundacja Bezpieczna Cyberprzestrzeń;
- 5) Fundacja ePaństwo;
- 6) Fundacja im. Stefana Batorego;
- 7) Fundacja Instytut Mikromakro;
- 8) Fundacja My Pacjenci;
- 9) Fundacja Nowoczesna Polska;
- 10) Fundacja Panoptikon;
- 11) Fundacja Projekt Polska;
- 12) Fundacja Przedsiębiorców Polskich Archiwizjoner;
- 13) Fundacja Pułaskiego;
- 14) Green Rev Institute;
- 15) Internet Society Poland Chapter;
- 16) Internet Society Poland;
- 17) ISAC-GIG;
- 18) ISAC-Kolej;
- 19) ISAC-Lotniczy;
- 20) Izba Domów Maklerskich;
- 21) Izba Gospodarcza Towarzystw Emerytalnych;
- 22) Izba Gospodarki Elektronicznej;
- 23) Konfederacja „Lewiatan”;
- 24) Krajowy Związek Banków Spółdzielczych;
- 25) Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji;
- 26) Krajowa Izba Gospodarcza;
- 27) Krajowa Izba Gospodarki Cyfrowej;
- 28) Krajowa Izba Gospodarki Morskiej;
- 29) Krajowa Izba Komunikacji Ethernetowej;
- 30) Krajowa Izba Rozliczeniowa;
- 31) Krajowa Spółdzielcza Kasa Oszczędnościowo-Kredytowej;

- 32) Naczelna Organizacja Techniczna;
- 33) Naczelna Rada Zrzeszeń Handlu i Usług;
- 34) Ogólnopolskie Porozumienie Organizacji Radioamatorskich;
- 35) Polskie Centrum Badań i Certyfikacji S.A.;
- 36) Polskie Stowarzyszenie Marketingu SMB;
- 37) Polskie Towarzystwo Informatyczne;
- 38) Polski Związek Krótkofalowców;
- 39) Polska Izba Brokerów Ubezpieczeniowych i Reasekuracyjnych;
- 40) Polska Izba Handlu;
- 41) Polska Izba Informatyki i Telekomunikacji;
- 42) Polska Izba Komunikacji Elektronicznej;
- 43) Polska Izba Producentów Urządzeń i Usług na rzecz Kolei;
- 44) Polska Izba Radiodifuzji Cyfrowej;
- 45) Polska Izba Ubezpieczeń;
- 46) Polska Organizacja Handlu i Dystrybucji;
- 47) Polska Organizacja Niebankowych Instytucji Płatności;
- 48) Polska Rada Biznesu;
- 49) Polska Wytwórnia Papierów Wartościowych;
- 50) Sektorowa Rada ds. Kompetencji – Telekomunikacja i Cyberbezpieczeństwo;
- 51) Stowarzyszenie Inżynierów Telekomunikacji;
- 52) Stowarzyszenie Polskich Brokerów Ubezpieczeniowych i Reasekuracyjnych;
- 53) Towarzystwo Gospodarcze Polskie Elektrownie;
- 54) Związek Banków Polskich;
- 55) Związek Importerów i Producentów Sprzętu Elektrycznego i Elektronicznego Branży RTV i IT – ZIPSEE „Cyfrowa Polska”;
- 56) Związek Pracodawców Branży Internetowej IAB Polska;
- 57) Związek Pracodawców Mediów Elektronicznych i Telekomunikacji Mediakom;
- 58) Związek Pracodawców Mediów Publicznych;
- 59) Związek Przemysłu Motoryzacyjnego;
- 60) Związek Telewizji Kablowych w Polsce Izba Gospodarcza.

W ramach opiniowania projekt (z terminem 30 dni na wyrażenie opinii) otrzymały następujące podmioty:

- 1) Agencja Bezpieczeństwa Wewnętrznego;
- 2) Agencja Wywiadu;
- 3) Biuro Bezpieczeństwa Narodowego;
- 4) Centralne Biuro Antykorupcyjne;
- 5) Komisja Nadzoru Finansowego;
- 6) Krajowa Rada Radiofonii i Telewizji;
- 7) Najwyższa Izba Kontroli;
- 8) Polski Komitet Normalizacyjny;
- 9) Prezes Głównego Urzędu Statystycznego;
- 10) Prezes Urzędu Komunikacji Elektronicznej;
- 11) Prezes Urzędu Ochrony Danych Osobowych;
- 12) Prezes Urzędu Ochrony Konkurencji i Konsumentów;
- 13) Prokuratura Generalna Rzeczypospolitej Polskiej;
- 14) Rada Dialogu Społecznego;
- 15) Rządowe Centrum Bezpieczeństwa;
- 16) Rzecznik Małych i Średnich Przedsiębiorców;
- 17) Rzecznik Praw Obywatelskich;
- 18) Służba Kontrwywiadu Wojskowego;

- 19) Służba Ochrony Państwa;
- 20) Służba Wywiadu Wojskowego;
- 21) Urząd Zamówień Publicznych;
- 21) Wojskowe Biuro Zarządzania Częstotliwościami.

Do projektu ustawy w ramach konsultacji publicznych uwagi zgłosiły następujące podmioty:

- 1) Akademia Górniczo Hutnicza;
- 2) Amerykańska Izba Handlowa w Polsce;
- 3) Apator S.A.;
- 4) Audytel S.A.;
- 5) Autobox Innovations sp. Z o.o. sp. J.;
- 6) Business Centre Club;
- 7) Centrum Łukasiewicz;
- 8) Audyt i Doradztwo Dominik Kisiel;
- 9) European AI Forum;
- 10) E-VAN sp. z o.o.;
- 11) Exatel S.A.;
- 12) FAIR MARKET INSTITUTE;
- 13) Federacja Konsumentów;
- 14) Federacja Przedsiębiorców Polskich;
- 15) FORYTEK & PARTNERZY;
- 16) Fundacja Bezpieczna Cyberprzestrzeń;
- 17) Fundacja Open Allies;
- 18) Fundacja OPOR;
- 19) Fundacji Rozwoju Obrotu Bezgotówkowego;
- 20) HIKVISION POLAND Sp. z o.o.;
- 21) HRO Personnel sp. z o.o.;
- 22) Huawei Polska sp. Z o.o.;
- 23) Inet group;
- 24) Instytut Kolejnictwa/ISAC Kolej;
- 25) Izba Gospodarcza Wodociągi Polskie;
- 26) Izba POLMED;
- 27) KGHM Polska Miedź;
- 28) Konfederacja Lewiatan;
- 29) Krajowa Izba Gospodarcza;
- 30) Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji;
- 31) Krajowa Izba Komunikacji Ethernetowej;
- 32) Krajowa Spółdzielcza Kasa Oszczędnościowo-Kredytowa;
- 33) Krzysztof Rożko i Wspólnicy Kancelaria Prawna;
- 34) KWKR Konieczny Wierzbicki i Partnerzy s.k.a.;
- 35) Międzynarodowe Centrum Bezpieczeństwa Chemicznego (ICCSS);
- 36) Morskiego Centrum Cyberbezpieczeństwa;
- 37) Naczelna Rada Zrzeszeń Handlu i Usług;
- 38) Ogólnopolska Federacja Przedsiębiorców i Pracodawców – Przedsiębiorcy.pl;
- 39) PERN S.A.;
- 40) PGE S.A.;
- 41) Polska Izba Gospodarki Odpadami;
- 42) Polska Izba Informatyki i Telekomunikacji;
- 43) Polska Izba Kolei;
- 44) Polska Izba Komunikacji Elektronicznej;

- 45) Polska Izba Przemysłu Chemicznego;
- 46) Polska Organizacja Handlu i Dystrybucji;
- 47) Polska Wytwórnia Papierów Wartościowych S.A.;
- 48) Polski Fundusz Rozwoju;
- 49) Polski Klaster Cyberbezpieczeństwa #CyberMadeInPoland;
- 50) Polski Związek Przemysłu Motoryzacyjnego;
- 51) Polskie Stowarzyszenie Fotowoltaiki;
- 52) Polskie Stowarzyszenie Magazynowania Energii;
- 53) Polskie Stowarzyszenie Menedżerów Logistyki i Zakupów;
- 54) Polskie Towarzystwo Informatyczne;
- 55) Polskiego Związku Pracodawców Przemysłu Farmaceutycznego – Krajowych Producentów Leków;
- 56) Polsko-Chińska Główna Izba Gospodarcza;
- 57) Porozumienie Zielonogórskie;
- 58) Pracodawcy RP;
- 59) SGS Polska Sp. z o.o.;
- 60) Skandynawska Izba Gospodarcza;
- 61) SNW sp. z o.o.;
- 62) Sobiesław Zasada Spółka Akcyjna S.K.A.;
- 63) Stowarzyszenie Absolwentów Studiów Cyberbezpieczeństwa MBA;
- 64) Stowarzyszenie Bezpieczeństwo Informacji w Telekomunikacji;
- 65) Stowarzyszenie Inżynierów Telekomunikacji;
- 66) Stowarzyszenie ISACA;
- 67) Stowarzyszenie ISSA Polska;
- 68) Stowarzyszenie Polska Izba Rozwoju Elektromobilności;
- 69) Sudecka Izba Przemysłowo-Handlowa;
- 70) Tauron Polska Energia S.A.;
- 71) TVN S.A.;
- 72) Urząd Miasta w Gliwicach;
- 73) Verita HR Polska sp. z o.o.;
- 74) XOPERO SOFTWARE S.A.;
- 75) Zakład Wodociągów i Kanalizacji sp. z o.o.;
- 76) Związek Banków Polskich;
- 77) Związek Cyfrowa Polska;
- 78) Związek Firm Biotechnologicznych;
- 79) Związek Pracodawców Branży Internetowej IAB Polska;
- 80) Związek Pracodawców i Przedsiębiorców;
- 81) Związek Pracodawców Klastry Polskie;
- 82) Związek Pracodawców Mediów Elektronicznych i Telekomunikacji Mediakom;
- 83) Związek Pracodawców Polska Miedź;
- 84) Związek Pracodawców Technologii Cyfrowych Lewiatan;
- 85) Związek Przedsiębiorców i Pracodawców;
- 86) Związek Telewizji Kablowych-Izba Gospodarcza.

A także 10 osób fizycznych.

Ponadto, w trybie opiniowania, opinie przedstawiły następujące podmioty:

- 1) Główny Urząd Nadzoru Budowlanego;
- 2) Komisja Nadzoru Finansowego;
- 3) Krajowa Rada Radiofonii i Telewizji;

- 4) Najwyższa Izba Kontroli;
- 5) Narodowy Bank Polski;
- 6) Naukowa i Akademicka Sieć Komputerowa - Państwowy Instytut Badawczy;
- 7) Polski Komitet Normalizacyjny;
- 8) Prezes Głównego Urzędu Statystycznego;
- 9) Prezes Urzędu Komunikacji Elektronicznej;
- 10) Prezes Urzędu Ochrony Danych Osobowych;
- 11) Prezes Urzędu Transportu Kolejowego;
- 12) Prezes Urzędu Zamówień Publicznych;
- 13) Rzecznik Małych i Średnich Przedsiębiorców;
- 14) Rzecznik Praw Obywatelskich;
- 15) Urząd Dozoru Technicznego;
- 16) Urząd Patentowy.

Projekt został przekazany do zaopiniowania przez Komisję Wspólną Rządu i Samorządu Terytorialnego i w dniu 14 stycznia 2025 r. uzyskał pozytywną wiążącą opinię Komisji Wspólnej Rządu i Samorządu Terytorialnego (opinię wydał Zespół do Spraw Społeczeństwa Informacyjnego, który został w tym celu upoważniony przez Komisję).

Minister Cyfryzacji przyjął propozycję strony samorządowej, aby wprowadzić obniżone wymogi z zakresu cyberbezpieczeństwa dla samorządowych jednostek budżetowych, samorządowych zakładów budżetowych, samorządowych instytucji kultury oraz spółek prawa handlowego wykonujących zadania o charakterze użyteczności publicznej w rozumieniu art. 1 ust. 2 ustawy z dnia 20 grudnia 1996 r. o gospodarce komunalnej (Dz. U. z 2021 r. poz. 679) oraz wprowadzić obniżone wymogi w zakresie zgłaszania incydentów.

Projekt został przekazany do zaopiniowania przez Radę Dialogu Społecznego - nie wniesiono uwag.

Projekt nie wymagał zaopiniowania przez:

- 1) Radę do Spraw Cyfryzacji, ponieważ stanowi wyłącznie regulację mającą zapewnić stosowanie przepisów dyrektywy unijnej – NIS 2;
- 2) Radę Działalności Pożytku Publicznego, gdyż nie dotyczy funkcjonowania organizacji pozarządowych oraz działalności pożytku publicznego oraz wolontariatu.

Omówienie uwag do projektu zostało przedstawione w załącznikach do niniejszego raportu z konsultacji. Załączniki zawierające stanowisko Ministra Cyfryzacji do przedstawionych uwag zostały udostępnione w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji, w serwisie Rządowy Proces Legislacyjny.

2. Przedstawienie wyników konsultacji projektu z właściwymi organami i instytucjami Unii Europejskiej, w tym Europejskim Bankiem Centralnym

Projekt ustawy nie wymagał przedłożenia instytucjom i organom Unii Europejskiej w celu uzyskania opinii, dokonania powiadomienia, konsultacji albo uzgodnienia, poza Europejskim Bankiem Centralnym, który w dniu 20 stycznia 2025 r. przedstawił swoją opinię do projektu ustawy¹. W wyniku tej opinii do projektu został dodany przepis o współpracy zespołów CSIRT

¹ <https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52025AB0002>

z Narodowym Bankiem Polskim w przypadku incydentów, mających wpływ na systemy płatności.

3. Wskazanie podmiotów, które zgłosiły zainteresowanie pracami nad projektem w trybie przepisów o działalności lobbingowej w procesie stanowienia prawa

Zgodnie z przepisami ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2025 r. poz. 677), projekt ustawy został zamieszczony w Biuletynie Informacji Publicznej.

W toku prac nad projektem wpłynęło jedno zgłoszenie lobbingowe do projektu ustawy, które zostało opublikowane w Biuletynie Informacji Publicznej Rządowego Centrum Legislacji w serwisie Rządowy Proces Legislacyjny.

Podmiot zgłaszający zainteresowanie pracami nad projektem w trybie przepisów o działalności lobbingowej w procesie stanowienia prawa – KRZYSZTOF ROŻKO I WSPÓLNICY KANCELARIA PRAWNA SPÓŁKA KOMANDYTOWA.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

Lp.	Zgłaszający uwagę	Jednostka redakcyjna	Treść uwagi	Stanowisko Ministra Cyfryzacji
Uwagi do projektu ustawy				
1.	Autobox Innovations sp. z o.o. sp. j. oraz E-Van sp. z o.o.	Uwaga ogólna	Działając w imieniu spółek Autobox Innovations sp. z o.o. sp. j. oraz E-VAN sp. z o.o. wskazuję, że reprezentowane przeze mnie Spółki rozumieją konieczność intensywnego zaangażowania organów państwa w zapewnianiu właściwego poziomu bezpieczeństwa cyfrowego. Jednakże wszelkie rozwiązania, które Państwo wdraża, by aktywnie przeciwdziałać zagrożeniom bezpieczeństwa cyfrowego - muszą być wprowadzane racjonalnie, z dużą dozą ostrożności i po dogłębnej analizie potencjalnych korzyści i strat. Muszą one być odpowiednio miarkowane - tak by przy osiąganiu nałożonych na nie celów, nie doprowadzić do szkód w rozwoju gospodarczym kraju. Takie założenia powinny przyświecać także implementacji do naszego systemu prawnego dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii. Dyrektywa NIS2 znacząco rozszerza katalog sektorów i podmiotów objętych systemem cyberbezpieczeństwa. Obok sektorów energii, transportu, zdrowia, bankowości, infrastruktury rynków finansowych, zaopatrzenia w wodę i infrastruktury cyfrowej, system ten obejmie również sektory ścieków, zarządzania ICT, przestrzeni kosmicznej, poczty, produkcji i dystrybucji chemikaliów jak również produkcji i dystrybucji żywności, ale także sektor produkcji pojazdów samochodowych, przyczep i naczep. Ostatnia z ww. branż stanowi kluczowy przedmiot działalności moich Mocodawców, którzy działają w zakresie produkcji pojazdów samochodowych (przedmiot przeważającej działalności: PKD 29, 20, pozostałej: PKD 29, 10 oraz, 29, 32) czyli działalności zgodne z tymi, o których mowa w sekcji C dział 29 klasyfikacji NACE Rev. 2. Dyrektywa NIS2, a w ślad za nią Projekt ustawy zamiast dotychczasowo stosowanych definicji „operatorów usług kluczowych” i „operatorów usług cyfrowych” wprowadza pojęcia „podmiotu kluczowego” oraz „podmiotu ważnego”, które mają być głównymi adresatami obowiązków wynikających z Ustawy Krajowym Systemie Cyberbezpieczeństwa. Projekt ustawy obejmuje swoim zakresem aż 18 branż, co przekłada się na 38 532 podmiotów, co jest absolutnym rekordem w skali europejskiej, w przypadku tego typu regulacji¹. Tym samym polski projekt implementacji NIS2 jest oceniany jako najbardziej ograniczający i restrykcyjny wśród wszystkich państw członkowskich UE pod względem zastosowania, zarówno co do liczby branż i jak i podmiotów. Załącznik II Dyrektywy NIS2 większość z nich bowiem zalicza do podmiotów ważnych. Podobnie w odniesieniu do „produkcji pojazdów samochodowych, przyczep i naczep (tj. przedsiębiorstw prowadzących którykolwiek z rodzajów działalności gospodarczej, o których mowa w sekcji C dział 29 klasyfikacji NACE Rev. 2) zalicza je do sektorów ważnych. Projekt polskiej ustawy natomiast przewiduje, że branża ta podpada pod sektory kluczowe. Tego typu zmiana klasyfikacji przez państwo członkowskie, choć uprawniona na podstawie art. 1 ust. 1 l i 2),	Wyjaśnienie uwagi Przy liczbie 38 000 podmiotów ok. 28 tys. to podmioty publiczne. Bezpośrednio z dyrektywy NIS2 wynika, że sektor produkcji podlega wymogom cyberbezpieczeństwa. Sektor produkcji zostanie przeniesiony do sektorów ważnych. Zgodnie z dyrektywą NIS2 wszystkie podmioty mają obowiązek dbać o bezpieczeństwo łańcuchów dostaw.

¹ <https://gsmonline.pl/artykuly/ksc-i-nis2-to-spore-zmiany-i-koszty-nie-tylko-dla-operatorow> [dostęp: 22 maja 2024 roku]

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

		w z w. z a r t. 2 u s t. 2 l i t. b)-e) Dyrektywy NIS2, nie jest jednak naszym zdaniem niczym uzasadniona. Nie ma powodu, by w zakresie produkcji pojazdów samochodowych dokonywać tak daleko idącej klasyfikacji. Ich produkcja z punktu widzenia cyberbezpieczeństwa mogłaby zostać uznana za potencjalnie niebezpieczną w sytuacji ew. szkodliwych powiązań gospodarczych, czy też stosowania zaawansowanych systemów informatycznych w finalnych produktach. Moi Mocodawcy nie produkują jednak (i nie mają w planach produkować) w pełni zautomatyzowanych pojazdów, które można by ewentualnie kwalifikować wysoko pod względem ryzyka cyfrowego (ze względu na bogato rozwiniętą elektronikę i cyfrowe rozwiązania). Produkowane przez moich Mocodawców pojazdy samochodowe, posiadają znacznie skromniejsze (i porównywalne do stosowanych we wszelkich obecnych urządzeniach elektronicznych) - systemy cyfrowe. Ich rozwiązania cyfrowe są zbyt skromne, by analizować je pod kątem zagrożenia cybernetycznego. Branża i skala w której działają moi Mocodawcy, nie może być uznana za kluczową, w porównaniu z takimi branżami jak: energia, transport, ochrona zdrowia, bankowość, infrastruktura rynków finansowych, zaopatrzenie w wodę czy wreszcie infrastruktura cyfrowa. W naszym Państwie produkcja pojazdów samochodowych jest rozwinięta na o wiele mniejszą skalę niż w innych krajach Unii (np. w Niemczech, czy we Francji), co powinno być brane przez rządzących pod uwagę. Choćby dlatego nie ma racjonalnych argumentów do zakwalifikowania podmiotów związanych z produkcją pojazdów samochodowych w Polsce, do podmiotów kluczowych. Projekt ustawy przewiduje także znaczący wpływ państwa na podmioty prowadzące działalność w zakresie dystrybucji towarów, których producenci będą mogli zostać uznani arbitralnie przez państwo polskie za Dostawców Wysokiego Ryzyka (za dostawców uznani mogą być zarówno producenci, jak i upoważnieni przedstawiciele, importerzy oraz dystrybutorzy). Podmioty podlegające pod zasady krajowego systemu cyberbezpieczeństwa nie będą mogły nabywać towarów wskazanych w decyzji o uznaniu danego podmiotu za Dostawcę Wysokiego Ryzyka. Co ważne, uznanie za Dostawcę Wysokiego Ryzyka w stosunku do produktu może mieć swoje źródło także w komponentach tego produktu, np. istotnej jego części lub oprogramowania, np. półprzewodników, wbudowanych komputerów czy też baterii oraz oprogramowania do zarządzania nimi. Pozbawia to kontrahentów możliwości dokonywania transakcji z takimi podmiotami w zakresie komponentów innego typu. Należy zwrócić tutaj uwagę, że Projekt ustawy jest niezwykle nieprecyzyjny i ogólnikowy w określeniu przesłanek uznania podmiotów za potencjalnie niebezpieczne. Zgodnie z Projektem ustawy właściwy minister ds. informatyzacji może wydać w stosunku do konkretnego podmiotu decyzję w sprawie uznania go za Dostawcę Wysokiego Ryzyka. Cel wydania takiej decyzji jest określony bardzo ogólnie jako „ochrona bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego” i dotyczyć ma wszelkich produktów, usług lub procesów wykorzystywanych przez podmioty kluczowe lub podmioty ważne. Decyzja wydawana jest wobec podmiotu, który „stanowi poważne zagrożenie dla obronności, bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego, lub życia i zdrowia ludzi” - planowany art. 67a ust. 15.	

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

		znowelizowanej ustawy. W przypadku wydania decyzji nowy sprzęt lub oprogramowanie takiego dostawcy nie będą mogły być wprowadzane do użytku, a dotychczas używane będą musiały być wycofane z systemów podmiotów kluczowych i podmiotów ważnych (w ciągu 4 lat przez przedsiębiorców telekomunikacyjnych i 7 lat przez pozostałe podmioty - planowany art. 67c. 1. znowelizowanej ustawy). Podkreślić należy, że powyższe rozwiązania nie wynikają z Dyrektywy NIS2, stanowiąc jedynie niepotrzebne wzmocnienie powołanych tam instytucji. Organy Unii Europejskiej nie wypracowały regulacji, które pozwoliłyby na wprowadzenie tak daleko posuniętych instrumentów prawnych w celu zapewnienia cyberbezpieczeństwa podmiotów objętych jej zakresem. Projekt polskiej ustawy zakłada wprowadzenie instytucji nieznanych w innych krajach członkowskich Unii Europejskiej. Stworzony instrument prawny, mimo znaczących w skutkach możliwości działania organów państwa, posiada niezwykle nieokreślone przesłanki stosowania. Krytycznie należy ocenić brak przyjęcia przez polski rząd w ww. Projekcie ustawy - definicji wystąpienia poważnego zagrożenia dla obronności, bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego, lub życia i zdrowia ludzi. Zbiór desygnatów tych pojęć może być w zależności od indywidualnych interpretacji bardzo szeroki. Tak szczególnie regulacja nie powinna dawać jednak organom tak dużego pola do swobodnego uznania. Krytycznie należy ocenić swobodę w działaniu organów państwa (przewidziana Projektem ustawy opinia, której organ ma obowiązek zasięgnąć nie jest dla niego w żadnym wypadku wiążąca) mogącą wywołać natychmiastowe skutki (Projekt ustawy zakłada rygor natychmiastowej wykonalności decyzji), które będą szczególne zauważalne z perspektywy podmiotów funkcjonujących w międzynarodowym obrocie handlowym. Brak z mian n a t y m p o l u p o w o d o w a ć b ędzie, że przedsiębiorcy ze wskazanych licznych branż, będą w stanie niepewności co do wyboru kontrahentów - w ciągłej obawie co do możliwości wywiązania się ze swoich bieżących zobowiązań. Projekt ustawy rodzi bardzo poważne konsekwencje dla kilkutysięcznej rzeszy podmiotów. Ponadto może spowodować poważne zaburzenia w gospodarce krajowej, poprzez utratę konkurencyjności przez niektóre podmioty i wywołanie antagonizmów ze światowymi partnerami spoza UE i NATO. Odmienne regulacje w zakresie cyberbezpieczeństwa pomiędzy poszczególnymi krajami członkowskimi stanowią istotne utrudnienie w ramach prowadzenia działalności gospodarczej na rynku europejskim, jak również zwiększają koszty działalności w zakresie utrzymania zgodności regulacyjnej, co finalnie przekłada się na ceny oferowane odbiorcom końcowym. Nie powinno to leżeć w interesie polskiego rządu. Moi Mocodawcy (jak i inne podmioty działające na polskim rynku pojazdów mechanicznych) choć są przedsiębiorstwami kwalifikującym się jako średnie, to posiadają znaczące plany rozwojowe. Działalność ta powinna być bez wątpienia ważna punktu widzenia naszego kraju i jego interesu gospodarczego. By mogła się prężnie rozwijać potrzebuje wsparcia publicznego. Moi Mocodawcy korzystają już ze wsparcia. Mowa tu o dofinansowaniu jakie uzyskała spółka Autobox Innovations w ramach Narodowego Centrum Badań i Rozwoju w ramach projektu „e- Van - uniwersalny pojazd dostawczy o napędzie elektrycznym kat. N1” finansowanego z funduszy europejskich Programu Operacyjnego Inteligentny Rozwój. W 2020 roku do konkursu	

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

		stanęło 10 firm, z czego w czwartym, ostatnim etapie zostały dwa podmioty. W sumie na projekt Autoboxu zostało przeznaczone 19 milionów złotych. Jest to pojazd o zasięgu 350 kilometrów, jednej tony ładowności, trzech rodzajach zabudowy i opcjonalnym napędzie 4x4². Spółka E-VAN sp. z o.o. natomiast zaangażowana jest w technologicznie innowacyjny projekt elektrycznej ciężarówki jako inteligentnego i energooszczędnego rozwiązania dla polskiego rynku logistycznego, usług miejskich i wewnątrzmiejskich. Te i inne projekty realizowane przez moich Mocodawców będą zagrożone, w związku z planowaną nowelizacją. Dyrektywa NIS2 przewiduje także, że organy zarządzające (kierownictwo) podmiotów kluczowych i ważnych zatwierdzają środki zarządzania ryzykiem w cyberbezpieczeństwie, nadzorują ich wdrażanie i ponoszą odpowiedzialność za naruszenie wymogów określonych w Dyrektywie. Ponadto członkowie organu zarządzającego mają obowiązek odbywać regularne szkolenia w celu zdobycia wystarczającej wiedzy i umiejętności. Pozwoli im to rozpoznać ryzyko i ocenić praktyki zarządzania ryzykiem w cyberbezpieczeństwie oraz ich wpływ na usługi świadczone przez te podmioty. Analogiczne szkolenia zalecane są pracownikom niższego szczebla zatrudnionym w podmiotach kluczowych i ważnych. Podmioty objęte zakresem implementacji Dyrektywy NIS 2 mają obowiązek wdrożenia środków (technicznych, organizacyjnych, operacyjnych) mających na celu identyfikację ryzyka wystąpienia incydentów, zapobieganie incydentom, wykrywanie ich, reagowanie na nie i przywracanie normalnego działania po ich wystąpieniu oraz łagodzenie ich skutków. Ma to na celu zapobieganie wpływowi incydentów na odbiorców ich usług lub na inne usługi bądź minimalizowania takiego wpływu. Środki zarządzania ryzykiem w cyberbezpieczeństwie powinny dotyczyć również bezpieczeństwa fizycznego i środowiskowego sieci i systemów informatycznych przez włączenie środków ochrony takich systemów przed awariami, błędem ludzkim, złośliwymi działaniami lub zjawiskami naturalnymi, zgodnie z normami europejskimi i międzynarodowymi, takimi jak normy zawarte w serii ISO/IEC 27000. To oczywiście stanowi tylko część licznych obowiązków i procedur jakich wymagać się będzie od podmiotów objętych projektem Ustawy. W tym miejscu należy wskazać, że obowiązki te wiązać się będą z ogromnymi kosztami, których poniesienie przez moich Mocodawców (i inne podmioty) nie będzie refundowane przez państwo. Dodatkowe obawy wóldarzy spółek E-Van oraz Autobox Innovations budzi fakt, że zgodnie z projektowanymi przepisami podmioty kluczowe i podmioty ważne, które nie wprowadzą nowych wymogów ustawowych, będą musiały się liczyć z dotkliwymi karami. Projekt Oceny Skutków Regulacji dot. przedmiotowej nowelizacji jest w opinii Moich Mocodawców niewystarczający przede wszystkim w odniesieniu do realnych skutków finansowych jakie poniosą podmioty kluczowe i ważne. Powinien on zawierać wyniki analizy wpływu projektowanego aktu normatywnego na podmioty, objęte jego regulacją. Próżno doszukać się w opublikowanym projekcie jakichkolwiek analiz z punktu wdziania wpływu regulacji na branżę moich Mocodawców. Ponadto	

² <https://www.autobox.pl/pl/e-van> [dostęp 24 maja 2024 roku].

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			przygotowany projekt nie określa kosztów wdrożenia nowych zobowiązań prawnych. Nawet jednak bez dogłębnej analizy można śmiało powiedzieć, że koszty wprowadzenia rozwiązań proponowanych przez polski rząd będą ogromne. Wobec powyższego moi Mocodawcy wskazują także na uzasadnioną konieczność powołania przez państwo polskie odpowiedniego funduszu celowego, bądź programu dofinansowań, które objęłyby branże mniejsze, rozwijające się, w zakresie pomocy we wdrożeniu odpowiednich wymogów przewidzianych w ramach implementacji Dyrektywy NIS2, niezależnie od ich powiązań gospodarczych. Projektowana ustawa wedle planów Ministerstwa ma wejść w życie po upływie 1 miesiąca od dnia jej ogłoszenia. Zauważyć przy tym należy, że ustawa przewiduje 6 miesięczny okres dostosowawczy dla podmiotów kluczowych i podmiotów ważnych. Takie rozwiązanie nie zapewnia odpowiedniego czasu tym podmiotom na przygotowanie się do wdrożenia zapisów ustawy. Co prawda polski rząd broni się tutaj terminem implementacji przepisów - ustalonym w art. 42 ust. 1 Dyrektywy NIS2 na 17 października 2024 r. Nie jest jednak winą podmiotów objętych zapisami ustawy, że procedura legislacyjna w zakresie przepisów wdrażających rozpoczęła się dopiero na pół roku przed tą datą. Szeroki zakres obowiązków jakich wymagać się będzie od podmiotów objętych w wyniku wdrożenia do polskiego systemu prawnego Dyrektywy NIS2 związany jest z koniecznością rozłożonego w czasie planu ich realizacji. Moi Mocodawcy nie wyobrażają sobie by obowiązków tych musieli dochować we wskazanych wyżej terminach. Koniecznym jest znaczące wydłużenie vacatio legis przepisów ustawy wdrożeniowej. Kończąc niniejsze stanowisko, wnoszę o wydłużenie terminu konsultacji społecznych. Wyznaczono bowiem na nie jedynie 30 dni, co powoduje poważne ryzyko, iż opinie oraz głosy przedstawicieli zainteresowanych branż mogą nie zostać w pełni wysłuchane. Projekt ustawy dotyczy materii skomplikowanej, a jednocześnie nakładającej na różne podmioty wiele dotkliwych obowiązków. W tego typu sprawach, by szeroki krąg potencjalnie zainteresowanych podmiotów mógł pochylić się nad propozycjami rządowymi, okres czasu na przysyłanie opinii powinien zostać wydłużony, bądź wyznaczony na nowo. Podsumowując powyższe rozważania, spółki Autobox Innovations sp. z o.o. sp. j. oraz E-VAN sp. z o.o. stoją na stanowisku konieczności podjęcia następujących działań: 1) dokonania ponownej weryfikacji listy podmiotów zaklasyfikowanych jako ważne i kluczowe z uwzględnieniem zasady proporcjonalności, celem uniknięcia nadmiernej kontroli, wzrostu kosztów regulacyjnych i kosztów przestrzegania przepisów, zarówno po stronie rządowej jak i po stronie poszczególnych podmiotów; 2) skupienia się na implementacji założeń wynikających wprost z dyrektywy NIS2, które nie obejmują klauzuli wysokiego ryzyka i kryterium kraju pochodzenia; 3) precyzyjnego określenia kryteriów uznania za dostawcę wysokiego ryzyka, w tym odpowiedniego, ustawowego zdefiniowania przesłanek ingerencji państwa w tym zakresie; 4) przedłużenia konsultacji społecznych o dalszy, przynajmniej 90 dniowy okres czasu oraz przeprowadzenia szerokiej debaty publicznej nad projektem ustawy;	

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			5) wprowadzenia mechanizmu partycypacji przez państwo w kosztach wdrożenia procedur i wymogów przewidzianych w ramach implementacji dyrektywy NIS2; 6) wydłużenia terminu wejścia w życie proponowanej nowelizacji oraz wprowadzenia odpowiednich dłuższych terminów na wdrożenie przez podmioty nią objęte wymogów jakie wobec nich przewiduje; 7) dokonania ponownej Oceny Skutków Regulacji po szczegółowej analizie wpływu na poszczególne branże wchodzące w zakres kluczowych i ważnych.	
2.	Business Centre Club	Uwaga ogólna	Business Center Club przedstawia stanowisko dotyczące kwestii postępowania w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka i przewidzianego w projekcie ustawy 4 letniego okresu na wycofanie przez przedsiębiorców telekomunikacyjnych typów produktów, rodzajów usług i konkretnych procesów ICT wskazanych w decyzji w sprawie uznania dostawcy za dostawcę wysokiego ryzyka (dalej „decyzja DWR”). Zgodnie z projektem ustawy, minister właściwy do spraw informatyzacji, po zaistnieniu określonych przesłanek, może w drodze decyzji DWR uznać dostawcę sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Skutkiem wydania decyzji DWR dla innych podmiotów, przewidzianym w art. 67c ust. 1 i 2 projektu KSC, jest m.in. konieczność wycofania z użytkowania typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT w zakresie objętym decyzją dostarczanych przez dostawcę wysokiego ryzyka, przy czym termin takiego wycofania jest zróżnicowany – projekt przewiduje generalny termin 7-letni na takie wycofanie, natomiast w przypadku przedsiębiorców telekomunikacyjnych, termin na wycofanie produktów, usług i procesów, zgodnie z art. 67c ust. 2 projektu KSC, wynosi jedynie 4 lata. Tego rodzaju rozwiązanie jest nieprawidłowe ponieważ: • Przedsiębiorcy telekomunikacyjni traktowani są w rażąco dyskryminujący sposób w stosunku do wszystkich innych pozostałych podmiotów, co nie ma uzasadnienia merytorycznego. W szczególności za takie uzasadnienie nie można traktować lakonicznego jednozdaniowego wskazania w uzasadnieniu do projektu ustawy że „Takie skrócenie okresu na wycofanie jest spowodowane szczególnym znaczeniem dla bezpieczeństwa państwa usług telekomunikacyjnych, szczególnie sprzętu lub oprogramowania wykorzystywanych do realizowania funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku nr 3 do ustawy”, gdyż taką argumentację można odnieść do wielu innych sektorów usługowych. • Znaczące skrócenie terminu na wycofanie z sieci przedsiębiorców telekomunikacyjnych sprzętu dostawcy uznanego za dostawcę wysokiego ryzyka – do 4 lat – może mieć swój wymiar praktyczny. Powstaje bowiem uzasadnione pytanie, czy w przypadku gdy tego rodzaju proces będzie obejmował wielu przedsiębiorców telekomunikacyjnych (np. kilku operatorów sieci mobilnych korzystających z urządzeń określonego dostawcy uznanego w decyzji DWR za dostawcę wysokiego ryzyka) – proces usunięcia z ich sieci sprzętów dostawcy DWR jest możliwy pod kątem logistycznym i technicznym – np. z punktu widzenia	Wyjaśnienie uwagi Skrócenie terminu wynika ze szczególnego znaczenia sieci telekomunikacyjnych dla funkcjonowania społeczeństwa informacyjnego. Niebezpieczny sprzęt i oprogramowanie powinny być wycofane szybciej z tego sektora, ponieważ od tych usług zależy świadczenie usług w innych sektorach.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			dostępności zewnętrznych ekip technicznych (podwykonawców) realizujących tego rodzaju proces w jednym (skrótowym) czasie na rzecz wielu różnych podmiotów. • Zgodnie z ogólnie dostępnymi informacjami sieć 5G w Polsce budowa jest aktualnie w tzw. modelu non-stand alone, co oznacza że nie jest samodzielną technologią, a dla swojego działania wykorzystuje elementy infrastruktury poprzedniej generacji tj. 4G. Powyższe oznacza, że konieczność wycofania z użytkowania sprzętów dostawcy uznanego za dostawcę wysokiego ryzyka może w praktyce mieć wpływ także na elementy infrastruktury 4G, a tym samym obejmować znaczące obszary sieci przedsiębiorców telekomunikacyjnych i mieć realny i zasadniczy wpływ na możliwość świadczenia usług telekomunikacyjnych przez te podmioty. • Projekt KSC nie przewiduje jakiegokolwiek formy rekompensaty z tytułu konieczności wycofania przez przedsiębiorców telekomunikacyjnych z ich sieci sprzętów dostawcy, w stosunku do którego została wydana decyzja DWR. Realizacja takiego procesu w skróconym horyzoncie czasowym (4 lata, zamiast 7 lat jak w przypadku innych podmiotów, lub nawet 5 lat jak w przypadku poprzednich wersji projektu KSC) oznacza zatem zwiększony coroczny wymiar finansowy dla każdego z przedsiębiorców telekomunikacyjnych, którego będzie dotyczyło takie działanie. Realizacja takiego – w założeniu bardzo kosztownego procesu – w skróconym okresie będzie zatem pogłębiała coroczny negatywny wpływ finansowy na przedsiębiorców telekomunikacyjnych. Biorąc pod uwagę fakt, że do tej pory ceny usług telekomunikacyjnych w Polsce były jednymi z najatrakcyjniejszych w krajach UE, z czego korzystali wszyscy użytkownicy końcowy (zarówno prywatni, jak i biznesowi – a więc także przedsiębiorcy zrzeszeni w BCC) BCC wyraża zasadniczą obawę, że wdrożenie środków przewidzianych w projekcie KSC może mieć poważne przełożenie na wzrost cen usług telekomunikacyjnych. • Doświadczenia międzynarodowe z innych krajów – np. USA czy Wielkiej Brytanii – w sposób jednoznaczny wskazują, że przyjęcie zbyt krótkiego czasu na realizację obowiązku wymiany elementów infrastruktury dostawcy wysokiego ryzyka skutkuje poważnymi problemami praktycznymi i docelowo i tak może wymagać jego wydłużenia. Biorąc pod uwagę całość powyższej argumentacji, jako BCC zwracamy się z prośbą do projektodawców ustawy o ponowną rewizję zasadności ustalania w projekcie ustawy 4 letniego okresu na wycofanie przez przedsiębiorców telekomunikacyjnych typów produktów, rodzajów usług i konkretnych procesów ICT wskazanych w decyzji w sprawie uznania dostawcy za dostawcę wysokiego ryzyka. W naszej ocenie termin ten nie powinien odbiegać od 7-letniego terminu przewidzianego w stosunku do innych niż przedsiębiorcy telekomunikacyjni podmiotów, a przynajmniej należałoby powrócić do przewidzianego w poprzednich wersjach projektu KSC terminu 5 letniego.	
3.	European AI Forum	Uwaga ogólna	Działając w imieniu European AI Forum - największego stowarzyszenia europejskich spółek AI (ponad 2000 podmiotów) - mam przyjemność przedłożyć uwagi do projektu ustawy. Ich skrótowa	Wyjaśnienie uwagi Nie jest możliwe dokładne oszacowanie wpływu projektu na koszty

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

		postać wynika ze zbyt krótkiego czasu jaki został przewidziany na tak znaczący projektu ustawy. W związku z tym zwracamy się z prośbą o wydłużenie procesu konsultacyjnego o dodatkowe 30 dni. Brak szacowania kosztów Projekt ustawy nie zawiera analizy kompleksowego wpływu ustawy na polską gospodarkę i polskich przedsiębiorców. W ustawie przewidziano blisko 18 sektorów jakie mają być objęte regulacjami jednak szereg z nich nie zawiera żadnych wyliczeń co do skutków. Błędne użycie 5G Toolbox W projekcie ustawy, w jego uzasadnieniu czy OSR projektodawca odwołuje się do 5G Toolbox. Projektodawca błędnie chce skorzystać z zapisów przeznaczonych dla sieci 5G w blisko 17 sektorach gospodarki. Nie znajdujemy uzasadnienia jak 5G toolbox ma związek np. z sektorem zdrowia, przestrzeni kosmicznej czy gospodarowania odpadami. Zalecamy ograniczenie 5G toolbox do sektora telekomunikacyjnego. Brak przewidywalności prawa i prowadzenia biznesu AI Spółki rozwijające produkty i usługi sztucznej inteligencji, szczególnie małe i średnie, wskazują na całkowity brak przewidywalności prawa i prowadzenia biznesu w obliczu wybrania tzw. kryteriów politycznych do oceny Dostawców Wysokiego Ryzyka w blisko 17 sektorach gospodarki. Spółki AI obawiają się, że dostawcy np. usług chmurowych i oprogramowania spoza sojuszu NATO zostaną wykluczeni z możliwości prowadzenia biznesu w Polsce. Spółki AI wykorzystują tego typu rozwiązania jako element swoich systemów IT. Spółki AI pragną zwrócić uwagę, że w świecie hiperłączości, szczególnie polskie MŚP korzystają z najtańszych rozwiązań i w konsekwencji często pochodzących z tzw. państw trzecich. Konieczność powołania funduszu rekompensat W obliczu wskazania całkowicie niemerytorycznych kryteriów ustalania DWR oraz z uwagi na brak jakiegokolwiek przewidywalności tego procesu spółki oferujące produkty i usługi AI wnoszą o ustanowienie, na wzór Amerykański, funduszu rekompensat dla mikro-, małych i średnich firm. Ponieważ projektodawca nie przedstawił analiz i szacunków kompleksowego wpływu ustawy na gospodarkę to spółki AI wnoszą aby ustalić ten fundusz bazując nie tylko na koszcie zakupu nowego produktu ale jego integracji i wdrożenia. Fundusz ten nie powinien posiadać limitu wydatków, gdyż rekompensaty mogą sięgnąć nawet dziesiątki miliardów złotych w skali całego kraju (zsumowane dla wszystkich sektorów podlegających ustawie). Spółki AI proponują by środki trafiały w pierwszej kolejności do małych i średnich polskich firm tworzących własność intelektualną w Polsce i płacących w Polsce podatki. W drugiej kolejności powinny być rozpatrywane wnioski spółek prowadzących jedynie w Polsce działalność usługowo-sprzedażową jednak niebędąca zarejestrowane w Polsce. Najbardziej restrykcyjna ustawa w Europie W stowarzyszeniu European AI Forum AISBL analitycy dokonali syntezy wdrożeń lub propozycji wdrożeń NIS2 w Unii Europejskiej oraz zestawili je również z oceną wdrożeń 5G Toolbox przedstawionych w załączniku 1 do projektu ustawy (<i>UZG Zał. nr 1 do OSR Dostawca wysokiego ryzyka (high risk vendor) i bezpieczeństwo sieci 5G Europy</i>). Analitycy European AI Forum	przedsiębiorców z uwagi na różny charakter usług oraz różną wielkość przedsiębiorców. Zgodnie z dyrektywą NIS 2 każdy podmiot kluczowy i podmiot ważny jest obowiązany dbać o bezpieczeństwo łańcuchów dostaw. Dlatego postępowanie ws. uznania za dostawcę wysokiego ryzyka wpisuje się w to. Dostawca wysokiego ryzyka to podmiot, który stwarza poważne zagrożenie dla bezpieczeństwa państwa, obronności, bezpieczeństwa i porządku publicznego lub zdrowia i życia ludzi. To są główne przesłanki uznania dostawcy za dostawcę wysokiego ryzyka, a nie kryteria państwowe. Przy obecnej sytuacji budżetowej nie jest możliwe wprowadzenie funduszu rekompensat – a nawet gdyby było możliwe to taki fundusz musiałby mieć limit wydatków.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			wskazują, że proponowane przepisy będą najbardziej restrykcyjne w całej Europie. Polska stanie się zatem liderem w „nadregulacji”. Żaden kraj nie wdraża bowiem mechanizmu 5G Toolbox i DWR we wszystkich proponowanych sektorach gospodarki, gdyż proponowane przepisy są ograniczone do sektora telekomunikacji. Spółki AI wskazują zatem, że przepisy 5G toolbox powinny dotyczyć jedynie sektora telekomunikacji, tak jak zostało to wdrożone w innych krajach europejskich.	
4.	Exatel	Uwaga Ogólna	Zmiany zaproponowane w przedmiotowym projekcie bez wątpienia pozytywnie wpłyną na system cyberbezpieczeństwa w Polsce. Wskazane rozwiązania wpisują się w szereg zmian, które umacniają obecność Polski w globalnej cyberprzestrzeni. Dla zapewnienia bezpieczeństwa Polski konieczne jest jednak przywrócenie do projektu ustawy przepisów dotyczących utworzenia strategicznej sieci bezpieczeństwa w wersji uzgodnionej już międzyresortowo i poddanej konsultacjom publicznym (druk sejmowy nr 3457 z dnia 3 lipca 2023 r.). Celem stworzenia strategicznej sieci bezpieczeństwa jest zapewnienie realizacji zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego w aspekcie telekomunikacyjnym. Strategiczna sieć bezpieczeństwa powinna zostać utworzona jako odrębna sieć od innych sieci telekomunikacyjnych, która zostanie uruchomiona i zarządzana przez operatora strategicznej sieci bezpieczeństwa - podmiot znajdujący się w całości pod kontrolą państwa. Powyższa konieczność wynika z narastającego napięcia międzynarodowego oraz sytuacji geopolitycznej Polski. Wojna, która toczy się za polską wschodnią granicą wpływa bezpośrednio na bezpieczeństwo Polski. Utworzenie strategicznej sieci bezpieczeństwa obejmującej mobilną sieć telekomunikacyjną na potrzeby realizacji bezprzewodowej sieci łączności specjalnej (usługi PPDR - Public Protection & Disaster Relief) jest kluczowe dla zapewnienia bezpieczeństwa m.in. na polskich granicach. Obecnie często dochodzi do sytuacji, w których brak jest niezbędnej komunikacji umożliwiającej skuteczną komunikację służb w obliczu hybrydowych zagrożeń. Eskalujący konflikt zwiększa dodatkowo potrzeby w tym zakresie, a wojna w Ukrainie pokazuje jak kluczowa jest bezpieczna i nowoczesna komunikacja w kontekście potrzeb nowoczesnego pola walki. Obecnie przy realizacji zadań z zakresu obronności czy bezpieczeństwa państwa organy administracji korzystają z usług operatorów znajdujących się - ze względu na strukturę właścicielską - pod wpływem podmiotów trzecich, niebędących pod kontrolą państwa polskiego. Sytuacja ta może zagrażać bezpieczeństwu przekazywanych informacji, a więc zagrażać bezpieczeństwu państwa. W związku z powyższym, niezbędne jest przywrócenie przepisów dotyczących strategicznej sieci bezpieczeństwa.	Uwaga nieuwzględniona Kwestie utworzenia strategicznej sieci bezpieczeństwa wykraczają poza zakres wpisu do wykazu prac legislacyjnych i programowych Rady Ministrów.
5.	Fundacja Bezpieczna Cyberprzestrzeń	Uwaga ogólna	Pomimo zaprezentowanego projektu nowelizacji wiele kwestii związanych z wdrożeniem wymogów NIS2 pozostaje nadal bez rozstrzygnięcia, nie wiadomo jak będą wyglądały akty wykonawcze do ustawy, ani jaki dokładnie zakres będą regulować. Sam projekt nowelizacji, bez prezentacji w postaci tekstu jednolitego ustawy pozostaje nieczytelny i wymaga wielkich nakładów czasowych od podmiotów biorących udział w konsultacjach	Wyjaśnienie uwagi Zakres aktów wykonawczych wynika z przepisów upoważniających. Tekst jednolity ustawy jest opracowywany przez Marszałka Sejmu zgodnie z ustawą o ogłaszaniu aktów normatywnych i niektórych innych aktów prawnych.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

6.	Fundacja Bezpieczna Cyberprzestrzeń	Uwaga ogólna	Zauważyliśmy, że nowelizacja zmienia wiele dobrze zdefiniowanych i przetestowanych rozwiązań jak np. wewnętrzne struktury cyberbezpieczeństwa i zewnętrzne w postaci podmiotów świadczących usługi z zakresu cyberbezpieczeństwa, takie działania wydają się bezzasadne powodując niepewność i niezrozumienie zarówno u podmiotów kluczowych i ważnych jak i dostawców technologii i usług z obszaru cyberbezpieczeństwa. Fundacja Bezpieczna Cyberprzestrzeń uważa, że obecnie prawidłowo działające mechanizmy powinny w swej istocie pozostać bez zmian, a w wypadku konieczności wprowadzenia korekt jedynie rozbudowane, a nie formułowane systemowo na nowo.i1) Nowelizacja pewne kwestie (nawet strategiczne) omawia bardzo zdawkowo, kiedy inne (często mało istotne) bardzo szczegółowo, przykładem braków (choćby tylko strategicznych) wymogów i rozwiązań jest jakże istotny obszar zapewnienia bezpieczeństwa łańcucha dostaw czy zagadnień dotyczących sztucznej inteligencji. W nowelizacji ogranicza się właściwie ten obszar do jednego zdania/wymogu. Brak w nowelizacji systemowej wizji w jaki sposób owo bezpieczeństwo łańcucha dostaw ma być zapewnione przez podmioty ważne i kluczowe. Natomiast przykładem gdzie nowelizacja sięga ewidentnie zbyt głęboko jest np. art. 10 ust. 7, mówiący o zniszczeniu wycofanej dokumentacji bezpieczeństwa systemów, zakończonej „protokołem brakowania” (sic!). Dwa skrajne przypadki, w których bardzo istotny dla zapewnienia bezpieczeństwa usług i działalności podmiotów obszar zostaje pozostawiony „odłogiem” , a drugi z ewidentnie nadmiarowymi wymogami regulującymi całkowicie oderwane od meritum NIS2 kwestie.	Uwaga częściowo uwzględniona Art. 14 ust. 1 dotyczący wewnętrznych struktur cyberbezpieczeństwa zostanie przywrócony. Rozbudowana zostanie kwestia bezpieczeństwa łańcuchów dostaw.
7.	Fundacja Bezpieczna Cyberprzestrzeń	Uwaga ogólna	Jako Fundacja zauważamy ponadto, że szereg definicji występujących w projekcie nowelizacji jest inny niż w brzmieniu dyrektywy NIS2. Dlatego należy je ujednolicić zgodnie z NIS2. Przykładami są „sieci i systemy informatyczne”, „bezpieczeństwo sieci i systemów informatycznych”, „incydent”, „podatność” czy „ryzyko”.	Wyjaśnienie uwagi Staramy się nie zmieniać definicji, które funkcjonują już od kilku lat w obrocie prawnym.
8.	Fundacja Bezpieczna Cyberprzestrzeń	Uwaga ogólna	Należy dołożyć wszelkich starań by krajowy system cyberbezpieczeństwa zintegrować z krajowym systemem zarządzania kryzysowego. Dalsze utrzymywanie odrębnych systemów jest nieefektywne i w istocie tworzy podatność systemu bezpieczeństwa RP, szczególnie w obszarze kompetencji organów oraz skoordynowanej reakcji na zagrożenia bezpieczeństwa państwa. Prowadzone aktualnie prace nad implementacją dyrektywy w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE są doskonałą okazją by połączyć obydwa systemy. Doświadczenia cyberincydentów w innych krajach, ale również w Polsce, wyraźnie pokazują, że nie jest możliwe wyraźne rozdzielenie sytuacji kryzysowej od incydentu poważnego lub krytycznego. W kontekście celu ogólnego (zapewnienia bezpieczeństwa państwa) nie ma to zresztą żadnego znaczenia.	Uwaga uwzględniona Będziemy podejmować działania mające na celu uspoźnienie obydwu systemów.
9.	Fundacja Bezpieczna Cyberprzestrzeń	Uwaga ogólna	W przedstawiona nowelizacji ustawy w niedostateczny sposób określa znaczenie i rolę podmiotów kluczowych i ważnych w całym systemie cyberbezpieczeństwa. Biorąc pod uwagę przewidywaną liczbę podmiotów objętych przepisami ustawy wskazaną w OSR wyraźnie widać, że dla sprawnego funkcjonowania systemu działania podmiotów kluczowych i podmiotów ważnych są najistotniejsze i to na zapewnieniu cyberbezpieczeństwa tych podmiotów powinna się koncentrować ustawa. Chodzi nie tylko o doprecyzowanie wymagań, ale przede wszystkim wsparcie ze strony potencjału państwa,	Wyjaśnienie uwagi Wiele z materii zawartej w projekcie stanowi materię ustawową – dotyczy to obowiązków nakładanych na przedsiębiorców, zakresu zgłaszanych incydentów, informacji zbieranych w

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			które zostało przewidziane w przepisach ustawy w sposób szcątkowy. Ustawa koncentruje się w dużej części na formalizowaniu spraw, które bez szkody dla treści ustawy mogą się być zawarte w rozporządzeniach lub nawet standardowych procedurach operacyjnych.	ramach zgłoszenia incydentu, kompetencji organów administracji publicznej, administracyjnych kar pieniężnych. Te kwestie nie mogą być przeniesione do aktów wykonawczych. Projekt ustawy przewiduje powołanie zespołów CSIRT sektorowych, które będą aktywnie wspierały podmioty kluczowe i podmioty ważne w cyberbezpieczeństwie.
10.	Fundacja Bezpieczna Cyberprzestrzeń	Uwaga ogólna	Fundacja Bezpieczna Cyberprzestrzeń uważa, że zaproponowane w projekcie nowelizacji zmiany nie tylko nie implementują wszystkich wymagań dyrektywy NIS2, która to dyrektywa przyczynić się miała do budowy sprawnego i bezpiecznego Krajowego Systemu Cyberbezpieczeństwa, a wręcz osłabiają ten obecnie istniejący. Nowelizacja wprowadza do Systemu cały szereg podatności i w efekcie czyni Krajowy System Cyberbezpieczeństwa gorzej przygotowanym do reakcji na zagrożenia. Zdaniem Fundacji, już dużo lepszym dla Systemu rozwiązaniem byłoby rozszerzenie zakresu podmiotowego obecnie obowiązującej ustawy wraz ze skopiowaniem wymogów bezpośrednio z art. 21 dyrektywy NIS2.	Wyjaśnienie uwagi Przepisy projektu zostaną poprawione. Natomiast wdrożenie NIS2 wymaga zdecydowanie głębszych zmian ustawowych niż zaproponowane w uwadze.
11.	Fundacja Open Allies	Uwaga ogólna	Na wstępie Fundacja zwraca się do Projektodawcy o analizę postanowień Projektu pod kątem ich niezbędności w odniesieniu do wdrożenia dyrektywy NIS2 do polskiego porządku prawnego. Ustawodawca europejski określił wymagany i proporcjonalny poziom cyberbezpieczeństwa, który jest adekwatny do zniwelowania zidentyfikowanych zagrożeń. Wprowadzanie proponowanych w Projekcie modyfikacji zmian modelu europejskiego systemu cyberbezpieczeństwa, z dużym prawdopodobieństwem doprowadzi do niepotrzebnego podniesienia kosztów prowadzenia działalności gospodarczej w Polsce – w tym działalności telekomunikacyjnej – względem innych Państw Członkowskich. Takie działanie będzie skutkowało pogorszeniem sytuacji polskich przedsiębiorców względem przedsiębiorców z innych Państw Członkowskich. Projekt, zgodnie z dyrektywą NIS2, wprowadza do krajowego systemu cyberbezpieczeństwa przedsiębiorców telekomunikacyjnych. Już ta okoliczność powoduje, że przedsiębiorcy telekomunikacyjni poniosą znaczne nakłady wdrożeniowe. Podnoszenie w polskiej ustawie standardów do wyższych niż określone w dyrektywie NIS2 postawi polskich przedsiębiorców w pozycji gorszej niż konkurentów z innych Państw Członkowskich.	Uwaga częściowo uwzględniona Część wymogów w zakresie audytów zostanie złagodzona.
12.	Fundacja Open Allies	Uwaga ogólna	Fundacja wnosi o uwzględnienie w polskich przepisach uprawnienia Państwa Członkowskiego, o którym mowa motywie 16 dyrektywy NIS2. Zwracamy się o wyraźne wskazanie w ustawie, że, mając na uwadze stopień niezależności, niektóre podmioty nie kwalifikują się jako podmioty ważne lub kluczowe. W szczególności, jeżeli dany podmiot jest niezależny względem sieci i systemów informatycznych lub ze względu na rzeczywisty brak powiązań, zasadne będzie wprowadzenie odpowiedniego wyjątku.	Uwaga uwzględniona Zostanie wprowadzony odpowiedni przepis.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

13.	Fundacja Open Allies	Uwaga ogólna	Open Allies zwraca się do Projektodawcy o analizę Projektu i nałożenie na podmioty ważne obowiązków, które są określone w dyrektywie. Nadmiarowe regulacje i obowiązki, szczególnie znacząco wyższe niż w innych Państwach Członkowskich, przyczynią się do zmniejszenia konkurencyjności polskiej gospodarki.	Uwaga uwzględniona Część wymagań zostanie złagodzona.
14.	Fundacji Rozwoju Obrotu Bezgotówkowego	Uwaga ogólna	Zgodnie z § 44 i § 45 Regulaminu, z uwagi na liczne uwagi zgłaszane dotychczas do nowelizacji oraz uwzględniając stosowaną praktykę przy wprowadzaniu tak istotnych zmian, Projektodawca powinien zorganizować konferencję uzgodnieniową. Prosimy także o przeprowadzenie wysłuchania publicznego, z uwagi na bardzo szeroki zakres regulowanych zagadnień oraz bardzo dużą liczbę podmiotów zainteresowanych nowymi regulacjami. Wnioskujemy również o wydłużenie okresu na konsultacji do 2 miesięcy.	Wyjaśnienie uwagi Nie planuje się konferencji uzgodnieniowej.
15.	HRO Personnel sp. z o.o.	Uwaga ogólna	Projekt ustawy wprowadza bardzo szerokie regulacje, które dotkną blisko 40 tysięcy podmiotów z 18 sektorów, w tym firmy zatrudniające co najmniej 50 osób lub mające 10 mln euro rocznego przychodu. Dla wielu przedsiębiorstw, zwłaszcza małych i średnich, koszty dostosowania się do nowych przepisów będą ogromne. Niespełnienie wymogów oznacza wielomilionowe kary, co stanowi olbrzymie obciążenie finansowe. Nasza firma, podobnie jak wiele innych, obawia się, że konieczność nagłego wprowadzenia technologicznych zabezpieczeń doprowadzi do wzrostu cen usług związanych z cyberbezpieczeństwem oraz braków specjalistów w tej dziedzinie. Proponowane zmiany w ustawie wprowadzają nadmierne regulacje na sektory, które nie muszą podlegać tak rygorystycznym przepisom, zgodnie z Dyrektywą NIS2. Nadregulacja prowadzi do nieuzasadnionych kosztów i obciążeń administracyjnych dla firm takich jak nasza. Polskie przedsiębiorstwa będą zmuszone do ponoszenia dodatkowych kosztów związanych z przestrzeganiem nowych przepisów, co może negatywnie wpłynąć na ich konkurencyjność na rynku.	Uwaga uwzględniona Część wymagań zostanie złagodzona. Co do zasady projekt obejmuje podmioty będące co najmniej średnimi przedsiębiorcami. Objęcie wymogami cyberbezpieczeństwa małych i mikroprzedsiębiorców to wyjątek.
16.	HRO Personnel sp. z o.o.	Uwaga ogólna	Problemy z procedurą uznania dostawcy za wysokiego ryzyka Proponowane przepisy zakładają wykluczanie dostawców na podstawie kryteriów politycznych i subiektywnych ocen, co jest bardzo problematyczne. Uważamy, że wykluczenie powinno dotyczyć konkretnych rozwiązań technologicznych, a nie całych dostawców. Decyzje te powinny opierać się na rzetelnych badaniach technicznych i certyfikacji, a nie na dowolnych kryteriach i niejawnych opiniach Kolegium ds. Cyberbezpieczeństwa. Takie podejście zapewniłoby bardziej wyważone i sprawiedliwe rozwiązania, które nie prowadziłyby do nieuzasadnionych strat finansowych i destabilizacji rynku. Proponujemy wprowadzenie mechanizmów certyfikacji opartych na obiektywnych kryteriach technicznych, co pozwoli na wykluczanie tylko tych rozwiązań, które rzeczywiście stanowią zagrożenie dla cyberbezpieczeństwa. Analiza zagrożeń, takich jak bezpieczeństwo narodowe czy kontrola przez państwa spoza UE lub NATO, jest skomplikowana i subiektywna. Takie podejście może prowadzić do wykluczeń na podstawie domniemań i podejrzeń, co nie jest sprawiedliwe. Zamiast tego, proponujemy wprowadzenie obiektywnych kryteriów merytorycznych i mechanizmów certyfikacji. Proponowane przepisy zakładają wykluczanie dostawców na podstawie kryteriów politycznych i subiektywnych ocen, co jest bardzo problematyczne. Uważamy, że wykluczenie powinno dotyczyć	Wyjaśnienie uwagi Kwestia certyfikacji może być niewystarczająca przy identyfikacji wszystkich zagrożeń jakie stwarza dostawca.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			konkretnych rozwiązań technologicznych, a nie całych dostawców. Decyzje te powinny opierać się na rzetelnych badaniach technicznych i certyfikacji, a nie na dowolnych kryteriach i niejawnych opiniach Kolegium ds. Cyberbezpieczeństwa. Takie podejście zapewniłoby bardziej wyważone i sprawiedliwe rozwiązania, które nie prowadziłyby do nieuzasadnionych strat finansowych. Proponujemy wprowadzenie mechanizmów certyfikacji opartych na obiektywnych kryteriach technicznych, co pozwoli na wykluczanie tylko tych rozwiązań, które rzeczywiście stanowią zagrożenie dla cyberbezpieczeństwa. Dodatkowo warto byłoby oprzeć się na skoordynowanych ocenach ryzyka – tak aby uwzględnić jednolite podejście na obszarze całej Unii Europejskiej.	
17.	HRO Personnel sp. z o.o.	Uwaga ogólna	Brak Oceny Skutków Regulacji (OSR) Niestety, OSR nie zawiera analizy kosztów wdrożenia tych obowiązków. Bez rzetelnych danych nie można oszacować, jakie będą długoterminowe skutki finansowe i operacyjne. Apelujemy o sporządzenie rzetelnej Oceny Skutków Regulacji, która pomoże ocenić, które obowiązki są rzeczywiście konieczne, a które zbyt kosztowne w stosunku do spodziewanych korzyści.	Wyjaśnienie uwagi Oszacowanie skutków finansowych dla przedsiębiorców jest trudne z uwagi na brak danych, różny charakter usług oraz wielkość przedsiębiorstw.
18.	HRO Personnel sp. z o.o.	Uwaga ogólna	Prosimy o ponowne przemyślenie proponowanych zmian. Apelujemy o przeprowadzenie rzetelnej Oceny Skutków Regulacji, eliminację dyskryminacyjnych kryteriów wykluczających oraz zapewnienie pełnej transparentności i możliwości odwoławczych w procesie decyzyjnym. Nadmierne i dyskryminacyjne przepisy mogą mieć negatywne konsekwencje dla całej gospodarki. Proponujemy, aby przepisy dotyczące wykluczania dostawców były oparte na obiektywnych kryteriach technicznych i certyfikacji, co zapewni uczciwe i efektywne rozwiązania, które nie będą nadmiernie obciążać polskich przedsiębiorstw.	Wyjaśnienie uwagi Kwestia certyfikacji może być niewystarczająca przy identyfikacji wszystkich zagrożeń jakie stwarza dostawca.
19.	Inet group	Uwaga ogólna	Działając w imieniu firmy Inet Group spółka z ograniczoną odpowiedzialnością, w związku z opublikowanym w dniu 24 kwietnia 2024 roku projektem ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw ¹ , zwracamy się ze stanowiskiem i wnioskiem o dokonanie zmian w Projekcie, które spowodują, że Projekt nie będzie swym zakresem szerszy niż Dyrektywa NIS2. iNET powstała jako grupa, która jest odpowiedzią na rosnące zapotrzebowanie klientów na wysokiej jakości usługi transmisji danych, w tym szerokopasmowy dostęp do Internetu. W założeniu iNET ma stanowić alternatywę dla wielkich telekomów istniejących na rynku, koncentrując się na integracji lokalnych firm telekomunikacyjnych, podwyższaniu jakości usług, minimalizowaniu kosztów. Analizując treść przepisów Projektu trzeba stwierdzić, że będzie on miał znaczny wpływ na wiele branż, w między innymi tym na obszar działalności iNET. Jak zostało wyżej wskazane jedną z głównych idei iNET jest zapewnienie alternatywy na rynku, podwyższenie jakości usług, minimalizacja kosztów. Z zaniepokojeniem jednak stwierdzamy, że z Projektu wynika, że „uderzy” on w wielu przedsiębiorców, nakładając na nich obowiązki, które będą niezwykle kosztowne. Przejrzeliśmy Ocenę Skutków Regulacji pod kątem kosztowym, ale niestety nie znaleźliśmy tam analizy, która by wskazywała jakie będą konsekwencje finansowe dla przedsiębiorców wdrożenia i utrzymania obowiązków zgodnie z Projektem. A takie konsekwencje finansowe i to znaczne będą na pewno. Wystarczy chociażby odwołać się do obowiązku przeprowadzania cyklicznego co 2 lata	Uwaga częściowo uwzględniona Dyrektywa NIS2 przewiduje okresowy audyt dla podmiotów kluczowych. Wymogi dotyczące audytu dla podmiotów kluczowych zostaną złagodzone. Część sektorów zostanie przeniesiona do sektorów ważnych. Projekt nie przewiduje natychmiastowego wycofania sprzętu, tylko nakazuje wycofanie w określonym czasie.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			audytu. Niewątpliwie będzie to stanowić znaczne obciążenie zarówno finansowe jak i administracyjne dla przedsiębiorców, a taki cykliczny obowiązek z dyrektywy NIS2 nie wynika. Jedną z kluczowych regulacji, na którą jednak naszym zdaniem należy zwrócić uwagę, jest mechanizm Dostawcy Wysokiego Ryzyka (ang. HRV – High Risk Vendor). Zakłada on, że Minister ds. informatyzacji decyzją administracyjną będzie mógł uznać dany podmiot za Dostawcę Wysokiego Ryzyka, co będzie skutkowało obowiązkiem wycofania i zakazu nabywania sprzętu, oprogramowania, procesów ICT przez podmioty kluczowe oraz ważne. Dla przedsiębiorców będzie to znaczące obciążenie, ponieważ nie zostały przewidziane żadne rekompensaty. Wątpliwości budzi sam proces uznania za HRV, ponieważ jedną z przesłanek jest kryterium nietechniczne państwa pochodzenia spoza UE lub NATO. Ocena ryzyka dostawcy na podstawie takiego kryterium jest skrajnie subiektywna i wobec tego z dużym prawdopodobieństwem można przewidywać, że zahamuje wiele procesów inwestycyjnych w nowe technologie. To natomiast już bezpośrednio przełoży się na dostawców usług cyfrowych, którzy mając ryzyko inwestycyjne, którego nie da się zaakceptować z uwagi na jego niemierzalność, będą zmuszeni do korzystania z innych, znacznie droższych dostawców, co przełoży się na niebagatelny wzrostu kosztów i cen świadczonych usług do klienta końcowego. W związku z powyższym jako iNET, firma, która w swych naczelnych wartościach stawia na dywersyfikację, pozwalającą na obniżenie kosztów i większą jakość świadczonych usług, czujemy się w obowiązku stanowczo wyrazić krytyczne stanowisko dla takiego kształtu proponowanych regulacji. W związku z powyższym zwracamy się do Pana Ministra z wnioskiem, żeby z Projektu zostały usunięte wszelkie obowiązki i kryteria nietechniczne, niewynikające z Dyrektywy NIS2, a ocena ryzyka była oparta na kryteriach technicznych, w szczególności certyfikacji. Wierzymy, że tylko w taki sposób będzie można w dalszym ciągu funkcjonować na rynku w Polsce w ramach swobodnej działalności gospodarczej opartej na zasadzie konkurencyjności. Zwracamy uwagę, że nakładanie na przedsiębiorców nowych obowiązków niewynikających z Dyrektyw NIS2 i mających nietechniczny charakter w naszej ocenie nie przyczyni się do poprawy bezpieczeństwa cybernetycznego, ale do upadku wielu przedsiębiorców i znacznego wzrostu cen dla odbiorców końcowych, co przecież nie jest celem dyrektywy NIS2. Pozostając do dyspozycji, uprzejmie prosimy o wnikliwą analizę wyżej podniesionych kwestii.	
20.	ISAC Kolej	Uwaga ogólna	Od kilku miesięcy trwały rozmowy dotyczące przyszłych sektorowych CSIRT-ów. Spotykaliśmy się wielokrotnie ze stwierdzeniem, że sektorowe CSIRT-y będą musiały obejmować kompletne sektory, co w przypadku sektora transportu podzielonego na cztery podsektory dedykowane różnym rodzajom transportu stwarzałoby dodatkowe poważne wyzwania. Poszczególne rodzaje transportu narażone są na odmienne ryzyka techniczne i eksploatacyjne, a także stosują odmienne zarówno technicznie jak i funkcjonalnie rozwiązania cyfrowe. Dlatego od początku wspomnianych rozmów członkowie ISAC-Kolej zawsze stali na stanowisku, że transport kolejowy powinien posiadać własny CSIRT sektorowy. Proponowane zapisy to umożliwiają i chcielibyśmy, aby tak pozostało.	Wyjaśnienie uwagi Potwierdzamy, że jest taka możliwość. Decyzja będzie należała do organu właściwego do spraw cyberbezpieczeństwa.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

21.	ISAC Kolej	Uwaga ogólna	W dyrektywie NIS2, podobnie jak w dyrektywie NIS, w wersji polskiej nasz podsektor określony jest jako „transport kolejowy”, ale w wersji angielskiej określony jest jako podsektor „rail” sektora „transport”. Ta drobna z pozoru różnica ma poważne konsekwencje w odniesieniu do zakresu zastosowania regulacji. Określenie „railway transport” oznacza „transport kolejowy”, a określenie „rail transport” transport szynowy w tym kolejowy. Określenie „rail transport” wskazuje więc, że zakres zastosowania powinien obejmować także metro i tramwaje. Jednocześnie przyznać należy, że rodzaje podmiotów w podsektorze zdefiniowane zostały w odniesieniu do regulacji UE dedykowanych dla kolei i nieobjmujących innych rodzajów transportu szynowego. Kwestię tą wskazujemy więc jako istotną do rozstrzygnięcia w ramach polskiego procesu legislacyjnego.	Wyjaśnienie uwagi Z uwagi na to, że dyrektywa NIS2 odnosi się do transportu kolejowego pozostawiono aktualne brzmienie przepisu.
22.	ISAC Kolej	Uwaga ogólna	W proponowanych zapisach brak jest jednolitości podejścia w odniesieniu do wskazywania tzw. organów właściwych. W przypadku części sektorów/podsektorów wskazane są właściwe ministerstwa, a w przypadku niektórych urzędy centralne odpowiedzialne za poszczególne rynki regulowane (KNF, UKE). Chcielibyśmy zwrócić Państwa uwagę, na fakt, że transport kolejowy jest takim właśnie rynkiem. Rolę regulatora i zarazem organu krajowego odpowiedzialnego za bezpieczeństwo kolei pełni Urząd Transportu Kolejowego UTK. W ramach swoich obowiązków wynikających z dyrektywy UE (dyrektywy RSD) w sprawie bezpieczeństwa kolei (2016/789) UTK daje, przedłuża, zawiesza i cofa certyfikaty bezpieczeństwa przewoźnikom i autoryzacje bezpieczeństwa zarządom infrastruktury – tym przewoźnikom i zarządom, których definicje wskazane zostały w dyrektywie NIS2, a wcześniej NIS przy określeniu rodzajów podmiotów krytycznych w podsektorze. Zaznaczyć dodatkowo należy, że przewoźnicy i zarządcy na bazie Ustawy o transporcie kolejowym (UoTK) są zobowiązani do ustanowienia i utrzymywania Systemów Zarządzania Bezpieczeństwem SMS, zgodnie z dyrektywą RSD, natomiast dotychczas nieliczni byli zobowiązani, na bazie Ustawy KSC, a obecnie w praktyce niemal wszyscy będą zobowiązani, po zmianie KSC wdrażającej dyrektywę NIS2, do ustanowienia i utrzymywania Systemów Zarządzania Bezpieczeństwem Informacji SZBI, zgodnie z dyrektywą NIS/NIS2. Zarówno systemy SMS jak i SZBI to rozbudowane regulacje wewnętrzne tworzone i doskonalone według zasad analizy, oceny i akceptacji ryzyka przy uwzględnieniu częstotliwości i spodziewanych skutków materializacji zagrożeń. Uwzględniając to, że SMS obejmują także ryzyka cyfrowe, w szczególności te związane z cyfrowymi systemami eksploatacyjnymi, a regulator rynku odpowiada za nadzór nad SMS i bezpieczeństwem systemu kolei, naturalnym wyborem dla podsektora byłoby wskazanie UTK jako organu właściwego. Pozytywne konsekwencje takiego podejścia widać nawet w samej propozycji zmiany ustawy KSC – nowy przedsiębiorca telekomunikacyjny zgłaszając się do UKE musi zadeklarować czy jego zdaniem podlega pod KSC, a w przypadku nowego przewoźnika brak jest takiego wymagania. Może to skutkować np. co najmniej kilkumiesięcznym świadczeniem usług przewozowych bez dbałości o cyberbezpieczeństwo.	Wyjaśnienie uwagi Minister właściwy do spraw transportu nadzoruje podsektor transportu kolejowego pod kątem cyberbezpieczeństwa od kilku lat i ma już stosowne doświadczenie. Zmiana w tym zakresie nie jest zasadna.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

23.	ISAC Kolej	Uwaga ogólna	Dyrektywy NIS oraz NIS2 bez wątpliwości obejmują zarówno systemy informacyjne IT jak i systemy eksploatacyjne OT. Proponowane zapisy KSC nie są w tym zakresie precyzyjne. W uwagach szczegółowych proponujemy konkretny zapis.	Wyjaśnienie uwagi Systemy OT są także objęte projektem ustawy. Definicja systemu informacyjnego ma objąć także systemy OT.
24.	ISAC Kolej	Uwaga ogólna	Zapisy w art. 8. ust. 1 przewidują konieczność uwzględniania zapisów norm ISO/IEC 27001, ISO/IEC 62443, ISO/IEC 22301, natomiast w art. 15 mowa jest o „audycie bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi”. Budzi to dwie istotne wątpliwości. Po pierwsze większość przewoźników i zarządców kolejowych wykorzystuje dziesiątki i setki systemów cyfrowych, więc audyt powinien obejmować nie jeden system a alternatywnie ogół systemów, wybrane systemy lub system wskazany przez właściwy organ. Po drugie istnieje obawa, że audytorzy powołując się na art. 8. ust. 1 żądać będą certyfikatów na poszczególne normy. Europejska praktyka w zakresie dopuszczania rozwiązań technicznych z wykorzystaniem jakościowych modułów oceny zgodności wskazuje, że w ramach audytu potwierdza się stosowanie systemu jakości dla konkretnego wyrobu weryfikując system zarządzania jakością w węższym zakresie, jeśli jest on objęty aktualnym certyfikatem systemu zarządzania jakością lub w szerszym zakresie, jeśli nie jest. Odzworowując to podejście należy zastrzec w art. 8, że potwierdzenie uwzględniania przez podmioty właściwych zapisów przywołanych norm nie wymaga certyfikacji na zgodność z tymi normami, szczególnie że w poszczególnych sektorach/podsektorach obowiązują także regulacje i normy sektorowe, które nie są w pełni spójne z przywołanymi normami. Art. 8. ust. 1 należy uzupełnić o stwierdzenie, że „Właściwy dobór wymagań z przedmiotowych norm zapewniający komplementarne stosowanie wymagań tych norm i regulacji branżowych oceniane jest w ramach audytów, o których mowa w art. 15 i nie wymaga certyfikowania podmiotów lub systemów na przywołane normy.”	Uwaga nieuwzględniona Projekt nie wymaga obowiązkowej certyfikacji na konkretne normy. Należy spełnić wymagania ustawy, a nie konkretnej normy.
25.	ISAC Kolej	Uwaga ogólna	Proponowane zapisy mają ograniczyć wykorzystywanie potencjalnie niebezpiecznych „technologii informacyjno-komunikacyjnych”. Jednocześnie nie uwzględnia się takich ograniczeń w odniesieniu do środków transportu, które obecnie w bardzo szerokim zakresie wykorzystują rozwiązania cyfrowe. W dobie postępującej cyfryzacji środków transportu (np. wdrażania cyfrowych sprzęgów w pociągach towarowych przewożących najróżniejsze ładunki) należy rozważyć rozszerzenie stosowania zapisów ograniczających wykorzystywanie potencjalnie niebezpiecznych technologii.	Wyjaśnienie uwagi Postępowanie w sprawie uznania za dostawcę wysokiego ryzyka czy badanie sprzętu lub oprogramowania z art. 33 także odnoszą się do systemów informacyjnych w transporcie.
26.	ISAC Kolej	Uwaga ogólna	Zarządcy i przewoźnicy kolejowi podobnie jak inne podmioty świadczące usługi transportowe zależą od łańcucha dostaw. Jednak w przeciwieństwie do transportu drogowego producenci pojazdów kolejowych nie zostali wskazani w polskiej wersji dyrektywy i co za tym idzie w proponowanych zapisach ustawy. Użyte w angielskiej wersji określenie „Manufacture of motor vehicles, trailers and semi-trailers” przetłumaczone na „produkcja pojazdów samochodowych, przyczep i naczep” odnosi się wyłącznie do transportu drogowego, podczas gdy także w przypadku transportu kolejowego mamy pojazdy z napędem (pojazdy z silnikami – pojazdy trakcyjne) i bez napędu (doczepne).	Wyjaśnienie uwagi Produkcja pojazdów kolejowych mieści się w ramach załącznika do dyrektywy NIS2 – załącznik odnosi się także do producentów innych środków transportu określonych w sekcji C 30 klasyfikacji NACE.
27.	ISSA Polska	Uwaga ogólna	Ustawa w całości pomija proces modelowania zagrożeń jednocześnie zobowiązując do prowadzenia procesu analizy ryzyka.	Wyjaśnienie uwagi

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			Modelowanie zagrożeń i modelowanie ryzyka to dwa kluczowe elementy cyberbezpieczeństwa, które mają różne cele w ocenie i zarządzaniu zagrożeniami oraz podatnościami. Modelowanie zagrożeń polega na systematycznym identyfikowaniu, dokumentowaniu i analizowaniu potencjalnych zagrożeń dla systemu lub organizacji. Skupia się na zrozumieniu różnych sposobów, w jakie atakujący mogą naruszyć bezpieczeństwo systemu, identyfikowaniu podatności oraz określaniu potencjalnych wektorów ataku. Celem modelowania zagrożeń jest proaktywne przewidywanie i zapobieganie naruszeniom bezpieczeństwa poprzez rozważenie różnych scenariuszy zagrożeń i ich potencjalnego wpływu na system. Z drugiej strony, modelowanie ryzyka koncentruje się na ocenie prawdopodobieństwa, że zagrożenie wykorzysta podatność, oraz potencjalnego wpływu lub szkód, jakie mogą wyniknąć z takiego zdarzenia. Modelowanie ryzyka wykracza poza identyfikowanie zagrożeń, aby także ocenić prawdopodobieństwo ich materializacji oraz nasilenie ich konsekwencji. Obejmuje ono kwantyfikację i priorytetyzację ryzyk na podstawie takich czynników jak prawdopodobieństwo wystąpienia, wpływ na zasoby oraz skuteczność istniejących kontroli w łagodzeniu tych ryzyk. Podczas gdy modelowanie zagrożeń skupia się na zrozumieniu natury potencjalnych zagrożeń i sposobów ich wykorzystania, modelowanie ryzyka zagłębia się bardziej w ocenę ogólnego stanu ryzyka organizacji, biorąc pod uwagę prawdopodobieństwo manifestacji zagrożeń oraz potencjalne konsekwencje ich materializacji. Modelowanie zagrożeń dotyczy bardziej identyfikacji i zrozumienia konkretnych zagrożeń, podczas gdy modelowanie ryzyka dotyczy oceny szerszego krajobrazu ryzyka i podejmowania świadomych decyzji dotyczących strategii łagodzenia ryzyka. W istocie, modelowanie zagrożeń to proaktywne ćwiczenie, które pomaga organizacjom przewidywać i zapobiegać incydentom bezpieczeństwa poprzez identyfikację i adresowanie podatności, zanim zostaną one wykorzystane przez atakujących. Należy również podkreślić, że ocena prawdopodobieństwa wystąpienia danego zdarzenia negatywnie oddziałującego na aplikację, system lub całość organizacji nie ma żadnego wpływu na jego materializację w trakcie cyklu życia ocenianego zasobu. Model ryzyka ma natomiast realne przełożenie na podniesienie cybernetycznej odporności ocenionego zasobu. Rekomendowane jest wprowadzenie do Ustawy obowiązku modelowania zagrożeń w zakresie w jakim jest wymagane prowadzenie analizy ryzyka. Modelowanie zagrożeń opisane jest, dla przykładu, w wytycznych NIST SP 800-154. (Analiza ryzyka ujęte jest w art. 53B projektu Ustawy Analogicznie dla ochrony fizycznej art. 10 projektu Ustawy.	Dyrektywa NIS2 wprost nie odnosi się do procesu modelowania zagrożeń, stąd nie został on ujęty w projekcie.
28.	Polskie Stowarzyszenie Fotowoltaiki	Uwaga ogólna	I. Główne wnioski – obowiązki w zakresie cyberbezpieczeństwa mające zastosowanie do podmiotów kluczowych oraz ważnych, jak i dostawców rozwiązań [Nadregulacja względem wdrażanej dyrektywy NIS2] 1. Rozwiązania zakładane w Projekcie w wielu obszarach (wskazanych szczegółowo poniżej) stanowią istotną nadregulację względem wymogów Dyrektywy NIS2, która nie przewiduje nakładania tak daleko idących środków w celu zapewnienia cyberbezpieczeństwa podmiotów objętych jej zakresem.	Wyjaśnienie uwagi Zgodnie z dyrektywą NIS2 wszystkie podmioty kluczowe i podmioty ważne są obowiązane dbać o bezpieczeństwo łańcuchów dostaw. Stąd też rozszerzono zakres postępowania w sprawie uznania za dostawcę wysokiego ryzyka na wszystkie sektory.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

		2. Biorąc pod uwagę skalę podmiotów objętych proponowanymi w Projekcie rozwiązaniami (szacuje się, że regulacja ma dotyczyć ponad 38 tys. podmiotów w Polsce), nakładanie tak daleko idących obowiązków, które będą wiązać się z koniecznością wdrożenia dodatkowych procesów, procedur, zatrudnienia dodatkowych zasobów ludzkich i zakupu usług firm trzecich, stanowić może istotne utrudnienie dla prowadzenia działalności gospodarczej w Polsce. 3. Regulacje przewidziane w Projekcie również – z wysokim prawdopodobieństwem – przyczynią się do braku pewności prowadzenia działalności gospodarczej oraz negatywnie wpłyną na konkurencyjność polskich przedsiębiorstw względem innych państw Unii Europejskiej. W szczególności w odniesieniu do szeregu podmiotów, które dotychczas nie były objęte podobnymi wymogami w zakresie cyberbezpieczeństwa, obowiązki te stanowić będą istotne wyzwanie w zakresie ich wdrożenia i duże utrudnienie w prowadzeniu działalności biznesowej w naszym kraju. 4. Należy przy tym wskazać, że Dyrektywa NIS2 jest dyrektywą przewidującą minimalną harmonizację, w związku z tym polski ustawodawca posiada możliwość zapewnienia niezbędnego poziomu cyberbezpieczeństwa podmiotów objętych zakresem tej dyrektywy, przy jednoczesnym zachowaniu warunków korzystnych dla prowadzenia działalności regulowanej i zakupu usług dostawców trzecich, które są niezbędne w kontekście prowadzenia tej działalności. Analiza projektu ustawy wskazuje jednak, że polski rząd postanowił przyjąć w tym zakresie bardzo rygorystyczne i niespotykane w innych krajach UE podejście. [Wpływ na transgraniczną działalność w energetyce] 5. Jak wskazuje sama Dyrektywa NIS2, wymogi nałożone przez jedno państwo członkowskie, które różnią się od wymogów nałożonych przez inne państwo członkowskie lub nawet są z nimi sprzeczne, mogą w istotny sposób wpływać na transgraniczną działalność poszczególnych podmiotów, oferujących towary transgranicznie. W odniesieniu do sektora energetyki, należy mieć na uwadze, iż odmienne regulacje w zakresie cyberbezpieczeństwa pomiędzy poszczególnymi krajami członkowskimi mogą nie tylko opóźniać, ale i utrudniać proces transgranicznych przepływów energii elektrycznej. [Dostawcy wysokiego ryzyka i możliwość żądania wycofania poszczególnych produktów] 6. Również dyskrecjonalne uprawnienia, wykraczające poza wymogi Dyrektywy NIS2, przewidziane dla organów właściwych w sprawach cyberbezpieczeństwa mogą powodować szereg negatywnych konsekwencji dla podmiotów wchodzących w skład krajowego systemu cyberbezpieczeństwa, a więc podmiotów posiadających szczególne znaczenie dla funkcjonowania naszego państwa. [Koszty przedsiębiorców związane z wycofaniem sprzętu lub oprogramowania] 7. Jednym z najważniejszych wyzwań nowego Projektu, istotnie wykraczającym poza wymogi Dyrektywy NIS2 będzie dla przedsiębiorców obowiązek wymiany sprzętu i rezygnacja z usług tzw. dostawców wysokiego ryzyka. O tym, jaki podmiot spełnia kryteria uznania za dostawcę wysokiego ryzyka będzie decydował minister właściwy do spraw informatyzacji w drodze decyzji administracyjnej oraz w oparciu o bardzo ogólne przesłanki. Wskazane w decyzji zakresy produktów ICT, rodzaje usług ICT lub konkretne procesy ICT pochodzące od dostawcy wysokiego ryzyka, będą	Pozostała część uwagi została wyjaśniona w odniesieniach do uwag szczegółowych.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

		musiały być wycofane z przedsiębiorstw. Oznacza to konieczność rezygnacji z produktów i usług, na które dane przedsiębiorstwo poniosło niekiedy istotne nakłady i które to produkty lub usługi są niezbędne z punktu widzenia prowadzenia przez daną firmę działalności. [Inne istotne elementy Projektu stanowiące nadregulację względem Dyrektywy NIS2] 8. Inne istotne przykłady nadregulacji w ramach Projektu, względem rozwiązań przewidzianych w ramach Dyrektywy NIS2, to m. in.: 8.1. uznanie dostawców usług zarządzanych w zakresie cyberbezpieczeństwa za PW niezależnie od ich wielkości (art. 5 KSC wg Projektu); 8.2. możliwość uznania mikro i małych przedsiębiorców za PK i PW w oderwaniu od ścisłych i możliwych do obiektywnej weryfikacji kryteriów wyznaczonych zgodnie z dyrektywą NIS2 (art. 7c KSC wg Projektu); 8.3. wprowadzenie stosunkowo krótkich terminów na wdrożenie wymagań ustawy przez podmioty podlegające automatycznej kwalifikacji jako PK lub PW, jak również te wyznaczone w drodze decyzji organu właściwego ds. cyberbezpieczeństwa (art. 7c ust. 6 KSC wg Projektu); 8.4. zakres wymagań względem systemu zarządzania bezpieczeństwem informacji oraz środków technicznych i organizacyjnych jakie PK lub PW powinien podjąć zgodnie z art. 8 ust. 1 KSC wg Projektu wykracza poza zakres określony w Dyrektywie NIS2 (art. 8 KSC wg Projektu) 8.5. Zakres wymagań względem systemu zarządzania bezpieczeństwem informacji jest jednakowy niezależnie od faktycznych okoliczności dot. danego podmiotu lub specyfiki prowadzonej przez nich działalności gospodarczej jak również ekspozycji na ryzyko zw. z cyberbezpieczeństwem, które w zależności od sektora jest różne (art. 8 KSC wg Projektu); 8.6. w przypadku wielu przedsiębiorstw, które będą kwalifikowane jako PK lub PW, realizacja wszystkich obowiązków określonych w art. 8 ust 1 KSC wg Projektu może stanowić istotne wyzwanie oraz utrudnienie w prowadzeniu działalności biznesowej. 8.7. projekt odnosi się ogólnie do dostawcy sprzętu lub oprogramowania, którym w rozumieniu Projektu jest również producent oraz importer (pośredni dostawca), podczas gdy Dyrektywa NIS2, przewiduje w art. 21 ust. 3 obowiązek uwzględnienia podatności charakterystycznych dla każdego bezpośredniego dostawcy i usługodawcy (art. 8 ust. 4 KSC wg Projektu); 8.8. obowiązek uwzględnienia dodatkowych wymagań dla systemu zarządzania bezpieczeństwem informacji przyjętych w drodze rozporządzenia Rady Ministrów dla danego rodzaju działalności, podczas gdy Dyrektywa NIS2 przyznaje wyraźne kompetencje Komisji w tym zakresie (art. 8a KSC wg Projektu); 8.9. dyrektywa NIS2 zobowiązuje do zapewnienia, aby osoby fizyczne odpowiedzialne za PK i PW mogły być pociągnięte do odpowiedzialności za niewywiązanie się z obowiązku zapewnienia przestrzegania niniejszej dyrektywy. Dyrektywa NIS2 nie wskazuje jednak odrębnego katalogu obowiązków wobec tych osób niezależnych od obowiązków PK lub PW (z wyłączeniem zapewnienia, że odbywają one regularne szkolenia z zakresu cyberbezpieczeństwa – vide art. 20 ust. 2 Dyrektywy NIS2) (art. 8c KSC wg Projektu)	

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

		8.10. nałożenie obowiązku uczestnictwa w wymianie informacji dotyczących cyberbezpieczeństwa stanowi nadregulację względem wymogów wynikających z Dyrektywy NIS2 (vide. art. 30 dot. dobrowolnego zgłaszania ważnych informacji). (art. 8h KSC wg Projektu) 8.11. zakres informacji jakie PK i PW jest zobowiązany do przekazania wraz ze zgłoszeniem incydentu wykracza poza zakres określony w art. 23 ust. 4(b) Dyrektywy NIS2 i obejmuje m.in. przyczynę zaistnienia incydentu poważnego; informacje o podjętych działaniach zapobiegawczych; informacje o podjętych działaniach naprawczych. Informacje te powinny zgodnie z Dyrektywą NIS2 być uwzględnione w sprawozdaniach, w szczególności sprawozdaniu końcowym. Wskazanie wszystkich informacji określonych w art. 12 ust. 3 KSC wg Projektu w terminie tam określonym może nie być realnie możliwe. (art. 12 KSC wg Projektu). 8.12. postanowienia Dyrektywy NIS2 nie obejmują obowiązku zapewnienia uprawnienia CSIRT do dokonywania badań urządzeń informatycznych lub oprogramowania, a jedynie przewidują wśród ich zadań monitorowanie i analizowanie cyberzagrożeń, podatności i incydentów na poziomie krajowym. Działania te wykraczają również poza pojęcie aktywnego, nieinwazyjnego skanowania publicznie dostępnych sieci i systemów informatycznych podmiotów kluczowych i ważnych (art. 11 ust. 3 Dyrektywy NIS2). (art. 33 KSC wg Projektu). 8.13. Przepisy Projektu w postanowieniach dotyczących odpowiedzialności PK, PW i osób fizycznych zarówno wykraczają istotnie poza zakres Dyrektywy NIS2 jak również zawierają nieprecyzyjne określenia (art. 53 KSC wg Projektu) 8.14. Przepisy dotyczące postępowania w sprawie uznania za dostawcę wysokiego ryzyka oraz poleceń zabezpieczających – w tym zakresie patrz uwagi w pkt 9 poniżej oraz szczegółowe uwagi w rozdziale IV. 8.15. Zakres obowiązków, niewykonanie których skutkuje nałożeniem kary pieniężnej wykracza znacząco poza zakres określony w Dyrektywie NIS2 (naruszenie obowiązków wskazanych w art. 21 i 23 Dyrektywy NIS2) (art. 73 i następne KSC wg Projektu). [Regulacje implementowane z poprzednich projektów ustaw nowelizujących KSC] 9. Projekt stanowi osiemną wersję nowelizacji KSC. Ostatnia wersja, tj. Projekt z 3 lipca 2023 r. w związku z zakończeniem prac Sejmu Rzeczypospolitej Polskiej IX kadencji został wycofany spod obrad. Aktualnie procedowany Projekt, przeciwnie do Projektu z 3 lipca 2023 r. ma na celu, w intencji wnioskodawców, implementację Dyrektywy NIS2 i w znacznej mierze różni się od projektu z 3 lipca 2023 r. Niemniej jednak, w Projekcie w niemalże niezmiennym brzmieniu powielone zostały instytucje proponowane w poprzedniej wersji ustawy, a które spotkały się z szeroką krytyką w trakcie konsultacji społecznych oraz negatywnym odbiorem przedstawicieli rynku: 9.1. ocena bezpieczeństwa systemów informacyjnych – proponowane w Projekcie art. 36a-36b wprowadzają uprawnienie do przeprowadzenia oceny bezpieczeństwa systemów informacyjnych wykorzystywanych przez podmioty krajowego systemu cyberbezpieczeństwa w celu identyfikacji podatności. Proponowana regulacja obejmuje szeroki zakres systemów informacyjnych, które mogą zostać poddane ocenie bez uzyskania zgody podmiotu użytkującego, w tym podmiotu kluczowego i	

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

		podmiotu ważnego. Co istotne, odstępstwo od zasady dobrowolności takiej oceny bezpieczeństwa nie było przewidziane Projekcie z 3 lipca 2023 r.; 9.2. postępowanie w sprawie uznania za dostawcę wysokiego ryzyka – uwagi odnośnie do wpływu tej regulacji zostały wskazane powyżej. Proponowane w Projekcie art. 67b – 67f w nieznaczny tylko sposób różnią się od treści odpowiednich postanowień Projektu z 3 lipca 2023 r., które spotkały się z szeroką krytyką przedstawicieli rynku. 10. Ponadto, do Projektu włączono propozycję nowych przepisów art. 67g i nast. nadających ministrowi właściwemu ds. informatyzacji kompetencje do wydania w drodze decyzji tzw. polecenia zabezpieczającego na wypadek incydentu krytycznego. Adresatem polecenia zabezpieczającego jest nieograniczony zakres odbiorców. Polecenie zabezpieczające zawiera obowiązek określonego zachowania zmniejszającego skutki incydentu krytycznego lub zapobiegającego jego rozprzestrzenianiu się. Instytucja polecenia zabezpieczającego była przedmiotem poprzednich projektów ustaw zmieniających KSC, w szczególności projektu z 8 września 2020 r. Pomimo jej wycofania z Projektu z 3 lipca 2023 r. na skutek szerokiej krytyki środowisk branżowych, instytucja ta ponownie została wprowadzona do Projektu. II. Główne wnioski – wpływ Projektu na sektor energetyczny 1. Jedną z podstawowych modyfikacji wprowadzanych Projektem w stosunku do obecnie obowiązującej regulacji jest rozszerzenie kręgu podmiotów, w stosunku do których omawiana regulacja będzie miała zastosowanie. Niemniej jednak, katalog podmiotów uznawanych odpowiednio za PK i PW znacznie odbiega od tego, określonego w Dyrektywie NIS2 w zakresie, w jakim rozszerza katalog podmiotów uznawanych za PK. W konsekwencji, przyjęcie takiej regulacji może skutkować powstaniem o wiele bardziej restrykcyjnego środowiska prawnego dla podmiotów z sektora energetycznego, w porównaniu do innych państw członkowskich UE. Powyższe może mieć wpływ na obniżenie efektywności operacyjnej kluczowych podmiotów z sektora energetycznego lub, w skrajnych wypadkach, zawieszenie działalności przez te podmioty na terenie kraju z uwagi na zbyt restrykcyjne wymogi prawne. 2. Terminy wycofania sprzętu lub oprogramowania ICT objętego decyzją o uznaniu za dostawcę wysokiego ryzyka są niewspółmierne do okresu użytkowania oraz standardów sektora energetycznego. W przypadku wielu środków trwałych wykorzystywanych w sektorze energetyki, okres ich amortyzacji może wynosić do 15 lat. Projektowana regulacja zakłada obowiązek ich wycofania w ciągu 7, a niekiedy nawet 4 lat. W efekcie, podmioty zobowiązanie będą do wycofania produktów przy jednoczesnym poniesieniu dodatkowych kosztów związanych z nabyciem produktów zamiennych. 3. Rygorystyczne podejście do kwestii cyberbezpieczeństwa przewidziane w Projekcie KSC może mieć szczególnie negatywny wpływ na sektor energetyczny w Polsce – a więc jeden z najbardziej wrażliwych sektorów gospodarki, zarówno z perspektywy przedsiębiorstw jak i konsumentów. Trudno przewidzieć, jakie skutki ekonomiczne może mieć nałożenie tak daleko idących obowiązków na przedsiębiorstwa sektora energetycznego. Wydaje się, że projektodawcy w ogóle nie uwzględnili	

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			w ramach przygotowanej Oceny Skutków Regulacji specyfiki tej branży i wpływu projektu na transformację energetyczną w Polsce. Rozwiązania przewidziane w projekcie, takie jak wspomniane uznanie za dostawcę wysokiego ryzyka, czy możliwość ingerencji w urządzenia i oprogramowanie w ramach audytów bezpieczeństwa IT, mogą przyczynić się do zakłócenia pracy, czy też wykluczenia poszczególnych urządzeń. 4. Jako przykład można podać inteligentne systemy opomiarowania (tzw. smart metering), których głównym celem jest poprawa zrównoważonego rozwoju całego systemu energetycznego. Działanie inteligentnych systemów opomiarowania opiera się na wykorzystaniu wielu komponentów technologicznych, w związku z czym istnieje potencjalne ryzyko obowiązku wycofania poszczególnych produktów ICT z użytku przez dany podmiot. W konsekwencji, projektowane zmiany stwarzają ryzyko naruszenia integralności danych pozyskanych w ramach inteligentnych systemów opomiarowania, a zakłócenie pracy urządzeń może skutkować destabilizacją dostaw energii elektrycznej. 5. Następnym przykładem projektowania regulacji w oderwaniu od specyfiki danego sektora, na który regulacja ta będzie oddziaływać jest możliwość stosowania poleceń zabezpieczających przez ministra właściwego ds. informatyzacji, którym nadano rygor natychmiastowej wykonalności. Projektowane zmiany rodzą potencjalne ryzyko, że wprowadzenie możliwości wydawania poleceń zabezpieczających posiadających rygor natychmiastowej wykonalności, oprócz zaburzenia prowadzenia działalności gospodarczej przez określone podmioty, obciążania tych podmiotów dodatkowymi kosztami, może także pośrednio wpływać na ciągłość dostaw energii elektrycznej. W konsekwencji, omawiana regulacja będzie oddziaływać nie tylko na sektor energetyczny, ale również na określonych odbiorców energii elektrycznej.	
29.	Stowarzyszenia FAIR MARKET INSTITUTE	Uwaga ogólna	działając w imieniu w imieniu Stowarzyszenia Fair Market Institute, jako podmiotu założonego w celu monitorowania zachowań rynkowych oraz wspierania wszelkich działań zmierzających do ograniczenia nieuczciwych praktyk gospodarczych, jak również mających na celu zwiększenie konkurencyjności uczciwych przedsiębiorców, w związku z prowadzonymi przez Ministerstwo konsultacjami publicznymi projektu ustawy o zmianie ustawy o krajowym systemie z 23 kwietnia 2024 r. (nr UC32 w wykazie prac legislacyjnych), niniejszym przedstawiamy stanowisko dotyczące procedowanego projektu z perspektywy zagrożeń dla konkurencji, jakie wiąże się z wprowadzeniem mechanizmu uznania za dostawcę wysokiego ryzyka. Jednocześnie postulujemy, aby Pan Minister w ramach prac legislacyjnych rozważył usunięcie kryteriów politycznych z mechanizmu identyfikacji dostawców wysokiego ryzyka i zastąpienie ich wprowadzeniem certyfikacji dostawców łańcuchów dostaw w możliwie najszerszym zakresie uwzględniając rozwiązania wynikające z opublikowanego projektu ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa z 21 maja 2024 r. (nr UC42 w wykazie prac legislacyjnych) Projektowane rozwiązania a zagrożenia dla konkurencji Uznanie za dostawcę wysokiego ryzyka (ang. <i>High Risk Vendor</i>, <i>HRV</i>) następować ma na podstawie decyzji Ministra ds. informatyzacji, który wydaje ją w oparciu o opinię Kolegium do spraw	Uwaga nieuwzględniona Aby zidentyfikować dostawcę wysokiego ryzyka należy wziąć pod uwagę zarówno kwestie techniczne jak i nietechniczne. Tylko wtedy uzyskamy pełny obraz działalności danego dostawcy.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

		Cyberbezpieczeństwa. Wydając opinię Kolegium bierze pod uwagę przesłanki wskazane w proponowanym art. 67b ust. 11 UKCS. Należy zwrócić uwagę, że kryteria te, poza kryteriami technicznymi i obejmują także kryteria pozatechniczne i subiektywne takie jak np. (i) zagrożenia bezpieczeństwa narodowego o charakterze ekonomicznym, wywiadowczym i terrorystycznym oraz zagrożeń dla realizacji zobowiązań sojuszniczych i europejskich, jakie stanowi dostawca, z uwzględnieniem informacji o zagrożeniach uzyskanych od państw członkowskich lub organów Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, (ii) prawdopodobieństwo z jakim dostawca znajduje się pod kontrolą państwa spoza terytorium Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, (iii) powiązania dostawcy z podmiotami określonymi w załączniku do rozporządzenia Rady (UE) 2019/796 z dnia 17 maja 2019 r. w sprawie środków ograniczających w celu zwalczania cyberataków zagrażających Unii lub jej państwom członkowskim. Tym samym decyzja taka wydawana będzie w oparciu o kryteria pozatechniczne, nie odnoszące się do cech sprzętu i oprogramowania, ale do cech dostawcy, przy czym cechy te i ich natężenie są niemierzalne a stwierdzenie ich występowania opiera się na subiektywnych ocenach organów państwa. (sam zresztą projekt mówi o „prawdopodobieństwie”). Co więcej, projekt posługuje się kryteriami niezwykle ogólnymi – co oznacza „znajdowanie się pod kontrolą państwa”? Cechę tę odnieść można do każdego podmiotu prowadzącego działalność na danym terytorium – w takim czy innym stopniu znajduje się „pod kontrolą państwa”. Decyzja o uznaniu dostawcy sprzętu lub oprogramowania HRV zawierać ma w szczególności wskazanie typów produktów ICT, rodzajów usług ICT lub konkretnych procesów ICT pochodzących od dostawcy sprzętu lub oprogramowania uwzględnionych w postępowaniu w sprawie uznania za dostawcę wysokiego ryzyka. W przypadku wydania takiej decyzji podmioty kluczowe i podmioty ważne (zgodnie z definicją proponowaną w UKCS) mają obowiązek powstrzymania się od wprowadzenia do użytkowania typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT w zakresie objętym decyzją, dostarczanych przez tego dostawcę oraz mają obowiązek wycofać z użytkowania takie typy produktów, usług i procesów, nie później niż 7 lat od dnia ogłoszenia lub udostępnienia informacji o decyzji. Dodatkowo, przedsiębiorcy telekomunikacyjni określani w UKSC, wycofują w ciągu 4 lat typy produktów ICT, rodzaje usług ICT, konkretne procesy ICT wskazane w decyzji i określone w UKSC jako funkcje krytyczne dla bezpieczeństwa sieci i usług. Niezależnie od innych skutków negatywnych planowanej regulacji, należy zwrócić uwagę na potencjalne skutki zmian dla konkurencji na rynkach produktowych. W praktyce, decyzja o uznaniu dostawcy za HRV może eliminować taki podmiot z obrotu rynkowego, także w odniesieniu do produktów, usług i procesów ICT nie objętych decyzją. Niezależnie bowiem od konieczności zaprzestania użytkowania określonych produktów, potencjalni nabywcy mogą, obawiając się wchodzenia w relacje z dostawcą, który został uznany za dostawcę wysokiego ryzyka, zrezygnować z jakichkolwiek kontaktów handlowych z takim podmiotem. Może to prowadzić do ograniczenia konkurencji na danym rynku właściwym, na którym oferowane są procesy, produkty i usługi takiego dostawcy. Proponowana zmiana UKCS wykracza daleko poza sektor ICT. Projekt wskazuje 17 sektorów gospodarki, których dotyczyć będą nowe regulacje, każdy	

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			z tych sektorów jest często podzielony na kilka podsektorów. Oznacza to, że zakresem proponowanych przepisów objętych będzie kilkadziesiąt rynków produktowych i prawie 39 tys. podmiotów. Eliminacja dostawcy z danego rynku będzie oznaczać zakłócenie na nim konkurencji, które to zakłócenie, w zależności od stopnia koncentracji dostawców na danym rynku, może być zakłóceniem o istotnych skutkach. W pewnych przypadkach eliminacja dostawcy uznanego za HRV może prowadzić do powstania na rynkach, na których działa niewielu dostawców, do powstania kolektywnej pozycji dominującej pozostałych dostawców co oznaczać będzie jeszcze dalej idące ograniczenie konkurencji (i zarazem prowadzić do naruszenia prawa). Sektor technologiczny (szczególnie w zakresie sprzętu i oprogramowania) charakteryzuje się wysokimi barierami wejścia (z uwagi na znaczne koszty badań i rozwoju oraz ochronę praw własności intelektualnej) oraz bardzo szybkim postępem technicznym. Działa na nim niewielka liczba dostawców będących w stanie zaoferować nowoczesne i konkurencyjne rozwiązania i produkty, które są w stanie sprostać ciągle rosnącym wymogom odbiorców. Wobec trudności z wejściem nowych dostawców sprzętu komputerowego i oprogramowania na rynek oraz ograniczonymi możliwościami zwiększenia produkcji i dostaw przez istniejących dostawców, może dojść do spowolnienia procesów cyfryzacji wszystkich sektorów polskiej gospodarki (także tych, nieobjętych planowaną nowelizacją UKSC), niemożliwości zaspokojenia popytu oraz wzrostem cen sprzętu i oprogramowania, który by nie wystąpił w warunkach wolnej konkurencji. Posiadanie najnowszych rozwiązań ICT jest warunkiem skutecznego konkurowania na świecie. Zmniejszenie presji konkurencyjnej może spowodować spowolnienie postępu technicznego na tak istotnym dla konkurencyjności polskiej gospodarki rynku produktów i usług ICT, a także znaczny wzrost kosztów ponoszonych użytkowników końcowych. Koszty zmniejszonej konkurencji a także wymiany osprzętu przez podmioty zobowiązane zostaną przeniesione na użytkowników końcowych i konsumentów. Koszty takie mogą być znaczne (należy zauważyć, że Ocena Skutków Regulacji nie podaje żadnych danych w tym zakresie, koncentrując się na kosztach administracji publicznej). Powyższe niekorzystne zjawiska osłabią konkurencyjność polskiej gospodarki oraz zmniejszą ogólny dobrobyt konsumentów. Uzasadnienie projektu ani Ocena Skutków Regulacji proponowanej ustawy nie zawiera analizy skutków planowanych rozwiązań dla konkurencji na rynkach właściwych oraz oszacowania związanych z tym kosztów i ryzyk dla polskiej gospodarki. Tymczasem, jak wskazano powyżej, skutki takie mogą być negatywne i daleko idące.	
30.	Międzynarodowe Centrum Bezpieczeństwa Chemicznego	Uwaga ogólna	W imieniu Międzynarodowego Centrum Bezpieczeństwa Chemicznego (ICCSS) pragnę przekazać nasze uwagi i propozycje dotyczące projektu ustawy o Krajowym Systemie Cyberbezpieczeństwa. ICCSS jest organizacją wiodącą w zakresie promowania i wdrażania standardów cyberbezpieczeństwa w przemyśle, szczególnie w kontekście Przemysłu 4.0. ICCSS regularnie przedkładał propozycje rozwoju i umocnienia krajowego systemu cyberbezpieczeństwa. ICCSS przewodniczył Grupie Zadaniowej ds. Cyberbezpieczeństwa dla Przemysłu 4.0 w ramach Grupy Roboczej ds. Cyberbezpieczeństwa, która nadzorował wdrażanie Krajowego Systemu	Uwaga nieuwzględniona W celu wykonywania zadań z projektu należy posiadać wykwalifikowany personel – nie ma potrzeby wprowadzać dodatkowych przepisów w tym zakresie.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			Cyberbezpieczeństwa przy Ministerstwie Cyfryzacji. ICCSS również kieruje międzynarodowym zespołem, który przygotował unikalne podejście i publikację na temat cyberbezpieczeństwa sektora energii i przemysłu chemicznego. Działania te podkreślają nasze zaangażowanie w rozwój standardów cyberbezpieczeństwa w przemyśle i pokazują nasze doświadczenie w tej dziedzinie. Wprowadzenie – Wdrożenie kwalifikacji w zakresie cyberbezpieczeństwa ważnym elementem realizacji NIS 2. Dyrektywa NIS 2 nakłada na państwa członkowskie obowiązek zapewnienia wysokiego poziomu cyberbezpieczeństwa. Wdrożenie kwalifikacji wynika z szeregu zapisów NIS 2: W szczególności, art. 7 (Krajowa strategia cyberbezpieczeństwa), nakłada na państwa członkowskie w para. 1.h) posiadanie planu, zawierającego kluczowe środki do podniesienia ogólnego poziomu wiedzy obywateli o cyberbezpieczeństwie; w para. 1.f): państwa członkowskie podejmują działania: promujące i rozwijające kształcenie i szkolenie w dziedzinie cyberbezpieczeństwa, umiejętności z zakresu cyberbezpieczeństwa, podnoszenia świadomości oraz inicjatyw badawczo-rozwojowych, a także wytyczne dotyczące dobrych praktyk i kontroli w zakresie cyberhigieny, skierowane do obywateli, zainteresowanych stron i podmiotów. W Art. 11 Dyrektywy, CSIRT promują przyjmowanie i stosowanie wspólnych lub znormalizowanych praktyk, systemów klasyfikacji i systematyki związanych z: a) procedurami obsługi incydentu; b) zarządzaniem kryzysowym; oraz c) skoordynowanym ujawnianiem podatności podkreśla znaczenie wdrażania środków zarządzania ryzykiem cyberbezpieczeństwa. Art. 12 (Skoordynowane ujawnianie podatności i europejska baza danych dotyczących podatności) wymaga zgłaszania incydentów cyberbezpieczeństwa, co wymaga odpowiednich kompetencji. Artykuły 13 i 14 ws. współpracy na poziomie krajowym, unijnym i międzynarodowym, stawiają jako priorytet wymianę informacji o zgłoszeniach incydentów, cyberzagrożeń i potencjalnych zdarzeń dla cyberbezpieczeństwa, co wymaga właściwych kompetencji dla przygotowania takich informacji. Art. 18 nakłada obowiązek oceny rozwoju zdolności w zakresie cyberbezpieczeństwa, co podkreśla potrzebę kwalifikacji i kompetencji. W powyższe trendy wpisują się niedawno dodane kwalifikacje zawodowe w ramach Zintegrowanego Rejestru Kwalifikacji (https://kwalifikacje.gov.pl/aktualnosci/995-trzy-kwalifikacje-zwiazane-z-cyberbezpieczenstwem-wlaczone-do-zskj)	
31.	Międzynarodowe Centrum Bezpieczeństwa Chemicznego	Uwaga ogólna	Wprowadzenie zapisów o konieczności posiadania kwalifikacji w zakresie niezawodności i cyberbezpieczeństwa do krajowej ustawy o cyberbezpieczeństwie jest kluczowe dla zapewnienia wysokiego poziomu ochrony sieci i informacji, w tym sieci przemysłowych. Te kwalifikacje zapewniają specjalistom odpowiednie kompetencje, co przekłada się na lepsze przygotowanie przedsiębiorstw do przeciwdziałania zagrożeniom cybernetycznym i minimalizowanie ich skutków. Włączenie tych zapisów do ustawy wspiera elementy Dyrektywy NIS 2, które podkreślają znaczenie kompetencji, zgłaszania incydentów, szkoleń oraz współpracy międzynarodowej. Dzięki temu krajowy system cyberbezpieczeństwa będzie bardziej efektywny i odporny na rosnące wyzwania w obszarze cyberbezpieczeństwa, w tym w szczególności przemysłowego.	Uwaga nieuwzględniona Aby wykonywać obowiązki zawarte w projekcie ustawy należy posiadać odpowiednio wykwalifikowany personel. W tym celu nie ma konieczności wprowadzania nowych przepisów.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			Deklarujemy gotowość włączenia się i wsparcia resortu cyfryzacji na każdym etapie prac nad przyjęciem ustawy o Krajowym Systemie Cyberbezpieczeństwa.	
32.	Morskie Centrum Cyberbezpieczeństwa Akademia Marynarki Wojennej w Gdyni	Uwaga ogólna	Spółki celowe świadczące usługi SOC Wiele mniejszych podmiotów (samorządy, placówki ochrony zdrowia...) nie jest w stanie samodzielnie budować zespołów SOC. Z różnych powodów nie chcą też korzystać z usług zewnętrznych podmiotów. Wydaje się zasadnym by ustawa <u>sugerowała możliwość powoływania zespołów SOC</u> w postaci np. spółek celowych. Obecnie, na podstawie naszych informacji, podmioty boją się korzystać z tej możliwości nie mając pewności jak rozwiązać kwestie dostępu do tajemnic przedsiębiorstwa.	Uwaga częściowo uwzględniona Wprowadzone zostaną odpowiednie przepisy w projekcie umożliwiające powoływanie zespołów SOC dla podmiotów publicznych.
33.	Morskie Centrum Cyberbezpieczeństwa Akademia Marynarki Wojennej w Gdyni	Uwaga ogólna	Incydenty dostawców usług zarządzanych w zakresie cyberbezpieczeństwa Wydaje się zasadne by zobowiązać dostawców usług zarządzanych w zakresie cyberbezpieczeństwa do informowania o incydentach cyberbezpieczeństwa, które potencjalnie mogły dotknąć podmioty kluczowe i ważne na analogicznych zasadach jak przedstawione w Art. 12. Należy również rozważyć nałożenie na te podmioty analogicznych wymagań bezpieczeństwa jak te nałożone z art. 8 na podmioty kluczowe i ważne.	Wyjaśnienie uwagi Dostawcy usług zarządzanych w zakresie cyberbezpieczeństwa będą uznani za podmioty kluczowe i będą zgłaszać incydenty oraz wdrażać system zarządzania bezpieczeństwem informacji, zgodnie z art. 8.
34.	Morskie Centrum Cyberbezpieczeństwa Akademia Marynarki Wojennej w Gdyni	Uwaga ogólna	Koordinacja incydentów w uczelniach i w placówkach medycznych Rekomendujemy wskazanie w ustawie, czy CSIRT NASK i CSIRT MON odpowiednio powinny koordynować incydenty w <u>uczelniach/placówkach ochrony zdrowia oraz uczelniach wojskowych/wojskowych placówkach ochrony zdrowia</u> . Obecnie te obszary nie są jednoznacznie przypisane.	Wyjaśnienie uwagi Zgodnie z obecnymi przepisami do CSIRT NASK zgłaszają incydenty uczelnie publiczne, a jednostki podległe i nadzorowane przez Ministra Obrony Narodowej zgłaszają incydenty do CSIRT MON. Obecnie z zakresu podmiotowego ustawy są wyłączone samodzielne publiczne zakłady opieki zdrowotnej, chyba że zostały uznane za operatora usługi kluczowej.
35.	Osoba fizyczna	Uwaga ogólna	Szanowni Państwo, jako praktyk - audytor wiodący normy ISO 27001, kierownik działu informatyki szpitala, wykładowca akademicki w zakresie cyberbezpieczeństwa, pragnę zgłosić swoje uwagi dotyczące zmiany UoKSC. Dotychczasowa ustawa, dyrektywa NIS, nowa dyrektywa NIS2 oraz rzeczowa, konsultowana zmiana UoKSC bardzo dokładnie wskazują podmioty objęte w/w aktami. Szeroko opisują również zakres obowiązków jakie spoczywają na podmiotach oraz wskazują konieczne do podjęcia działania - czy to w zakresie formalnym, czy też w obszarach technicznych. Jednak żaden z tych aktów w literalny sposób nie określa wymogu zapewnienia służb technicznych mających realizować te obowiązki w konkretnej liczbie. Domyślnie jest przyjęte, że realizować te zadania będą lokalne działy informatyki. I tutaj pojawia się moja uwaga wynikająca z praktyki. Czy	Wyjaśnienie uwagi Wskazywanie liczby personelu w ustawie nie jest właściwe. Podmiot powinien dysponować adekwatnymi zasobami ludzkimi celem realizacji zadań. Zauważmy też, że projekt dotyczy wielu podmiotów o zarówno średnich, jak dużych, a wyjątkowo także i małych. Już to powoduje nieadekwatność w

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			nie można zawrzeć obok szeregu wymogów, takiego który zagwarantuje zatrudnienie stosownego personelu na odpowiednim poziomie ilościowym, np. zgodnie ze standardami ITILowymi? Codzienna sytuacja wygląda tak, że przeciętny dział informatyki szpitala składa się 1-4 osób w zależności od wielkości jednostki, realizujących cały wachlarz czynności związanych z codziennym utrzymaniem i funkcjonowaniem systemów, przy stałym wzroście ilości tych obowiązków związanych chociażby z wymogami NFZ. Sytuacja w gminach (szczególnie małych) jest jeszcze gorsza. Tam bardzo często dział IT to jedna osoba i to często zatrudniona na część etatu, lub jako firma zewnętrzna świadcząca usługi wsparcia informatycznego w ograniczonym zakresie. W tego typu podmiotach, pomimo wdrożeń różnego rodzaju systemów typu SIEM, EDR na które pozyskuje się środki z projektów celowych, nie ma ich kto obsługiwać. Po prostu nie ma na to czasu podczas codziennej pracy. Budujemy pozorne cyfrowe fortece, bez zagwarantowania solidnych fundamentów w postaci odpowiednio wykwalifikowanego personelu.	wyznaczaniu minimalnej liczby personelu w ustawie.
36.	PFR	Uwaga ogólna	Ustawa, stanowiąc implementację dyrektywy NIS2 (dyrektywa UE 2022/2555 w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium UE), istotnie rozszerza listę podmiotów zobowiązanych, które pod znowelizowaną ustawą będą kwalifikowane jako „podmioty kluczowe” i „podmioty ważne”. Jako jeden z podmiotów kluczowych został wskazany Polski Fundusz Rozwoju S.A. Na podstawie aktualnie procedowanego brzmienia Ustawy, przy uwzględnieniu zawężającej wykładni co do zakresu podmiotowego nakładanych Ustawą obowiązków, rozumiemy, że sam fakt uznania jednego z podmiotów wchodzących w skład grupy kapitałowej (w przypadku podmiotów działających w formie spółek prawa handlowego) za „podmiot kluczowy”, nie rozciąga automatycznie statusu „podmiotu kluczowego” w rozumieniu Ustawy na pozostałe podmioty grupy kapitałowej, choćby w sytuacji, gdy podmiot z grupy uznany za „podmiot kluczowy” jest podmiotem dominującym w danej grupie kapitałowej. Zwracamy jednak uwagę, na potencjalną konieczność zaadresowania w Ustawie rozkładu obowiązków i wzajemnych relacji pomiędzy podmiotami w sytuacji, w której dany podmiot uznany za „podmiot kluczowy”, przekazał wszystkie czynności związane z IT i cyberbezpieczeństwem do realizacji innemu podmiotowi, wydzielonemu w ramach swojej grupy kapitałowej - odrębnej spółce prawa handlowego. Wyżej opisana sytuacja stanowi częstą praktykę w dużych grupach kapitałowych, w ramach których tworzone są swego rodzaju centra usług wspólnych, świadczące m.in. usługi IT i usługi związane z cyberbezpieczeństwem wobec pozostałych spółek z grupy kapitałowej.	Wyjaśnienie uwagi Przywrócony zostanie art. 14 ust. 1 i wskazane zostanie, że podmiot kluczowy i podmiot ważny realizuje zadania za pomocą wewnętrznych struktur cyberbezpieczeństwa lub za pomocą zewnętrznego dostawcy.
37.	Polska Izba Przemysłu Chemicznego	Uwaga ogólna	Nadmiarowa klasyfikacja podmiotów ważnych nich jako kluczowe. Projekt ustawy wbrew definicjom zawartym w <i>Dyrektywie Parlamentu Europejskiego i Rady (UE) 2022/2555</i> klasyfikuje większość podmiotów objętych regulacjami ustawy jako podmioty kluczowe. Czyni tak również w odniesieniu do podmiotów, które w dyrektywie zostały sklasyfikowane jako podmioty ważne. Przykładem takich podmiotów są podmioty z grupy „Produkcja, wytwarzanie i dystrybucja chemikaliów”, które w dyrektywie klasyfikowane są jako ważne, a w projekcie ustawy	Uwaga uwzględniona Sektory produkcji, produkcji żywności, produkcji chemikaliów zostaną przeniesione do sektorów ważnych. Wymagania nadzorcze dla podmiotów ważnych zostaną złagodzone.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			jako kluczowe. Naszym zdaniem należy ujednolicić klasyfikację podmiotów przedstawioną w projekcie z klasyfikacją zawartą w dyrektywie. Brak rozróżnienia obowiązków pomiędzy podmiotami ważnymi i kluczowymi. Projekt ustawy zasadniczo nie zawiera żadnego, poza nazwą, rozróżnienia pomiędzy obowiązkami podmiotów kluczowych i ważnych. W rezultacie podmioty ważne zostaną objęte reżimem i obowiązkami zupełnie nieproporcjonalnymi do ich profilu i skali działalności. Naszym zdaniem należy dokonać, idąc w ślad za dyrektywą, rozróżnienia obowiązków pomiędzy podmiotami kluczowymi i ważnymi. Vacatio legis Biorąc pod uwagę skalę nowych obowiązków nakładanych na adresatów projektowanego rozporządzenia i fakt, że obecnie w wielu przypadkach infrastruktura tych podmiotów nie spełnia wymogów ustawowych przewidziane 6 miesięczne vacatio legis jest zbyt krótkie na rzetelne wdrożenie zmian w organizacjach. Postulujemy, aby przesłużyć vacatio legis przynajmniej do 12 miesięcy. Poniżej załączamy również tabelę ze szczegółowymi uwagami do rozporządzenia. Finalny kształt ustawy dot. krajowego systemu cyberbezpieczeństwa niewątpliwie będzie miał bardzo duży wpływ na działalność przedsiębiorstw branży chemicznej w związku z czym zwracamy się z uprzejmą prośbą o zapoznanie się z przedstawionymi przez nas argumentami oraz uwzględnienie proponowanych przez nas rozwiązań na dalszych etapach prac nad projektem ustawy. Jednocześnie zwracamy się z prośbą o uwzględnienie Polskiej Izby Przemysłu Chemicznego przy opiniowaniu wszelkich nowych inicjatyw ustawodawczych podejmowanych przez Ministerstwo Cyfryzacji we wszelkich kwestiach dotyczących funkcjonowania przemysłu chemicznego.	
38.	PZPM	Uwaga ogólna	W związku z konsultacjami publicznymi dotyczącymi projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw, poniżej przekazuję uwagi Polskiego Związku Przemysłu Motoryzacyjnego do projektu. Przede wszystkim pragnę zwrócić uwagę na globalny charakter branży motoryzacyjnej oraz kluczową z punktu widzenia organizacji łańcuchów dostaw harmonizację wymagań. Różne wymagania w różnych krajach członkowskich Unii Europejskiej mogą utrudniać organizację produkcji, dostępność produktów i tym samym wpływać na konkurencyjność naszego kraju w kontekście inwestycji zagranicznych. Dlatego też, bardzo istotne jest, aby implementacja dyrektywy nie wykraczała poza ramy wskazane w akcie unijnym. Zwracamy też uwagę, że implementacja powinna opierać się na kryteriach weryfikowalnych, technicznych i proporcjonalnych, aby unikać arbitralnego podejścia i uwzględnić zasadę pewności prawa oraz obrotu gospodarczego. Uprzejmie prosimy również o uwzględnienie Polskiego Związku Przemysłu Motoryzacyjnego w dalszych pracach nad krajowym systemem cyberbezpieczeństwa.	Wyjaśnienie uwagi Wymagania dla sektora produkcji zostaną złagodzone.
39.	Kasa Krajowa SKOK	Uwaga ogólna	Projekt ustawy stanowi implementację Dyrektywy Parlamentu Europejskiego i Rady:(UE) 2022/2555 . z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniającą rozporządzenie (UE) nr 910/2014 i dyrektywę	Wyjaśnienie uwagi Nie przewiduje się kolejnej tury konsultacji publicznych, natomiast

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			(UE) 2018/1972 oraz uchylającą dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz. Urz. UE L 2022/2555 z 27.12.2022), (zwana dalej „dyrektywą NIS 2”), która utworzyła nowe ramy systemu zapewnienia cyberbezpieczeństwa w Unii Europejskiej. Jak wskazano w uzasadnieniu ze względu na odwołania w samej dyrektywie NIS 2 (...) projekt będzie zależny od projektów ustaw transponujących lub służących stosowaniu: (...) dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylającą dyrektywę Rady 2008/114/WE (Dz. Urz. UE L 2022/2557 z 27.12.2022)- zwana dalej „dyrektywą CER”; rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (Dz. Urz. UE L 2022/2554 z 27.12.2022) - zwane dalej „rozporządzeniem DORA”. W chwili przygotowywania projektu nie są jeszcze dostępne projekty ustaw wdrażającej dyrektywę CER oraz służącej stosowaniu rozporządzeniu DORA. Z tego powodu stosownie do prac legislacyjnych niniejszy projekt będzie ulegał zmianom, głównie w obszarze siatki pojęciowej, mającym na celu dostosowanie projektu do regulacji transponujących rozporządzenie DORA i dyrektywę CER. Mając na uwadze powyższe, zwracam się z prośbą o umożliwienie Kasie Krajowej zaopiniowania zapowiedzianej kolejnej wersji projektu, która będzie dostosowana do projektu ustawy implementującego dyrektywę 2022/2557 i projektu wdrażającego rozporządzenie 2022/2554.	projekt będzie publicznie dostępny na stronach RCL.
40.	Krajowa Izba Gospodarcza	Uwaga ogólna	Krajowa Izba Gospodarcza zrzeszającą ponad 160 Izb Gospodarczych w Polsce jest największą organizacją gospodarczą w naszym kraju. Przedsiębiorcy zrzeszeni w naszych Izbach zgłaszają szereg uwag i wniosków do nowelizacji istotnej ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (implementacja dyrektywy NIS2). Przyszła znowelizowana ustawa będzie bardzo ważnym aktem prawnym szczególnie dla podmiotów związanych z techniką cyfrową i bezpieczeństwem cyfrowym społeczeństwa i organów Państwa. Przyszła ustawa będzie zawierała elementy prawa wspólnotowego, jak również będzie definiowała zasady ładu prawnego w otaczającej nas cyfrowej rzeczywistości. Ponadto przyszła ustawa ma wymiar wielowektorowy i wielowątkowy. Całość nowego aktu prawnego wymaga przede wszystkim wnikliwej i bardzo głębokiej analizy. Wyznaczony, 30-to dniowy czas na odniesienie się do przedstawionego tekstu oraz przygotowanie propozycji zmian jest w praktyce zadaniem niewykonalnym W związku z pismem DP.MC.WL.0211.16.2024, z dnia 24 kwietnia 2024 roku Krajowa izba Gospodarcza wnioskuje o przedłużenie terminu konsultacji nad nowelizacją w/w ustawy do 28 czerwca 2024r	Wyjaśnienie uwagi Termin 30 dni to standardowy termin na konsultacje projektu ustawy.
41.	KIKE	Uwaga ogólna	W pierwszej kolejności należy podkreślić, że celem projektu ustawy, wyrażonym w jego uzasadnieniu, jest transpozycja dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniającej rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającej dyrektywę (UE) 2016/1148 (dyrektywa NIS 2). Ustawa o krajowym systemie	Wyjaśnienie uwagi Wspomniany art. 8 wskazuje, że podmiot ważny i podmiot kluczowy wdraża proporcjonalne środki techniczne i organizacyjne, dlatego uważamy, że ten obowiązek jest proporcjonalny.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

		cyberbezpieczeństwa w brzmieniu nadanym projektem ustawy (nowa KSCU) zawiera jednak długi szereg daleko idących obowiązków, które wykraczają poza wymagania określone tą dyrektywą. Już w tym miejscu wypada podkreślić, że najbardziej dotkliwym aspektem nadregulacji w projekcie ustawy jest wyśrubowanie obowiązków i ciężarów spoczywających na przedsiębiorcach telekomunikacyjnych MŚP w taki sposób, że – choć dyrektywa NIS2 tego nie wymaga – projektodawca zrównuje obowiązki nałożone na MŚP z obowiązkami spoczywającymi na podmiotach największych, nie zachowując przy tym zasady proporcjonalności. Dobrym przykładem dotkliwej nadregulacji jest art. 8 ust. 1 nowej KSCU (transpozycja art. 21 dyrektywy NIS 2 „Środki zarządzania ryzykiem w cyberbezpieczeństwie”). Przepis ten nakłada jednakowe obowiązki na podmioty kluczowe i ważne (a w tym przedsiębiorców telekomunikacyjnych dużych oraz MŚP), to są one określone na takim poziomie ogólności, że możliwe będzie realizowanie tych obowiązków (proporcjonalnie do wielkości przedsiębiorcy. Jednakże już rozporządzenie, które może być wydane na podstawie art. 8a nowej KSCU, jak i przede wszystkim przepis art. 10 nowej KSCU stanowią w całości daleko idącą nadregulację. Obowiązki w zakresie zarządzania ryzykiem w cyberbezpieczeństwie są w tych przepisach na tyle szczegółowe, że nie pozostawiają przestrzeni na proporcjonalne dostosowanie ich do wielkości przedsiębiorcy. Kolejnym przykładem nadregulacji, nieuzasadnionej żadnymi przesłankami faktycznymi, jest definicja incydentu, która obejmuje również zdarzenie, które może (ale nie musi) mieć niekorzystny wpływ na bezpieczeństwo systemów informacyjnych. Izba tym zakresie postuluje poprawienie tej definicji zgodnie z brzmieniem w dyrektywie NIS2. iCel ustawy o krajowym systemie cyberbezpieczeństwa (KSCU), który powinien być brany pod uwagę, został wskazany w jej art. 3: <i>„Krajowy system cyberbezpieczeństwa ma na celu zapewnienie cyberbezpieczeństwa na poziomie krajowym, w tym niezakłóconego świadczenia usług przez podmioty kluczowe i podmioty ważne, przez osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych służących do świadczenia tych usług oraz zapewnienie obsługi incydentów.”</i> Zwracam uwagę na zwrot „na poziomie krajowym”, co zostało pominięte przy nakładaniu obowiązków na przedsiębiorców telekomunikacyjnych działających na poziomie lokalnym (często w obrębie jednej – dwóch gmin, rzadziej jednego - dwóch powiatów). O ile prawdą jest, że dyrektywa NIS 2 stanowi tzw. dyrektywę harmonizacji minimalnej („nie uniemożliwia państwow członkowskim przyjęcia lub utrzymania przepisów zapewniających wyższy poziom cyberbezpieczeństwa” – por. art. 5 dyrektywy NIS2), o tyle przyjmowanie przepisów wykraczających poza wymogi dyrektyw unijnych są co do zasady niezgodne z art. 67 ustawy – Prawo przedsiębiorców (PP), zgodnie z którym: <i>i„Opracowując projekt aktu normatywnego określającego zasady podejmowania, wykonywania lub zakończenia działalności gospodarczej, należy kierować się zasadami proporcjonalności i adekwatności, a w szczególności:</i> <i>1) dążyć do nienakładania nowych obowiązków administracyjnych, a jeżeli nie jest to możliwe, dążyć do ich nakładania jedynie w stopniu koniecznym do osiągnięcia ich celów;</i>	Art. 10 dotyczy prowadzenia dokumentacji z zakresu cyberbezpieczeństwa. Chodzi o niezbędne udokumentowanie aspektów cyberbezpieczeństwa na potrzeby kontroli lub audytów.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

		2) dążyć do ograniczenia obowiązków informacyjnych, zwłaszcza gdy wymagane informacje są przekazywane przez obowiązanych organom władzy publicznej na podstawie obowiązujących przepisów; 3) dążyć do umożliwienia realizacji obowiązków informacyjnych w postaci elektronicznej; 4) implementując prawo Unii Europejskiej i prawo międzynarodowe, dążyć do nakładania wyłącznie obowiązków administracyjnych niezbędnych do osiągnięcia celów implementowanych przepisów [podkreślenie i wytłuszczenie nasze]”. W pierwszej kolejności zwracam uwagę na pkt 1 tego przepisu. Obowiązki nakładane w przepisach na przedsiębiorców powinny być w takim zakresie w jakim jest to niezbędne do osiągnięcia określonych celów. Ma to być realizowane w ramach zasad proporcjonalności i adekwatności (które <i>nota bene</i> również są powtórzone w dyrektywie NIS 2). Tymczasem większość obowiązków w Projekcie, stanowi znaczącą nadregulację w stosunku do celu jakim ma być cyberbezpieczeństwo kraju (a nie poszczególnych podmiotów gospodarczych). Kwestię zakazu nadregulacji podkreśla w dodatku pkt 4 tego przepisu, wskazując na ograniczenia w implementacji unijnych przepisów do niezbędnych środków dla osiągnięcia zakładanych celów. Całość Projektu powinna również zostać przeanalizowana pod kątem zgodności z pkt 2 tego przepisu. Projekt bowiem nakłada na przedsiębiorców (w tym przedsiębiorców telekomunikacyjnych) do wykonania dużej ilości obowiązków informacyjnych, które są dublowane na wielu poziomach. Co więcej, art. 7 Konstytucji RP stanowi, że: <i>„Organy władzy publicznej działają na podstawie i w granicach prawa [wytłuszczenie nasze]”.</i> Wyjątkowa skala obowiązków, których dyrektywa NIS2 nie wymaga, a które miałyby zostać nałożone na przedsiębiorców, szczególnie na przedsiębiorców MŚP, prowadzi do wniosku, że projekt ustawy daleko wykracza poza „nakładanie wyłącznie obowiązków administracyjnych niezbędnych do osiągnięcia celów implementowanych przepisów”. Poddanie konsultacjom publicznym takiego projektu ustawy jest niezrozumiałe, skoro – jak wynika z art. 67 pkt 4 PP w zw. z art. 7 Konstytucji RP – wymóg powstrzymywania się od nadregulacji jest wymogiem ustawowym i zarazem obowiązkiem Ministra Cyfryzacji jako organu władzy publicznej. Kolejnym polskim aktem prawnym, który nakazuje powstrzymanie się przed tworzeniem przepisów wykraczających poza samo wdrożenie prawa UE, jest Regulamin pracy Rady Ministrów (Regulamin RM). Zgodnie z § 30 ust. 2 zdanie pierwsze Regulaminu RM: <i>„Projekt ustawy mającej na celu wdrożenie prawa Unii Europejskiej może zawierać przepisy wykraczające poza ten cel wyłącznie w szczególnie uzasadnionych przypadkach [podkreślenie i wytłuszczenie nasze]”.</i> Należy z całą mocą podkreślić, że uzasadnienie projektu ustawy nie zawiera żadnych rozważań mających wykazać, że w przypadku transpozycji niemal każdego kolejnego postanowienia dyrektywy NIS2 występują „szczególnie uzasadnione przypadki”, domagające się uchwalenia przepisów wykraczających poza wymagania ujęte w tej dyrektywie. Co więcej, do projektu ustawy nie dołączono tabelarycznego zestawienia projektowanych przepisów ustawy wykraczających poza cel	

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			wdrożenia prawa UE „wraz z wyjaśnieniem niezbędności objęcia ich tym projektem”, czyli tzw. odwróconej tabeli zgodności, co stanowi wymóg wyrażony w § 30 ust. 2 zdanie drugie Regulaminu RM. wI.	
42.	KIKE	Uwaga ogólna	Problem tzw. nadregulacji (‘nadmiernie rygorystyczne wdrażanie’) – wymiar unijny Nawet sama Komisja Europejska uznaje ‘gold-plating’ za zjawisko, które powinno być stosowane wyjątkowo, ponieważ stanowi barierę w rozwoju jednolitego rynku. Warto zwrócić uwagę na Komunikat0 Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów w sprawie określania i usuwania barier na jednolitym rynku z 10 marca 2020 r. (COM(2020) 93 final), który powstał w oparciu o dowody zebrane przez Komisję w dwóch sprawozdaniach. W Komunikacie tym wskazano 13 najważniejszych barier na jednolitym rynku, zidentyfikowano pięć pierwotnych przyczyn tych barier, a dla każdej pierwotnej przyczyny określono priorytety dla związanych z nią działań, w tym istniejące i możliwe przyszłe inicjatywy. Na pierwszą z pierwotnych przyczyn barier rozwoju jednolitego rynku, zatytułowaną „1. Wybory regulacyjne na szczeblu unijnym i krajowym”, składa się między innymi wyzwanie określone jako „Prawodawstwo UE może pozostawić pewną elastyczność w poziomie harmonizacji lub praktykach państw członkowskich („nadmiernie rygorystyczne wdrażanie”)”, opisane następująco: „Niektóre kwestie związane z jednolitym rynkiem są w pełni zharmonizowane na poziomie UE. Prawodawca unijny uregulował w sposób wyczerpujący daną kwestię, równoważąc potrzebę otwarcia rynku z potrzebą realizacji celów leżących w interesie publicznym. W odniesieniu do tych kwestii przepisy UE określają zarówno „poziom bazowy”, jak i „pułap”: nie ma już miejsca na dodawanie wymogów na szczeblu krajowym49. W wielu dziedzinach (takich jak niektóre aspekty ochrony konsumentów) niektóre kwestie są przedmiotem minimalnej harmonizacji na poziomie UE, co pozostawia państwom członkowskim swobodę ustalania norm ponad ustalony poziom bazowy. Może to prowadzić do powstania częściowo rozbieżnych przepisów na jednolitym rynku, które mogą nakładać obciążenia na podmioty rynkowe („nadmiernie rygorystyczne wdrażanie”) [wyróżnienie nasze]. Te rozbieżne przepisy mogą również utrudnić konsumentom zrozumienie podstawy prawnej i zakresu ich ochrony podczas dokonywania zakupów transgranicznych. W kwestiach, które nie są w pełni zharmonizowane na szczeblu UE, państwa członkowskie mogą zdecydować o ustanowieniu dodatkowych wymogów na szczeblu krajowym, o ile są one konieczne i proporcjonalne do celu realizacji określonych uzasadnionych interesów publicznych. Jednak często przekłada się to na dodatkowe obciążenia regulacyjne lub administracyjne dla przedsiębiorstw, co ma szczególnie wpływ na MŚP. Nadmiernie rygorystyczne wdrażanie jest szczególnie problemem w odniesieniu do sektora usług [wyróżnienie i podkreślenie nasze]. Wymogi te mają również pośredni wpływ na konsumentów w zakresie, w jakim mogą być oni pozbawieni korzyści wynikających z ofert zagranicznych przedsiębiorstw, a w szczególności innowacyjnych MŚP. [...] Komisja przypomina o obowiązku przestrzegania przez państwa członkowskie prawa UE i wzywa je do zintensyfikowania działań na rzecz uproszczenia i zmniejszenia niepotrzebnych obciążeń	Uwaga uwzględniona Przepisy dotyczące audytów w przypadku podmiotów ważnych zostaną złagodzone.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			administracyjnych⁵⁰[wyróżnienie nasze]. Dodatkowe wymogi krajowe muszą być uzasadnione nadrzędnym względem interesu publicznego, muszą być niedyskryminacyjne, proporcjonalne, łatwe do zrozumienia i zgodne z minimalnymi normami zharmonizowanymi⁵¹. Ponadto, nawet w ramach przepisów prawa, w świetle celu, jakim jest jednolity rynek, różnice należy ograniczyć do minimum [wyróżnienie nasze].[...]" W związku z powyższym należy podkreślić, że KIKE protestuje przeciwko niemal całkowitemu zniwelowaniu różnic pomiędzy podmiotami kluczowymi i ważnymi, którego dokonano w ramach projektu ustawy. W szczególności negatywny sposób odbija się na podmiotach ważnych, czyli podmiotach z sektora MŚP.	
43.	KIKE	Uwaga ogólna	Mikro-, mali i średni przedsiębiorcy telekomunikacyjni W opinii Izby Minister Cyfryzacji, jako organ publiczny, powinien nie tylko powstrzymywać się przed nakładaniem nadmiernych obowiązków na MŚP, lecz aktywnie dążyć do ograniczania obowiązków. Art. 68 PP stanowi bowiem: „Art. 68 W przypadku stwierdzenia wpływu projektu aktu normatywnego na mikroprzedsiębiorców, małych i średnich przedsiębiorców, przy opracowaniu projektu aktu normatywnego dąży się do proporcjonalnego ograniczania obowiązków administracyjnych wobec tych przedsiębiorców albo uzasadnia brak możliwości zastosowania takich ograniczeń”. Ponownie apeluję zatem, aby Minister Cyfryzacji, jako organ władzy publicznej, działał na podstawie i w granicach prawa powszechnie obowiązującego, w szczególności przestrzegał art. 68 PP. Także i w tym przypadku wypada zauważyć, że Komisja Europejska konsekwentnie podkreśla potrzebę różnicowania obowiązków nakładanych na przedsiębiorców dużych oraz przedsiębiorców MŚP. W Komunikacie Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów Strategia MŚP na rzecz zrównoważonej i cyfrowej Europy z 10 marca 2020 r. (COM(2020)103) wskazano: „25 mln małych i średnich europejskich przedsiębiorstw (MŚP) stanowi trzon gospodarki UE. Zatrudniają one około 100 mln osób, odpowiadają za ponad połowę europejskiego PKB i odgrywają kluczową rolę w tworzeniu wartości dodanej we wszystkich sektorach gospodarki. [...] Zapewniają one dwie trzecie miejsc pracy [...] oraz wspierają dobrobyt społeczeństwa, także na obszarach oddalonych i wiejskich. [wyróżnienie nasze] Każdy obywatel europejski zna kogoś, kto jest przedsiębiorcą lub pracuje dla niego. Codzienne wyzwania, przed którymi stoją europejskie MŚP, związane z przestrzeganiem przepisów i dostępem do informacji, rynków i finansów stanowią zatem wyzwania dla całej Europy. [...]" Przestrzeganie przepisów, norm, etykiet i formalności administracyjnych dotyczy w większym stopniu MŚP niż większych przedsiębiorstw ze względu na ich ograniczone zasoby finansowe i ludzkie. [wyróżnienie nasze] Na przykład w sektorze usług dla przedsiębiorstw koszty ponoszone przez MŚP przy spełnianiu formalności administracyjnych mogą sięgać 10 000 EUR¹⁶. [...]" Ze swojej strony Komisja zobowiązała się do zmniejszenia obciążeń dla MŚP i do nadania im większego znaczenia w ramach cyklu lepszego stanowienia prawa. Zgodnie z programem sprawności	Wyjaśnienie uwagi Nie jest prawdą, że projekt KSC nie przewiduje wsparcia dla sektora telekomunikacyjnego. Będzie utworzony odrębny CSIRT sektorowy dla tego sektora, którego zadaniem będzie nie tylko przyjmowanie zgłoszeń o incydentach, ale również wspieranie przedsiębiorców telekomunikacyjnych w obsłudze takich incydentów.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			i wydajności regulacyjnej (REFIT) Komisja systematycznie monitoruje obowiązujące przepisy UE w celu zmniejszenia obciążeń i uproszczenia prawodawstwa. [...] Aby zapewnić, że nowe przepisy są przyjazne dla MŚP, pełnomocnik UE ds. MŚP22 przeanalizuje inicjatywy UE we współpracy z zainteresowanymi MŚP, aby zasygnalizować Komisji te, które zasługują na szczególną uwagę z perspektywy MŚP.” Pierwsze z kluczowych działań w ramach Strategii MŚP brzmi: „Pełnomocnik UE ds. MŚP i sieć krajowych pełnomocników ds. MŚP wniosą wkład w prace działającej w ramach Komisji Grupy Zadaniowej ds. Egzekwowania Przepisów dotyczących Jednolitego Rynku, która zostanie utworzona w wyniku realizacji planu działania na rzecz egzekwowania przepisów, aby między innymi rozwiązać problem nadmiernie rygorystycznego wdrażania przepisów w procesie transpozycji z myślą o ograniczeniu do minimum obciążenia regulacyjnego MŚP” [wyróżnienie nasze]. Tymczasem projekt ustawy nakłada obowiązki na mikro, małych i średnich przedsiębiorców dokładnie takie same jak na dużych przedsiębiorców. Brak jest wyjaśnienia braku proporcjonalnego ograniczenia obowiązków wobec MŚP w projekcie, tym bardziej że występuje tu również nadregulacja wobec dyrektywy NIS 2. Unijne przepisy wprost różnicują niektóre obowiązki wobec mikro i małych przedsiębiorców telekomunikacyjnych, co nie znalazło odzwierciedlenia w projekcie ustawy. Izba wskazuje, że przy regulacji telekomunikacyjnych MŚP, nie została wzięta pod uwagę specyfika polskiego rynku telekomunikacyjnego. Wg danych UKE 99,5% przedsiębiorców telekomunikacyjnych w Polsce to MŚP (podobna sytuacja w UE występuje tylko w Finlandii). MŚP obsługują około 37,3% wszystkich użytkowników Internetu stacjonarnego i 10% użytkowników telefonii stacjonarnej. Jednocześnie przychód MŚP stanowi jedynie 15,1% przychodu rynku stacjonarnego. Nałożenie na MŚP (a zwłaszcza na mikro i małych przedsiębiorców telekomunikacyjnych) symetrycznych względem dużych przedsiębiorców i międzynarodowych korporacji doprowadzi do znacznego obniżenia rentowności działalności MŚP. To z kolei przełoży się na rozwój w Polsce oligopolu kosztem użytkowników końcowych. Z tego względu Izba postuluje, aby na mikro i małych przedsiębiorców telekomunikacyjnych obowiązki przewidziane w projekcie ustawy były tożsame z obecnymi obowiązkami wynikającymi z ustawy – Prawo telekomunikacyjne. Posiłkując się informacjami od organów związanych z cyberbezpieczeństwem z konferencji Secure24 Izba zwraca uwagę na fundamentalny brak w projekcie ustawy: nowa KSCU właściwie nie konkretyzuje żadnych obowiązków CSIRT w zakresie zwalczania przez nich incydentów poprzez wsparcie techniczne i kadrowe zaatakowanych podmiotów. Projekt ogranicza się do nic nieznaczących ogólników o „wspierciu” czy „koordynacji” podczas gdy doświadczenia z cyberwojny na Ukrainie wskazują, że podmioty prywatne same nie poradzą sobie z wyspecjalizowanymi atakami przez służby wrogiego państwa. Brak wyraźnych obowiązków po stronie rządowej spowoduje brak realizacji celów ustawy i całkowite przerzucenie jej kosztów na przedsiębiorców. Izba w tym zakresie wskazuje na swoje doświadczenie przy wdrażaniu mechanizmów antyfraudowych w komunikacji	

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			elektronicznej, gdzie brak realnych obowiązków na podmiotach publicznych spowodował, że podmioty te do dziś nie przystąpiły do zwalczania tych nadużyć.	
44.	KIKE	Uwaga ogólna	KIKE pragnie podkreślić, że w motywie 56 dyrektywy NIS 2 wskazano, że: <i>„W krajowych strategiach cyberbezpieczeństwa państwa członkowskie powinny uwzględniać szczególne potrzeby małych i średnich przedsiębiorstw związane z cyberbezpieczeństwem. W całej Unii małe i średnie przedsiębiorstwa stanowią znaczny odsetek rynku przemysłu oraz gospodarki i często mają trudności, by dostosować się do nowych praktyk biznesowych w coraz bardziej cyfrowym świecie i do środowiska cyfrowego, z pracownikami pracującymi z domów, a działalnością gospodarczą w coraz większym stopniu prowadzoną w internecie. Niektóre małe i średnie przedsiębiorstwa mierzą się ze szczególnymi wyzwaniami w zakresie cyberbezpieczeństwa, takimi jak niska świadomość zagadnień cyberbezpieczeństwa, brak zdalnych zabezpieczeń informatycznych, wysokie koszty rozwiązań dotyczących cyberbezpieczeństwa oraz zwiększony poziom zagrożeń, np. oprogramowanie wymuszające okup, w związku z czym powinny otrzymywać wskazówki i pomoc. Małe i średnie przedsiębiorstwa coraz częściej stają się celem ataków w łańcuchu dostaw ze względu na ich niewystarczający poziom zarządzania ryzykiem w cyberbezpieczeństwie i zarządzania w razie ataków oraz fakt, że mają one ograniczony dostęp do zasobów na potrzeby bezpieczeństwa. Takie ataki w łańcuchu dostaw wpływają nie tylko na małe i średnie przedsiębiorstwa i działalność każdego z nich z osobna, lecz także mogą mieć efekt kaskadowy w postaci większych ataków na zaopatrywane przez nie podmioty. Państwa członkowskie powinny, za pośrednictwem krajowych strategii cyberbezpieczeństwa, pomagać małym i średnim przedsiębiorstwom w reagowaniu na wyzwania dotyczące łańcuchów dostaw. Państwa członkowskie powinny posiadać punkt kontaktowy dla małych i średnich przedsiębiorstw na szczeblu krajowym lub regionalnym, który zapewniałby wskazówki i pomoc małym i średnim przedsiębiorstwom albo kierowałby je do właściwych organów udzielających wskazówek i pomocy w sprawach związanych z cyberbezpieczeństwem. Państwa członkowskie zachęca się również, aby oferowały usługi takie jak konfiguracja stron internetowych i funkcje logowania małym przedsiębiorstwom i mikroprzedsiębiorstwom, które nie posiadają tych zdolności”</i> [wyróżnienie nasze]. Tymczasem w art. 69 nowej KSCU, który reguluje treść Strategii Cyberbezpieczeństwa RP, o potrzebach MŚP mowa jest tylko w art. 69 ust. 1 pkt 9, który stanowi: <i>„Strategia określa: [...] 9) rozwiązania wzmacniające podstawowy poziom cyberodporności i higieny cyfrowej małych i średnich przedsiębiorstw;”.</i> Biorąc pod uwagę skalę działalności MŚP, w szczególności przedsiębiorców telekomunikacyjnych z tego sektora, postulujemy, aby Strategia zawierała dalej idące rozwiązania mające na celu wsparcie MŚP – w tym nie tylko małych i średnich, lecz również mikroprzedsiębiorców.	Wyjaśnienie uwagi Jak wskazano w uwadze małe i średnie przedsiębiorstwa zostały wprost wskazane w pkt 9. Nie oznacza to jednak, że inne elementy strategii nie będą odnosiły się do tych podmiotów. Choćby kwestie związane z bezpieczeństwem łańcucha dostaw będą mogły być stosowane przez wszystkie zainteresowane podmioty. W związku z tym te kwestie będą uwzględnione w Strategii.
45.	KIKE	Uwaga ogólna	W opinii KIKE przedsiębiorcy zrzeszeni w Izbie z pewnością zostaną dotknięci skutkami regulacji dotyczących dostawcy wysokiego ryzyka. Należy podkreślić, że formalnie obowiązek usuwania sprzętu lub oprogramowania dostawcy uznanego za dostawcę wysokiego ryzyka będzie spoczywał na przedsiębiorcach telekomunikacyjnych osiągających przychody z tytułu działalności	Wyjaśnienie uwagi Postępowanie w sprawie uznania za dostawcę wysokiego ryzyka ma na celu zabezpieczenie polskiej gospodarki i

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

		telekomunikacyjnej wyższe od kwoty 10 milionów złotych, zatem obowiązek ten formalnie teoretycznie nie dotknie podmiotów mikro (mikroprzedsiębiorca, zgodnie z prawem przedsiębiorców, osiąga przychody niższe niż równowartość 2 milionów euro), lecz dotknie już przedsiębiorców co najmniej małych (mały przedsiębiorca osiąga przychody niższe niż równowartość 10 milionów euro). Co więcej, skutki regulacji w zakresie dostawcy wysokiego ryzyka dotkną podmioty, do których stosuje się ustawę – Prawo zamówień publicznych oraz podmioty publiczne. Mikro i mali lokalni polscy dostawcy internetu bardzo często startują w przetargach publicznych i obsługują podmioty publiczne. W związku z tym nawet jeśli nie bezpośrednio, to co najmniej pośrednio odczuliaby skutki regulacji w zakresie dostawcy wysokiego ryzyka. Z załącznika nr 1 do Oceny Skutków Regulacji wynika, że 5G Toolbox został wdrożony w różnorodny sposób w państwach członkowskich. Zabezpieczenie łańcucha dostaw przed dostawcami wysokiego ryzyka może być zatem realizowane w różnorodny sposób, niekoniecznie tak bardzo restrykcyjny, jak ujęty w projekcie ustawy. Ponownie, jak przy wdrażaniu dyrektywy NIS 2, także i w przypadku 5G Toolbox z niezrozumiałych powodów projekt ustawy zmierza do obciążenia polskich przedsiębiorców, w tym MŚP, ciężarami niespotykanymi nigdzie indziej w Europie. Należy podkreślić, że skoro punktem wyjścia dla rozwiązań w zakresie dostawcy wysokiego ryzyka był dokument 5G Toolbox, a Komisja Europejska w swoich wystąpieniach wprost wskazuje konkretnych dostawców sprzętu i oprogramowania pochodzących z Chin – należy spodziewać się, że to dostawcy chińscy mogą być w pierwszej kolejności adresatem ew. decyzji wyznaczającej dostawcę wysokiego ryzyka. Niezwykle niepokojący jest przy tym art. 67b ust. 11 pkt 2 nowej KSCU, zgodnie z którym opinia, o którą powinien wystąpić Minister Cyfryzacji przed wydaniem ww. decyzji, powinna zawierać analizę p.,2) <i>prawdopodobieństwa, z jakim dostawca sprzętu lub oprogramowania znajduje się pod kontrolą państwa spoza terytorium Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, z uwzględnieniem:</i> <i>a) przepisów prawa regulujących stosunki między dostawcą sprzętu lub oprogramowania, a tym państwem oraz praktyki stosowania prawa w tym zakresie,</i> <i>b) prawodawstwa oraz stosowania prawa w zakresie ochrony danych osobowych, w szczególności w przypadku, gdy nie ma porozumień w zakresie ochrony tych danych między Unią Europejską i tym państwem,</i> <i>c) struktury własnościowej dostawcy sprzętu lub oprogramowania,</i> <i>d) zdolności ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania;”.</i> Jednocześnie jedyną przesłanką wydania decyzji jest sytuacja, gdy „dostawca ten stanowi poważne zagrożenie dla obronności, bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego, lub życia i zdrowia ludzi” (por. art. 67b ust. 15 nowej KSCU). Co więcej, z góry zakłada się, że jawność tego postępowania będzie wyłączona, w tym przesądza się, że sąd rozpatrujący skargę na taką decyzję także będzie ją rozpatrywał w trybie niejawnym i tylko Minister Cyfryzacji będzie mógł zapoznać się z pełnym uzasadnieniem wyroku sądu (art. 67e nowej KSCU).	polskiego społeczeństwa przed dostawcą sprzętu lub oprogramowania, który stwarza poważne zagrożenie dla bezpieczeństwa państwa, obronności, bezpieczeństwa i porządku publicznego lub zdrowia i życia ludzi. W ramach postępowania administracyjnego będą brane pod uwagę zarówno aspekty techniczne związane z dostarczaniem przez dostawcę sprzętem i oprogramowaniem jak również aspekty nietechniczne związane z dostawcą. Dzięki temu zostanie zidentyfikowany pełen obraz zagrożeń jakie stwarza dostawca sprzętu lub oprogramowania. Postępowanie umożliwia badanie dostawcy sprzętu lub oprogramowania dla wszystkich sektorów gospodarki wskazanych w ustawie. Jest to wskazane z uwagi na to, że każdy podmiot kluczowy i podmiot ważny musi dbać o bezpieczeństwo łańcuchów dostaw. Podmioty kluczowe i podmioty ważne mają istotny charakter dla funkcjonowania współczesnej gospodarki i społeczeństwa informacyjnego. Zakłócenie funkcjonowania tych podmiotów poprzez atak przez łańcuch dostaw może spowodować niepowetowane straty. Z uwagi na charakter tego postępowania wyłączono część przepisów Kodeksu postępowania administracyjnego. Przede wszystkim nie jest możliwe przeprowadzenie postępowania administracyjnego przy udziale wszystkich podmiotów, które wykorzystują sprzęt lub oprogramowanie

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

		Powyższe oznacza, że dopuszcza się możliwość, iż chiński dostawca sprzętu i oprogramowania może zostać uznany za dostawcę wysokiego ryzyka, a jego sprzęt może zostać objęty nakazem usunięcia (por. art. 67c nowej KSCU), gdy tylko zostanie stwierdzone, że dostawca znajduje się pod kontrolą państwa spoza terytorium UE lub NATO, przy czym pojęcie takiej „kontroli” jest rozumiane niezwykle szeroko. Nie jest warunkiem koniecznym, aby podjęcie decyzji z art. 67b ust. 15 nowej KSCU przez Ministra Cyfryzacji było uzależnione także od tego, czy np. kiedykolwiek doszło do incydentu poważnego lub czy w sprzęcie lub oprogramowaniu takiego dostawcy zidentyfikowano celowo umieszczone backdoory. Oznacza to, że w pełni możliwy jest scenariusz wydania takiej decyzji z powodów wyłącznie politycznych, bez jakiegokolwiek przesłanki merytorycznej. Potencjalnie w pełni sprawny i bezpieczny sprzęt może być objęty obowiązkiem usunięcia. Warto przy tym dodać, że od czasu przyjęcia 5G Toolbox w obiegu prawnym pojawił się akt o cyberbezpieczeństwie oraz niedługo pojawi się akt o cyberodporności. Przepisy tych aktów zapewniają szerokie możliwości daleko idącego zabezpieczenia sprzętu i oprogramowania. Pomijając już względy ekologii, usuwanie bezpiecznego i sprawnego sprzętu nie ma nic wspólnego ze zwiększaniem poziomu cyberbezpieczeństwa sieci komunikacji elektronicznej. Wręcz przeciwnie: bezpieczeństwo sieci mogłoby w takim przypadku zostać bardzo zachwiane, gdyby wszyscy przedsiębiorcy byli zobowiązani w podobnym czasie wymieniać duże partie sprzętu, szkolić pracowników z zakresu działania nowego sprzętu. Przede wszystkim Izba apeluje zatem do Ministra Cyfryzacji, aby dokonał rzetelnej Oceny Skutków ww. Regulacji dla przedsiębiorców. Argumentem za brakiem takiej analizy nie może być to, że dopóki nie znamy projektu decyzji o uznaniu dostawcy za dostawcę wysokiego ryzyka i nie znamy listy sprzętu, który będzie usuwany, takiej Oceny nie można dokonać. Po pierwsze, wiemy, że w pierwszej kolejności decyzja może dotyczyć funkcji określonych w załączniku nr 3 do projektu ustawy. Po drugie, wiemy, że w pierwszej kolejności kandydatami na dostawców wysokiego ryzyka będą dostawcy z Chin. Po trzecie, możliwe jest dokonywanie szacowania Oceny Skutków Regulacji. Po czwarte, przywołane w uzasadnieniu projektu ustawy badanie BEREK, dotyczące m.in. żywotności sprzętu ICT, dotyczy tylko sieci 5G. Po piąte, przywołane w uzasadnieniu projektu ustawy badanie BEREK, dotyczące m.in. żywotności sprzętu ICT, nie bierze pod uwagę, że żywotność sprzętu ma różne aspekty tzn. w przypadku wielu sprzętów, zwłaszcza użytkowanych w sieci szkieletowej lub wyżej w warstwie dostępowej (np. OLT w sieci stacjonarnej) żywotność sprzętu jako takiego potrafi być bardzo długa. Najczęściej zużywają się różne elementy, takie jak np. zasilacze, wkładki, moduły – ale główny sprzęt nie podlega wymianie. Po szóste, brak Oceny Skutków Regulacji na etapie projektu ustawy oznacza, że ta ocena nie zostanie wykonana nigdy. Kwestie finansowych skutków regulacji nie będą brane pod uwagę ani przy wydawaniu opinii przez Kolegium, ani przy wydawaniu właściwej decyzji przez Ministra Cyfryzacji. Tymczasem skutki nakazu usunięcia sprzętu sieciowego dostawców chińskich z sieci polskich MŚP (nawet jeżeli miałyby być to skutki pośrednie, jak wskazano na początku rozważań w niniejszym punkcie pisma) mają potencjał katastroficzny dla telekomunikacyjnych MŚP. Ilustracją tego, jak	pochodzące od danego dostawcy. Rygor natychmiastowej wykonalności jest konieczny z uwagi na to, że kwestia dotyczy poważnego zagrożenia dla bezpieczeństwa państwa. Nie przewiduje się rekompensat za wycofanie sprzętu lub oprogramowania, ponieważ ten sprzęt i tak z czasem podlegałby wymianie z uwagi na naturalne zużycie. Termin 7 lat na wycofanie sprzętu wydaje się terminem adekwatnym. Jednocześnie skrócono ten termin do 4 lat dla sprzętu i oprogramowania realizującego funkcje krytyczne w zakresie bezpieczeństwa sieci i usług. Wycofanie sprzętu/pochodzącego od dostawcy wysokiego ryzyka w terminie 4 lat dla przedsiębiorców telekomunikacyjnych jest zasadne z uwagi na to, że chodzi o funkcje krytyczne dla sieci i usług. Zauważyć należy, że sprzęt i oprogramowanie i tak wymagałby okresowej wymiany z uwagi na naturalne zużycie sprzętu.

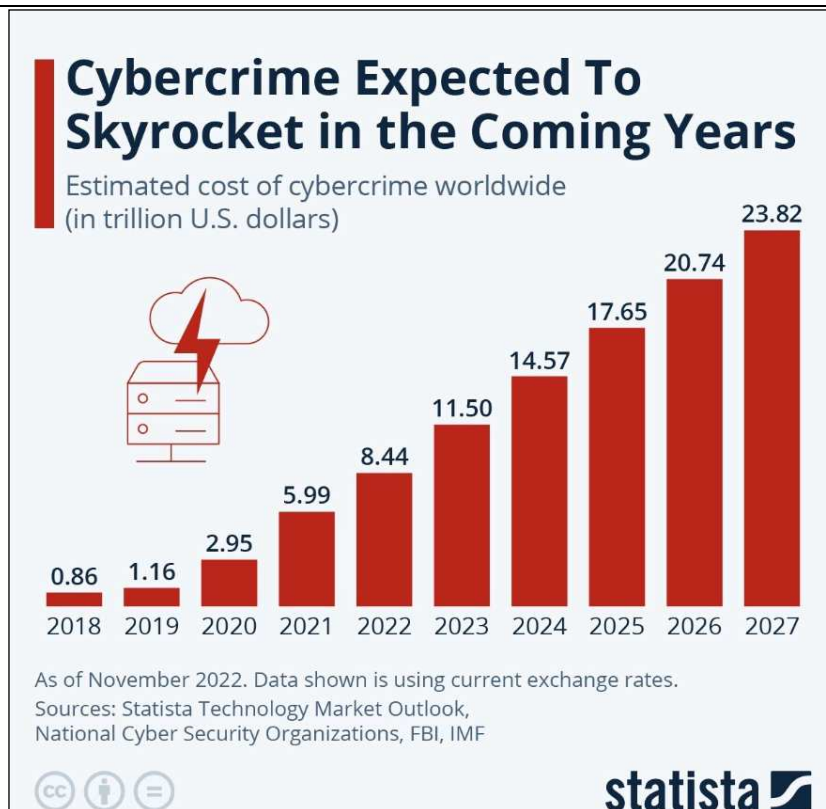
Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			groźne mogłyby być te skutki, może być Badanie KIKE z 2020 r., które załączamy do niniejszego Stanowiska Izby. Taka decyzja może spowodować falę upadłości (lub akwizycji) telekomunikacyjnych MŚP oraz skokowy wzrost cen usług dostępu do internetu, gdyż sprzęt i oprogramowanie dostawców innych niż chińscy jest wielokrotnie droższe. Należy także podkreślić, że sprzęt dostawców innych niż chińscy jest droższy nie tylko w czasie jego zakupu, lecz również jest droższy w utrzymaniu i niesie ze sobą wyższe ryzyko w zakresie cyberbezpieczeństwa w razie ujawniania podatności. Z doświadczeń członków naszej Izby wynika, że chińscy dostawcy sprzętu w krótkim czasie usuwają wszelkie podatności w sprzęcie i oprogramowaniu, niedługo po jego zgłoszeniu. Z kolei dostawcy europejscy i amerykańscy albo ograniczają swoją aktywność w zakresie usuwania podatności do podatności najbardziej krytycznych, albo traktują usuwanie podatności jako kolejną drogą usługę. W opinii Izby, skala zakupu sprzętu od producentów europejskich lub amerykańskich, jaką są w stanie wygenerować polscy MŚP, jest zbyt niska, aby mogli oni liczyć na satysfakcjonujący serwis posprzedażowy. Ponownie przypominamy, że polski rynek jest unikatowy w skali UE pod względem liczby MŚP świadczących usługi komunikacji elektronicznej. Izba zwraca uwagę, że proponowany mechanizm dostawcy wysokiego ryzyka jest sprzeczny z projektowaną ustawą o krajowym systemie certyfikacji cyberbezpieczeństwa. Pomija on bowiem całą planowaną procedurę certyfikacji sprzętów i oprogramowania ICT, w ramach której dany produkt ICT ma być analizowany przez wyspecjalizowane instytucje techniczne pod kątem bezpieczeństwa. Możliwe będzie wystąpienie sytuacji gdzie produkt ICT danego dostawcy uzyska krajową certyfikację a jednocześnie z przyczyn politycznych zostanie uznany za zakazany produkt dostawcy wysokiego ryzyka. Pod względem realizacji celu bezpieczeństwa stosowanych w Polsce produktów ICT, mechanizm dostawcy wysokiego ryzyka dubluje system certyfikacji krajowej i powinien zostać usunięty.	
46.	KIGEIT	Uwaga ogólna	Dyrektywa NIS2 jest rekomendacją wdrożenia ochrony przed wszystkimi możliwymi rodzajami cyberataków (o charakterze kryminalnym i wrogim – realizującym cele APT) realizowanych przy pomocy oprogramowanych urządzeń elektronicznych. Celem cyberataków mogą być obiekty i systemy infosfery (sygnały sterujące, dane, informacje, oprogramowanie i wiedza) oraz technosfery (wszelkiego typu obiekty materialne oraz ludzie). Cele cyberataków kryminalnych, dywersyjnych i wojennych mogą być zbliżone lub takie same. Wraz z rozwojem przestępczości i frontów walki cyfrowej, zwiększa się różnorodność technologii, sprzętu i strategii służących do realizacji cyberataków. Tempo wzrostu skali i różnorodności zagrożeń jest tak duże, że dyrektywa NIS (Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148), nad którą prace zakończono w roku 2015, zdezaktualizowała się. Dlatego Ustawa KSC powinna być przygotowana jako nowa ustawa z uwzględnieniem m.in. następujących faktów: celem ataków są zarówno obiekty funkcjonujące w infosferze jak i w technosferze, • technologie ataków stosowane w infosferze różnią się od ataków w technosferze, • technologie ataków na urządzenia przyłączone do sieci energetycznych, na systemy automatyki przemysłowej itp. różnią się w sposobach realizacji i celach,	Wyjaśnienie uwagi Ministerstwo Cyfryzacji jest zawsze otwarte na propozycje spotkań roboczych w zakresie cyberbezpieczeństwa. Projekt ustawy nakłada ogólne ramy SZBI w art. 8 i zakłada też, że wdrażane środki mają być proporcjonalne do wielkości podmiotu i charakteru świadczonych usług. Przewiduje się także możliwość wydania rozporządzeń doprecyzowujących wymagania SZBI dla poszczególnych sektorów. Ponadto zostaną utworzone CSIRT sektorowe, które będą wspierały przedsiębiorców w poszczególnych sektorach. Będą więc

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

		- cyber-broń (narzędzie cyberataku) może mieć postać: - kodu oprogramowania, - oprogramowanego układu elektronicznego zainstalowanego w fazie produkcji, - nieoprogramowanych układów wykonawczych, - aktywatora kodu lub układów wykonawczych, - kodu aktywacji wcześniej zainstalowanych obiektów wykonawczych, - pamięci niedostępnej dla użytkownika. - cyberataki mogą być realizowane nie tylko na obiekty przyłączone do sieci transmisji danych, lecz również na urządzenia znajdujące się poza kontrolą operatorów systemów działających poprzez sieci transmisji danych, w tym na obiekty nieprzyłączone do żadnej sieci, - uruchomienie cyber-broni może nastąpić: - poprzez sieć telekomunikacyjną, do której przyłączony jest obiekt, - drogą radiową, - poprzez połączenie lokalne zrealizowane przez osobę nieświadomą swej roli w aktywacji określonej cyber-broni - poprzez wcześniej zainstalowane podczas procesu produkcji wrogie kody oprogramowania lub celowo umieszczone w układach IC sprzętowe „bomby logiczne” wyzwalane zdalnie określonymi sygnałami komunikacyjnymi, czasowo lub funkcyjnie bez użycia żadnego kanału komunikacji (praktycznie nie do wykrycia przy rozsądnym koszcie - atak na łańcuch dostaw) - poziom cyfryzacji i cyberbezpieczeństwa różnych sieci, zakładów, instytucji i systemów jest bardzo zróżnicowany technicznie, organizacyjnie i pod względem zaawansowania technologicznego, wybór celów cyber-ataków jest pochodną stosunku kosztów ataku do korzyści (lub strat, jeśli celem ataku jest spowodowanie strat). W związku z powyższym stosowanie jednolitego rozwiązania prawnego dla wszystkich podmiotów jest błędne systemowo i ekonomicznie. Narzędzia prawne do walki z cyberatakami powinny być dopasowane do poziomu już ponoszonych strat oraz uwzględniać dynamikę ich wzrostu. Straty są pochodną struktury i poziomu zaawansowania technologicznego wszystkich obszarów gospodarki państwa. Skuteczne metody ich szacowania pojawiły się dopiero w ubiegłej dekadzie. Wiarygodne dane dot. strat ponoszonych przez Polskę nie są publikowane, ale można je oszacować na podstawie dostępnych danych o stratach globalnych (wykres poniżej).	znały specyfikę danego sektora. Sektory obejmujące automatykę przemysłową są ujęte w projekcie jak np. sektor produkcji.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I



Gospodarka Polski stanowi 1% gospodarki światowej. Przyjmując, że straty powodowane cyberatakami są proporcjonalne do PKB, straty Polski wynoszą ok. 115 mld \$, co stanowi ponad 10% PKB. Zatem prawdopodobna jest teza, że nakłady na obronność są co najmniej 3 razy mniejsze od strat z tytułu niskiego poziomu ochrony cyberbezpieczeństwa. Powszechna jest opinia, że w krajach wysokorozwiniętych straty powodowane cyberatakami są większe w proporcji do PKB niż w krajach niżej rozwiniętych.

W ramach niniejszych konsultacji firmy członkowskie zrzeszone w KIGEiT, zgłosiły zastrzeżenia do ponad 20-u artykułów przesłanego do zaopiniowania projektu. Zestawione w całość - sygnalizują niski poziom zaufania firm do merytorycznej wartości zapisów Ustawy o KSC. Struktura i treść proponowanych zmian wskazuje, że nakłady na przygotowanie Ustawy KSC są nieproporcjonalnie małe do skali problemu, który ma rozwiązać. Uważamy, że bez adekwatnej analizy źródeł i skali strat

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

		oraz potrzeb polskiej gospodarki w tym zakresie, przygotowywana Ustawa KSC nie zahamuje tempa wzrostu tych strat. Uwzględniając powyższe, wspieramy jak najszybsze uchwalenie Ustawy KSC i wydanie szczegółowych rozporządzeń wykonawczych i rekomendacji wspierających uKSC. Skala strat i wysoka dynamika zmian technologicznych wymaga umocowania ustawowego Zespołu Monitorującego składającego się z ekspertów ze wszystkich regulowanych branż, działającego pod przewodnictwem Pełnomocnika Rządu ds. Cyberbezpieczeństwa, którego obowiązkiem będzie ciągłe badanie stanu cyberbezpieczeństwa i na podstawie zebranych danych, doroczne proponowanie zmian w uKSC, polegających na likwidacji przepisów zbędnych i poprawiających skuteczność jej działania. Lista 11-u organów właściwych wskazanych w art. 41 UKSC powinna być uzupełniona o sektor automatyki przemysłowej (sieciowej i produkcyjnej). Zespół Monitorujący powinien być równoprawnym uczestnikiem procesu przygotowywania sprawozdań, celem komunikowania stanu cyberbezpieczeństwa w przedsiębiorstwach komercyjnych, uprawnionym do proponowania rozwiązań legislacyjnych. KIGEiT deklaruje gotowość delegowania ekspertów branżowych do pracy w proponowanym Zespole Monitorującym. oRekomendacje otrzymane przez KIGEiT od podmiotów sektora telekomunikacyjnego były diametralnie różne od rekomendacji formułowanych przez producentów sprzętu i oprogramowania dla sieci energetycznych. Nie są to jednak stanowiska sprzeczne lecz uzupełniające się, potwierdzające tezę, że jedno rozwiązanie dla wszystkich problemów związanych z cyber-bezpieczeństwem jest nieefektywne ekonomicznie. oPodmioty telekomunikacyjne nie widzą uzasadnienia dla wdrożenia restrykcyjnych przepisów weryfikujących dostawców i produkty, więc są przeciwne wdrażaniu przepisów, które służą stworzeniu takiego systemu. Opinia jest pochodną ich doświadczenia z obecnymi dostawcami i wiedzy na temat zagrożeń dla funkcjonowania sieci telekomunikacyjnych i ew. kosztów z tym związanych. Nie przedstawiono żadnych informacji, które zachęcałyby do ponoszenia wysokich kosztów wymiany sprzętu. rNatomiast producenci sprzętu i oprogramowania dla rynku energetycznego nie widzą ryzyka gospodarczego związanego z wprowadzeniem rygorystycznego systemu kontroli produktów cyfrowych instalowanych w sieciach energetycznych. Branża energetyczna pilnie potrzebuje procedur oceny dostawców i weryfikacji produktów wprowadzanych na polski i europejski rynek. Są świadomi rosnących strat generowanych w technosferze, m.in. w energetyce. Ich zdaniem, wprowadzenie ścisłej kontroli dostawców ograniczy ryzyka i możliwości ataków cyfrowych na sieci infrastruktury energetycznej. Branża ta nie jest jeszcze zdominowana przez sprzęt z krajów trzecich i ma nadzieję na ochronę polskiej suwerenności technologicznej dzięki ustawie KSC i rozporządzeniom precyzującym stosowanie doboru dostawców sprzętu tak, by maksymalnie ograniczyć rozpoznane i nierozpoznane ryzyka. rZestawiając powyższe dane z treścią uzasadnienia do opiniowanej Ustawy KSC, bardzo trudno zaufać, skuteczności obecnej polityki cyberbezpieczeństwa, czego wyrazem jest również poziom nakładów na odpowiednie przygotowanie Ustawy KSC. Według naszej oceny wysiłek finansowy i organizacyjny administracji Państwa jest nieproporcjonalnie mały do poziomów zagrożeń i wielkości ponoszonych strat. Niestety, waga i złożoność problemu nie mają odzwierciedlenia w budżecie przeznaczonym na stworzenie	

Tabela uwag zgłoszonych w ramach konsultacji publicznych do *projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw* (UC32) cz. I

			obrony cyfrowej polskiej gospodarki. Opiniowana Ustawa KSC w założeniu miała być generalna i dotycząca wszystkich. W praktyce jest skomplikowana i oderwana od realiów gospodarczych w niektórych branżach, a spełniająca oczekiwania innych. Świadomi, że przedsiębiorca potrzebuje prostego, jasnego prawa, tworzącego warunki równej konkurencji, proponujemy w sposób odrębny uwzględnić obecną wiedzę, możliwości i potrzeby: Niestety, waga i złożoność problemu nie mają odzwierciedlenia w budżecie przeznaczonym na stworzenie obrony cyfrowej polskiej gospodarki. Opiniowana Ustawa KSC w założeniu miała być generalna i dotycząca wszystkich. W praktyce jest skomplikowana i oderwana od realiów gospodarczych w niektórych branżach, a spełniająca oczekiwania innych. Świadomi, że przedsiębiorca potrzebuje prostego, jasnego prawa, tworzącego warunki równej konkurencji, proponujemy w sposób odrębny uwzględnić obecną wiedzę, możliwości i potrzeby: Niestety, waga i złożoność problemu nie mają odzwierciedlenia w budżecie przeznaczonym na stworzenie obrony cyfrowej polskiej gospodarki. Opiniowana Ustawa KSC w założeniu miała być generalna i dotycząca wszystkich. W praktyce jest skomplikowana i oderwana od realiów gospodarczych w niektórych branżach, a spełniająca oczekiwania innych. Świadomi, że przedsiębiorca potrzebuje prostego, jasnego prawa, tworzącego warunki równej konkurencji, proponujemy w sposób odrębny uwzględnić obecną wiedzę, możliwości i potrzeby: Niestety, waga i złożoność problemu nie mają odzwierciedlenia w budżecie przeznaczonym na stworzenie obrony cyfrowej polskiej gospodarki. Konkurencyjny rynek operatorów infrastruktury sieciowej zmusza do stałej redukcji kosztów sprzętowych, w ramach obowiązującego prawa. Dlatego każda regulacja powodująca wzrost kosztów prowadzenia działalności gospodarczej będzie kontestowana tym bardziej, im słabsze będzie uzasadnienie dla jej wprowadzenia. Jednak opór będzie mniejszy, jeśli wzrost kosztów będzie mógł być skompensowany możliwością zwiększenia przychodów. W tym zakresie Państwo może podjąć określone decyzje. W przypadku producentów i operatorów, zadaniem ustawodawcy jest uwzględnić postulaty rzeczywiście spełniające cel regulacji, natomiast odrzucać te, które mogą być pomysłem na budowanie barier pozataryfowych, obniżających konkurencyjność i tempo rozwoju gospodarczego. Duże znaczenie będą miały szczegółowe rozporządzenia wykonawcze do KSC, które powinny uwzględniać specyfikę i sytuację w poszczególnych branżach. Trwający od lat spór wokół kolejnych projektów Ustawy KSC jest pochodną stanu zaufania i jakości komunikacji pomiędzy interesariuszami tego procesu. Możemy mieć tylko nadzieję, że wyższa świadomość skali problemu, może być podstawą do ustanowienia właściwego budżetu na systematyczną analizę zagrożeń i poprawę funkcjonowania systemu cyberbezpieczeństwa. rZgodnie z powyższym przedstawiamy w sposób odrębny uwagi sformułowane przez Sekcję Operatorów Telekomunikacyjnych (SOT) i Sekcję Inteligentnych Sieci - Smart Grids SIS-SG. Obie sekcje działają w ramach KIGEiT.r	
47.	KIGEIT	Uwaga ogólna	Projekt KSC znacząco rozszerza regulację dotyczącą krajowego systemu cyberbezpieczeństwa (dalej: „Ustawa KSC”) na różne sektory gospodarki, które obecnie nie podlegają pod przepisy w tym zakresie, a mimo tego w ramach konsultacji publicznych nie uwzględniono przedstawicieli większości z tych sektorów, stąd niepokój Izby dotyczący tego jak Ministerstwo Cyfryzacji dokonało analizy wpływu projektowanych przepisów i jak planuje budować świadomość co do konieczności dostosowania się do nowych obowiązków.	Wyjaśnienie uwagi Projekt był dostępny publicznie na stronach Rządowego Centrum Legislacji i każdy mógł zgłosić uwagi.
48.	KIGEIT	Uwaga ogólna	Projekt KSC zakłada przeregulowanie (w porównaniu z regulacjami UE i innych krajów UE) w zakresie sektorów gospodarki objętych nowymi przepisami. m.in. uwzględnienie jako podmiotów	Uwaga uwzględniona

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			kluczowe sektorów wskazanych w Dyrektywie NIS jako ważne (zwiększenie tym samym wobec nich nadzoru regulacyjnego oraz zagrożenia sankcjami) – zdaniem Izby jest to przykład nieuzasadnionego tzw. gold-platingu, czyli nadimplementacji prawa unijnego przez państwo członkowskie.	Wymogi dla podmiotów ważnych zostaną złagodzone.
49.	KIGEIT	Uwaga ogólna	Projekt KSC wprowadza dodatkowe regulacje względem Dyrektywy NIS2 poprzez propozycję dokonywania procedury oceny dostawcy wysokiego ryzyka, w konsekwencji której możliwy jest zakaz używania oraz nakaz wycofania produktów, usług i procesów ICT wobec wszystkich podmiotów uznanych za podmioty kluczowe oraz ważne (dalej: „Procedura DWR”). Pomimo odwoływania się w kontekście Procedury DWR w uzasadnieniu oraz Ocenie Skutków Regulacji (dalej: „OSR”) Projektu KSC do tzw. 5G Toolbox , czyli dokumentu unijnego dotyczącego bezpieczeństwa sieci 5G, narzędzie to adresowane jest nie tylko do sektora telekomunikacyjnego i sieci 5G, ale o wiele szerzej względem wszystkich podmiotów kluczowych i ważnych.	Wyjaśnienie uwagi Zgodnie z dyrektywą NIS2 wszystkie podmioty kluczowe oraz podmioty ważne muszą dbać o bezpieczeństwo łańcucha dostaw. Z tego powodu zasadne jest, aby istniała możliwość identyfikacji dostawców wysokiego ryzyka dla wszystkich podmiotów kluczowych i ważnych.
50.	KIGEIT	Uwaga ogólna	Ocena skutków regulacji Projektu KSC nie zawiera nawet szacunkowych analiz wpływu projektowanych przepisów na konkurencyjność gospodarki i polskich firm w odniesieniu do konkretnych sektorów i podsektorów objętych regulacjami. W przypadku wprowadzania narzędzia tak daleko idącego i godzącego w swobodę prowadzenia działalności gospodarczej, jak wskazana powyżej Procedura DWR, minimalnym działaniem powinno być szacowanie jaki wpływ na gospodarkę i poszczególne sektory objęte tymi przepisami (zgodnie z OSR ponad 38 tys. podmiotów kluczowych i ważnych) może mieć wydanie decyzji w ramach Procedury DWR. Brak uprzednich analiz, estymacji i symulacji oddziaływania Procedury DWR oraz wydania decyzji stwarza bardzo duże ryzyko - nie tylko dla dalszego rozwoju gospodarczego, ale również dla możliwości dalszego korzystania z obecnie świadczonych przez podmioty kluczowe i ważne usług.	Wyjaśnienie uwagi Bardzo trudno jest oszacować koszty wdrożenia z uwagi na brak danych, różnorodność podmiotów, ich usług czy wielkość.
51.	KIGEIT	Uwaga ogólna	Brak świadomości podmiotów objętych nowymi regulacjami co do obowiązków i możliwości skorzystania z Procedury DWR przez Ministra Cyfryzacji, w tym brak skierowania Projektu KSC do konsultacji publicznych względem wszystkich ujętych w regulacji sektorów. Pomimo tego, że Ustawa KSC już obecnie funkcjonuje, projektowane zmiany zakładają znaczące rozszerzenie podmiotów nią objętych, jak i zmiany w zakresie wymaganych obowiązków. Wskazywane w ramach OSR objęcie Projektem KSC ponad 38 tys. podmiotów świadczy o tym, jak duży będzie wpływ projektowanych regulacji na polską gospodarkę. Wyznaczony czas 30 dni na konsultacje projektu, którego 70% stanowią całkowicie nowe propozycje (jak wskazał sam Projektodawca przy publikacji) i który dotyczyć będzie działań podejmowanych przez ponad 38 tys. podmiotów, to bardzo krótki czas - zważywszy na to, że do konsultacji publicznych nie zostały zaproszone izby gospodarcze czy podmioty z wszystkich sektorów objętych nowymi regulacjami. Biorąc pod uwagę zobowiązania rządu co do zmiany i podwyższenia standardów prowadzenia procesów legislacyjnych, niestety w tym przypadku podjęte przez Projektodawcę kroki nie są	Wyjaśnienie uwagi Każdy mógł się wypowiedzieć w ramach konsultacji publicznych. Projekt był dostępny na stronach Rządowego Centrum Legislacji.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			wystarczające. Wersja projektu KSC przygotowana przez poprzedni rząd³, zakładała finalnie oddziaływanie proponowanych regulacji na kilka razy mniejszą liczbę podmiotów, a na konsultacje wyznaczony był taki sam czas, ponadto do konsultacji publicznych zaproszonych zostało 51 podmiotów, a w przypadku obecnie procedowanego projektu, którego wpływ gospodarczy jest nieporównywalnie większy, zaproszenie do konsultacji publicznych skierowane zostało tylko do 60 podmiotów. Przy czym nie wymaga aż tak wielkiego zaangażowania i wysiłku szybkie wyszukanie przedstawicieli sektorów objętych projektowanymi obowiązkami, jak np. Polska Izba Przemysłu Chemicznego, Izba Gospodarcza „FARMACJA POLSKA”, Ogólnopolska Izba Gospodarcza Wyrobów Medycznych POLMED, PSF Polskie Stowarzyszenie Fotowoltaiczne, Polska Federacja Szpitali itp. Biorąc pod uwagę objęcie nowymi przepisami 17 sektorów gospodarki (zgodnie z Dyrektywą NIS2 18, jednak Projektodawca złączył dwa sektory w jeden), obecny sposób prowadzenia analiz wpływu regulacji oraz konsultacji mija się w tym co zapowiadali Ministrowie obejmując kierownictwo nad Ministerstwem Cyfryzacji. Minister Cyfryzacji Krzysztof Gawkowski deklarował, że jego resort jest świadom konsekwencji wprowadzanych rozwiązań: „<i>Chcemy, aby projekt ustawy o Krajowym Systemie Cyberbezpieczeństwa był gotowy w II kw., ale zdajemy sobie sprawę z wagi tego prawa. Dlatego postanowiliśmy, że będziemy prowadzili politykę bardzo otwartych drzwi w ramach szerokich konsultacji</i>”⁴, podobnie wiceminister Paweł Olszewski wskazywał: „<i>W marcu będzie projekt ustawy wdrażający dyrektywę NIS2. Będzie on poddany szerokim konsultacjom: wewnętrznym, społecznym, międzyresortowym.</i>”⁵. Rozumiejąc zbliżający się termin implementacji Dyrektywy NIS2, Izba zwraca uwagę, że to nie przedsiębiorcy powinni ponosić odpowiedzialność za opóźnienie administracji publicznej w przeprowadzeniu procesu legislacyjnego. Biorąc pod uwagę szeroki zakres regulacji i podmiotów zobowiązanych do jej stosowania, konieczność poniesienia wysokich kosztów dodatkowych związanych z przygotowaniem do wdrożenia oraz realizacją nowych obowiązków, zapewniony powinien być odpowiedni czas na analizę projektowanych przepisów przez wszystkie podmioty zobowiązane do stosowania przepisów.	
52.	Naczelna Rada Zrzeszeń Handlu i Usług	Ogólna	Jako Naczelna Rada Zrzeszeń Handlu i Usług, od 90 lat reprezentująca małych i średnich przedsiębiorców - polskich kupców, pragniemy przekazać nasze uwagi do opublikowanego w dniu 24 kwietnia 2024 r. projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (dalej „projekt nowelizacji KSC”).	Wyjaśnienie uwagi Termin 30 dni to standardowy termin na konsultacje projektu ustawy.

³ <https://legislacja.rcl.gov.pl/projekt/12337950/katalog/12716608#12716608>

⁴ <https://biznes.pap.pl/en/news/pap/info/3562822,rzad-rozpocznie-prace-nad-ustawa-o-ksc-w-iii-kw---fundusz-cyberbezpieczenstwa-wiekszy-o-150-proc->

⁵ <https://www.gazetaprawna.pl/wiadomosci/kraj/artykuly/9444051,olszewski-trzeba-zbudowac-przejrzysty-system-walki-z-dezinformacja-w.html>

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			Korzystając z możliwości wzięcia udziału w konsultacjach publicznych do projektu nowelizacji KSC, poniżej przesyłamy uwagi, które w naszej ocenie wpłyną na prawidłowość obrotu gospodarczego oraz rozwoju polskiej przedsiębiorczości. Powyższe dwa elementy gospodarki są dla podmiotów stowarzyszonych w naszym Zrzeszeniu niezwykle istotne. Obawiamy się, iż wprowadzenie przepisów prowadzących finalnie do ograniczenia wymiany handlowej z państwami spoza Unii Europejskiej oraz państw członkowskich NATO (np. Korea Południowa, Argentyna, Indie, Chiny, Brazylia) przełoży się na zmiany w polskim handlu w sposób bardzo negatywny. Ograniczone zostanie bowiem korzystanie z pewnych grup dostawców, których produkty, procesy czy też usługi są dostarczane innym podmiotom w Polsce właśnie przez członków Zrzeszenia. Ostatnie lata były bardzo trudne dla mniejszych podmiotów, z obawą spoglądają oni w przyszłość, która to obawa pogłębia się w obliczu projektowania przepisów. Czynią one sytuację gospodarczą i prawną wyjątkowo niepewną. Dlatego kierujemy prośbę do Pana Ministra o wydłużenie terminu konsultacji publicznych o 30 dni, aby zainteresowane strony mogły rzetelnie i skrupulatnie dokonać oceny projektu nowelizacji KSC. Mówiąc o problemach wynikających z niepewnej sytuacji gospodarczej i prawnej, nie sposób nie wspomnieć o zaprojektowanych przepisach odnoszących się do ograniczenia procedury administracyjnej. Wiemy jak ważna jest transparentność i uczciwość w prowadzeniu biznesu, niezależnie od wielkości danego podmiotu, stąd też dziwi nas przyjęte rozwiązanie, które uniemożliwia podmiotowi uzyskanie pełnej informacji o jego statusie i tym samym podjęcie działań naprawczych. Chcemy, aby polski rynek był rynkiem zdrowej konkurencji oraz uczciwej współpracy, gdzie ocena polega na kryteriach sprawdzalnych oraz mierzalnych a nie politycznych i co ważne, ocena ta jest dla podmiotu weryfikowanego jawna. Obawiamy się, że proponowane przepisy utrudnią działalność kupców w pewnych obszarach oraz spowolnią handel. Wierzymy, że dodatkowe 4 tygodnie na konsultacje społeczne oraz zmiana brzmienia przepisów na taki, który nie będzie blokował gospodarki, jest możliwa. Pokazuje to sytuacja w innych krajach Unii, gdzie tam ostrego podejścia nigdzie nie wdrożono. Chcemy, aby polski handel rozwijał się nie tylko na rynku krajowym, ale także na arenie międzynarodowej, osiągnięcie tego celu będzie możliwe tylko wtedy, kiedy zostanie zapewniona stabilność i zaufanie do gospodarki krajowej.	
53.	OPOR	Uwaga ogólna	Na podkreślenie zasługuje również fakt, że po zapoznaniu się z Projektem stwierdzamy, że w znacznej mierze stanowi on nadregulację względem dyrektywy NIS2. W naszej ocenie implementacja dyrektywy NIS2 powinna się odbyć z poszanowaniem zasady proporcjonalności i unikania nakładania nadmiernych obowiązków, które nie wynikają z dyrektywy NIS2, o co również niniejszym postulujemy. Należy wskazać, że OSR powinien zwierać dokonanie w określonym czasie od dnia wejścia regulacji jej ewaluację aby ocenić czy zawarte w niej przepisy faktycznie realizują założone cele.	Uwaga częściowo uwzględniona Wymagania co do audytów dla podmiotów ważnych zostaną złagodzone. OSR przewiduje ewaluację projektu.
54.	OPOS	Uwaga ogólna	Projekt analizowanej ustawy przewiduje nadanie urzędом gmin statusu podmiotów kluczowych, co spowoduje wymóg zapewnienia bezpieczeństwa informacji w oparciu o normy ISO 27001 oraz	Wyjaśnienie uwagi

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

		31000. Zważywszy jednakże na aktualny stan podejścia JST do przedmiotowej kwestii zauważyć należy, że jest to w pełni zasadne. O konieczności systemowych rozwiązań w omawianym zakresie świadczą chociażby wyniki kontroli NIK (Nr ewidencyjny: I/23/001/LSZ) dotyczące zapewnienia bezpieczeństwa teleinformatycznego przez jednostki samorządu terytorialnego w województwie zachodniopomorskim, które wyraźnie wskazują, że w urzędach gmin nie funkcjonują Systemy Zarządzania Bezpieczeństwem Informacji pomimo obowiązku ich stosowania. Wdrożenie Systemu Zarządzania Bezpieczeństwem w mniejszych urzędach gmin (które stanowią około 2/3 ogółu urzędów gmina w Polsce) może stanowić trudne do realizacji wyzwanie ze względu na brak kadry z odpowiednią wiedzą specjalistyczną w dziedzinie bezpieczeństwa informacji w tym teleinformatycznego. Chociaż gminy miały możliwość uzyskania środków na wdrożenie systemu zarządzania bezpieczeństwem informacji w ramach projektu „Cyberbezpieczny Samorząd”, nie są upublicznione dane o liczbie beneficjentów programu, którzy ubiegali się o środki na ten cel. Kolejnym aspektem, na który należy zwrócić uwagę jest braku świadomości w szeroko pojętym zarządzaniu bezpieczeństwem informacji w gminach. Powyższe wynika z ograniczonej wiedzy kadry zarządzającej w obszarze bezpieczeństwa informacji oraz brak stosowanych procedur zarządczych w tym zakresie (np. ISO 27001). W odniesieniu do powyższych uwag, w celu sprawnego wdrożenia zawartych w projekcie ustawy rozwiązań systemowych w zakresie bezpieczeństwa informacji niezbędne w naszej ocenie jest: 1. opracowanie rozwiązań dotyczących wsparcia w szczególności małych gmin w zakresie budowania kompetencji i infrastruktury bezpieczeństwa informacji. Na przykład, organizację szkoleń i warsztatów, oraz udostępnianie zasobów i narzędzi wspierających wdrożenie normy ISO 27001. 2. Wdrożenie modelu współpracy między gminami w zakresie dzielenia się zasobami, know-how i najlepszymi praktykami w zarządzaniu bezpieczeństwem informacji, co może obniżyć koszty i zwiększyć efektywność działań. 3. Rozważenie wprowadzenia udogodnień legislacyjnych lub finansowych dla gmin, które aktywnie pracują nad podnoszeniem standardów bezpieczeństwa informacji.	Będziemy podejmować działania mające na celu wsparcie gmin w realizacji tych obowiązków. W ramach inwestycji C3.1.1 Cyberbezpieczeństwo - CyberPL, infrastruktura przetwarzania danych i dostarczania usług cyfrowych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo – Komponent Cyberbezpieczeństwo (subinwestycja C3.1.1.1), planowane jest uruchomienie czterech projektów dedykowanych dla wybranych grup podmiotów krajowego systemu cyberbezpieczeństwa, w tym dla jednostek sektora finansów publicznych. Aktualnie trwają prace do przygotowania naborów, z uwzględnieniem ich celu określonego w Krajowym Planie Odbudowy i zwiększania odporności. Docelowe grupy odbiorców wsparcia będą wynikały bezpośrednio z tych założeń. Uruchamianie naborów dla tych projektów planowane jest sukcesywnie w kolejnych kwartałach bieżącego roku. Najszerszy zakres wsparcia planowany jest w ramach projektu pn. „Wsparcie 500 podmiotów krajowego systemu cyberbezpieczeństwa w modernizacji i rozbudowie infrastruktury cyberbezpieczeństwa w sieciach IT, w tym wsparcie podmiotów wykorzystujących technologie informacyjne (IT) oraz operacyjne (OT) stosowane w przemysłowych systemach sterowania (ICS)”, o którym mowa jest w dokumencie, który stanowi Załącznik do decyzji wykonawczej Rady UE,

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

				dostępnym pod adresem https://www.gov.pl/web/planodbudowy/o-kpo (strona 125 - pozycja C23G w tabeli). Wsparcie umożliwi wzmocnienie cyberbezpieczeństwa w obszarach organizacji (procedur), kompetencji personelu oraz technologii. Informacje o ogłoszeniu naborów oraz ich szczegółowe warunki będą na bieżąco publikowane na stronie Jednostki wspierającej plan rozwojowy - Centrum Projektów Polska Cyfrowa (CPPC) https://www.gov.pl/web/cppc/. Zwrócić należy jednak uwagę na fakt, że zgodnie z zasadami obowiązującymi w KPO podatek VAT stanowi koszt niekwalifikowany, wobec czego niezbędne jest zaangażowanie na ten cel własnych środków pochodzących z budżetu jednostki.
55.	PIKE	Uwaga ogólna	PIKE apeluje o rezygnację ze wszystkich rozwiązań, które wykraczają poza wymagania określone w dyrektywie NIS2, czyli z tzw. nadregulacji (ang. 'gold-plating'). Projekt ustawy zawiera wyjątkowo dużo rozwiązań, które nie tylko stanowią nadregulację, lecz również nadregulacja ta jest równoznaczna z niezwykle uciążliwymi i kosztownymi obowiązkami, których prawo UE na podmioty kluczowe i ważne nie nakłada. Najbardziej rażącym, choć nie jedynym przykładem tej nadregulacji, są potencjalne skutki wydania decyzji o uznaniu dostawcy sprzętu i oprogramowania za dostawcę wysokiego ryzyka. Z załącznika nr 1 do OSR wynika, że żadne państwo członkowskie nie przewidziało tak daleko idących skutków tej instytucji prawnej, jak polski projektodawca. <u>Państwa członkowskie, jak wskazuje Komisja Europejska w dokumencie „Better Regulation Guidelines” SWD(2021) 305 final), powinny powstrzymać się przed nieuzasadnioną nadregulacją, aby zapewnić równe szanse wszystkim podmiotom działającym na jednolitym rynku.</u> Izba w pełni się zgadza z Komisją Europejską w tym zakresie i wskazuje, że projekt ustawy zawiera dużo nieuzasadnionych rozwiązań, wykraczających poza wymagania dyrektywy NIS2, czyli pod hasłem wdrażania prawa UE polscy przedsiębiorcy będą <u>zmuszeni do spełnienia znacznie większej liczby potencjalnie niezwykle kosztownych obowiązków niż przedsiębiorcy w innych państwach członkowskich.</u> <u>Szczegółowa argumentacja uzasadniająca potrzebę rezygnacji z nadregulacji została ujęta w piśmie przewodnim do niniejszych uwag szczegółowych.</u>	Uwaga częściowo uwzględniona Wymogi projektu zostały złagodzone.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

56.	PIKE	Uwaga ogólna	Dyrektywa NIS2 zawiera wielokrotne odesłania do dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylającej dyrektywę Rady 2008/114/WE (dyrektywa CER). Z kolei z motywu 30 dyrektywy NIS2 wynika, że prace nad wdrożeniem dyrektywy NIS2 oraz dyrektywy CER powinny być skoordynowane. Taka koordynacja z pewnością byłaby ułatwiona, a terminy transpozycji miałyby większą szansę na dotrzymanie, gdyby we wdrażaniu obu dyrektyw zakres niepotrzebnych obowiązków, których prawo UE wcale nie nakłada, został ograniczony do minimum. Wspomniany motyw 30 stanowi: „Zważywszy na powiązania między cyberbezpieczeństwem a bezpieczeństwem fizycznym podmiotów, należy zapewnić spójność podejścia między dyrektywą Parlamentu Europejskiego i Rady (UE) 2022/2557 (13) a niniejszą dyrektywą. W tym celu podmioty zidentyfikowane jako podmioty krytyczne na mocy dyrektywy (UE) 2022/2557 powinny być uznawane za podmioty kluczowe na podstawie niniejszej dyrektywy. Ponadto każde państwo członkowskie powinno zapewnić, aby w jego krajowej strategii dotyczącej cyberbezpieczeństwa przewidziano ramy polityki umożliwiające zwiększoną koordynację w obrębie tego państwa członkowskiego między jego właściwymi organami na podstawie niniejszej dyrektywy i tymi na podstawie dyrektywy (UE) 2022/2557 w kontekście wymiany informacji na temat ryzyka, cyberzagrożeń i incydentów, a także ryzyka, cyberzagrożeń i incydentów poza cyberprzestrzenią, a także wykonywania zadań nadzorczych. Właściwe organy na podstawie niniejszej dyrektywy i te na podstawie dyrektywy (UE) 2022/2557 powinny ze sobą współpracować i wymieniać się informacjami bez zbędnej zwłoki, w szczególności w odniesieniu do identyfikacji podmiotów krytycznych, ryzyka, zagrożenia i incydentów w cyberprzestrzeni oraz ryzyka, zagrożeń i incydentów poza cyberprzestrzenią wpływających na podmioty krytyczne, co obejmuje środki dotyczące cyberbezpieczeństwa i środki fizyczne stosowane przez podmioty krytyczne, a także wyniki działań nadzorczych przeprowadzonych wobec takich podmiotów. Ponadto aby usprawnić działania nadzorcze między właściwymi organami na podstawie niniejszej dyrektywy oraz tymi na podstawie dyrektywy (UE) 2022/2557 oraz zminimalizować obciążenie administracyjne podmiotów, których to dotyczy, te właściwe organy powinny starać się zharmonizować wzory zgłoszeń incydentów i procesy nadzorcze. W stosownych przypadkach właściwe organy działające na podstawie dyrektywy (UE) 2022/2557 powinny móc zwrócić się do właściwych organów na podstawie niniejszej dyrektywy, aby wykonały swoje uprawnienia nadzorcze i wykonawcze w stosunku do podmiotu, który został zidentyfikowany jako podmiot krytyczny na podstawie dyrektywy (UE) 2022/2557. Właściwe organy na podstawie niniejszej dyrektywy i te na podstawie dyrektywy (UE) 2022/2557 powinny, w miarę możliwości w czasie rzeczywistym, współpracować i prowadzić wymianę informacji w tym celu”.	Uwaga uwzględniona, Planujemy koordynację w zakresie dyrektywy CER.
57.	PIKE	Uwaga ogólna	Na podstawie motywu 16 dyrektywy NIS2 PIKE wnosi o dodanie do ustawy regulacji umożliwiającej niestosowanie (ewentualne stosowanie w ograniczonym zakresie) obowiązków wynikających z ustawy o krajowym systemie cyberbezpieczeństwa przez tych przedsiębiorców telekomunikacyjnych, którzy wchodzi w skład grupy kapitałowej i którzy korzystają z CUW, świadczone przez spółkę z grupy uznaną za podmiot kluczowy lub podmiot ważny.	Uwaga uwzględniona

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

58.	Polska Izba Gospodarki Odpadami	Uwaga ogólna	Konieczne jest wydłużenie czasu na dostosowanie realnych możliwości i potrzeb sektora do zmienionych przepisów. Nowe wymagania są znacznie bardziej rygorystyczne w porównaniu do obecnego stanu w branży. Wprowadzenie tych zmian będzie kosztowne i czasochłonne, wymagając zaangażowania dodatkowych zasobów ludzkich. Nowe przepisy wiążą się z wysokimi kosztami wdrożenia. Należy zaznaczyć, że ewentualne przeniesienie działań dostosowujących dany podmiot do KSC na podmiot trzeci (outsourcing) a w szczególności zarządzanie obszarem cyberbezpieczeństwa, nie będzie w tym zakresie skutecznym i realnym rozwiązaniem. Ryzyko wystąpienia incydentu w tym obszarze jest bardzo wysokie, co może skutkować nałożeniem na spółkę oraz na jej zarządzających wysokich kar. W związku z tym sugerujemy wprowadzenie okresów przejściowych oraz programów wsparcia finansowego lub ulg podatkowych dla przedsiębiorstw, aby umożliwić im płynne przejście do nowych wymagań. Aby zapewnić spójność i jednolitość działań, konieczne jest ponadto uzyskanie jasnych wytycznych dotyczących standardów, do których przedsiębiorstwa powinny się stosować. Sugerujemy także wprowadzenie programów edukacyjnych i szkoleń dla pracowników branży, aby zapewnić im odpowiednie kompetencje i wiedzę niezbędną do przestrzegania nowych regulacji. Wsparcie w tym zakresie może znacząco przyspieszyć proces adaptacji do nowych wymagań.	Wyjaśnienie uwagi W projekcie wprowadzono okres przejściowy na dostosowanie się do regulacji.
59.	Polska Izba Kolei	Uwaga ogólna	Działając w imieniu Polskiej Izby Kolei, mając na względzie opublikowany w dniu 24 kwietnia 2024 roku projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw¹, który ma implementować dyrektywę NIS22, niniejszym zwracamy się do Pana Ministra z wnioskiem o rozważenie zmiany postanowień projektu i usunięcie nieproporcjonalnych środków zarządzania cyberbezpieczeństwem z projektu ustawy, w tym dotyczących wykluczania dostawców w oparciu o kryteria nietechniczne oraz przeprowadzenie rzetelnej oceny skutków regulacji na sektor transportu kolejowego, a także szerokich konsultacji branżowych. Sektor transportu jest niezwykle istotny z perspektywy gospodarczej Polski. Polska będąc położona centralnie w Europie. Środkowo-Wschodniej stanowi ważny szlak komunikacyjny dla transportu osób oraz towarów w Europie. Rozwój technologiczny branży transportowej niesie ze sobą nowe możliwości w zakresie innowacji, natomiast niewątpliwie również powoduje konieczność zaadresowania wyzwań i zagrożeń w zakresie cyberbezpieczeństwa. Dlatego uważamy, że Projekt w sposób bezpośredni i znaczący wpłynie na branżę transportu, a ponieważ zagadnienie cyberbezpieczeństwa jest niezwykle istotne z punktu widzenia funkcjonowania nowoczesnego transportu, to wymaga szerokiej i dogłębnej analizy z punktu widzenia wprowadzanych środków bezpieczeństwa; które z jednej strony zapewnią bezpieczeństwo, ale z drugiej powinny być proporcjonalne, aby były kosztowo efektywne i sprzyjały rozwojowi innowacji w transporcie. W związku z powyższym konieczna jest dogłębna analiza w ocenie skutków regulacji kosztów zarówno wdrożenia jak i następnie kosztów operacyjnych wiążących się z wypełnieniem obowiązków wskazanych w Projekcie. Podkreślenia wymaga, że pod uwagę w takiej analizie należy również wziąć obciążenia finansowe dla przedsiębiorców wynikające z konieczności wymiany sprzętu w przypadku wydania decyzji administracyjnej o dostawcy wysokiego ryzyka. Branża transportowa niewątpliwie współpracuje z dostawcami spoza Unii Europejskiej oraz NATO i	Uwaga nieuwzględniona Ocena ryzyka dostawców wysokiego ryzyka powinna obejmować wszystkie aspekty działalności dostawcy, zarówno aspekty techniczne jak i nietechniczne.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			potencjalnie uznanie takiego dostawcy za tzw. dostawcę HRV spowoduje znaczące koszty wymiany sprzętu, oprogramowania, procesów ICT. W ocenie skutków regulacji również ta kwestia nie została poddana analizie, podczas gdy ma ona fundamentalne znaczenie z punktu widzenia operacyjnego przedsiębiorstw z branży transportowej. Również przy analizie kosztów pod uwagę powinna zostać wzięta także kwestia amortyzacji sprzętu i tego czy okres na wycofanie sprzętu jest kompatybilny ze wspomnianym okresem amortyzacji sprzętu dla branży transportowej. Podkreślenia również wymaga, że w kontekście oceny ryzyka dostawcy zasadne jest skupienie się na przesłankach technicznych takich jak certyfikacja, co pozwoli na zapewnienie stabilności i pewności w zakresie funkcjonowania podmiotów na rynku. Jak zostało wyżej wspomniane Projekt w znaczny sposób będzie oddziaływał na przedsiębiorstwa z branży transportu kolejowego. Wielu przedsiębiorców natomiast nawet nie ma świadomości, że za około pół roku mają zacząć obowiązywać przepisy, które w sposób fundamentalny wpłyną na koszty ich działalności na polskim rynku. W związku z tym konieczna jest odpowiednia komunikacja i zorganizowanie uzgodnień międzyresortowych także z udziałem branży transportowej.	
60.	Polskie Stowarzyszenie Fotowoltaiki	Uwaga ogólna	Jako organizacja przedsiębiorców działających w sektorze wielkoskalowej energetyki słonecznej, w związku z publikacją projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (nr UC 32, „Projekt”), pragniemy przedstawić nasze uwagi do Projektu Sektor odnawialnych źródeł energii to obecnie jeden z kluczowych obszarów gospodarki. W celu umożliwienia rozwoju opartego na czystych źródłach energii potrzebne są stabilne i przewidywalne ramy prawne, które nie będą nakładały nieproporcjonalnych obowiązków na inwestorów. Bez takich uwarunkowań „zielona transformacja” może nie tylko zostać w Polsce znacznie spowolniona, ale wręcz cofnięta. Jak wiadomo, celem Projektu jest implementacja Dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 z 14 grudnia 2022 roku w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii Europejskiej, zmieniającej rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającej dyrektywę (UE) 2016/1148 (dalej: „NIS2”). Wyrażamy oczywiście całkowite zrozumienie dla tworzenia mechanizmów prawnych podnoszących bezpieczeństwo państwa w kluczowych obszarach oraz potrzebę kontroli narzędzi komunikacyjnych. Jednakże w obecnym kształcie, Projekt wprowadza obowiązki dla przedsiębiorców, które nie wynikają z przepisów NIS2 lub przyjmuje rozwiązania dużo bardziej rygorystyczne niż ustawodawca unijny. Poniżej przedstawiamy tylko przykładowe problemy, które udało nam się zauważyć: 1. Regularne audyty – NIS2 nie wprowadza obowiązków czasowych. Tymczasem Projekt przewiduje obowiązek przeprowadzenia audytu raz na dwa lata, bez względu na wcześniejszą ocenę ryzyka; 2. Dostawcy wysokiego ryzyka (DWR) – Projekt wprowadza procedurę DWR w 18 sektorach, co nie wynika ani z NIS2. Tylko Polska stosuje DWR w 18 sektorach w zależności od kraju pochodzenia, podczas gdy żaden z krajów UE w transpozycji NIS2 nie uzależnia DWR od kraju pochodzenia.	Wyjaśnienie uwagi NIS2 przewiduje regularne audyty stąd też w projekcie wskazano czas tych audytów. Czas na wycofanie sprzętu pochodzącego od dostawcy wysokiego ryzyka pokrywa się z cyklem życia produktu.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

		3. Ponadto Projekt przewiduje, naszym zdaniem, nieprzejrzystą procedurę administracyjną wobec DWR w odniesieniu do krajów spoza UE/NATO, która pozbawia strony wielu gwarancji procesowych, w tym m.in. ograniczenie dostępu do informacji oraz prawa odwołania. 4. Arbitralne stosowanie oceny bezpieczeństwa. Projekt przyjmuje możliwość przeprowadzania oceny bezpieczeństwa bez żadnych doprecyzowujących warunków, pozostawiając zbyt szeroki zakres uznania administracyjnego. NIS2 wymaga przeprowadzania ocen bezpieczeństwa wedle proporcjonalnych, przejrzystych i niedyskryminujących kryteriów. 5. Krótki czas na wycofanie sprzętu ICT: Projekt wprowadza obowiązek wycofania procesu, usługi, produktu ICT w okresie 7 lat, co może poważnie zachwiać stabilnością finansową przedsiębiorstw. Z zaniepokojeniem stwierdzamy, że projektowane przepisy prowadzą do przeregulowania rynku oraz mogą zahamować tempo zielonej transformacji polskiej gospodarki. Zwracamy uwagę, że podmioty objęte nowymi obowiązkami zostały narażone na znaczące obciążenia finansowe, co w żaden sposób nie zostało poddane analizie w Ocenie Skutków Regulacji. W związku z tym, potrzeba zdecydowanie więcej czasu na analizę potencjalnych gospodarczych konsekwencji Projektu. Polski sektor energetyczny, w tym branża OZE, podlega dynamicznej digitalizacji. W związku z tym, wszelkie zmiany dotyczące cyberbezpieczeństwa w sposób znaczący wpływają na rozwój odnawialnych źródeł energii i transformację gospodarki. Wszystkie OZE, a w szczególności wielkoskalowa energetyka słoneczna, są w dużym stopniu uzależnione od nowoczesnych technologii informatycznych i komunikacyjnych (ICT). Inteligentne sieci energetyczne, systemy zarządzania energią, platformy monitoringu i sterowania - to tylko przykłady kluczowych elementów infrastruktury, które są istotnie powiązane z cyberbezpieczeństwem. Pragniemy zwrócić uwagę, że energetyka to nie tylko duże podmioty, ale również z małe i średnie przedsiębiorstwa. Tymczasem Projekt nie różnicuje zakresu nakładanych obciążeń z uwagi na skalę prowadzonej działalności. Wysokie koszty związane z wdrażaniem nowych przepisów cybernetycznych mogą zatem stanowić znaczące obciążenie dla MŚP, zniechęcając je do rozwijania działalności w branży odnawialnej. Tymczasem małe elektrownie słoneczne czy farmy wiatrowe są często kluczowe dla funkcjonowania lokalnych rynków energii. Nieproporcjonalne wymagania prawne mogą znacząco utrudnić ich działalność, co wpłynie na zahamowanie rozwoju rozproszonej energetyki. Wprowadzenie Projektu w obecnym kształcie, zwłaszcza jeśli nakładane obowiązki nie będą dostosowane do skali działalności i specyfiki różnych podmiotów, może mieć również niekorzystny wpływ na rentowność projektów fotowoltaicznych. Obowiązkowe audyty bezpieczeństwa, wdrażanie dodatkowych obowiązkowych zabezpieczeń, a także konieczność częstej wymiany sprzętu ICT, będą generować dodatkowe koszty operacyjne, które ostatecznie przełożą się na wzrost cen energii elektrycznej. Niewątpliwie przyczyni się to również do obniżenia rentowności projektów, co z kolei może wywołać efekt mrozący wobec zaangażowania w rozwój projektów OZE. Warto zauważyć, że Projekt wprowadza instytucję Dostawcy Wysokiego Ryzyka, który to status będzie nadawany w drodze decyzji administracyjnej. Takie rozstrzygnięcie będzie oznaczać obowiązek wycofania procesu, usługi, produktu ICT w okresie 7 lat. Tak krótki czas na wycofanie sprzętu, który w sektorze energetyki podlega zazwyczaj	

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			kilkunastoletniej amortyzacji może poważnie zachwiać stabilnością finansową przedsiębiorstw, co może dalej przełożyć się na ceny energii i bezpieczeństwo energetyczne Polski. Masowe wycofanie z eksploatacji sprzętu ICT w może także zakłócić działanie istniejącej infrastruktury energetycznej, prowadząc do spotęgowania zjawiska przerw w dostawie energii oraz potencjalną destabilizację polskiego systemu elektroenergetycznego. Proponowane regulacje mogą zatem, w naszej ocenie, doprowadzić do znaczącego spowolnienia obecnych inwestycji w energię słoneczną oraz do osłabienia długofalowej atrakcyjności Polski dla podmiotów chcących inwestować w zieloną transformację naszej gospodarki. Skutki zwolnienia tej dynamiki inwestycyjnej odczują wszystkie podmioty gospodarcze w Polsce oraz zwykli obywatele, przede wszystkim w rachunkach za energię elektryczną. W związku z powyższym absolutnie kluczowe jest, aby zostały przeprowadzone szerokie konsultacje publiczne i dogłębna analiza projektowanych przepisów pod względem ich skutków ekonomicznych. Aby mogło do tego dojść konieczne jest naszym zdaniem przedłużenie konsultacji publicznych, przynajmniej do 60 dni. Liczymy na uwzględnianie głosu branży słonecznej na dalszych etapach procesu legislacyjnego.	
61.	Porozumienie Zielonogórskie	Uwaga ogólna	W związku z przekazaniem do konsultacji społecznych projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw Federacja Związków Pracodawców Ochrony Zdrowia „Porozumienie Zielonogórskie” zgłasza uwagi: Zdaniem Federacji realizacja obowiązków zawartych w przedstawionym projekcie przez małe podmioty udzielające świadczeń podstawowej opieki zdrowotnej, stomatologii, czy ambulatoryjnej opieki specjalistycznej będzie niemożliwa lub bardzo utrudniona z powodu małych zasobów kadrowych i finansowych. Federacja proponuje wykluczyć z podmiotów objętych proponowaną regulacją wszystkie małe i średnie podmioty/przedsiębiorstwa, w tym Samodzielne Publiczne Zakłady Opieki Zdrowotnej, udzielające świadczeń ambulatoryjnych w ramach umowy z Narodowym Funduszem Zdrowia. yRozumiejąc potrzebę wdrażania rozwiązań w zakresie cyberbezpieczeństwa wskazujemy na konieczność prac nad rozwiązaniami realnymi do wdrożenia w małych podmiotach. Takimi rozwiązaniami mogą być przygotowywane z reprezentacją środowiska dobre praktyki, wytyczne postępowania itp. i Federacja jest gotowa do współpracy w tym zakresie.	Uwaga częściowo uwzględniona Nie jest możliwe wykluczenie średnich przedsiębiorstw, ponieważ one wchodzą w zakres dyrektywy NIS2. Natomiast zostanie wprowadzona zmiana zgodnie z którą co najmniej średni SPZOZ będzie podlegał ustawie.
62.	Sobiesław Zasada Spółka Akcyjna S.K.A.	Uwaga ogólna	Co więcej wątpliwości budzi zakres podmiotowy Projektu, który jest znacznie szerszy od tego, który został wskazany w dyrektywie NIS 2. Wiele tysięcy podmiotów zostanie obciążone obowiązkiem wdrożenia dodatkowych wewnętrznych procedur, których wprowadzenie będzie przede wszystkich czasochłonne, a ponadto znacząco obciąży budżet wielu podmiotów gospodarczych. Liczna grupa podmiotów zostanie zakwalifikowana jako podmiot kluczowy lub ważny jedynie ze względu na powiązania wewnątrz korporacyjne. Obarczenie zatem podmiotów obowiązkami i kosztami, które jako jednostka by nie ponosiła, stanowi zagrożenie dla bytu i funkcjonowania wielu podmiotów gospodarczych.	Uwaga częściowo uwzględniona Wymogi projektu zostaną złagodzone, w szczególności dla podmiotów ważnych.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

63.	Sobiesław Zasada Spółka Akcyjna S.K.A.	Uwaga ogólna	Obciążenie tak rygorystycznymi obowiązkami ogromnej liczby podmiotów gospodarczych, w szczególności małych przedsiębiorstw, które będą związane takimi samymi obowiązkami jak wielkie podmioty gospodarcze stanowi naruszenie zasady proporcjonalności wyrażonej w dyrektywie NIS 2.	Uwaga częściowo uwzględniona Wymogi projektu zostaną złagodzone, w szczególności dla podmiotów ważnych.
64.	Sobiesław Zasada Spółka Akcyjna S.K.A.	Uwaga ogólna	Przyjęte rozwiązania implementujące dyrektywę NIS 2 rodzą poważne konsekwencje dla wielu sektorów gospodarki kraju. Proponowane w Projekcie rozwiązania nie wynikają wprost z treści dyrektywy NIS 2, a co więcej z nieuzasadnionych względów stanowią ich zaostrzenie, wprowadzając restrykcyjne normy, niewymagane dyrektywą NIS 2. Zgodnie z treścią dyrektywy NIS 2 państwa ją implementujące powinny ją wprowadzić do krajowego porządku prawnego zapewniając minimum niezbędnego poziomu wdrożenia cyberbezpieczeństwa, co zdaje się być pominięte w Projekcie, tworząc szeroki katalog obostrzeń. Przez nadregulację dyrektywy NIS 2, uchwalenie Projektu w proponowanym brzmieniu spowoduje poważne i nieodwracalne zaburzenie w gospodarce krajowej, spowodowane utratą konkurencyjności, utratą partnerów spoza UE i NATO oraz zahamowaniem gospodarki kraju poprzez wzrost cen niektórych usług i produktów. Implementacja dyrektywy NIS 2 w brzmieniu zaproponowanym w Projekcie spowoduje powstanie niekorzystnych warunków dla prowadzenia działalności gospodarczej oraz inwestycji. Skutkiem tego może być zamknięcie wielu przedsiębiorstw oraz lokowanie kapitału zagranicznego w innych krajach niż Polska.	Uwaga częściowo uwzględniona Wymogi projektu zostaną złagodzone, w szczególności dla podmiotów ważnych.
65.	Sobiesław Zasada Spółka Akcyjna S.K.A.	Uwaga ogólna	Mając na względzie istotny interes gospodarczy wielu podmiotów krajowych postulujemy za złagodzeniem warunków implementacji dyrektywy NIS 2 do polskiego porządku prawnego. Unijna dyrektywa winna przewidywać minimalne środki wdrażające europejskie przepisy, z uwzględnieniem zachowania korzystnych warunków do prowadzenia inwestycji w kraju. Przede wszystkim przepisy krajowe winne być przejrzyste, niebudzące wątpliwości oraz nieograniczające w tak dużym stopniu podmioty gospodarcze. Obowiązki przedsiębiorców powinny być dostosowane do każdej gałęzi gospodarczej, przy zachowaniu zasady proporcjonalności i równego traktowania.	Uwaga częściowo uwzględniona Wymogi projektu zostaną złagodzone, w szczególności dla podmiotów ważnych.
66.	Rada Bezpieczeństwa Biznesowego Grupy MiŚOT	Uwaga ogólna	1. Przepisy projektowanej ustawy znacząco wykraczają poza wymogi dyrektywy NIS2, którą powinny wdrażać. Przykłady nadregulacji: a) W ustawie o krajowym systemie cyberbezpieczeństwa w brzmieniu nadanym projektem nowelizacji (KSC) ujęto m.in. art. 32 ust. 2 KSC. Przepis ten, niewymagany przez dyrektywę NIS2, a kierowany do wszystkich podmiotów będących w systemie cyberbezpieczeństwa (podmiotów ważnych i kluczowych), nakazuje usunięcie podatności – właściwie bez żadnych dodatkowych przesłanek. b) Obowiązek tworzenia dokumentacji zgodnie z normami ISO 27001 i 22301 zamiast poprzestania na obowiązku zarządzania ryzykiem i tworzenia dokumentacji w sposób proporcjonalny do ryzyka związanego z działalnością danego przedsiębiorcy. c) Wbrew dyrektywie NIS2 zdecydowana większość obowiązków została nałożona na podmioty ważne oraz podmioty kluczowe w niemal takim samym zakresie. Jako szczególnie jaskrawy przykład należy wskazać art. 15 ust. 1 KSC, zgodnie z którym nie tylko podmioty kluczowe, lecz również podmioty ważne mają obowiązek przeprowadzać cykliczny audyt bezpieczeństwa systemu informacyjnego „wykorzystywanego do świadczenia usługi”. Rada Bezpieczeństwa Biznesowego	Uwaga częściowo uwzględniona Zmniejszony zostanie obowiązek audytowy dla podmiotów ważnych. W przepisach o dokumentacji zostaną usunięte odwołania do norm technicznych. Termin na zgłoszenie wczesnego ostrzeżenia dla przedsiębiorców telekomunikacyjnych wyniesie 24 godzin. Od zaleceń pokontrolnych można odwołać się w skardze do sądu administracyjnego na decyzję o nałożeniu kary za niewykonanie zaleceń.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

		Grupy MiŚOT postuluje wykreślenie z KSC wszystkich regulacji niewynikające z dyrektywy NIS2. Zbyt rygorystyczne regulacje, w szczególności względem wymagań przepisów europejskich, stawia przedsiębiorców prowadzących działalność w Polsce w gorszej pozycji konkurencyjnej względem innych podmiotów z UE. 2. KSC zakłada krótszy czas zgłoszenia wczesnego ostrzeżenia o incydencie poważnym dla przedsiębiorców telekomunikacyjnych względem wszystkich pozostałych podmiotów kluczowych i ważnych: zamiast 24 godzin jest to 12 godzin. Tak drastyczne skrócenie czasu zgłoszenia wczesnego ostrzeżenia o incydencie nie ma uzasadnienia w treści dyrektywy NIS2 ani w innych regulacjach. 3. Niezwykle niepożądanym rozwiązaniem w KSC jest brak środków odwoławczych od zaleceń pokontrolnych. Zdarza się, że organy kontrolujące umieszczają w zaleceniach pokontrolnych wymogi, które nie mają oparcia w przepisach. Z kolei brak wdrożenia zaleceń pokontrolnych zagrożony jest (bardzo wysoką) karą administracyjną (art. 59 ust. 2). Niedopuszczalna powinna być sytuacja, gdy od zaleceń pokontrolnych nie przysługuje chociażby skarga do sądu administracyjnego lub odwołanie do Sądu Ochrony Konkurencji i Konsumentów, ponieważ może to prowadzić (i aktualnie zdarza się na gruncie obowiązujących przepisów, że prowadzi!) do nakładania na przedsiębiorców obowiązków bez podstawy prawnej i bez możliwości wniesienia odwołania. 4. Regulacja dostawców wysokiego ryzyka: a) Niezależnie od ustalonej wielkości przedsiębiorców telekomunikacyjnych formalnie objętych obowiązkiem wycofania z użytkowania sprzętu pochodzącego od dostawcy uznanego za dostawcę wysokiego ryzyka, obowiązek ten dotknie mikro i małych przedsiębiorców telekomunikacyjnych – jeśli nie bezpośrednio to co najmniej pośrednio. Mikro i mali przedsiębiorcy telekomunikacyjni obsługują bowiem bardzo często podmioty publiczne, organy samorządu terytorialnego, czy spółki samorządowe. b) Uważamy, że nie żaden organ nie powinien mieć możliwości wyznaczania dostawcy sprzętu i oprogramowania za dostawcę wysokiego ryzyka. Można sobie wyobrazić zakaz uzależniania się od jednego dostawcy, ponieważ w każdym sprzęcie mogą pojawić się podatności. Każdy przedsiębiorca telekomunikacyjny, korzystając być może ze wskazówek/ zaleceń ze strony Rządu powinien samodzielnie szacować ryzyko związane z konkretnym dostawcą. W przypadku, gdy dany sprzęt będzie mieć podatności lub ukryte celowo backdoory, każdy przedsiębiorca telekomunikacyjny szybko zrezygnuje z takiego sprzętu, ponieważ zapewnienie możliwości bezpiecznego świadczenia usług telekomunikacyjnych to podstawowy obowiązek przedsiębiorcy telekomunikacyjnego i kwintesencja działalności telekomunikacyjnej odkąd istnieje telekomunikacja. c) Ograniczono katalog podmiotów mogących brać udział w postępowaniu w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka (poza samymi <i>potencjalnymi</i> dostawcami wysokiego ryzyka, tylko przedsiębiorcy telekomunikacyjni o rocznych obrotach powyżej ok. 150 mln PLN mogą być dopuszczeni do takiego postępowania). Jednocześnie uniemożliwiono udział w tym postępowaniu organizacjom społecznym (art. 67b ust. 1-3).	Rygor natychmiastowej wykonalności administracyjnej kary pieniężnej będzie nakładany w sytuacji szczególnej. Postępowanie w sprawie uznania za dostawcę wysokiego ryzyka ma zapewnić bezpieczeństwo narodowe i nie możemy od niego odstąpić.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			d) Bardzo krótkie okresy na wycofanie produktów ICT, usług ICT i procesów ICT pochodzących od dostawców wysokiego ryzyka: wskazane w KSC terminy (7 lat na wycofanie sprzętu z użytkowania). Z doświadczenia członków Rady Bezpieczeństwa Biznesowego MiŚOT wynika, że różne sprzęty mają niezwykle różnorodną żywotność. Przykładem bardzo ważnego urządzenia w światłowodowej sieci dostępowej jest OLT, w przypadku którego może dochodzić do konieczności wymiany wkładek lub modułów, lecz samo urządzenie (które jest bardzo drogie) ma żywotność przekraczającą dotychczasowy czas trwania III RP. Oznacza to, że raz zakupiony OLT nie był dotychczas wymieniany przez żadnego z członków Rady. W planach biznesowych nie zakłada się zatem wydatków związanych z wymianą OLT. Z kolei ewentualny nakaz wymiany OLT wiązałaby się także z koniecznością wymiany wszystkich urządzeń ONT u użytkowników, co istotnie zwiększyłoby koszt wymiany takiego sprzętu. Nie można wyciągać średniej z czasu żywotności niezwykle różnorodnych urządzeń, a następnie oczekiwać, że taki średni czas żywotności będzie adekwatny w przypadku urządzeń o najdłuższej żywotności. 5. Należy wykreślić z KSC możliwość nałożenia rygору natychmiastowej wykonalności na decyzję nakładającą karę administracyjną (art. 74 ust. 2 KSC).	
67.	KIGEIT	Uwaga ogólna (OSR)	Ocena skutków regulacji i wpływ na gospodarkę. Brak oceny wpływu Projektu KSC na konkurencyjność gospodarki i polskich firm. Punkt 7 Oceny Skutków Regulacji „<i>Wpływ na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców oraz na rodzinę, obywateli i gospodarstwa domowe</i>” jest w zakresie skutków pieniężnych niewypełniony, a w zakresie ujęcia niepieniężnego - bardzo ogólny. Projektodawca wskazując kilkanaście (17) sektorów objętych nowymi regulacjami, w tym Procedurą DWR, której zastosowanie ingerować będzie w konstytucyjne zasady swobody prowadzenia działalności gospodarczej i obciążać będzie bezpośrednio przedsiębiorców, nie podjął się próby analizy i oszacowania jaki wpływ mogą mieć przygotowane ogólnie przepisy na kilkanaście sektorów, takich jak m.in.: sektor zdrowia, obejmujący producentów leków oraz opiekę zdrowotną, sektor transportu, sektor produkcji, obejmujący produkcję urządzeń, maszyn itp., ale również produkcję wyrobów medycznych i wyrobów do diagnostyki in vitro, sektor gospodarowania odpadami czy sektor energii. ⁶Biorąc pod uwagę istotność dla polskiej gospodarki oraz dostępności dla konsumentów produktów i usług sektorów, które objąć mają konsekwencje Procedury DWR, niezbędne jest dokonanie dokładnych sektorowych analiz dotyczących tego, jaki praktyczny wpływ może mieć wydanie decyzji dot. wycofania i zakazania używania produktów, usług i procesów ICT dostawców. Brak szczegółowych analiz i symulacji wpływu wydania decyzji, w tym w oparciu o przesłanki polityczne, które od kilku już lat wskazywane są przez ekspertów jako wprost wymierzone w przedsiębiorców chińskich⁶, a więc możliwe jest zakreślenie i zbadanie np. wykorzystania produktów i usług dostawców azjatyckich, chińskich, nie tylko narusza zasady wskazane w art. 67	Wyjaśnienie uwagi Bardzo trudno jest oszacować koszty wdrożenia z uwagi na brak danych, różnorodność podmiotów, ich usług czy wielkość.

⁶ <https://www.money.pl/gospodarka/mieso-czy-cyberbezpieczenstwo-rolnicy-krytykuja-kluczowy-projekt-rzadu-6700817173838784a.html>

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			Prawo przedsiębiorców⁷ w zakresie kierowania się zasadą proporcjonalności i adekwatności przy nakładaniu nowych obowiązków oddziałujących na działalność gospodarczą, ale przede wszystkim stanowi zagrożenie dla działalności kilkunastu sektorów polskiej gospodarki. W związku z proponowanym kształtem Projektu KSC koszty ponoszone przez przedsiębiorców podlegających pod zmieniane przepisy odnosić się będą nie tylko do bieżącego zapewnienia bezpieczeństwa zarządzania informacjami i reagowania na incydenty, ale także do potencjalnej wymiany lub ograniczenia możliwych do wykorzystania produktów od dostawców sprzętu, co w przypadku niektórych rynków może mieć konsekwencje w postaci wzrostu cen produktów. Dodatkowo konsekwencje dotyczące zastosowania Procedury DWR wobec podmiotów kluczowych i ważnych z 17 sektorów gospodarki mogą ponosić również konsumenci, użytkownicy usług. Projekt KSC w sposób szeroko zakrojony definiuje pojęcie dostawcy sprzętu lub oprogramowania. W obecnym kształcie podmioty objęte KSC powinny nie tylko mieć na uwadze ryzyko objęcia Procedurą DWR nie tylko producentów sensu stricto ale również m.in. dystrybutorów. Powyższe rodzi ryzyko zapewnienia ciągłości świadczenia usług przez podmioty kluczowe i podmioty ważne. Biorąc pod uwagę istotność dla polskiej gospodarki oraz dostępności dla konsumentów produktów i usług sektorów, które objąć mają konsekwencje Procedury DWR, niezbędne jest dokonanie dokładnych sektorowych analiz dotyczących tego, jaki praktyczny wpływ może mieć wydanie decyzji dot. wycofania i zakazania używania produktów, usług i procesów ICT dostawców. Brak szczegółowych analiz i symulacji wpływu wydania decyzji, w tym w oparciu o przesłanki polityczne, które od kilku już lat wskazywane są przez ekspertów jako wprost wymierzone w przedsiębiorców chińskich⁸, a więc możliwe jest zakreślenie i zbadanie np. wykorzystania produktów i usług dostawców azjatyckich, chińskich, nie tylko narusza zasady wskazane w art. 67 Prawo przedsiębiorców⁹ w zakresie kierowania się zasadą proporcjonalności i adekwatności przy nakładaniu nowych obowiązków oddziałujących na działalność gospodarczą, ale przede wszystkim stanowi zagrożenie dla działalności kilkunastu sektorów polskiej gospodarki. W związku z proponowanym kształtem Projektu KSC koszty ponoszone przez przedsiębiorców podlegających pod zmieniane przepisy odnosić się będą nie tylko do bieżącego zapewnienia bezpieczeństwa zarządzania informacjami i reagowania na incydenty, ale także do potencjalnej. Dodatkowo, zwraca uwagę Izby Punkt 8 Oceny Skutków Regulacji „Zmiana obciążeń regulacyjnych (w tym obowiązków informacyjnych) wynikających z projektu”, który w zakresie wskazania: „Wprowadzane są obciążenia poza bezwzględnie wymaganymi przez UE” jest niewypełniony, a do opublikowanych dokumentów Projektu KSC nie załączono tabeli zgodności / odwrotnej tabeli zgodności. d	

⁷ Ustawa z dnia 6 marca 2018 r. - Prawo przedsiębiorców (t.j. Dz.U. z 2024 r. poz. 236).

⁸ <https://www.money.pl/gospodarka/mieso-czy-cyberbezpieczenstwo-rolnicy-krytykuja-kluczowy-projekt-rzadu-6700817173838784a.html>

⁹ Ustawa z dnia 6 marca 2018 r. - Prawo przedsiębiorców (t.j. Dz.U. z 2024 r. poz. 236).

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

68.	KIGEIT	Uwaga ogólna (OSR i procedura DWR tj. art. 67b i nast.)	Przeregulowanie w porównaniu z innymi krajami UE w zakresie wykorzystania Procedury DWR nie tylko wobec produktów, usług i procesów ICT używanych w sektorze telekomunikacyjnym (za tzw. 5G Toolbox), ale szerzej na produkty usługi i procesy ICT wszystkich podmiotów kluczowych i ważnych. W ramach Punktu 3 Oceny Skutków Regulacji „<i>Jak problem został rozwiązany w innych krajach, w szczególności krajach członkowskich OECD/UE?</i>” oraz dokonanych analiz stanowiących załącznik nr 1 do OSR (<i>Dostawca wysokiego ryzyka (high risk vendor) i bezpieczeństwo sieci 5G w Europie</i>) Projektodawca odnosząc się do Procedury DWR odwołuje się wyraźnie do wdrożenia zaleceń z tzw. 5G Toolbox, a więc zaleceń dotyczących cyberbezpieczeństwa sieci 5G. Jak wskazują przywoływane w dokumentach analizy, faktycznie w części krajów Unii Europejskiej wprowadzone zostały rozwiązania prawne umożliwiające wyłączenie z budowy sieci 5G dostawcy uznanego za potencjalne zagrożenie, natomiast wprowadzane w tych krajach procedury są adresowane zgodnie z założeniami 5G Toolbox do sieci telekomunikacyjnych wykorzystujących technologię 5G, a więc sektora telekomunikacyjnego – żaden z krajów Unii Europejskiej nie zdecydował się na tak szerokie stosowanie procedury wyznaczania dostawcy wysokiego ryzyka i w konsekwencji ingerowania w prowadzoną działalność gospodarczą przez wszystkich przedsiębiorców kwalifikowanych w ramach wdrożenia Dyrektywy NIS2 jako podmioty kluczowe i ważne. Przedstawiona OSR nie zawiera analiz i uzasadnienia dla tak daleko idącego rozszerzenia zakresu podmiotowego zastosowania regulacji odnoszących się do Procedury DWR, wręcz przeciwnie - przedstawione dokumenty potwierdzają, że Projekt KSC wychodzi dalej niż wdrożenia dokonane w innych krajach unijnych i stawia polskich przedsiębiorców w dużo trudniejszej - z perspektywy ryzyka prowadzenia działalności - organizacji i kosztów sytuacji. sZarówno uzasadnienie do Projektu KSC jak i OSR nie wskazuje na podstawowy problem związany z Procedurą DWR dla podmiotów, których dotyczy Załącznik nr 3 do projektu, mianowicie nie zwrócono uwagi, że wymiana sprzętu dla sieci 5G wymaga wymiany sprzętu również dla 4G (wykorzystywana obecnie konfiguracja 5G non-standalone), nie tylko na tych samym lokalizacjach ale de facto w całej sieci. W konsekwencji jest to dużo bardziej złożony projekt niż budowa sieci 5G obejmujący wielokrotnie więcej lokalizacji fizycznych. Skala inżynierska projektu jest tak duża że próba jego realizacji w ciągu 4 lat będzie ograniczona ze względu na brak dostępności wyspecjalizowanych ekip instalacyjnych (podkreślenia wymaga, że wymiany będą dokonywane przez kilku przedsiębiorców telekomunikacyjnych równolegle).yWymiana sprzętu zaś to uruchomienie bardzo dużego programu obejmującego nie jeden, ale co najmniej kilka projektów, dotyczących równoległe zmiany kilku systemów w tym samym czasie oraz dostosowanie pozostałych systemów do współpracy z nowym rozwiązaniem. Podkreślić, należy że ryzyko nie dotrzymania wskazanego w Projekcie KSC terminu z art. 67c może być całkowicie niezależne od przedsiębiorcy telekomunikacyjnego w sytuacji gdy, pozostali dostawcy oferujący dany typ rozwiązania (ilość ich jest również ograniczona), nie będą w stanie wywiązać się z zamówień od nowych klientów w określonym czasie.zW związku z powyższym postulujemy odstąpienie przez Ministerstwo od regulacji wykraczających poza zakres postanowień objętych Dyrektywą.	Wyjaśnienie uwagi Kwestia bezpieczeństwa sieci 5G oraz szerzej bezpieczeństwa łańcucha dostaw ma istotne znaczenie dla cyberbezpieczeństwa państwa i nie możemy od niej odstępować.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

69.	KIGEIT	Uwaga ogólna	Brak informacji o planie dokonania wymaganej regulacjami unijnymi notyfikacji TRIS w związku z wprowadzanymi poprzez procedurę DWR zmianami technicznymi odnoszącymi się do swobodnego przepływu towarów. Podobnie jak w przypadku wersji projektu KSC przygotowanej przez poprzedni rząd (pomimo wskazań ministra właściwego do spraw członkostwa RP w UE), dokumenty uzasadnienia i OSR opublikowane wraz z Projektem KSC nie zawierają informacji o planie dokonania wymaganej regulacjami unijnymi notyfikacji TRIS w związku z wprowadzanymi poprzez procedurę DWR zmianami technicznymi, odnoszącymi się do swobodnego przepływu towarów. Ze względu na skalę ingerencji Projektu KSC w swobody działalności gospodarczej oraz definicją przepisów technicznych zawartą w rozporządzeniu¹⁰ (przepisy techniczne odnoszą się min. do specyfikacji technicznej; przepisów dotyczących usług; regulacji wprowadzających zakaz produkcji, przywozu lub wprowadzania produktu do obrotu, świadczenia usług lub prowadzenia działalności polegającej na świadczeniu usług; regulacji pośrednio ograniczających wprowadzenie do obrotu produktów, świadczenie usług lub prowadzenie działalności polegającej na świadczeniu usług), zdaniem Izby nie ma wątpliwości co do konieczności notyfikacji technicznej Projektu KSC w zakresie wprowadzanej Procedury DWR. kPrawidłowe przeprowadzenie procesu legislacyjnego, uwzględniającego notyfikację Komisji Europejskiej projektów aktów prawnych zawierających przepisy techniczne, jest istotne z perspektywy konsekwencji jakie zarówno dla Polski, jak i przedsiębiorców, może nieść za sobą brak wymaganej notyfikacji: - na podstawie art. 258 <i>Traktatu o funkcjonowaniu Unii Europejskiej</i> Komisja Europejska w przypadku ominięcia przez państwo członkowskie procedury notyfikacji, może wszcząć postępowanie oraz skierować sprawę do Trybunału Sprawiedliwości UE (<i>dalej: „TSUE”</i>); - zainteresowane podmioty (osoby fizyczne i prawne) mogą dochodzić swoich praw przed sądem krajowym; - dotychczasowe orzecznictwo TSUE potwierdza, że: - niedopełnienie obowiązku notyfikacji powoduje, że dane przepisy techniczne stają się nieważne, a zatem nie mają one mocy obowiązującej w stosunku do osób fizycznych (sprawa C-194/94 CIA Security), - niezgodne z prawem unijnym przepisy krajowe nie powinny być stosowane, pomimo ich dalszego obowiązywania (sprawa C-106/77 Simmenthal). Powyższe konsekwencje braku dokonania wymaganej notyfikacji są wskazywane przez Ministerstwo Rozwoju i Technologii¹¹. Izba zwraca uwagę na konieczność kompleksowego zaadresowania elementów odnoszących się do dopełnienia obowiązku notyfikacji biorąc pod uwagę daleko idące, nieodwracalne konsekwencje	Wyjaśnienie uwagi Decyzja o uznaniu dostawcy za dostawcę wysokiego ryzyka może być notyfikowana.

¹⁰ Rozporządzenie Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. poz. 2039, ze zm.).

¹¹ <https://www.gov.pl/web/rozwoj-technologie/notyfikacja-przepisow-technicznych>

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			projektowanych regulacji dla przedsiębiorców oraz możliwe negatywne konsekwencje prawne i chaos regulacyjny, jaki może powstać w wyniku braku notyfikacji przepisów do Komisji Europejskiej.	
70.	KIGEIT – Sekcja Inteligentnych Sieci – Smart Grids SIS-SG	Uwaga ogólna (art. 67b i nast.)	Sektor producentów i dostawców dla energetyki od dawna oczekuje regulacji zaostrażających przepisy w zakresie dopuszczania do polskiego rynku produktów smart (oprogramowanych, z funkcjonalnością dwukierunkowej transmisji danych, realizujących np. zadania urządzeń automatyki przemysłowej), które są instalowane w infrastrukturze krytycznej sieci elektroenergetycznej. Bezpieczeństwo pracy systemu elektroenergetycznego powinno być chronione w szczególnie sposób, tymczasem mamy do czynienia z zupełnie niekontrolowanym napływem urządzeń takich jak liczniki smart (oprogramowane liczniki energii elektrycznej z funkcjonalnością dwukierunkowej transmisji danych, czasem przeznaczone do sterowania lokalną siecią energetyczną), dla których nie dokonano żadnej weryfikacji technicznej pod kątem cyberbezpieczeństwa. W sytuacji, w której nie powstał wspólny europejski system oceny urządzeń smart pracujących w sieci elektroenergetycznej pod kątem cyberbezpieczeństwa oraz, że nie mamy jeszcze krajowego systemu weryfikacji i certyfikacji urządzeń cyfrowych pracujących w kluczowych miejscach infrastruktury elektroenergetycznej, skutecznym rozwiązaniem jest wprowadzenie przepisów dyrektywy NIS 2 w krajowej implementacji KSC, zmniejszających wrażliwość inteligentnej infrastruktury elektroenergetycznej na cyberataki. Sektorowe regulacje dotyczące dokonywania procedury oceny dostawcy wysokiego ryzyka (DWR) wobec wszystkich podmiotów uznanych za podmioty kluczowe i ważne, są uzasadnione celami cyfryzacji i automatyzacji zarządzania systemami energetycznymi. Zamawianie liczników LZO bez żadnej weryfikacji produktów i dostawców, powoduje gwałtowny wzrost ryzyka potencjalnego ataku cyfrowego na sieć elektroenergetyczną ze strony dostawców z obszarów wysokiego ryzyka. Obserwujemy, że operatorzy sieci elektroenergetycznych - bezkrytycznie i bez sprawdzenia - instalują już na swoich sieciach urządzenia z obszarów wysokiego ryzyka. Skala zagrożenia związanego z wdrożeniami masowymi na przykład liczników LZO pochodzącymi z obszarów podwyższonego ryzyka wymaga adekwatnych regulacji. Prawo może dopuszczać natychmiastowe wycofanie z sieci pracujących już urządzeń, które zostały negatywnie zweryfikowane i mogą stać się potencjalnym narzędziem cyberataku. Dla sektora elektroenergetycznego wprowadzenie procedury DWR oceny dostawców będzie miało pozytywny wpływ. Większość dostawców dla tego sektora, to polskie i europejskie firmy mające dobrze rozwinięte własne technologie i działające od dawna na naszym rynku. Co więcej uważamy, że brak adekwatnego systemu kontroli dostawców doprowadziło do nieuczciwej konkurencji ze strony podmiotów z krajów trzecich, które prawdopodobnie są subsydiowane. Firmy UE ponoszą znaczne koszty związane z realizacją zobowiązań klimatycznych, wdrażaniem społecznej odpowiedzialności i przestrzegania praw człowieka oraz dokumentowania i rozliczania tych czynności (ESG). Bez wyrównania pola konkurencji poziom zagrożenia cyberatakami na sieci energetyczne będzie rósł. Trwająca już wojna cyfrowa w obszarze energetyki szkodzi działającym w tym sektorze podmiotom z Polski i UE. Ważnym celem tej wojny jest osłabianie tych podmiotów poprzez nieuczciwą konkurencję. Inicjatywy typu „levelling playing ground on competition” są podejmowane w większości krajów UE oraz na poziomie całej Unii Europejskiej przez	Wyjaśnienie uwagi Sektor produkcji, w tym produkcji urządzeń elektrycznych będzie także objęty procedurą wycofania sprzętu/oprogramowania od dostawcy wysokiego ryzyka.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			organizacje branżowe - np. działania branżowych izb współpracujących z Komisją Europejską takich jak ESMIG czy izb krajowych takich jak KIGeIT .iPostępowanie innych krajów UE takich jak Czechy, Niemcy czy Litwa wyraźnie zmierza do poszerzenia wymagań minimalnych NIS2 w sektorze energetyki. Za absolutnie konieczne działanie w sektorze energetycznym uznano tam postępowanie prewencyjne wobec dostawców liczników energii smart. Takie działania podjęły na przykład Czechy, które także wyraźnie zastrzegają wymagania dla dostawców sprzętu smart dla energetyki. Ustawodawca słusznie poszerzył grono podmiotów kluczowych w sektorze energetycznym na dostawców sprzętu i urządzeń elektrycznych . iZgodnie z naszą oceną sytuacji większość polskich i europejskich producentów działających w branży elektroenergetycznej zmagają się z nieuczciwą konkurencją z krajów trzecich, w których konkurencja jest zaburzona poprzez wsparcie realizujące cele ataków APT. Wielkoskalowe wdrożenia technologii smart w Polsce już się rozpoczęły i na polski rynek trafiają zupełnie niezaweryfikowane, niesprawdzone pod kątem cyfrowego bezpieczeństwa produkty, w cenach które mogą rodzić poważne obawy o nierówne traktowanie dostawców. W elektroenergetyce zagraża to całemu branżom produkcyjnym z dziesiątkami tysięcy miejsc pracy w Polsce.iCała branża elektroenergetyczna jest narażona w co najmniej równym stopniu na potencjalne ataki ze strony „high risk vendor” podobnie jak dla tzw. 5G toolbox. W naszej ocenie narażenie jest wyższe niż w branży telekomunikacyjnej, które bardzo często posiadają nie tylko komunikację dwukierunkową ale także urządzenia wykonawcze (styczniki wyłączające zasilanie, ograniczniki mocy itp.). oSektor energetyczny potrzebuje dedykowanego rozporządzenia regulującego dopuszczanie do instalacji w sieciach urządzeń typu smart będących elementem sieciowej automatyki przemysłowej. Powinno zawierać listę kryteriów technicznych, lokalizacyjnych, logistycznych, serwisowych i organizacyjnych zapewniających poziom kontroli cech jakościowych i funkcjonalnych adekwatnie do zagrożeń, jakie mogą spowodować jako elementy infrastruktury krytycznej. pW stanowisku KIGeIT z dnia 04.08.2023 precyzyjnie określiliśmy, które kraje nie należą do obszarów podwyższonego ryzyka. Są to kraje dla których: p„1. Główna siedziba producenta powinna być położona w kraju będącym sygnatariuszem porozumienia GPA2 (Government Procurement Agreement), podpisanego w ramach WTO (World Trade Organization) w sprawie zasad realizacji zamówień publicznych; p2. Miejsce produkcji urządzeń nie powinno znajdować się poza obszarem Europejskiego Obszaru Gospodarczego (EOG) lub Europejskiego Stowarzyszenia Wolnego Handlu (EFTA).”. zPostulujemy zaliczenie podmiotów produkujących dla branży elektroenergetycznej do podmiotów kluczowych co otwiera drogę do szybkiego skutecznego uruchomienia prewencyjnych procedur DWR (ponieważ przetargi bez weryfikacji już się rozpoczęły).	
71.	Osoba Fizyczna	Uwaga ogólna	Zaproponowane w ustawie regulacje pozwalają na nałożenie kar o dowolnej wysokości, co może prowadzić do nieprzewidywalności i braku stabilności prawnej dla podmiotów działających na rynku. Warto rozważyć wprowadzenie bardziej szczegółowych wytycznych co do maksymalnej wysokości kar, co może zapewnić większą przejrzystość i uczciwość procesu sankcyjnego.	Uwaga nieuwzględniona Projektowane przepisy odzwierciedlają przepisy o karach przewidziane w dyrektywie NIS 2 oraz są proporcjonalne, adekwatne, odstraszające. W projekcie przewidziano różne sankcje oraz różną

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

				ich wysokość w zależności od ukaranego podmiotu. Ponadto przewidziany został katalog kryteriów, które należy brać pod uwagę przy wymiarze kary – kary nie będą zatem dowolne. Określona została zarówno minimalna, jak i maksymalna wysokość kary.
72.	Osoba fizyczna	Uwaga ogólna	Projekt ustawy nie adresuje kwestii kumulacji obowiązków wynikających jednocześnie z RODO i nowego systemu cyberbezpieczeństwa. Może to prowadzić do konfliktu regulacji oraz nadmiernej obciążenia podmiotów, zwłaszcza tych mniejszych. Należy rozważyć usprawnienie przepisów w taki sposób, aby unikać dublowania się obowiązków i zapewnić koordynację między różnymi organami nadzorczymi.	Wyjaśnienie uwagi Obowiązki z zakresu SZBI pokrywają się z obowiązkami z RODO. Wprowadzono przepisy o współpracy Prezesa UODO w zakresie kontroli i nadzoru. Umożliwia się zgłoszenie incydentu i naruszenia ochrony danych osobowych jednym kanałem – systemem S46.
73.	Osoba fizyczna	Uwaga ogólna	Brak jest wyraźnych wytycznych dotyczących procedur stosowania i egzekwowania przepisów, co może wprowadzać zamieszanie wśród podmiotów zobowiązanych do przestrzegania ustawy. Sugeruje się wprowadzenie bardziej szczegółowych procedur operacyjnych, które wyjaśniają procesy decyzyjne, kryteria oceny oraz metody egzekwowania zgodności.	Uwaga nieuwzględniona Charakter uwagi jest zbyt ogólny aby projektodawca mógł podjąć odpowiednie działania. W ocenie projektodawcy przepisy dotyczące nadzoru i egzekwowania przepisów są jasne i precyzyjne, implementują w całości dyrektywę NIS 2 do porządku krajowego. Wszelkie wątpliwości interpretacyjne wyjaśnia również szczegółowe uzasadnienie do projektowanych przepisów.
74.	Osoba fizyczna	Uwaga ogólna	Wsparcie dla podmiotów: Projekt nie zawiera wystarczających mechanizmów wsparcia dla podmiotów w procesie dostosowywania się do wymogów ustawy, szczególnie dla mniejszych przedsiębiorstw. Proponuje się stworzenie programów szkoleniowych oraz funduszy pomocowych, które pomogą podmiotom w implementacji niezbędnych zmian technologicznych i proceduralnych.	Wyjaśnienie uwagi Jednym z zadań CSIRT sektorowych będzie wspieranie podmiotów w wykonywaniu obowiązków z zakresu cyberbezpieczeństwa.
75.	Osoba fizyczna	Uwaga ogólna	W kontekście nowych obciążeń regulacyjnych ważne jest zapewnienie ciągłego dialogu z przedstawicielami różnych sektorów gospodarki. Sugeruje się regularne konsultacje z interesariuszami w celu dostosowania przepisów do realiów rynkowych oraz szybko zmieniającego się krajobrazu cyberzagrożeń.	Uwaga uwzględniona Ministerstwo Cyfryzacji jest otwarte na spotkania.
76.	Osoba fizyczna	Uwaga ogólna	Z moich doświadczeń praktycznych wynika, że jeśli ustawodawca nie wprowadzi do ustawy o KSC zapisów mówiących wprost o konieczności, OBOWIĄZKOWEGO powołania SOC (własny lub jako	Uwaga uwzględniona

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			usługa) i konieczności zapewnienia odrębności SOC wewnętrznego od jakichkolwiek struktur OUK, to dalej będzie funkcjonowała absurdalna praktyka dedykowania tych zadań do bieżących obowiązków wybranych pracowników IT. Doskonale Państwo zdają sobie sprawę jakie negatywne skutki pociąga za sobą taka praktyka.	Zostanie przywrócony i dostosowany przepis art. 14 ust. 1
77.	Osoba fizyczna	Uwaga ogólna	mam ogóle pytanie w ramach konsultacji, czy nowa ustawa dot. cyberbezpieczeństwa wpłynie na wdrażanie systemów Linuxowych m. in. w przedsiębiorstwach na sprzęcie znajdującym się w organizacji i w chmurze. Czy to ograniczy w jakimś stopniu na możliwość używania systemów Linuxowych takich jak Ubuntu 26.04, openSUSE Leap po wejściu w życie zapisów z ustawy o cyberbezpieczeństwie (w przedsiębiorstwach itp.)?	Wyjaśnienie uwagi Projekt ustawy jest neutralny technologicznie. Projekt nie ogranicza używania systemów linuxowych.
78.	Osoba fizyczna	Uwaga ogólna	Proponowana Ustawa nie tylko osłabia bezpieczeństwo Polski w Cyberprzestrzeni ale wręcz niweczy wysiłki i niszczy jakakolwiek aktywność Polaków związaną z możliwością aktywnego uczestniczenia Osób prywatnych i podmiotów prywatnych w poprawie poziomów bezpieczeństwa nie tylko Polski i Polaków ale również Unii Europejskiej. Nie ulega wątpliwości, że "uwierzytelnianie" oraz następnie kontrola dostępu do zasobów cyfrowych i udostępnienie zasobów cyfrowych "uwierzytelnionym użytkownikom" jest podstawą kształtowania bezpieczeństwa danych Osobowych i danych wrażliwych a nawet "bezpiecznego" - czyli realizującego zgodnie ze specyfikacją wymagań funkcjonalnych i niefunkcjonalnych systemów informatycznych usług kluczowych i ważnych. Zatem, bez wątpienia "uwierzytelniony" np. administrator baz danych czy też administrator serwera aplikacyjnego lub administrator fragmentu "zinformatyizowanej" infrastruktury przemysłowej jako OT podmiotu, który wdrożył i korzysta z systemów IT współpracujących z OT - w postaci mniej lub bardziej zinformatyizowanych "węzłów", "sterowników" o określonej np. "inteligencji" używanej w procesie zarządzania "procesem" czy też "urządzeniem". Zatem, "uwierzytelniony" użytkownik lub proces ma istotny wpływ na bezpieczeństwo całego procesu - przykłady incydentów z "błędami danymi" przekazywanymi sterownikom np. w Elektrowni Jądrowej, miały miejsce już w poprzedniej dekadzie. Zatem, oczywiste jest, że bezpieczny system uwierzytelniania dostępu do zasobów w tym infrastruktury usług kluczowych i ważnych wymaga DOOKREŚLENIA JAKI POZIOM ZAUFANIA MA OBOWIĄZYWAĆ ORAZ JAKI POZIOM BEZPIECZEŃSTWA USTANOWIONY W ROZPORZĄDZENIU WYKONAWCZYM (UE)910/2014 WYMIENIONE art. 8.2 MA OBOWIĄZYWAĆ PODMIOTY KLUCZOWE I WAŻNE. NIE ULEGA WĄTPLIWOŚCI, ŻE JEŚLI OBOWIĄZUJE UE910/2014 art. 8.2 TO OBOWIĄZUJE RÓWNIEŻ (UE)910/2014 art. 8.3 KTÓRY ZOBOWIĄZUJE DO PRZESTRZEGANIA ORAZ ODNIESIENIA SIĘ DO Rozporządzenie wykonawcze Komisji (UE) 2015/1502 z dnia 8 września 2015 r. w sprawie ustanowienia minimalnych specyfikacji technicznych i procedur dotyczących poziomów zaufania w zakresie środków identyfikacji elektronicznej na podstawie art. 8 ust. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (Tekst mający znaczenie dla EOG). Zatem, jeśli nie będzie w ustawie o Cyberbezpieczeństwie odniesienia wprost do UE1502/2015 r w kontekście uwierzytelniania i nadal będzie obowiązywało w tym zakresie Ustawa o usługach zaufania	Uwaga nieuwzględniona Podstawowym założeniem dyrektywy NIS2 jest adekwatność zastosowanych środków bezpieczeństwa do zagrożeń zidentyfikowanych w ramach procesu szacowania ryzyka. Dlatego też to każdy z obowiązanych podmiotów będzie musiał dokonać szacowania ryzyka i dopiero na podstawie tego procesu będzie możliwe precyzyjne określenie jego potrzeb w obszarze cyberbezpieczeństwa.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			i identyfikacji elektronicznej (Dz.U. 2020 poz 1173) art. 21a treść ust 4. "Uwierzytelnienie użytkownika systemu teleinformatycznego w celu realizacji usługi online wymaga użycia środka identyfikacji elektronicznej na poziomie bezpieczeństwa określonym przez podmiot świadczący tę usługę." to nie ulega, żadnej wątpliwości, że nie będzie żadnych poziomów bezpieczeństwa a w szczególności nie będzie QuantumResists o czym świadczy między innymi treść Ustawy o mObywatel (Dz.U.2023 poz.1234) art. 4. <i>Uwierzytelnienie z wykorzystaniem profilu mObywatel jest dokonywane przy użyciu co najmniej dwóch czynników uwierzytelniania należących do co najmniej dwóch różnych kategorii, o których mowa w przepisach wydanych na podstawie art. 8 ust. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE.</i> natomiast, bez wątpienia mObywatel ujawnia dane identyfikacyjne chociażby na potrzeby identyfikacji w wyborach powszechnych, zatem bezspornie zamiast conajmniej 2FA obligatoryjnie na podstawie UE1502/2015 załącznik pkt.2.3.1 powinno to być "uwierzytelnianie dynamiczne" o wiele bezpieczniejsze i QuantumResists od 2FA - zatem nie ulega wątpliwości, że albo wdrożenia UE1502/2015 w usługach kluczowych i ważnych celem poprawy bezpieczeństwa albo dalsze procedowanie w atmosferze "dywersji" i "zdrady stanu" - bo nie ulega żadnej wątpliwości, że zapisy PN270001 nie uwzględniają żadnych wytycznych zawartych w UE1502/2015. a wszelkie "uniki" oraz pomijanie ustanowień UE1502/2015 jest tylko potwierdzeniem zaniechań równoważnych z "dywersją" i pozbycie się "suwerenności w domenie cyberbezpieczeństwa" jako działanie osłabiające bezpieczeństwo Infrastruktury Krytycznej na miarę "zdrady stanu" .	
79.	Pracodawcy RP	Uwaga ogólna	Po pierwsze członkowie wskazują na istotne zagrożenia związane z nadregulacją, która przekracza wymogi dyrektywy NIS 2 i 5G Toolboxa, wprowadzając rygorystyczne przepisy mogące negatywnie wpłynąć na konkurencyjność i nieproporcjonalność procedur, które mogą prowadzić do dyskryminacji dostawców na podstawie kryteriów niemierzalnych, szczególnie dotycząc podmioty korzystające z usług dostawców pochodzących z krajów nienależących do Unii Europejskiej czy NATO. Postulują również przedłużenie okresu przeznaczonego na konsultacje publiczne oraz zaproszenie do nich szerszego grona reprezentantów wszystkich sektorów, które zostaną objęte nowymi regulacjami – w szczególności tych, którzy po raz pierwszy zostaną objęci obowiązkami. Jest to kluczowe dla zapewnienia, że wprowadzane zmiany będą służyć bezpieczeństwu i dobru publicznemu, jednocześnie nie stawiając nieuzasadnionych barier dla rozwoju przedsiębiorczości.	Uwaga uwzględniona Przepisy projektu zostaną złagodzone.
80.	Pracodawcy RP	Uwaga ogólna	Obecny projekt jest znacznie bardziej surowy niż jego poprzednie wersje z lat 2020-2023. Choć poprzednie wersje również zakładały wykluczenia dostawcy z rynku na podstawie kryteriów nietechnicznych, aktualna propozycja transpozycji dyrektywy zakłada jeszcze bardziej rygorystyczne przepisy — zarówno w kontekście katalogu podmiotów objętych DWR, postępowania, jak i skróconego terminu na usunięcie sprzętu lub oprogramowania dostawcy.	Wyjaśnienie uwagi Wszystkie podmioty kluczowe i podmioty ważne są zobowiązane do dbania o bezpieczeństwo łańcuchów dostaw, stąd też rozszerzono zakres podmiotów obowiązanych do wycofania sprzętu i oprogramowania pochodzących od dostawcy wysokiego ryzyka.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

81.	Pracodawcy RP	Uwaga ogólna	W ocenie członków projekt jest nadregulacją — wprowadza obowiązki przekraczające zakres dyrektywy NIS 2, a także 5G Toolboxa, którego wdrożenie znajduje się w zakresie projektu	Uwaga uwzględniona Przepisy projektu zostaną złagodzone.
82.	Pracodawcy RP	Uwaga ogólna	W ocenie członków objęte projektem wpłyną na niekorzyść polskiej gospodarki, m.in. poprzez zwiększenie kosztów przy jednoczesnym zmniejszeniu dostępu do najnowszych technologii. Podmioty objęte regulacją będą musiały ponieść dodatkowe nakłady finansowe w celu wdrożenia wymagań wynikających z projektu ustawy, takich jak regularne audyty bezpieczeństwa systemów informatycznych przeprowadzanie nie rzadziej niż raz na 2 lata na własny koszt podmiotu objętego audytem. Istnieje również ryzyko hamowania ich innowacyjności w związku ze zbyt szerokim katalogiem podmiotów objętych procedurą uznania za DWR, co wpłynie negatywnie na konkurencyjność polskiej gospodarki. Należy nadmienić, że wiele sektorów zostanie objętych przepisami po raz pierwszy — podmioty z tych sektorów nie są świadome nadchodzących obowiązków, a czas na ich wdrożenie będzie bardzo krótki. Do konsultacji publicznych zostało zaproszone zbyt wąskie grono podmiotów reprezentujących sektory objęte ustawą o KSC, a aż 10 sektorów w ogóle nie otrzymało zaproszenia do uczestnictwa w konsultacjach.	Uwaga uwzględniona Przepisy projektu zostaną złagodzone.
83.	Pracodawcy RP	Uwaga ogólna	Na ten moment wobec projektu nie została rozpoczęta procedura notyfikacji technicznej TRIS. Ominięcie tej procedury może prowadzić do znaczących komplikacji prawnych, w tym możliwości wniesienia skargi do Komisji Europejskiej, co może opóźnić wprowadzenie zmian lub skutkować koniecznością ich rewizji. Procedura notyfikacji technicznej TRIS — ryzyko związane z wprowadzeniem restrykcyjnych przepisów dot. DWR Na wstępie należy zaznaczyć, że w trakcie prac nad nowelizacją ustawy o krajowym systemie cyberbezpieczeństwa w 2020 roku, pojawiły się problemy proceduralne związane z nieprzekazaniem projektu do Komisji Europejskiej w ramach notyfikacji technicznej TRIS, zgodnie z Dyrektywą 2015/1535. Niezastosowanie się do tej procedury jest powtórzeniem błędu proceduralnego, który miał miejsce również przy poprzednich wersjach projektu. Procedura TRIS wymaga od państw członkowskich UE notyfikacji wszelkich nowych lub zmienionych regulacji technicznych, co ma na celu zapobieganie tworzeniu barier w handlu wewnętrznym Unii Europejskiej. Ominięcie tej procedury może prowadzić do znaczących komplikacji prawnych, w tym możliwości wniesienia skargi do Komisji Europejskiej, co może opóźnić wprowadzenie zmian lub skutkować koniecznością ich rewizji. Jest to szczególnie istotne w kontekście, gdy nowelizacja ustawy ma kluczowe znaczenie dla wzmocnienia cyberbezpieczeństwa w kraju. Skarga do Komisji Europejskiej na naruszenie procedury notyfikacji technicznej TRIS w ramach Dyrektywy 2015/1535 może być złożona na podstawie artykułów Traktatu o Funkcjonowaniu Unii Europejskiej (TFUE), które regulują procedury naruszenia prawa Unii przez państwa członkowskie. Kluczowe przepisy prawne, mogące stanowić podstawę działania w takiej sytuacji, to: Artykuł 258 TFUE — umożliwia Komisji Europejskiej wszczęcie postępowania przeciwko państwu członkowskiemu, które nie wypełnia zobowiązań wynikających z prawa Unii. Jeżeli po otrzymaniu formalnego zawiadomienia państwo członkowskie nie dostosuje się do uwag Komisji, może ona	Wyjaśnienie uwagi Decyzja ws. dostawcy wysokiego ryzyka może być notyfikowana.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			przekazać sprawę do Trybunału Sprawiedliwości Unii Europejskiej.c Artykuł 260 TFUE — w przypadku, gdy Trybunał Sprawiedliwości stwierdzi naruszenie prawa Unii przez państwo członkowskie, a to państwo nie wykonuje wyroku Trybunatu, Komisja może ponownie skierować sprawę do Trybunału, który może nałożyć na państwo członkowskie kary finansowe.	
84.	Pracodawcy RP	Uwaga ogólna	Konsultacjami publicznymi objęte zostało zbyt mało podmiotów, które ponadto nie reprezentują wszystkich sektorów objętych regulacją — zaledwie 7 z 17 sektorów zostało wziętych pod uwagę przy ustalaniu listy podmiotów. Pominięte zostały między innymi sektory, które po raz pierwszy zostaną objęte obowiązkami, takie jak zarządzanie usługami ICT, odprowadzanie ścieków, czy badania naukowe. Biorąc pod uwagę liczbę podmiotów, na które będzie miała wpływ regulacja (ok. 38 tysięcy podmiotów), konsultacje zostały zaplanowane na zbyt krótki czas (30 dni).	Wyjaśnienie uwagi Każdy mógł zgłosić uwagi do projektu, który jest dostępny na stronie Rządowego Centrum Legislacji.
85.	Pracodawcy RP	Uwaga ogólna (OSR)	Przedstawiona ocena skutków regulacji wraz z załącznikami nie zostały wykonane wystarczająco rzetelnie. Nie przeprowadzona została dokładna analiza skutków ekonomicznych nowelizacji, a analiza przepisów dotyczących dostawców wysokiego ryzyka w państwach członkowskich zawiera rozbieżności ze stanem faktycznym, m. in. poprzez pominięcie najnowszego słoweńskiego projektu ustawy o bezpieczeństwie informacji, który nie zawiera już procedury wykluczenia urzędów podmiotu uznanego za DWR.	Wyjaśnienie uwagi Bardzo trudno jest oszacować koszty wdrożenia z uwagi na brak danych, różnorodność podmiotów, ich usług czy wielkość.
86.	Pracodawcy RP	Uwaga ogólna	Analiza legislacji państw członkowskich UE prowadzi do wniosku, że żadne z nich nie wprowadziło przepisów, ani nie dyskutuje nad projektem implementacji, który umożliwiłby wykluczenie dostawcy ze względu na państwo pochodzenia we wszystkich 18 obszarach określonych w dyrektywie NIS 2. Uznanie sieci RAN jako funkcji krytycznej jest w krajach członkowskich bardzo rzadkie. Co więcej Polska jest jedynym krajem, który uwzględnił to w projekcie implementacji NIS 2.	Wyjaśnienie uwagi Dyrektywa NIS2 wskazuje, że wszystkie podmioty kluczowe i podmioty ważne są obowiązane dbać o bezpieczeństwo łańcuchów dostaw. Z tego względu rozszerzono skutki postępowania HRV na pozostałe sektory.
87.	Pracodawcy RP	Uwaga ogólna	Środki w zakresie cyberbezpieczeństwa i audyt — perspektywa sektorowa Dyrektywa NIS2, w stosunku do poprzednio obowiązującej dyrektywy NIS, znacznie rozbudowuje katalog obowiązków nałożonych na podmioty ważne i kluczowe. Zostały one przeniesione do polskiego projektu transpozycji NIS2 bez zmian. Tym samym polski projekt jest obciążony tymi samymi problemami. Dociążenie sektorów nowymi obowiązkami, niezależnymi od rozmiaru podmiotu Kluczową kwestią jest trudność w oszacowaniu zakresu prac wymaganych do pełnego dostosowania się do wymogów regulacji. Z perspektywy organizacji trudne jest zaplanowanie rozwiązań wymagających wdrożenia, bazując jedynie na przepisach ustawy. Projekt odwołuje się w tym zakresie bezpośrednio do norm ISO. Zatem dopiero zapoznając się z wymogami ISO można realnie zmapować, jaki zakres obowiązków będą musiały wdrożyć zarówno podmioty kluczowe, jak i ważne. Warto zauważyć, że NIS2 nie zawiera rozróżnienia na poszczególne sektory w zakresie obowiązków. Również polska Nowelizacja nakłada identyczne obowiązki zarówno na podmioty kluczowe, jak i ważne we wszystkich sektorach. Jedyne różnice występują na gruncie kontroli, która wobec podmiotów kluczowych prowadzona jest ex ante, zaś wobec podmiotów ważnych ex post.cJeżeli podmioty nowo	Uwaga uwzględniona Wymogi audytów dla podmiotów ważnych zostaną złagodzone.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			zobowiązane do wdrożenia szeregu dodatkowych wymogów, zostaną obarczone jednocześnie koniecznością usuwania sprzętu, instalowania nowego i ciągłego weryfikowania nowych dostawców, realne wdrożenie celów dyrektywy NIS2 może okazać się utrudnione. Podany w art. 16 nowelizacji ustawy o KSC termin 6 miesięczny na zastosowanie się do nowych obowiązków na wdrożenie obowiązków jest całkowicie nieadekwatny. Także i w tym przypadku ustawodawca nie decyduje się na uwzględnienie perspektywy poszczególnych graczy na rynku. Proponowane rozwiązanie nie uwzględnia faktu, że znacząca część podmiotów będzie wypełniać swoje obowiązki pod raz pierwszy (np. producenci wyrobów medycznych czy przedsiębiorstwa wodociągowo-kanalizacyjne).	
88.	Pracodawcy RP	Uwaga ogólna	Negatywne konsekwencje nadregulacji dla konkurencyjności polskiej gospodarki Dyrektywa NIS2, mająca na celu wzmocnienie cyberbezpieczeństwa na terenie całej Unii Europejskiej, została zaprojektowana tak, aby zwiększyć odporność cyfrową wszystkich państw członkowskich w możliwie jednolitym stopniu. Jednak wprowadzenie przez Polskę dodatkowych środków, które umożliwiają Ministrowi Cyfryzacji wykluczanie dostawców z rynku na podstawie decyzji administracyjnej, może doprowadzić do istotnych konsekwencji dla konkurencyjności polskich przedsiębiorstw. Kluczowe ryzyka dla konkurencyjności. Ograniczenie dostępności technologii Polskie firmy będą zmuszone do korzystania z ograniczonej liczby dostawców, co nie tylko zwiększy koszty, ale także zmniejszy dostęp do najnowszych technologii. To stawia polskie przedsiębiorstwa w niekorzystnej sytuacji w porównaniu do firm z innych krajów UE, które mają swobodę wyboru między szeroką gamą dostawców technologicznych. Dobrym przykładem jest sytuacja na rynku 5G, w którym dwóch dostawców europejskich (Ericsson ze Szwecji i Nokia z Finlandii) ma pozycję wiodącą, a trzecią pozycję zajmuje spółka chińska (Huawei). W takiej sytuacji wykluczenie trzeciego dostawcy z uwagi na państwo pochodzenia kreuje duopol, który uniemożliwia realną konkurencję. Z podobną sytuacją będziemy mieć do czynienia w innych sektorach, w których nie występuje duża dywersyfikacja dostawców. W najbardziej skrajnych przypadkach może dojść do sytuacji, w której konkretny podmiot uznany za DWR jest jedynym dostawcą danego rozwiązania — na takie ryzyko narażone są sektory wysoce wyspecjalizowane, gdzie sprzęt lub oprogramowanie jest dostarczane przez mały krąg podmiotów. Bariera w adaptacji do szybko zmieniającego się środowiska technologicznego Szybkość adaptacji do nowych technologii i procesów jest kluczowa dla utrzymania konkurencyjności na rynku globalnym. Ograniczenia nałożone przez władze będą hamować zdolność polskich firm do innowacji, co jest szczególnie ważne w sektorach intensywnie wykorzystujących technologie, takich jak finanse, zdrowie czy energetyka. Analiza porównawcza z innymi państwami UE Pozostałe państwa UE, które nie przyjęły tak rygorystycznych regulacji, mogą oferować swoim przedsiębiorstwom stabilniejsze i bardziej przewidywalne środowisko do rozwoju biznesu cyfrowego, co przekłada się na ich przewagę konkurencyjną. Wzrost regulacyjnej niepewności w Polsce zniechęci zagranicznych inwestorów oraz partnerów technologicznych do współpracy z polskimi firmami, co dodatkowo osłabia ich pozycję na rynku. Rozszerzenie uprawnień Ministra Cyfryzacji do wykluczania dostawców będzie miało	Wyjaśnienie uwagi Postępowanie w sprawie uznania za dostawcę wysokiego ryzyka ma na celu identyfikację dostawcy, który w poważny sposób zagraża bezpieczeństwu narodowemu. Gospodarka nie jest w stanie bezpiecznie rozwijać się za pomocą sprzętu/oprogramowania pochodzących od dostawcy wysokiego ryzyka.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			dalekosiężne konsekwencje dla sektorów objętych NIS2 w Polsce, ograniczając ich konkurencyjność wobec firm z innych krajów UE, które korzystają z bardziej otwartego i elastycznego podejścia do zarządzania cyberbezpieczeństwem. Dla utrzymania konkurencyjności na rynku europejskim, Polska powinna rozważyć strategię minimalizującą te ryzyka, skupiając się na wspieraniu innowacji i swobody wyboru technologicznego.	
89.	Pracodawcy RP	Uwaga ogólna	Nie została zapewniona reprezentacja każdego z sektorów. Przykładowo, sektory związane z ICT są bardzo szeroko reprezentowane (26 podmiotów). Zaś inne sektory kluczowe dla bezpieczeństwa strategicznego kraju jak energetyka, zdrowie czy transport zostały uwzględnione w niewielkim zakresie. W dodatku, sektory są reprezentowane niejednolicie a reprezentacja ta nie uwzględnia kluczowych stowarzyszeń i izb funkcjonujących w ramach reprezentowanego sektora. Część sektorów została pominięta całkowicie Niereprezentowane sektory stanowią znaczącą większość. Nieuwzględnienie ich w procesie konsultacji projektu ustawy o krajowym systemie cyberbezpieczeństwa może prowadzić do szeregu poważnych błędów. Ryzyko to jest szczególnie istotne biorąc pod uwagę fakt, że objęte dyrektywą ponad 36 tys. podmiotów w Polsce ma tylko 30 dni na konsultacje publiczne w tym zakresie. Tak krótki termin w porównaniu z niewystarczającą reprezentacją podmiotów z sektorów kluczowych i ważnych w ramach konsultacji stwarza ryzyko zaprojektowania regulacji niedostosowanej do specyfiki większości sektorów gospodarki. Ponadto decyzja o pominięciu w zaproszeniu do konsultacji publicznych reprezentantów sektorów nowych a gruncie ustawy jest wyjątkowo nietrafiona, ponieważ to właśnie dla nowych podmiotów transpozycja dyrektywy NIS 2 stanowi największe wyzwanie. Podejście pomijające zdanie sektorów o niskiej świadomości cyberbezpieczeństwa jest jednym z największych błędów tej nowelizacji. Szczególnie biorąc pod uwagę fakt, że okres dostosowawczy dla tych podmiotów jest taki sam jak dla podmiotów w sektorach objętych wcześniej dyrektywą NIS i obecnie obowiązującą ustawą o krajowym systemie cyberbezpieczeństwa (6 miesięcy), które już znają swoje obowiązki. Pozostałe kluczowe zarzuty do prowadzonej procedury konsultacji nowelizacji dotyczą następujących obszarów: Niska świadomość sektorowa: Sektory nieobjęte dyrektywą NIS, są w niewielkim stopniu świadome tego, jakie obciążenia regulacyjne będą na nie nałożone wraz z przyjęciem Nowelizacji. Nieuwzględnienie ich w procesie konsultacji pogłębi tę nieświadomość. Z drugiej strony uwzględnienie tych podmiotów pozwoli im na wskazanie swoich wątpliwości w procesie tworzenia ustawy. Da im to również szansę na dokładne zapoznanie się z treścią tworzonych przepisów. Zaniedbanie perspektywy użytkownika końcowego: Organizacje reprezentujące konsumentów, powinny być aktywnie zaangażowane w proces konsultacji, aby zapewnić, że interesy użytkowników końcowych są odpowiednio chronione. Brak ich głosu może prowadzić do opracowania przepisów, które nie uwzględniają odpowiednio ochrony danych osobowych i prywatności. Potencjalne konsekwencje ekonomiczne: Nieadekwatne przepisy mogą prowadzić do obciążeń administracyjnych dla przedsiębiorstw, zwłaszcza mniejszych, które mogą mieć trudności z dostosowaniem się do skomplikowanych wymogów prawnych. Włączenie szerszego grona interesariuszy w konsultacje może	Wyjaśnienie uwagi Zakres podmiotowy Dyrektywy NIS2 jest znany od kilku lat. Projekt został udostępniony na stronie internetowej Rządowego Centrum Legislacji i każdy mógł zgłosić do niego uwagi.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			pomóc zidentyfikować takie ryzyka i zaproponować rozwiązania minimalizujące potencjalne negatywne skutki ekonomiczne.	
90.	Przedsiębiorcy.p 1	Uwaga ogólna	Polska do dnia 17 października 2024 r. zobowiązana jest do wdrożenia unijnej dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniającej rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającej dyrektywę (UE) 2016/1148 (dyrektywa NIS 2). Wymóg dostosowania przepisów prawa krajowego do tejże dyrektywy w w/w terminie wynika z przepisu art. 41 ust. 1 dyrektywy NIS 2. Projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw z dnia 23 kwietnia 2024 r. opublikowany na stronach Rządowego Centrum Legislacji w dniu 24 kwietnia 2024 r. w sposób rażący wykracza poza regulacje dyrektywy NIS 2, stanowiąc tym samym tzw. nadregulację, która powoduje daleko idące negatywne skutki dla wielu podmiotów - przedsiębiorców oraz dla administracji publicznej, w tym dla jednostek samorządu terytorialnego. Innymi słowy, w/w projekt ustawy zawiera bardziej restrykcyjne uregulowania niż dyrektywa unijna NIS 2. W niniejszym stanowisku zaprezentowane one zostaną w sposób możliwie najbardziej syntetyczny i czytelny.	Uwaga częściowo uwzględniona Wymagania w zakresie audytów dla podmiotów ważnych zostały złagodzone. Część sektorów została przeniesiona z powrotem do sektorów ważnych.
91.	Przedsiębiorcy.p 1	Uwaga ogólna	Rozszerzenie podmiotów kluczowych o nowe sektory i podsektory - nadregulacja w stosunku do dyrektywy NIS 2 W pierwszej kolejności projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (dalej również: „projekt ustawy o KSC”) w sposób znaczący - w stosunku do dyrektywy NIS 2 - rozszerza ilość podmiotów kluczowych, których ustawa ta ma dotyczyć, w tym identyfikując jako sektory kluczowe, sektory które w dyrektywie NIS 2 traktowane są jedynie jako ważne, a zatem podlegające mniejszemu zakresowi nadzoru. Klasyfikacja przez projekt ustawy o KSC podmiotów ważnych jako podmiotów kluczowych wiąże się z podwyższeniem stopnia nadzoru nad tymi podmiotami również o nadzór prewencyjny. To znaczące wyjście poza wymogi dyrektywy NIS 2 neguje podstawowe zasady, zgodnie z którymi powinna następować implementacja dyrektyw unijnych. Dyrektywa NIS 2 przewiduje, że jednym z kryteriów pozwalających na zakwalifikowanie danego podmiotu, jako podmiotu kluczowego lub ważnego, jest zaliczenie działalności tego podmiotu do sektora kluczowego, które wyszczególnione są odpowiednio w załączniku nr I i załączniku nr II do dyrektywy NIS 2. Z kolei w polskim projekcie ustawy o KSC, polski prawodawca znacznie rozszerzył listę sektorów gospodarki umożliwiając tym samym zakwalifikowanie większej liczby podmiotów jako podmiotów kluczowych i jednocześnie ograniczając listę sektorów gospodarki pozwalających na zaliczenie podmiotu do kategorii podmiotów ważnych. Co więcej, polski projektodawca objął zakresem regulacji - w przeciwieństwie do dyrektywy NIS 2 - również lokalne jednostki samorządu, a także instytucje edukacyjne, co powoduje konieczność wdrożenia przez te podmioty obowiązków, których koszty mogą być szacowane w milionach złotych. Dodatkowo dochodzi do tego ryzyko wszczęcia - rodzącej bardzo niebezpieczne konsekwencje - procedury uznania dostawcy sprzętu lub oprogramowania dla tych podmiotów (zarówno dla podmiotów kluczowych, jak i ważnych), za dostawcę wysokiego ryzyka, co	Uwaga częściowo uwzględniona Wymagania w zakresie audytów dla podmiotów ważnych zostały złagodzone. Część sektorów została przeniesiona z powrotem do sektorów ważnych. Jednostki samorządu terytorialnego od 2012 r. są obowiązane wdrożyć system zarządzania bezpieczeństwem informacji w swoich systemach teleinformatycznych. Projekt będzie przewidywał możliwość uwspólnienia obowiązków w administracji publicznej, co pozwoli na adekwatne wykorzystanie zasobów. Postępowanie w sprawie uznania za dostawcę wysokiego ryzyka ma zabezpieczyć polskie społeczeństwo i gospodarkę przed dostawcą, który w poważny sposób zagraża bezpieczeństwu państwa.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			wiązało się będzie z koniecznością pozbycia się takiego sprzętu w określonym czasie (co do zasady 7 lat) i nabycia nowego, co w konsekwencji generowało będzie ogromne koszty.	
92.	Przedsiębiorcy.p 1	Uwaga ogólna	Nowe sektory i podsektory wskazane w projekcie ustawy o KSC - nadregulacja Projekt ustawy o KSC w zakresie podmiotów kluczowych obejmuje - w przeciwieństwie do dyrektywy NIS 2 - hurtownie farmaceutyczne, przedsiębiorców posiadających pozwolenie na dopuszczenie do obrotu produktu leczniczego, importerów i wytwórców produktów leczniczych / substancji czynnych, importerów równoległych i wytwórców produktów leczniczych / substancji czynnych, importerów równoległych, dystrybutorów substancji czynnej oraz apteki. Zgodnie natomiast z załącznikiem nr 1 do dyrektywy NIS 2 status podmiotów kluczowych przysługuje tylko tym podmiotom, które prowadzą działalność badawczo-rozwojową w zakresie produktów leczniczych, podmiotom produkującym podstawowe substancje farmaceutyczne oraz leki i pozostałe wyroby farmaceutyczne, a także podmiotom produkującym wyroby medyczne, przy czym tym ostatnim jedynie wówczas, gdy wyroby te uznane są za mające krytyczne znaczenie podczas stanu zagrożenia zdrowia publicznego. Dyrektywa NIS 2 w przeciwieństwie do projektu ustawy o KSC nie zawiera zatem tak szerokiego katalogu podmiotów. W stosunku do niektórych z nich zawiera stosowny warunek, który musi zaistnieć, aby podmioty te zakwalifikowane zostały jako podmioty kluczowe. Warunkiem tym jest uznanie ich za mające krytyczne znaczenie podczas stanu zagrożenia zdrowia publicznego. Polski prawodawca wyeliminował z projektu ustawy o KSC tenże warunek, uznając a priori podmioty produkujące wyroby medyczne za podmioty kluczowe. Projekt ustawy o KSC poszerza również - w stosunku do dyrektywy NIS 2 - sektor energii o podsektor wydobywania kopalin pomimo tego, iż sektor energetyka wskazany w załączniku I do dyrektywy NIS 2 nie zalicza do usług kluczowych podsektora wydobywania kopalin. Podsektor wydobywania kopalin nie został zaliczony w dyrektywie NIS 2 nawet do grupy sektorów ważnych. Projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa, jako podmioty kluczowe klasyfikuje podmioty, które w dyrektywie NIS 2 uznane zostały jedynie jako podmioty ważne i tym samym do podmiotów kluczowych zalicza takie sektory i podsektory jak: produkcja, wytwarzanie i dystrybucja chemikaliów; produkcja, przetwarzanie i dystrybucja żywności; produkcja w tym podsektor produkcji wyrobów medycznych i wyrobów medycznych do diagnostyki in vitro, podsektor produkcji komputerów, wyrobów elektronicznych i optycznych, podsektor produkcji urządzeń elektrycznych, podsektor produkcji maszyn i urządzeń, gdzie indziej niesklasyfikowaną, oraz podsektor produkcji pojazdów samochodowych, przyczep i naczep.	Uwaga częściowo uwzględniona Dyrektywa NIS2 pozwala państwom członkowskim na zachowanie dotychczas zidentyfikowanych podmiotów jako operatorów usług kluczowych. Hurtownie farmaceutyczne, przedsiębiorcy posiadający pozwolenie na dopuszczenie do obrotu produktu leczniczego, importerzy i wytwórcy produktów leczniczych/substancji czynnych, importerów równoległych i wytwórców produktów leczniczych/substancji czynnych, importerzy równolegli, dystrybutorzy substancji czynnej oraz apteki ogólnodostępne podlegają obecnym wymogom z ustawy o krajowym systemie cyberbezpieczeństwa. Podobnie jest z sektorem wydobywania kopalin. Stąd też zachowano te rodzaje podmiotów w nowelizacji. Część sektorów została przeniesiona z powrotem do sektorów ważnych.
93.	Przedsiębiorcy.p 1	Uwaga ogólna	Rozszerzenie podmiotów kluczowych o jednostki samorządu terytorialnego oraz ich związki oraz inne jednostki sektora finansów publicznych Projekt ustawy o KSC rozszerza zakres podmiotów kluczowych o jednostki sektora finansów publicznych o których mowa w art. 9 pkt 1-6, 8 i 10-13 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2023 r., poz. 1270, z późn. zm.), a zatem m.in. o jednostki samorządu terytorialnego oraz ich związki, ale również samodzielne publiczne zakłady opieki zdrowotnej, czy uczelnie publiczne. Należy podkreślić, że zarówno jednostki samorządu terytorialnego, jak i co do	Wyjaśnienie uwagi Jednostki samorządu terytorialnego od 2012 r. są obowiązane wdrożyć system zarządzania bezpieczeństwem informacji w swoich systemach teleinformatycznych. Projekt będzie przewidywał możliwość uwspólnienia

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

		zasady instytucje edukacyjne nie są uznane za podmioty kluczowe przez dyrektywę NIS 2. Dyrektywa NIS 2 wskazuje jedynie, że te ostatnie powinny być kwalifikowane za podmioty kluczowe jedynie wówczas, gdy prowadzą działalność badawczą o krytycznym znaczeniu. Polski projektodawca nie wprowadza tego warunku. W wyniku tego zatem wszystkie instytucje edukacyjne będą zobowiązane do realizacji kosztownych wymogów w zakresie cyberbezpieczeństwa. W tym miejscu należy podkreślić, że dyrektywa NIS 2 w art. 2 ust. 2 lit. f) stanowi, że jednostki na poziomie regionalnym mogą zostać uznane za podmioty administracji publicznej tylko wtedy, gdy świadczą usługi, których zakłócenie mogłoby mieć znaczący wpływ na krytyczną działalność społeczną lub gospodarczą, co powinno być potwierdzone oceną opartą na analizie ryzyka. Projekt ustawy o KSC nie odnosi się do powyższego warunku. Dyrektywa NIS 2 - w sposób bezwarunkowy - jako podmioty kluczowe obejmuje tylko podmioty administracji publicznej na poziomie rządu centralnego, zaś projektodawca polski rozszerza podmioty kluczowe o m.in. jednostki samorządu terytorialnego, co generuje niepotrzebne, gigantyczne koszty dla tychże jednostek samorządu terytorialnego. Sektor administracji publicznej w Ocenie Skutków Regulacji projektu ustawy o KSC wyliczony został na 27.905 podmiotów, a przyjmuje się, że liczba ta - jak zresztą liczba wszystkich podmiotów CG kluczowych i ważnych - nie została doszacowana. Należy tutaj podkreślić, że przeważająca większość tych podmiotów, to jednostki samorządu terytorialnego i jednostki im podległe. Włączenie w projekcie ustawy o KSC takich podmiotów jak jednostki samorządu terytorialnego do kategorii podmiotów kluczowych, wbrew wymaganiom dyrektywy NIS 2, może prowadzić do znaczących trudności w ich funkcjonowaniu, nie przyczyniając się jednocześnie do realnego wzrostu bezpieczeństwa cybernetycznego kraju. Jednostki samorządu terytorialnego zobowiązane będą do wyłożenia olbrzymich pieniędzy na zrealizowanie licznych rygorystycznych i sformalizowanych obowiązków, nałożonych przez projekt ustawy o KSC oraz objęte są ryzykiem gigantycznych, wielomilionowych kar za niezrealizowanie tychże obowiązków, które mogą być nałożone nawet wówczas, gdy doszło do jednorazowego naruszenia. Projekt ustawy o KSC nakłada osobistą odpowiedzialność na osoby kierujące danym podmiotem. Do tego dochodzi perspektywa wyeliminowania dostawcy sprzętu dla danej jednostki samorządu terytorialnego, w przypadku uznania przez Ministra Cyfryzacji tegoż dostawcy za dostawcę wysokiego ryzyka. Ten aspekt dotyczy wszystkich podmiotów kluczowych i ważnych i co więcej nie został on w ogóle przewidziany w dyrektywie NIS 2, co zostanie omówione osobno w dalszej części stanowiska. Należy tutaj jeszcze wskazać na to, że podmioty kluczowe podlegały będą bardzo szerokiemu nadzorowi sprawowanemu przez organy właściwe do spraw cyberbezpieczeństwa. Będzie on miał charakter nie tylko następczy (jak w przypadku podmiotów ważnych), ale również prewencyjny (art. 53 ust. 3 projektu ustawy o KSC). W pełni nieuzasadnione jest kwalifikowanie jednostek samorządu terytorialnego za podmiot kluczowy. Jednostki samorządu terytorialnego nie są newralgicznymi	obowiązków w administracji publicznej, co pozwoli na adekwatne wykorzystanie zasobów. Podmioty publiczne powinny być także kontrolowane ex ante, ponieważ świadczą zadania publiczne na rzecz obywateli. Przykładowo Najwyższa Izba Kontroli skontrolowała ex ante niektóre gminy pod kątem cyberbezpieczeństwa¹². Pominięcie jednostek samorządu terytorialnego w KSC w sytuacji wielu cyberzagrożeń jak również i ciągłego ich wsparcia w postaci programów typu Cyberbezpieczny Samorząd byłoby niezasadne.

¹² <https://www.nik.gov.pl/aktualnosci/zachodniopomorskie-gminy-cyberzagrozenia.html>

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			podmiotami narażonymi na cyberzagrożenia. To zdecydowanie zbyt daleko idąca ingerencja polskiego projektodawcy, wykraczająca poza regulacje dyrektywy NIS 2. Warto w tym miejscu podkreślić, że kraje takie, jak: Niemcy, Belgia, Węgry, Finlandia i Austria, które wdrożyły już dyrektywę NIS 2 lub przedstawiły projekt jej transpozycji, nie objęły zakresem nowych przepisów jednostek samorządu terytorialnego.	
94.	Przedsiębiorcy.p l	Uwaga ogólna	Znaczące - w stosunku do dyrektywy NIS 2 - rozszerzenie katalogu podmiotów kluczowych i ważnych, na 18 sektorów (łącznie ponad 38.000 podmiotów), łączy się z daleko idącymi obowiązkami dla tychże podmiotów. Wskazać tutaj należy chociażby na obowiązkowe, cykliczne - co najmniej raz na 2 lata - audyty bezpieczeństwa, nałożone nie tylko na podmioty kluczowe, ale również na podmioty ważne, przy czym pierwszy audyt (audyt wstępny) należy przeprowadzić już w ciągu 12 miesięcy. Audyty te (wstępny oraz cykliczne) muszą być przeprowadzane przez osoby o odpowiednich kompetencjach, a udostępnienie wyników audytu właściwemu organowi ma nastąpić w ciągu 3 dni od ich otrzymania. Projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa nakłada na podmioty szereg nowych obowiązków, takich jak: obowiązek stworzenia systemów zarządzania bezpieczeństwem informacji, zgodnie z normami ISO, obowiązek wdrożenia zabezpieczeń przed incydentami cyberbezpieczeństwa, w oparciu o analizę ryzyka i najnowszy stan wiedzy, obowiązek dokonywania do organu nadzorczego zgłoszeń incydentów (wczesne ostrzeżenie już w terminie 12 h/24 h, kolejne w terminie 72 h) oraz powiadamiania o incydentach własnych użytkowników. Nadto wskazać należy na: obowiązek wdrożenia rozbudowanej dokumentacji dotyczącej cyberbezpieczeństwa, obowiązek rejestracji w krajowym systemie informatycznym oraz wymiany informacji za jego pośrednictwem, obowiązek zarządzania ryzykiem łańcucha dostawców usług, obowiązek zapewnienia dostępu do wiedzy pozwalającej na zrozumienie cyberzagrożeń dot. cyberbezpieczeństwa wśród własnych pracowników. Dodatkowo, dla każdego sektora Rada Ministrów może określić, w drodze rozporządzenia, odrębnie dla danego rodzaju działalności szczegółowe wymagania. To olbrzymie proceduralne, techniczne i biznesowe (kosztotwórcze) przedsięwzięcie, z którym będą musieli się zmierzyć - nieświadomi jeszcze tych obowiązków - przedsiębiorcy, reprezentujący szeroko zakreślone - w stosunku do dyrektywy NIS 2 - sektory, ale również jednostki samorządu terytorialnego. Za ich niespełnienie przewidziane zostały wielomilionowe kary - do 10.000.000 euro lub 2% przychodów osiągniętych przez podmiot kluczowy z działalności gospodarczej. Nie sposób oszacować kosztów wdrożenia tych przepisów, które w sektorze prywatnym mogą wynosić od kilkudziesięciu, kilkuset tysięcy złotych nawet do ponad miliona (w stosunku do pojedynczej firmy), nie mówiąc o wielomilionowych nakładach dla sektora administracji publicznej. Poza kosztami wdrożenia, wskazać należy na koszty coroczne, jakie podmioty kluczowe i ważne muszą wykładać w celu spełnienia obowiązków. Ułomności przedstawia w tym zakresie Ocena Skutków Ryzyka, która nie zawiera jakiegokolwiek estymacji w/w kosztów. Projekt ustawy nakłada szereg nowych obowiązków w tym m.in. obowiązek stworzenia systemów zarządzania bezpieczeństwem, zgodnie z normami ISO27001 oraz ISO22301 podczas gdy dyrektywa	Uwaga częściowo uwzględniona Wymagania dotyczące audytów dla mniejszych podmiotów zostaną złagodzone. Termin na wykonanie pierwszego audytu dla podmiotów kluczowych zostanie wydłużony do 24 miesięcy. Nie było oraz nie ma w projekcie obowiązku wdrożenia SZBI zgodnego z ISO 27001 czy SZCD zgodnego z ISO 22301. Proponowany przepis miał przesądzić, że wdrożenie tych norm zapewnia spełnienie obowiązków ustawowych. Pod wpływem różnych uwag koncepcja ta została zmieniona. Wprowadzone zostanie mapowanie różnych dokumentów normalizacyjnych na przepisy ustawy. Wprowadzenie zabezpieczeń przed incydentami, zgłoszeń incydentów wynika z dyrektywy NIS2. Liczba podmiotów w szczególności wynika z dyrektywy NIS2.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			NIS 2 wskazuje, że standardy powinny być promowane, a nie narzucane (art. 25 dyrektywy NIS 2) i wskazuje, że podmioty kluczowe i ważne powinny wdrażać odpowiednie i proporcjonalne środki techniczne, operacyjne i organizacyjne wykorzystując najnowszy stan wiedzy oraz normy europejskie i organizacyjne (art. 21 ust. 1 dyrektywy NIS 2). Niezasadne jest zatem narzucenie przez polskiego projektodawcę obowiązku stosowania konkretnych norm. Warto w tym miejscu wspomnieć, że polski projekt ustawy o KSC zacierza rozróżnienie podmiotów na kluczowe i ważne, gdyż przewiduje dla tychże podmiotów takie same obowiązki. Projektodawca krajowy nakłada na podmioty kluczowe i ważne obowiązek przeprowadzenia na ich koszt audytu bezpieczeństwa (art. 15 ust. 1 projektu ustawy o KSC) podczas, gdy w dotychczasowej wersji ustawy obowiązek przeprowadzenia audytu bezpieczeństwa dotyczył systemu informacyjnego wykorzystywanego jedynie do świadczenia usługi kluczowej.	
95.	Przedsiębiorcy.p l	Uwaga ogólna	Projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa reguluje całkowicie nieprzewidzianą w dyrektywie NIS 2 procedurę uznania dostawcy sprzętu lub oprogramowania dla danego podmiotu kluczowego lub ważnego za dostawcę wysokiego ryzyka. Aspekt ten dotyczy zarówno podmiotów kluczowych, jak i ważnych. Zatem z tego punktu widzenia nie ma żadnych rozbieżności w różnicowaniu w/w podmiotów na kluczowe i ważne. Procedura dostawcy wysokiego ryzyka (HRV - high risk vendor) wprowadzona została przez projektodawcę w 18 sektorach. Projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa wprowadzając powyższą procedurę zawiera nadregulację w stosunku do dyrektywy NIS 2. Tym samym każda firma lub jednostka samorządu terytorialnego (szerzej - administracja publiczna), które w projekcie ustawy zakwalifikowane są jako podmioty kluczowe lub ważne, stoi przed perspektywą uznania swojego dostawcy (np. sprzętu komputerowego) za dostawcę wysokiego ryzyka. Przesłanki do takiego uznania przez organ (Minister Cyfryzacji) są bardzo nieostre, a konsekwencje bardzo daleko idące. Dostawcę wysokiego ryzyka produktów, usług, procesów informacyjno - komunikacyjnych (ICT) wskazuje Minister Cyfryzacji w oparciu o opinię (art. 67 b ust. 10 projektu ustawy o KSC), sporządzoną przez tzw. Kolegium, w którym przewodniczącym jest Prezes Rady Ministrów, w której to opinii bierze się pod uwagę nieostre i polityczne kryteria takiej jak: prawdopodobieństwo, z jakim dostawca sprzętu lub oprogramowania znajduje się pod kontrolą państwa spoza terytorium Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, z uwzględnieniem np. struktury własnościowej dostawcy sprzętu lub oprogramowania lub zdolności ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Dla firmy lub administracji publicznej oznacza to konieczność usunięcia przez nią takiego dostawcy, co jak nie trudno sobie wyobrazić, pociągnie za sobą gigantyczne koszty. W konsekwencji, doprowadzi to do osłabienia konkurencyjności polskich przedsiębiorców na rynku obejmującym podmioty kluczowe i ważne, a nawet do powstania duopolu czy monopolu. Wycofanie z użytkowania dostawcy wysokiego ryzyka (co do zasady w ciągu 7 lat) ma się odbywać na koszt danego przedsiębiorcy lub jednostki samorządu terytorialnego, i projektodawca nie przewiduje tutaj jakiegokolwiek rekompensaty, co	Wyjaśnienie uwagi Postępowanie w sprawie uznania za dostawcę wysokiego ryzyka ma na celu zabezpieczenie polskiej gospodarki i polskiego społeczeństwa przed dostawcą sprzętu lub oprogramowania, który stwarza poważne zagrożenie dla bezpieczeństwa państwa, obronności, bezpieczeństwa i porządku publicznego lub zdrowia i życia ludzi. W ramach postępowania administracyjnego będą brane pod uwagę zarówno aspekty techniczne związane z dostarczaniem przez dostawcę sprzętem i oprogramowaniem jak również aspekty nietechniczne związane z dostawcą. Dzięki temu zostanie zidentyfikowany pełen obraz zagrożeń jakie stwarza dostawca sprzętu lub oprogramowania. Postępowanie umożliwia badanie dostawcy sprzętu lub oprogramowania dla wszystkich sektorów gospodarki wskazanych w ustawie. Jest to wskazane z uwagi na to, że każdy podmiot kluczowy i podmiot ważny musi dbać o bezpieczeństwo łańcuchów dostaw.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			zresztą przyznane jest wprost w Ocenie Skutków Ryzyka (s. 30 OSR). Projekt nie zakłada nawet możliwości poprawy (w zakresie zabezpieczeń) swojego produktu, usługi przez danego dostawcę, uznanego za dostawcę wysokiego ryzyka, który w ramach takiego postępowania sanacyjnego powinien mieć prawo do poprawy swojego produktu lub usługi w zakresie zabezpieczeń. Sam już proces, w ramach którego rozstrzygane będzie, czy dany dostawca jest dostawcą wysokiego ryzyka, może wiązać się dla niego ze swoistego rodzaju ostracyzmem ze strony jego klientów, niezależnie od wyniku zakończenia tego procesu. Biorąc pod uwagę szeroką definicję dostawcy sprzętu lub oprogramowania zawartą w projekcie ustawy o KSC - mowa tu o dostawcy w rozumieniu importera, dystrybutora, jak i producenta oraz upoważnionego przedstawiciela (art. 2 pkt 4 c projektu ustawy o KSC), to decyzja o uznaniu takiego dostawcy za dostawcę wysokiego ryzyka dotknie bardzo dużej liczby podmiotów. Należy w tym miejscu podkreślić, że dyrektywa NIS 2 w art. 24 ust. 1 wskazuje jedynie, że państwa członkowskie mogą wymagać od podmiotów kluczowych i ważnych stosowania konkretnych produktów, usług i procesów ICT nabytych od osób trzecich, certyfikowanych zgodnie z europejskimi programami certyfikacji cyberbezpieczeństwa. I to powinien być punkt odniesienia dla polskiego projektodawcy. Należy tutaj zwrócić jeszcze uwagę na fakt, że polski projektodawca w Ocenie Skutków Ryzyka nie wskazał, w jaki sposób dokonywać recyklingu oprogramowania, sprzętu, którego dany podmiot kluczowy lub ważny będzie musiał się pozbyć, a jest to przecież bardzo ważny aspekt z punktu widzenia założeń, którymi kieruje się Unia Europejska.	Podmioty kluczowe i podmioty ważne mają istotny charakter dla funkcjonowania współczesnej gospodarki i społeczeństwa informacyjnego. Zakłócenie funkcjonowania tych podmiotów poprzez atak przez łańcuch dostaw może spowodować niepowetowane straty. Z uwagi na charakter tego postępowania wyłączono część przepisów Kodeksu postępowania administracyjnego. Przede wszystkim nie jest możliwe przeprowadzenie postępowania administracyjnego przy udziale wszystkich podmiotów, które wykorzystują sprzęt lub oprogramowanie pochodzące od danego dostawcy. Rygor natychmiastowej wykonalności jest konieczny z uwagi na to, że kwestia dotyczy poważnego zagrożenia dla bezpieczeństwa państwa. Nie przewiduje się rekompensat za wycofanie sprzętu lub oprogramowania, ponieważ ten sprzęt i tak z czasem podlegałby wymianie z uwagi na naturalne zużycie. Termin 7 lat na wycofanie sprzętu wydaje się terminem adekwatnym. Jednocześnie skrócono ten termin do 4 lat dla sprzętu i oprogramowania realizującego funkcje krytyczne w zakresie bezpieczeństwa sieci i usług. Wycofanie sprzętu/pochodzącego od dostawcy wysokiego ryzyka w terminie 4 lat dla przedsiębiorców telekomunikacyjnych jest zasadne z uwagi na to, że chodzi o funkcje krytyczne dla sieci i usług. Zauważyć należy, że sprzęt i

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

				oprogramowanie i tak wymagałby okresowej wymianie z uwagi na naturalne zużycie sprzętu.
96.	Przedsiębiorcy.p 1	Uwaga ogólna	Działanie projektodawcy, polegające na dokonaniu swoistego rodzaju „transferu” wybranych sektorów (podsektorów) z sektora ważnego do sektora kluczowego, rozszerzenie w ramach podmiotów kluczowych sektorów o inne podsektory, wprowadzenie nieuregulowanej w dyrektywie NIS 2 procedury wydania decyzji, co do uznania danego dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka (HRV), pozostaje w sprzeczności z prawem unijnym, a to z racji, że wprowadza środki nieprzewidziane w tejże dyrektywie. Implementacja dyrektywy NIS 2 z tak daleko idącymi różnicami (obostrzeniami) w stosunku do tejże dyrektywy nakłada na projektodawcę obowiązek przygotowania tzw. tabeli niezgodności, który to obowiązek nie został wykonany. Na tle innych państw Unii Europejskiej, które wprowadziły już w swoim porządku prawnym dyrektywę NIS 2, polski projekt ustawy regulujący cyberbezpieczeństwo jest najbardziej restrykcyjny. Dotyczy największej liczby sektorów i podmiotów oraz wprowadza nieuregulowaną w dyrektywie NIS 2 procedurę umożliwiającą uznanie danego dostawcy za dostawcę wysokiego ryzyka (HRV - high risk vendor), czego konsekwencje finansowe - liczone niekiedy w wielu milionach złotych - ponosić będą podmioty kluczowe i ważne, a na koniec, co przysądzi projektodawca w Ocenie Skutków Ryzyka - konsumenci (s. 29 i s. 30 OSR), gdyż podmioty kluczowe i ważne doliczą do swoich towarów (usług) koszty związane z operacją wyeliminowania i zakupu nowych produktów lub usług. Należy zwrócić uwagę na niemalże całkowity brak świadomości podmiotów objętych nową regulacją, co do obowiązków i możliwości skorzystania z procedury uznania dostawcy tychże podmiotów za dostawcę wysokiego ryzyka i związanych z tym konsekwencji (wyeliminowanie produktów). Na krytykę zasługuje również nieskierowanie projektu ustawy o KSC do konsultacji z uwzględnieniem wszystkich ujętych w regulacji sektorów. Nowe przepisy mają wejść w życie po upływie 1 miesiąca od dnia ogłoszenia, a podmioty kluczowe i ważne będą miały 6 miesięcy na zrealizowanie niektórych już obowiązków wskazanych w projekcie ustawy. W kontekście powyższych uwag do projektu ustawy o KSC, Ogólnopolska Federacja Przedsiębiorców i Pracodawców przedstawia najbardziej kluczowe postulaty wnosząc o: 1. Dostosowanie zakresu podmiotów kluczowych i ważnych do zakresu wynikającego z dyrektywy NIS 2, w tym usunięcie z kategorii podmiotów kluczowych jednostek samorządu terytorialnego - dostosowanie zakresu podmiotowego ustawy do zakresu wynikającego z dyrektywy NIS 2; 2. Wyeliminowanie procedury uznania w drodze decyzji danego dostawcy sprzętu, usługi dla podmiotu kluczowego lub podmiotu ważnego, za dostawcę wysokiego ryzyka. 3. Odstąpienie od rygorystycznego wymagania stosowania norm technicznych do wytworzenia dokumentacji, zgodnie z wymaganiami ISO 27001 lub normy jej równoważnej i ISO 22301 lub normy jej równoważnej.	Uwaga częściowo uwzględniona Sektory produkcji; Produkcji, wytwarzania i dystrybucji chemikaliów; Produkcji, przetwarzania i dystrybucji żywności zostaną przeniesione do sektorów ważnych. Projekt był dostępny na stronach Rządowego Centrum Legislacji i każdy mógł do niego złożyć uwagi. Termin na dostosowanie się do wymogów ustawy pozostanie 6 mies. Bardzo trudno jest oszacować koszty wdrożenia z uwagi na brak danych, różnorodność podmiotów, ich usług czy wielkość. Wymagania dotyczące dokumentacji zostaną złagodzone.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			4. Oszacowanie w Ocenie Skutków Regulacji kosztów wdrożenia obowiązków przez podmioty kluczowe i ważne oraz kosztów przeprowadzania cyklicznych obowiązkowych audytów bezpieczeństwa; oszacowanie wpływu wydania decyzji o uznaniu dostawcy sprzętu i oprogramowania za dostawcę wysokiego ryzyka.	
97.	Przedsiębiorcy RP	Uwaga ogólna (OSR)	W ramach oceny skutków regulacji („OSR”) zostały przedstawione wnioski i szacunki dotyczące kosztów nowelizacji. Nie uwzględniają one jednak w wystarczającym stopniu tego, że procedura uznawania określonych dostawców za DWR stanowi potencjalnie jeden z największych kosztów wdrożenia nowelizacji. Co więcej w zakresie dotyczącym kosztów związanych z wycofaniem sprzętu lub oprogramowania od dostawców wysokiego ryzyka przytoczony jest termin 5 lat oraz 7 lat, które to odnoszą się do standardowego terminu (7 lat) oraz do terminu dla podmiotów, które nabyły produkt w drodze zamówienia publicznego (5 lat lub 7 lat w zależności od tego czy usługi ICT wykorzystywane są do wykonywania funkcji krytycznych). Nie został jednak wzięty pod uwagę istotny, najkrótszy termin 4-letni dla przedsiębiorców telekomunikacyjnych — a to on jest skrajnie niekorzystny w świetle skali zmian, która czeka przedsiębiorców telekomunikacyjnych. Realne koszty będą zatem znacznie wyższe względem poczynionej analizy w zależności od polityki Ministerstwa Cyfryzacji. Jeśli przepisy dotyczące DWR są wymierzone w konkretne podmioty, to powinna zostać przeprowadzona szczegółowa analiza udziału tych podmiotów w rynku w roli dostawców produktów, usług i procesów ICT w poszczególnych sektorach. Obecnie OSR nie zawiera takiej analizy, co uniemożliwia realną ocenę skutków decyzji o uznaniu danego podmiotu za DWR. Jednakże skutki mogą się różnić w zależności od sektora. iWarto na przykład zauważyć, że w sektorze energetyki europejscy producenci zaspokajają niecałe 2% zapotrzebowania na fotowoltaikę i, natomiast aż 97% importowanej fotowoltaiki pochodzi z Chin. Można zatem zdecydowanie założyć, że wycofanie sprzętu wpłynie negatywnie na transformację energetyczną w Polsce i realne wykorzystanie funduszy w ramach Krajowego Planu Odbudowy i Zwiększania Odporności, którego celem jest między innymi zielona transformacja i cyfrowa transformacja. Wyższe koszty sprawiają, że te środki będą przeznaczone na mniejszą liczbę inwestycji. Co więcej nie zostały ocenione koszty wdrożenia Nowelizacji w podmiotach nią objętych. Biorąc pod uwagę rynkowe analizy jakie były w tym zakresie przeprowadzane można wskazać kilka prawidłowości na poziomie UE (dane pochodzą z raportu Frontier Economics³): o Szacowany roczny koszt wdrożenia dyrektywy NIS2 w całej UE wynosi 31,2 mld euro. Stanowi to około 0,31% całkowitego obrotu we wszystkich sektorach objętych dyrektywą NIS2. Wzrost kosztów przestrzegania przepisów dla sektorów już regulowanych na mocy pierwotnej dyrektywy NIS wynosi 1,3 mld euro rocznie (0,20% całkowitego obrotu sektora). Nowe sektory wchodzące w zakres dyrektywy NIS2 ponoszą dodatkowe koszty przestrzegania przepisów w wysokości 29,9 mld euro rocznie (0,32% ich całkowitych przychodów). Dodatkowe koszty przestrzegania przepisów jako procent obrotu są najwyższe dla małych firm, około 1,8%, w porównaniu do 0,6% dla średnich firm, a nawet mniej dla dużych firm.	Wyjaśnienie uwagi Bardzo trudno jest oszacować koszty wdrożenia z u wagi na brak danych, różnorodność podmiotów, ich usług czy wielkość.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			W wartościach bezwzględnych, średnie firmy ponoszą najwyższe całkowite koszty zapewnienia zgodności z przepisami, co odzwierciedla zarówno ich liczbę, jak i skalę wymaganych usprawnień w zakresie cyberbezpieczeństwa. Przed wprowadzeniem NIS2 średnie wydatki na bezpieczeństwo ICT w przedsiębiorstwach szacowano na około 0,52% obrotów w 2020 roku. NIS2 znacznie zwiększa ten odsetek, zwłaszcza w niektórych sektorach.	
98.	Pracodawcy RP	Uwaga ogólna	Ostatecznie porównanie polskiego projektu implementacji dyrektywy NIS 2 do legislacji innych państw członkowskich wykazało, że polski projekt odbiega od standardów europejskich. Założenia polskiego ustawodawcy są wyjątkowo surowe na tle przepisów proponowanych lub przyjętych przez inne państwa członkowskie. Pozostałe państwa członkowskie prezentują liberalne podejście do możliwości wykluczenia sprzętu ze względu na państwo pochodzenia dostawcy. Chociaż w Polsce w aktualnie obowiązującym prawie nie ma jeszcze przepisów, które by to umożliwiały, projekt nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa nie tylko zakłada taką możliwość, ale do tego w stosunku do kręgu podmiotów znacznie bardziej rozszerzonego niż przewidziano w 5G Toolbox. Ponadto Polska jako jedyny kraj zdecydowała się w ramach transpozycji dyrektywy NIS 2 wprowadzić możliwość wykluczenia sprzętu ze względu na państwo pochodzenia dostawcy oraz zaklasyfikować sieć RAN jako krytyczną. Wszystko to sprawia, że projekt nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa jest aktualnie najsurowszym w Europie. Wdrożenie 5G Toolbox Ujęcie 5G Toolboxa w ramach implementacji NIS 2 jest chybione i wprowadza zbędny chaos dla przedsiębiorców, którzy będą podlegać regulacji. Trzeba mieć bowiem na względzie, że Polski ustawodawca zdecydował, aby rozszerzyć zakres wdrażania zasad wynikających z 5G Toolboxa (dedykowanych dla podmiotów z sektora 5G) także do innych sektorów znanych z NIS 2 (w tym sektory produkcyjne, transport, energia itd.). Takie podejście oznacza w praktyce znaczne rozszerzenie zarówno obowiązków wynikających z 5G Toolboxa, jak i z dyrektywy NIS 2 — niespotykane na arenie międzynarodowej. Polska jako jedyne państwo w Unii Europejskiej w projekcie implementacji Dyrektywy NIS 2 planuje wdrożyć 5G Toolbox, w tym regulacje dot. DWR. Równocześnie Polska jako jedyne państwo wprowadza możliwość wykluczenia sprzętu ze względu na państwo pochodzenia dostawcy łącznie z przyjęciem zasad implementacji dyrektywy NIS 2. Należy zwrócić uwagę, że o ile niektóre inne państwa członkowskie wprowadziły przepisy prawne regulujące zarówno procedurę uznania podmiotu jako DWR jak i skutki takiej klasyfikacji, Polski projekt jest wyjątkowy ze względu na swój szeroki zakres zastosowania — dotyczy wszystkich 18 sektorów wskazanych w dyrektywie NIS 2. Implementacja w swoim obecnym kształcie pozwalałaby na wykluczenie dowolnego dostawcy sprzętu, usługi czy programu ICT w dowolnym sektorze. Żaden inny kraj unijny nie wprowadził tak daleko idących w skutkach rozwiązań legislacyjnych. Jedynym państwem którego projekt zbliża się rozwiązaniami do polskiej propozycji implementacji są Niemcy. Jednakże nawet niemiecki projekt aktu implementującego NIS 2 ogranicza możliwość wykluczenia dostawców w 10 sektorów (nie tak	Wyjaśnienie uwagi Wszystkie podmioty kluczowe i podmioty ważne mają obowiązek dbania o bezpieczeństwo łańcuchów dostaw. Stąd też ujęcie instytucji dostawcy wysokiego ryzyka w projekcie ma swoje uzasadnienie.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			jak w Polsce — 18 sektorów), a dodatkowo nie uwzględnia w kryterium pochodzenia państw należących do NATO (odnosi się wyłącznie do EOG). Polska jako jedyne państwo w Unii Europejskiej w projekcie implementacji Dyrektywy NIS 2 planują wdrożyć 5G Toolbox, w tym regulacje dot. DWR. Równocześnie Polska jako jedyne państwo wprowadza możliwość wykluczenia sprzętu ze względu na państwo pochodzenia dostawcy łącznie z przyjęciem zasad implementacji dyrektywy NIS 2. Należy zwrócić uwagę, że o ile niektóre inne państwa członkowskie wprowadziły przepisy prawne regulujące zarówno procedurę Nie powinno dziwić, że polskie podejście w stosunku do szerokich kompetencji Ministra Cyfryzacji jest odosobnione. Polskie przepisy de facto nadają Ministrowi Cyfryzacji pełną władzę nad uznaniem jakiegokolwiek dostawcy działającego w Polsce za DWR. Takie działanie może wg. członków naruszać zasadę proporcjonalności.	
99.	SinoCham	Uwaga ogólna	W związku z publicznymi konsultacjami dotyczącymi projektu nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa, które trwają w związku z wprowadzaniem przez Polskę unijnej dyrektywy NIS2 oraz mając na uwadze jej szczególne znaczenie dla rynku, chcielibyśmy wyrazić nasze głębokie zaniepokojenie i przedstawić nasze opinie odnośnie do przewidywanych zmian. Niniejsze stanowisko poprzedza zgłoszenie kompleksowych uwag do projektu - niemniej ze względu na wagę poruszanych zagadnień, a także możliwość istotnego wpływu na polską gospodarkę, pozwalamy sobie już teraz zwrócić się do Pana Premiera. Nowe przepisy wprowadzają znaczące obciążenia dla przedsiębiorstw, przekraczając nawet wymagania dyrektywy NIS2. Chodzi tu o obowiązek przeprowadzania regularnych audytów bezpieczeństwa co dwa lata, a także o dodatkowe kontrole systemów informatycznych, które nie są wymagane przez dyrektywę. Te zmiany wprowadzają znaczne obciążenia finansowe dla firm, szacowane na kwoty od kilkudziesięciu tysięcy do nawet miliona złotych, co może negatywnie wpłynąć na ich konkurencyjność. Dodatkowo, planowane regulacje, szczególnie te dotyczące zakazu nabywania i konieczności usunięcia produktów, usług i procesów ICT od podmiotów uznanych za dostawców wysokiego ryzyka, wprowadzają znaczne ryzyko dla stabilności operacyjnej i finansowej firm w Polsce. Pragniemy podkreślić, że kryterium wyboru takich dostawców, oparte głównie na państwie pochodzenia, może być percepcyjnie niekorzystne dla międzynarodowych stosunków handlowych, w szczególności z krajami spoza UE i NATO, takimi jak Chiny, Indie, Korea Południowa, Izrael czy Tajwan. W imieniu naszych Członków prosimy o rozważenie wprowadzanych regulacji, uwzględnienie ich szerokiego wpływu na działalność gospodarczą oraz zbadanie alternatywnych metod, które mogłyby równoważyć potrzebę bezpieczeństwa z racjonalnym podejściem ekonomicznym. Zwracamy się także z prośbą o rozważenie bardziej elastycznego podejścia do implementacji dyrektywy NIS2, które uwzględniałoby specyfikę i skalę działalności poszczególnych przedsiębiorstw. Jako izba zrzeszająca przede wszystkim inwestorów zagranicznych, zwracamy się z prośbą o uwzględnienie naszej organizacji w procesie konsultacji publicznych i umożliwienie przedkładania stanowisk w ich toku. Z przykrością stwierdzamy, że pomimo faktu, iż nasza Izba zrzesza członków	Wyjaśnienie uwagi Dyrektywa NIS2 wskazuje na obowiązek przeprowadzania okresowych audytów dla podmiotów kluczowych. Jednocześnie dla podmiotów ważnych wymogi w tym zakresie zostaną złagodzone. Postępowanie w sprawie uznania za dostawcę wysokiego ryzyka ma zabezpieczyć polską gospodarkę przed dostawcą zagrażającym bezpieczeństwu narodowemu. Nie ma tutaj kryteriów narodowych.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			bezpośrednio podlegających pod przepisy projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw, zostaliśmy pominięci w zaproszeniu do konsultacji publicznych. O fakcie ich prowadzenia dowiedzieliśmy się ze znacznym opóźnieniem, co ogranicza możliwości naszych Członków do przeprowadzenia wnikliwej analizy i wypowiedzenia się przez wszystkich zainteresowanych co do konkretnych rozwiązań zawartych w projekcie nowelizacji. W związku z powyższym, zwracamy się z prośbą o uwzględnienie Izby w przyszłych konsultacjach dotyczących tej nowelizacji. Jednocześnie z uwagi na konieczność przeprowadzenia analizy dotyczącej wpływu proponowanej transpozycji na działalność naszych członków oraz przygotowania konstruktywnego stanowiska zwracamy się z wnioskiem o wydłużenie konsultacji o dodatkowy miesiąc. Wniosek o wydłużenie uzasadniony jest również nie przedstawieniem tabeli zgodności i odwróconej tabeli zgodności, które są wymagane w procesie legislacyjnym, co dodatkowo utrudnia nam ustosunkowanie się do treści projektu ustawy.	
100.	Związek Przedsiębiorców i Pracodawców	Uwaga ogólna (art. 8e, 53, 73a)	Zgodnie z dyrektywą NIS2, państwa członkowskie muszą zapewnić, że zarządy kluczowych i ważnych podmiotów zatwierdzają i nadzorują wdrażanie środków zarządzania ryzykiem cyberbezpieczeństwa, zgodnie z artykułem 21. Odpowiedzialność za naruszenia tego artykułu może spoczywać na tych organach. Polski projekt implementacji określa obowiązki zarządów oraz zasady dotyczące kar finansowych (artykuł 8c do 8e i artykuł 73a). Kara może być nałożona, jeśli zarząd nie spełni swoich obowiązków lub jeśli podmiot nie wypełni swoich obowiązków wynikających z implementacji NIS2. Kara nie może przekroczyć 600% wynagrodzenia ukaranej osoby. Te przepisy różnią się od zasad określonych w dyrektywie, ponieważ nie uwzględniają zdolności finansowej osoby karanej. Ponadto, artykuł 53 ust. 1 projektu daje władzom szersze uprawnienia egzekucyjne, w tym możliwość zawieszenia lub cofnięcia licencji, usunięcia z rejestru działalności, czasowego zakazu pełnienia funkcji przez zarząd oraz nakazu przeprowadzania audytów bezpieczeństwa. Rozszerzenie tych uprawnień może prowadzić do nadmiernej ingerencji w działalność podmiotów, co może destabilizować ich funkcjonowanie. Zalecamy ponowną analizę przepisów w celu znalezienia bardziej zrównoważonego rozwiązania, które zapewni bezpieczeństwo, minimalizując jednocześnie ryzyko nadmiernych obciążeń i zakłóceń.	Wyjaśnienie uwagi Projektodawca wskazuje, że projekt implementuje do porządku prawnego dyrektywę NIS 2, która określa środki nadzorcze oraz odpowiedzialność kierownika podmiotu. Jednocześnie projektodawca korzysta z tego, że dyrektywa obarczona jest harmonizacją minimalną, zatem może podejmować dodatkowe, adekwatne środki jeśli pozostają one w zgodzie z celem dyrektywy. Jednocześnie nieprawdą jest, że projekt nie uwzględnia zdolności finansowej osoby karanej (kierownika podmiotu) bowiem w art. 76a projektu w ust. 1 określono, że organ właściwy do spraw cyberbezpieczeństwa bierze pod uwagę możliwości finansowe kierownika podmiotu kluczowego lub podmiotu ważnego. Również nietrafny jest zarzut rozszerzenia kompetencji nadzorczych bowiem dyrektywa NIS2 zobowiązuje państwa do wyposażenia organów państwowych w kompetencje pozwalające na zawieszenie, cofnięcie licencji, koncesji, zezwoleń.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

101.	Związek Przedsiębiorców i Pracodawców	Uwaga ogólna	Dyrektywa NIS2 (art. 36) wymaga, aby państwa członkowskie ustanowiły skuteczne, proporcjonalne i odstraszające kary za naruszenia. Polski projekt implementacji (art. 73 ust. 1) określa kary finansowe dla kluczowych i ważnych podmiotów, podobnie jak dyrektywa, z wyjątkiem dwóch przypadków, gdzie możliwe są wyższe kary: do 100 000 000 PLN oraz od 500 PLN do 100 000 PLN za każdy dzień opóźnienia. W naszej opinii wysokie kary mogą być nieproporcjonalne do naruszeń, co może prowadzić do nadmiernej represji wobec podmiotów. Surowe kary za drobne uchybienia mogą nadmiernie obciążyć kluczowe i ważne podmioty. Dodatkowo, pragniemy podkreślić, że przyznanie organom prawa do nakładania wysokich kar oraz decydowania o zawieszeniu lub cofnięciu licencji stwarza ryzyko arbitralności i nadużycia władzy. Sugerujemy ponowne rozważenie wysokości kar oraz wprowadzenie mechanizmów zapewniających proporcjonalność i sprawiedliwość w egzekwowaniu przepisów.	Wyjaśnienie uwagi Projektodawca wskazuje, że w projekcie przewidziana została wysokość kar w oparciu o przepisy dyrektywy NIS 2. Także kryteria, na podstawie których organ właściwy do spraw cyberbezpieczeństwa będzie miarkował karę, zostały zaimplementowane z uwzględnieniem kryteriów wskazanych w dyrektywie NIS 2. W związku z tym projekt w tym zakresie jest zgodny z prawem unijnym.
102.	ISSA	Uwaga ogólna dot. sankcji	Sankcje w ustawie KSC – nieproporcjonalne i potencjalnie represyjne (art. 73, 74 ust. 2, 76b ustawy KSC) Ustawa KSC wprowadza system kar finansowych, które mogą osiągać wyjątkowo wysokie kwoty, znacznie przewyższające powszechne standardy. Według art. 73 tej ustawy, zgodnie z NIS2 maksymalna wysokość kary pieniężnej może wynieść do 10 milionów euro lub 2% rocznych przychodów podmiotu kluczowego, przy czym przyjęta jest zasada, że stosuje się wyższą z tych kwot. W przypadku nowo powstałych przedsiębiorstw lub takich, które nie osiągnęły przychodów, podstawa wymiaru kary wynosi równowartość 500 000 euro. Dla podmiotów ważnych maksymalna wysokość kary została określona na 7 milionów euro lub 1,4% rocznych przychodów, co również jest znaczącym obciążeniem finansowym. Dodatkowo, w przypadku szczególnie poważnych naruszeń zagrażających bezpieczeństwu publicznemu, życiu i zdrowiu ludzi lub powodujących poważne szkody majątkowe, możliwa jest kara do 100 milionów złotych. Co jednak istotne, wprowadzono także mechanizm okresowych kar pieniężnych w wysokości od 500 zł do 100 000 zł za każdy dzień opóźnienia w wykonaniu nałożonych obowiązków, co może stanowić znaczące obciążenie dla podmiotów które z różnych przyczyn nie są w stanie szybko dostosować się do wymagań ustawy. Standard dotyczący kar administracyjnych zaczyna się zwykle na poziomie 1000 zł (np. w przepisach dotyczących ochrony środowiska). Dotychczas ustawa o KSC przewidywała w art. 73 ust. 4 pułapy 1000, 5000 i 15000 zł. Dodatkowo brak jest mechanizmu odstąpienia od wymierzenia kary w uzasadnionych przypadkach, który jest znany przepisom dotyczącym zgodności wyrobów (np. sformułowany w przepisach dotyczących wyrobów budowlanych w formie obowiązku umorzenia postępowania). Tak wysokie sankcje, szczególnie w połączeniu z rygiorem natychmiastowej wykonalności, mogą mieć represyjny charakter i stawiać przedsiębiorstwa w sytuacji, w której muszą podejmować pośpieszne decyzje, potencjalnie niekorzystne z długoterminowego punktu widzenia. W efekcie może to prowadzić nie tylko do finansowych trudności, ale również do ograniczenia innowacyjności i rozwoju technologicznego w kraju. W przepisie art. 73a ust. 4 ustawy o KSC pojawiła się również nieścisłość – jest tam mowa o karze w wysokości do 600% otrzymywanego przez ukaranego wynagrodzenia obliczanego według zasad obowiązujących przy ustalaniu	Wyjaśnienie uwagi Przepisy z zakresu kar pieniężnych stanowią wdrożenie postanowień dyrektywy NIS 2. Jednocześnie projektodawca korzysta z uprawnienia państw członkowskich UE do wdrażania środków nieprzewidzianych w dyrektywie, które jednak pozostają w zgodzie z jej celem. Wynika to z harmonizacji minimalnej, którą objęte są dyrektywy. Obowiązkiem państw członkowskich jest zapewnienie, że kary będą proporcjonalne, odstraszające, a tym samym odpowiednio wysokie, aby zapewniały prawidłową realizację obowiązków. Zmiany w przepisach dotyczących kar pieniężnych wynikają także z analizy przepisów obecnie obowiązującej ustawy. W przedmiocie wynagrodzenia kierownika podmiotu wskazać należy, że podobne instytucje funkcjonują już w obrocie prawnym. Jednakże nie doprecyzowują okresu otrzymywanego wynagrodzenia. W ocenie projektodawcy nie zachodzi potrzeba dookreślenia tego

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			ekwiwalentu pieniężnego za urlop. Nie określono okresu, którego ma dotyczyć wynagrodzenie przyjęte za podstawę wyliczenia kary	w przepisie – organ będzie brał pod uwagę wynagrodzenie otrzymywane obecnie, które zostanie ustalone na podstawie dokumentacji przekazanej przez kierownika podmiotu.
103.	KIKE	Uwaga ogólna	Środki odpowiednie i proporcjonalne – rekomendacje i kontrole Jak już wskazano, zarówno Prawo przedsiębiorców jak i dyrektywa NIS2 nakazują, aby obowiązki nałożone na przedsiębiorców telekomunikacyjnych miały charakter proporcjonalny i aby były adekwatne (odpowiednie) do celów/zadań. Tymczasem, poza ogólną formułą w art. 8 ust. 1 uKSC w całym projekcie brak jest potwierdzenia tych zasad przy nakładaniu obowiązków na podmioty kluczowe czy ważne. Przykładowo, zarówno rekomendacje z art. 33 uKSC (będące później podstawą decyzji o dostawcy wysokiego ryzyka) czy zalecenia pokontrolne z art. 59 uKSC w ogólnie nie odnoszą się do zasad proporcjonalności i adekwatności. Na podstawie tych przepisów organy mogą narzucić (w trybie nie podlegającym kontroli sądowej!) podmiotom kluczowym i podmiotom ważnym obowiązki wykraczające poza adekwatność i proporcjonalność. Przykładem takiego narzucania podejmowania działań jest art. 32 ust. 2 i art. 11 ust. 1 pkt 6 uKSC w zakresie likwidacji stwierdzanych podatności. Uprawnienia organów w tym zakresie nie są niczym ograniczone w kontekście proporcjonalności i adekwatności. Co więcej, obowiązek usuwania podatności powinien spoczywać na tym, kto taką podatność wygenerował, czyli dostawca sprzętu lub oprogramowania, a nie na przedsiębiorcy komunikacji elektronicznej. Ponadto działania te mają w stosunku do podmiotów ważnych charakter działań prewencyjnych co nie powinno mieć miejsca. Izba postuluje ograniczenie tych dwóch regulacji do podmiotów kluczowych. Wskazuję przy tym na brak kontroli sądowej tych działań organów. Dodatkowo Izba postuluje, aby zalecenia pokontrolne podlegały trybowi odwoławczemu do sądu administracyjnego. Z tego względu powinny one mieć sformalizowany charakter postanowień administracyjnych podlegających odwołaniu do sądu wojewódzkiego. Doświadczenia członków Izby z analogiczną luką prawną w regulacjach telekomunikacyjnych wskazuje, że zalecenia pokontrolne umożliwiają (pod rygorem natychmiastowej kary finansowej) nakładanie nowych obowiązków z pominięciem przepisów. Z kolei sądy w przypadku odwołań od nałożenia kary finansowej wynikających z niewykonania zaleceń pokontrolnych nie badają legalności samych zaleceń a jedynie fakt ich niewykonania. zDodatkowym problemem przy zaleceniach pokontrolnych jest możliwość nadania rygoru natychmiastowej wykonalności decyzji nakładającej karę finansową za niewykonanie zaleceń pokontrolnych. Taka konstrukcja prawna oznacza, że każdy przedsiębiorca telekomunikacyjny, nawet jeśli nie będzie zgadzał się z proporcjonalnością i adekwatnością nakazów w zaleceniu pokontrolnym, będzie je wykonywał w obawie przed karą finansową. Z tego względu Izba postuluje, aby wprowadzić zapis do art. 74 ust. 2 uKSC, że decyzje o nałożeniu kary finansowej nie mogą posiadać rygoru natychmiastowej wykonalności. W takiej sytuacji wystarczającą dolegliwością dla podmiotu stwarzającego zagrożenie dla Krajowego Systemu Cyberbezpieczeństwa	Wyjaśnienie uwagi Obowiązek usuwania podatności funkcjonuje już od kilku lat w KSC. Z uwagi na charakter zaleceń pokontrolnych nie przysługuje od nich odwołanie do sądu. W przypadku nałożenia kary za niewykonanie zaleceń podmiot może złożyć skargę do WSA. Doszczegółowienie wymagań SZBI w drodze rozporządzenia odpowiada na te głosy, które mówią, że wymogi NIS2 są zbyt ogólne – rozporządzenie będzie je konkretyzowało, żeby dać wskazówkę podmiotom kluczowym i podmiotom ważnym. Polecenie zabezpieczające ma być adekwatne do zidentyfikowanych ryzyk – aspekt proporcjonalności został tu uwzględniony.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			powinno być zagrożenie wykreśleniem z rejestru prowadzenia działalności gospodarczej. Nadanie karze finansowej rygoru natychmiastowej wykonalności ogranicza podmiotom uprawnienia do kontroli sądowej decyzji organów. ZIzba wskazuje również, że czynności z art. 53 uKSC w zakresie wykreślenia podmiotu z rejestrów działalności gospodarczej powinny być czynnościami, od których przysługuje odwołanie do sądu administracyjnego. Jest to bowiem czynność władcza organu państwowego mająca doniosłe skutki dla podmiotu gospodarczego i powinna podlegać kontroli sądowej. Co więcej, sama „decyzja o wykreśleniu” (a właściwie to powinno być postanowienie administracyjne) powinno podlegać analizie pod kątem adekwatności i proporcjonalności tego środków. Obecna propozycja sugeruje, że organ ds. cyberbezpieczeństwa ma pełną uznaniowość w zakresie zwrócenia się do właściwego organu o wykreślenie z rejestru prowadzenia działalności gospodarczej, a organ ten ma się do tego żądania zastosować. Zdaniem Izby, jeżeli wykreślenie z rejestru działalności gospodarczej nie będzie poddane kontroli sądowej należy usunąć z Projektu tę kompetencję. ZIzba jednocześnie postuluje zmodyfikowanie art. 8a uKSC stanowiącego delegację ustawową do określania wymogów systemu zarządzania informacją, tak aby nie kolidował on z art. 8 uKSC gdzie podmiot sam decyduje o wdrażanych środkach biorąc pod uwagę ich adekwatność i proporcjonalność. W tej sytuacji przepis ten powinien raczej stanowić rekomendację niż obowiązek. ZDuże wątpliwości w kontekście stosowania zasad adekwatności i proporcjonalności budzi mechanizm poleceń zabezpieczających z art. 67g uKSC. Zdaniem Izby, z uwagi na jego wyjątkowość, powinien o być stosowany wyłącznie w stosunku do podmiotów kluczowych a nie ważnych. Jest to tym istotniejsze, że nadzór nad podmiotami ważnymi ma się opierać na zasadach następczych, co nie powinno mieć zastosowania do poleceń zabezpieczających. Co więcej, wydawane polecenie powinno opierać się na zasadach proporcjonalności nakazanego środka do incydentu oraz rozmiaru incydentu (zasięg krajowy a nie lokalny). Z tego samego powodu w przypadku podmiotów ważnych ewentualne polecenie zabezpieczające powinno trwać jedynie do czasu likwidacji incydentu, a nie na z góry określony czas (co sugeruje nadzór prewencyjny).	
104.	Osoba fizyczna	Uwaga ogólna	Zapisy ustawy uKSC2 w wielu miejscach są niespójne i niekonsekwentne w określaniu, co jest podstawowym przedmiotem regulacji, a co jest tego rozszerzeniem. Jako podstawowy przedmiot regulacji należy przyjąć i konsekwentnie stosować system informacyjny, który jest odpowiednikiem (zamiennikiem) przedmiotu NIS2 – sieci i systemów informatycznych. Regulacja powinna przede wszystkim definiować wszelkie kwestie bezpieczeństwa systemu informacyjnego i zarządzania bezpieczeństwem tegoż systemu, w tym obsługi incydentów w systemie informacyjnym. Jako rozszerzenie zakresu należy przyjąć i konsekwentnie stosować usługę podmiotu, na której ciągłość, stabilność i jakość wpływa bezpieczeństwo, ciągłość, stabilność i jakość systemu informacyjnego oraz na którą mają wpływ skutki incydentu w systemie informacyjnym. Usługa jest i powinna być wskazywana jako obszar skutków oddziaływania bezpieczeństwa, ciągłości, stabilności i jakości systemu informacyjnego oraz jego zakłóceń i incydentów. Całe skupienie regulacji powinno być na warstwie systemu informacyjnego.	Wyjaśnienie uwagi Projekt posługuje się pojęciami ustalonymi w dyrektywie NIS2 w związku z czym krajowy ustawodawca nie może zmieniać relacji między nimi.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

105.	Osoba fizyczna	Uwaga ogólna	Kwestia bezpieczeństwa usług podmiotów, szczególnie usług kluczowych dla krytycznej działalności społecznej i gospodarczej i bezpieczeństwa państwa, realizowanych z wykorzystaniem infrastruktury (krytycznej) przez podmioty określone operatorami infrastruktury krytycznej jest w jurysdykcji organów zarządzania kryzysowego i ustawy o zarządzaniu kryzysowym. Proponuję, aby kwestie bezpieczeństwa, ciągłości, stabilności i jakości pozostałych, nie krytycznych, usług ważnych, istotnych dla państwa, odpowiadających sektorom, podsektorom i rodzajom działalności podmiotów wskazanych w załącznikach 1 i 2 NIS2/uKSC2 zostały zaadresowane w znowelizowanej ustawie o zarządzaniu kryzysowym, implementującej CER i zapewniającej integrację regulacji NIS2-CER oraz uKSC2-uZK.	Uwaga nieuwzględniona Proponowane rozwiązanie jest niezgodne z dyrektywą NIS2. Cyberbezpieczeństwo i zarządzanie kryzysowe są pokrewnymi dziedzinami co zauważył ustawodawca europejski przygotowując równoległe dyrektywy NIS2 i CER. Równocześnie jednak oba te akty prawne mają różne zakresy podmiotowe. Dlatego obowiązki z tych dwóch dyrektyw muszą być przygotowane odrębnie tak aby precyzyjnie odnosiły się do tych podmiotów, które mają stosować dane przepisy.
106.	Osoba fizyczna	Uwaga ogólna	Proponuję, aby zapisy dotyczące usług i wszelkich wymaganych dla nich działań i ich bezpieczeństwa oraz dotyczące systemów informacyjnych oraz wszelkich wymaganych dla nich działań i ich bezpieczeństwa zawsze były lokowane w odrębnych artykułach, aby zapewnić jednoznaczność zapisów stawianych wymagań. Aktualny układ treści, niestety, zawiera pomieszczone treści adresowane do usług i systemów informacyjnych, co sprawia ogromne trudności interpretacyjne i implementacyjne.	Wyjaśnienie uwagi Każda odrębna treść jest lokowana w odrębnym artykule.
107.	Sudecka Izba Przemysłowo – Handlowa w Świdnicy	Uwaga ogólna	Po analizie projektu ustawy uważamy, że zbędne są regulacje rozszerzające uprawnienia organu właściwego wobec podmiotów kluczowych i ważnych. W naszej ocenie zakres uprawnień organów właściwych w dyrektywie był wystarczający i nie ma potrzeby rozszerzać uprawnień dotyczących usuwania podatności, poleceń zabezpieczających czy eliminacji możliwości odwołania się od zaleceń pokontrolnych.	Uwaga nieuwzględniona W ocenie projektodawcy uwaga ma charakter ogólny i nie wskazuje proponowanych rozwiązań. Należy zwrócić uwagę na to, że projektowane przepisy wdrażają do porządku krajowego przepisy dyrektywy i na niej bazują. Zgodnie jednak z zasadą harmonizacji minimalnej państwa członkowskie uprawnione są do wdrożenia przepisów, których dyrektywa nie przewiduje, a które pozwolą na realizację celu dyrektywy. Tym samym projektodawca uwzględniając specyfikę krajową dąży do zapewnienia odpowiednich i skutecznych środków nadzoru i egzekwowania przepisów. Projektowane regulacje realizują to założenie.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

108.	Stowarzyszenie Inżynierów Telekomunikacji	Uwaga ogólna	Stowarzyszenie Inżynierów Telekomunikacji, w związku z zaproszeniem do przedstawienia stanowiska w konsultacjach publicznych projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw, przedstawia poniżej uwagi dotyczące tej kluczowej dla rynku telekomunikacyjnego i polskiej gospodarki projektu. Uwagi szczegółowe: W toku prac nad poprzednimi wersjami projektu nowelizacji ustawy, w wyniku debat ze środowiskiem osiągnięto kompromis dotyczący uregulowanego w projekcie ustawy (art. 67c ust. 2 projektu) tj. terminu dla przedsiębiorców telekomunikacyjnych na wycofanie z ich sieci określonych produktów, usług oraz procesów ICT tzw. dostawców wysokiego ryzyka (dostawców HRV). Proponowany przez nas termin 7 lat wynika z aspektów praktycznych związanych z wyminą sprzętu i zmianami w sieci skutkującymi wpływem na dostępność usług dla abonentów. W ocenie Stowarzyszenia Inżynierów Telekomunikacji przyjęty w projekcie ustawy termin 4 lat na wycofanie z sieci przez przedsiębiorców telekomunikacyjnych produktów dostawcy uznanego w drodze decyzji za dostawcę wysokiego ryzyka: w- może być niemożliwy do dotrzymania z punktu widzenia logistyki przeprowadzenia całego procesu i takich czynników jak chociażby dostępność niezbędnych ekip podwykonawców oraz sam koszt całego procesu. Zwracamy uwagę, że w przypadku wydania decyzji HRV proces usunięcia może dotyczyć wielu przedsiębiorców telekomunikacyjnych w jednym czasie. Stawia to pod poważnym znakiem zapytania możliwość przeprowadzenia takiego procesu zarówno z punktu widzenia jego logistyki jak i potężnych kosztów finansowych dla poszczególnych przedsiębiorców telekomunikacyjnych i łącznie całego rynku telekomunikacyjnego; u- z pewnością rzutuje na koszt świadczenia usług telekomunikacyjnych, a tym samym rodzi ryzyko wzrostu cen usług telekomunikacyjnych dla wszystkich użytkowników końcowych w Polsce. Analiza projektu ustawy wskazuje, że nie przewidziano w nim jakichkolwiek mechanizmów związanych z pokryciem kosztów przedsiębiorców telekomunikacyjnych przeprowadzenia tak rozległego procesu jakim byłoby usunięcie z sieci telekomunikacyjnych sprzętu pochodzącego od podmiotu uznanego za dostawcę wysokiego ryzyka; y- rodzi istotne ryzyko po stronie zachowania ciągłości i interoperacyjności świadczonych usług telekomunikacyjnych. W tym kontekście zwracamy m.in. uwagę, że w zakresie sieci 5G w Polsce jesteśmy na etapie jej realizacji w modelu 5G NSA (Non Stand Alone). Oznacza to, że dla świadczenia usług w oparciu o infrastrukturę sieci 5G niezbędne są określone komponenty już istniejącej infrastruktury 4G stanowiące tzw. „kotwicę” (anchor). Tym samym ewentualny obowiązek usunięcia z sieci poszczególnych komponentów związanych z siecią 5G będzie miał swoje przełożenie na znacznie szersze obszary sieci telekomunikacyjnych, czego projektodawca przepisów zdaje się nie dostrzegać; y- rodzi istotne ryzyko po stronie zachowania ciągłości i interoperacyjności świadczonych usług telekomunikacyjnych. W tym kontekście zwracamy m.in. uwagę, że w zakresie sieci 5G w Polsce jesteśmy na etapie jej realizacji w modelu 5G NSA (Non Stand Alone). Oznacza to, że dla świadczenia usług w oparciu o infrastrukturę sieci 5G niezbędne są określone komponenty już istniejącej infrastruktury 4G stanowiące tzw. „kotwicę” (anchor). Tym- jest wyrazem niezrozumiałej i faktycznie niewyjaśnionej na poziomie projektu	Uwaga nieuwzględniona Z uwagi na krytyczność funkcji zasadne jest pozostawienie 4 letniego terminu na wycofanie.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			ustawy (w tym jego uzasadnienia) dyskryminacji sektora telekomunikacyjnego (przedsiębiorców telekomunikacyjnych) w stosunku do podmiotów z innych sektorów. Jako przedstawiciele środowiska telekomunikacyjnego zdecydowanie protestujemy przeciwko takiemu podejściu. W związku z powyższym Stowarzyszenie Inżynierów Telekomunikacji apeluje o zmianę przyjętego w projekcie ustawy rozwiązania poprzez ustalenie dla przedsiębiorców telekomunikacyjnych takiego samego terminu jak dla innych podmiotów (tj. 7 lat) na wycofanie ze swoich sieci komponentów wskazanych w decyzji w sprawie uznania za dostawcę wysokiego ryzyka, względnie przynajmniej powrót do proponowanego w poprzedniej wersji projektu ustawy terminu 5 lat, który i tak jest terminem ambitnym, ale z pewnością bardziej realnym niż termin 4 lat.	
109.	Stowarzyszenie Inżynierów Telekomunikacji	Uwaga ogólna	W opinii Stowarzyszenia Inżynierów Telekomunikacji projekt wykracza poza wymagania dyktowane dyrektywą NIS 2. Implementuje obowiązki dla przedsiębiorców ponad wymagania wynikające z dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniającą rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającą dyrektywę (UE) 2016/1148 (NIS 2). Dokonuje wdrożenia postanowień NIS 2 w szerszym zakresie niż wymagają tego postanowienia tej dyrektywy. W konsekwencji nowymi regulacjami zostanie objęta w Polsce największa liczba podmiotów wśród wszystkich krajów UE które dotychczas dokonały wdrożenia NIS2.	Wyjaśnienie uwagi Część wymagania zostanie złagodzona. Ponadto należy podkreślić, że liczba podmiotów jest zwiększona o liczbę podmiotów publicznych.
110.	Stowarzyszenie Inżynierów Telekomunikacji	Uwaga ogólna	Brak Oceny Skutków Regulacji. W Ocenie Skutków Regulacji (OSR) nie przeprowadzono żadnych analiz dotyczących organizacyjnych i finansowych skutków wprowadzenia nowych obowiązków w Projekcie. Na stronie nr 30 OSR projektodawca stwierdza, iż „nie jest możliwe oszacowanie kosztów dostosowania się przedsiębiorców do wymogów określonych w nowelizacji”, pomimo że z pewnością nowe regulacje będą generowały dodatkowe koszty dla przedsiębiorców, co jest wprost przyznane na s. 28 OSR. Koszty te nie zostały więc ocenione, w szczególności nie została poddana ocenie ich wysokość pod kątem zasady proporcjonalności. OSR powinno więc zostać uzupełnione, dla każdego z sektorów, o analizę kosztów organizacyjnych i finansowych, jakie powstaną w związku z wprowadzeniem przewidzianych w projekcie obowiązków.	Wyjaśnienie uwagi Bardzo trudno jest oszacować koszty wdrożenia z u wagi na brak danych, różnorodność podmiotów, ich usług, czy wielkość.
111.	Stowarzyszenie Inżynierów Telekomunikacji	Uwaga ogólna	Ponadto, w odniesieniu do przedstawionych powyżej uwag szczegółowych, decyzja w sprawie dostawcy wysokiego ryzyka podejmowana przez ministra właściwego do spraw informatyzacji powinna być podejmowana we współpracy z innymi ministrami. Z uwagi na wpływ tej decyzji na stosunki międzynarodowe z innymi państwami lub bezpieczeństwo wewnętrzne oraz skomplikowany charakter prawny, powinny uczestniczyć w jej podejmowaniu także inni ministrowie odpowiedzialni za obszary istotne z perspektywy chronionych wartości (obronność, bezpieczeństwo i porządek publiczny, zdrowie i życie ludzi) lub za obszary właściwe merytorycznie z perspektywy sektora, którego dotyczy decyzja (rozwój i technologia). Pozytywną opinię powinien wyrazić także Prezes Urzędu Ochrony Konkurencji i Konsumentów.	Wyjaśnienie uwagi Przed podjęciem decyzji o uznaniu dostawcy za dostawcę wysokiego ryzyka minister właściwy do spraw informatyzacji zasięgnie opinii Kolegium do Spraw Cyberbezpieczeństwa, w którym zasiadają kluczowi ministrowie odpowiedzialni za bezpieczeństwo państwa. W przygotowaniu opinii weźmie też udział Prezes UOKiK.
112.	Stowarzyszenie Inżynierów	Uwaga ogólna	Przedłużenie okresu konsultacji. Z racji implementacji w projekcie dyrektywy NIS2, apelujemy także o wydłużenie okresu na konsultacje do 2 miesięcy. Obecnie termin 30 dni na konsultacje dla projektu,	Wyjaśnienie uwagi

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

	Telekomunikacji		który dotyczy również branż, które nie były objęte dotychczas zakresem poprzednich projektów ustawy, jest zbyt krótki, by uwzględnić uwagi wszystkich podmiotów objętych regulacją. Celowym również wydaje się, wobec zakresu projektowanych regulacji, zorganizowanie konferencji uzgodnieniowej, aby wyjaśnić potencjalnie budzące kontrowersje kwestie oraz zgłoszone w toku konsultacji uwagi.	Jest to standardowy termin na konsultacje projektu ustawy.
113.	SNW sp. Z o.o.	Uwaga ogólna	Projekt ustawy wprowadza bardzo szerokie regulacje, które dotkną blisko 40 tysięcy podmiotów z 18 sektorów, w tym firmy zatrudniające co najmniej 50 osób lub mające 10 mln euro rocznego przychodu. Dla wielu przedsiębiorstw, zwłaszcza małych i średnich, koszty dostosowania się do nowych przepisów będą ogromne. Niespełnienie wymogów oznacza wielomilionowe kary, co stanowi olbrzymie obciążenie finansowe. Nasza firma, podobnie jak wiele innych, obawia się, że konieczność nagłego wprowadzenia technologicznych zabezpieczeń doprowadzi do wzrostu cen usług związanych z cyberbezpieczeństwem oraz braku specjalistów w tej dziedzinie. Proponowane zmiany w ustawie wprowadzają nadmierne regulacje na sektory, które nie muszą podlegać tak rygorystycznym przepisom, zgodnie z Dyrektywą NIS2. Nadregulacja prowadzi do nieuzasadnionych kosztów i obciążeń administracyjnych dla firm takich jak nasza. Polskie przedsiębiorstwa będą zmuszone do ponoszenia dodatkowych kosztów związanych z przestrzeganiem nowych przepisów, co może negatywnie wpłynąć na ich konkurencyjność na rynku. Problemy z procedurą uznania dostawcy za wysokiego ryzyka Proponowane przepisy zakładają wykluczanie dostawców na podstawie kryteriów politycznych i subiektywnych ocen, co jest bardzo problematyczne. Uważamy, że wykluczenie powinno dotyczyć konkretnych rozwiązań technologicznych, a nie całych dostawców. Decyzje te powinny opierać się na rzetelnych badaniach technicznych i certyfikacji, a nie na dowolnych kryteriach i niejawnych opiniach Kolegium ds. Cyberbezpieczeństwa. Takie podejście zapewniłoby bardziej wyważone i sprawiedliwe rozwiązania, które nie prowadziłyby do nieuzasadnionych strat finansowych i destabilizacji rynku. Proponujemy wprowadzenie mechanizmów certyfikacji opartych na obiektywnych kryteriach technicznych, co pozwoli na wykluczanie tylko tych rozwiązań, które rzeczywiście stanowią zagrożenie dla cyberbezpieczeństwa. Analiza zagrożeń, takich jak bezpieczeństwo narodowe czy kontrola przez państwa spoza UE lub NATO, jest skomplikowana i subiektywna. Takie podejście może prowadzić do wykluczeń na podstawie domniemań i podejrzeń, co nie jest sprawiedliwe. Zamiast tego, proponujemy wprowadzenie obiektywnych kryteriów merytorycznych i mechanizmów certyfikacji. Proponowane przepisy zakładają wykluczanie dostawców na podstawie kryteriów politycznych i subiektywnych ocen, co jest bardzo problematyczne. Uważamy, że wykluczenie powinno dotyczyć konkretnych rozwiązań technologicznych, a nie całych dostawców. Decyzje te powinny opierać się na rzetelnych badaniach technicznych i certyfikacji, a nie na dowolnych kryteriach i niejawnych opiniach Kolegium ds. Cyberbezpieczeństwa. Takie podejście zapewniłoby bardziej wyważone i sprawiedliwe rozwiązania, które nie prowadziłyby do nieuzasadnionych strat finansowych. Proponujemy wprowadzenie mechanizmów certyfikacji opartych na obiektywnych kryteriach technicznych, co pozwoli na	Wyjaśnienie uwagi Oparcie identyfikacji niebezpiecznego sprzętu w oparciu o certyfikację sprzętu może być niewystarczające. Nie można wtedy zidentyfikować wszystkich zagrożeń związanych z dostawcą. Poza tym certyfikowany będzie konkretny sprzęt/oprogramowanie, a dostawca wysokiego ryzyka może dalej działać i oferować sprzęt/oprogramowanie w nowszych wersjach z ukrytymi podatnościami.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			wykluczanie tylko tych rozwiązań, które rzeczywiście stanowią zagrożenie dla cyberbezpieczeństwa. Dodatkowo warto byłoby oprzeć się na skoordynowanych ocenach ryzyka – tak aby uwzględnić jednolite podejście na obszarze całej Unii Europejskiej. Brak Oceny Skutków Regulacji (OSR) Niestety, OSR nie zawiera analizy kosztów wdrożenia tych obowiązków. Bez rzetelnych danych nie można oszacować, jakie będą długoterminowe skutki finansowe i operacyjne. Apelujemy o sporządzenie rzetelnej Oceny Skutków Regulacji, która pomoże ocenić, które obowiązki są rzeczywiście konieczne, a które zbyt kosztowne w stosunku do spodziewanych korzyści. Podsumowanie Prosimy o ponowne przemyślenie proponowanych zmian. Apelujemy o przeprowadzenie rzetelnej Oceny Skutków Regulacji, eliminację dyskryminacyjnych kryteriów wykluczających oraz zapewnienie pełnej transparentności i możliwości odwoławczych w procesie decyzyjnym. Nadmierne i dyskryminacyjne przepisy mogą mieć negatywne konsekwencje dla całej gospodarki. Proponujemy, aby przepisy dotyczące wykluczania dostawców były oparte na obiektywnych kryteriach technicznych i certyfikacji, co zapewni uczciwe i efektywne rozwiązania, które nie będą nadmiernie obciążać polskich przedsiębiorstw.	
114.	Stowarzyszenie Absolwentów Studiów Cyberbezpieczeństwa MBA	Uwaga ogólna	Rozważyć należy wprowadzenie do Ustawy o krajowym systemie cyberbezpieczeństwa lub do ustawy – Prawo zamówień publicznych odrębnej fakultatywnej podstawy wykluczenia wykonawcy zamówienia publicznego, po stwierdzeniu przez właściwy organ celowego jego działania prowadzącego do naruszenia dostępności, poufności, spójności bądź ciągłości działania urzędu technicznego eksploatowanego przez podmiot kluczowy lub podmiot ważny. Ewentualnie wprowadzenie podstawy do wydania zawiadomienia wykluczającego produkty lub usługi danego wykonawcy z ofert akceptowanych w ramach postępowań o udzielenie zamówienia publicznego, po stwierdzeniu spowodowania przez ten podmiot zagrożenia cyberbezpieczeństwa.	Wyjaśnienie uwagi Obecny katalog wyłączeń wykonawcy w ustawie – Prawo zamówień publicznych jest ściśle regulowany przez dyrektywy unijne i bardzo trudno jest od niego odstąpić.
115.	Stowarzyszenie Absolwentów Studiów Cyberbezpieczeństwa MBA	Uwaga ogólna	Zasadne jest przywrócenie przepisów dotyczących ISAC, projektowanych w poprzednich wersjach aktu mające na celu regulację struktur typu ISAC, w tym realizowanych w ramach grup kapitałowych. Obecne formuły współpracy tego typu realizowane są w ramach umów co w praktyce utrudnia poziomą współpracę pomiędzy poszczególnymi podmiotami w ramach grupy.	Wyjaśnienie uwagi Projekt odwołuje się do obecnej praktyki, w której podmioty tworzą ISAC w drodze porozumień.
116.	Stowarzyszenie Absolwentów Studiów Cyberbezpieczeństwa MBA	Uwaga ogólna	Zasadne jest objęcie przez CSIRT GOV aktywnej roli CSIRT sektorowego oraz wejście w rolę ISAC dla infrastruktury krytycznej, albo powołanie takiego ciała. Celem jest promowanie bezpośredniej współpracy i wymiany informacji pomiędzy podmiotami infrastruktury krytycznej, w obecnej chwili wymiana informacji zachodzi jedynie pomiędzy podmiotami i CSIRT GOV bez współpracy poziomej.	Wyjaśnienie uwagi Uwaga nie dotyczy Ministra Cyfryzacji.
117.	Stowarzyszenie Absolwentów Studiów Cyberbezpieczeństwa MBA	Uwaga ogólna	Należy do Ustawy o krajowym systemie cyberbezpieczeństwa wprowadzić obowiązek publikowania rocznego raportu z danymi statystycznymi dotyczącymi liczby i klasyfikacji incydentów obsługiwanych przez wszystkie zespoły CSIRT, poziomowi krajowego włącznie. Za informację publiczną powinny zostać uznane dane statystyczne niestanowiące informacji niejawnych, za to umożliwiające wszystkim podmiotom, w tym osobom fizycznym, a nie tylko wyspecjalizowanym organom Państwa	Uwaga uwzględniona

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			analizę trendów w zakresie cyberbezpieczeństwa. Informacje w tym zakresie mogłyby być uzyskane również na bieżąco, w trybie dostępu do informacji publicznej, na podstawie wniosku do Pełnomocnika Rządu ds. Cyberbezpieczeństwa.	
118.	Stowarzyszenie Absolwentów Studiów Cyberbezpieczeństwa MBA	Uwaga ogólna	Brak spójności z projektem ustawy – Prawo Komunikacji Elektronicznej Projekt nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa wykazuje brak spójności terminologicznej z równolegle procedowaną ustawą – Prawo komunikacji elektronicznej. Wskazane jest zachowanie spójności terminologicznej w ramach procedowanych dwóch aktów normatywnych. Ta niespójność terminologiczna może prowadzić do poważnych problemów interpretacyjnych, które z kolei wpłyną na efektywność i skuteczność stosowania przepisów nowelizacji. Proponuję przeprowadzenie rewizji terminologicznej projektu nowelizacji w celu zapewnienia jego zgodności z aktualnym stanem prawnym i uniknięcia przyszłych problemów implementacyjnych.	Wyjaśnienie uwagi Będziemy dążyć do uspoźnienia obydwu projektów.
119.	Verita HR Polska sp. z o.o.	Uwaga ogólna	Jako podmiot oferujący usługi outsourcingowe w zakresie IT i telekomunikacji, jesteśmy poważnie zaniepokojeni proponowanymi zmianami w ustawie o krajowym systemie cyberbezpieczeństwa. Bezpośrednie obowiązki wynikające z dyrektywy NIS2 mogą nas bezpośrednio nie dotyczyć, planowane przepisy dotyczące wykluczenia dostawców spoza UE i NATO istotnie i negatywnie wpłyną na konkurencyjność polskich firm w całej UE. Projekt ustawy wprowadza bardzo szerokie regulacje, które dotkną blisko 40 tysięcy podmiotów z 18 sektorów, w tym firmy zatrudniające co najmniej 50 osób lub mające 10 mln euro rocznego przychodu. Dla wielu przedsiębiorstw, zwłaszcza małych i średnich, koszty dostosowania się do nowych przepisów będą ogromne. Niespełnienie wymogów oznacza wielomilionowe kary, co stanowi olbrzymie obciążenie finansowe. Nasza firma, podobnie jak wiele innych, obawia się, że konieczność nagłego wprowadzenia technologicznych zabezpieczeń doprowadzi do wzrostu cen usług związanych z cyberbezpieczeństwem oraz braków specjalistów w tej dziedzinie. Proponowane zmiany w ustawie wprowadzają nadmierne regulacje na sektory, które nie muszą podlegać tak rygorystycznym przepisom, zgodnie z Dyrektywą NIS2. Nadregulacja prowadzi do nieuzasadnionych kosztów i obciążeń administracyjnych dla firm takich jak nasza. Polskie przedsiębiorstwa będą zmuszone do ponoszenia dodatkowych kosztów związanych z przestrzeganiem nowych przepisów, co może negatywnie wpłynąć na ich konkurencyjność na rynku. Problemy z procedurą uznania dostawcy za wysokiego ryzyka. Proponowane przepisy zakładają wykluczanie dostawców na podstawie kryteriów politycznych i subiektywnych ocen, co jest bardzo problematyczne. Uważamy, że wykluczenie powinno dotyczyć konkretnych rozwiązań technologicznych, a nie całych dostawców. Decyzje te powinny opierać się na rzetelnych badaniach technicznych i certyfikacji, a nie na dowolnych kryteriach i niejawnych opiniach Kolegium ds. Cyberbezpieczeństwa. Takie podejście zapewniłoby bardziej wyważone i sprawiedliwe rozwiązania, które nie prowadziłyby do nieuzasadnionych strat finansowych i destabilizacji rynku. Proponujemy wprowadzenie mechanizmów certyfikacji opartych na	Wyjaśnienie uwagi Bardzo trudno jest oszacować koszty wdrożenia z uwagi na brak danych, różnorodność podmiotów, ich usług czy wielkość.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			obiektywnych kryteriach technicznych, co pozwoli na wykluczanie tylko tych rozwiązań, które rzeczywiście stanowią zagrożenie dla cyberbezpieczeństwa. Analiza zagrożeń, takich jak bezpieczeństwo narodowe czy kontrola przez państwa spoza UE lub NATO, jest skomplikowana i subiektywna. Takie podejście może prowadzić do wykluczeń na podstawie domniemań i podejrzeń, co nie jest sprawiedliwe. Zamiast tego, proponujemy wprowadzenie obiektywnych kryteriów merytorycznych i mechanizmów certyfikacji. Proponowane przepisy zakładają wykluczanie dostawców na podstawie kryteriów politycznych i subiektywnych ocen, co jest bardzo problematyczne. Uważamy, że wykluczenie powinno dotyczyć konkretnych rozwiązań technologicznych, a nie całych dostawców. Decyzje te powinny opierać się na rzetelnych badaniach technicznych i certyfikacji, a nie na dowolnych kryteriach i niejawnych opiniach Kolegium ds. Cyberbezpieczeństwa. Takie podejście zapewniłoby bardziej wyważone i sprawiedliwe rozwiązania, które nie prowadziłyby do nieuzasadnionych strat finansowych. Proponujemy wprowadzenie mechanizmów certyfikacji opartych na obiektywnych kryteriach technicznych, co pozwoli na wykluczanie tylko tych rozwiązań, które rzeczywiście stanowią zagrożenie dla cyberbezpieczeństwa. Dodatkowo warto byłoby oprzeć się na skoordynowanych ocenach ryzyka – tak aby uwzględnić jednolite podejście na obszarze całej Unii Europejskiej. Brak Oceny Skutków Regulacji (OSR). Niestety, OSR nie zawiera analizy kosztów wdrożenia tych obowiązków. Bez rzetelnych danych nie można oszacować, jakie będą długoterminowe skutki finansowe i operacyjne. Apelujemy o sporządzenie rzetelnej Oceny Skutków Regulacji, która pomoże ocenić, które obowiązki są rzeczywiście konieczne, a które zbyt kosztowne w stosunku do spodziewanych korzyści. Podsumowanie Prosimy o ponowne przemyślenie proponowanych zmian. Apelujemy o przeprowadzenie rzetelnej Oceny Skutków Regulacji, eliminację dyskryminacyjnych kryteriów wykluczających oraz zapewnienie pełnej transparentności i możliwości odwoławczych w procesie decyzyjnym. Nadmierne i dyskryminacyjne przepisy mogą mieć negatywne konsekwencje dla całej gospodarki. Proponujemy, aby przepisy dotyczące wykluczania dostawców były oparte na obiektywnych kryteriach technicznych i certyfikacji, co zapewni uczciwe i efektywne rozwiązania, które nie będą nadmiernie obciążać polskich przedsiębiorstw.	
120.	XOPERO	Uwaga ogólna	1. Wprowadzenie W świetle obowiązującej ustawy o krajowym systemie cyberbezpieczeństwa (KSC) - propozycji jej zmiany, kluczowym jest wdrożenie scentralizowanego systemu backupu oraz monitoringu. Proponowane rozwiązanie powinno zapewniać ochronę jednostek podległych oraz kompatybilność z storage'em blokowym. W związku z rosnącym ryzykiem cyberataków na polskie instytucje publiczne i urzędników, zabezpieczenie danych poprzez odpowiednie rozwiązania backupowe stało się niezbędne. 2. Zabezpieczenie Endpointów	Wyjaśnienie uwagi Dziękujemy za uwagę. Backup danych oraz monitoring systemu jest konieczny do zapewnienia bezpieczeństwa systemów informacyjnych.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

		Wybór odpowiedniego rozwiązania powinien obejmować ochronę danych końcowych (Endpoint Protection), która obejmuje: ● Ochrona Danych (Protected Data): Zabezpieczenie przed utratą, kradzieżą i nieuprawnionym dostępem do danych. ● Backup i Odzyskiwanie po Awarii (Backup and Disaster Recovery): Regularne tworzenie kopii zapasowych oraz szybkie przywracanie danych w przypadku awarii. ● Migracja Danych (Data Migration): Bezpieczne i efektywne przenoszenie danych między różnymi systemami i lokalizacjami. ● Ochrona Brzegowa (Edge Protection): Wykrywanie anomalii, backupowanie danych wrażliwych, szyfrowanych oraz identyfikowanie potencjalnych zagrożeń (Threat Hunting). 3. Geolokalizacja Usług Mając na uwadze bezpieczeństwo danych, zaleca się korzystanie z rozwiązań krajowych. Dostawcy oprogramowania powinni operować w 100% polskim kapitałem, tworzyć oprogramowanie na terenie kraju oraz przechowywać dane w polskiej przestrzeni internetowej. Takie podejście minimalizuje ryzyko związane z korzystaniem z usług międzynarodowych dostawców, którzy mogą podlegać innym regulacjom prawnym i być mniej transparentni. 4. Zabezpieczenie Łańcucha Dostaw i Przechowywanie Kodu Źródłowego Zabezpieczenie łańcucha dostaw i przechowywanie kodu źródłowego jest kluczowe dla utrzymania integralności systemów informatycznych. W kontekście współpracy z firmami trzecimi oraz dostawcami, niezbędne jest, aby kod źródłowy wytwarzany dla jednostek publicznych był bezpiecznie przechowywany i dostępny dla odpowiednich organów w razie potrzeby. Przykładowe działania obejmują: ● Repozytoria Kodów: Użycie bezpiecznych repozytoriów do przechowywania i zarządzania kodem źródłowym. ● Kontrola Dostępu: Wprowadzenie ścisłych polityk kontroli dostępu do kodu źródłowego, aby zapobiec nieautoryzowanemu użyciu lub modyfikacji. ● Regularne Audyty: Przeprowadzanie regularnych audytów bezpieczeństwa kodu źródłowego oraz systemów zarządzających tym kodem. 5. Backup Skrzynek Pocztowych W obliczu rosnących zagrożeń dla polskich urzędników i polityków, backupowanie skrzynek pocztowych powinno stać się standardem. Dzięki temu możliwe będzie: ● Wykrywanie Anomalii: Szybsze identyfikowanie nieprawidłowości w komunikacji mailowej, które mogą wskazywać na próbę szpiegostwa lub wycieku danych. ● Monitorowanie Zachowań Szpiegowskich: Analiza i monitorowanie skrzynek pocztowych w celu wykrywania potencjalnych działań szpiegowskich. Zabezpieczenie Przed Utratą Danych: Regularne	

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

		tworzenie kopii zapasowych maili, co umożliwi szybkie przywrócenie dostępu do ważnych informacji w przypadku incydentu. 6. Chmura Obliczeniowa i Centralizacja Usług W ocenie propozycji zmiany ustawy KSC, należy uwzględnić zapisy dotyczące centralnej chmury obliczeniowej zabezpieczonej oprogramowaniem backupującym i archiwizującym dane centralnie. Kluczowe aspekty to: ● Centralna Chmura: Usługi powinny być scentralizowane i kompatybilne, należące do tego samego producenta, aby zapewnić spójność i łatwość zarządzania. ● Bezpieczeństwo Narodowe: Dane powinny być przechowywane na terytorium kraju, co zwiększa bezpieczeństwo narodowe i zapewnia zgodność z lokalnymi przepisami. ● Zbieranie Danych przez Endpointy: Endpointy powinny zbierać dane i tworzyć lokalne kopie zapasowe, trzymając się reguły 3-2-1 dla kopii zapasowych. Ta reguła zakłada przechowywanie trzech kopii danych na dwóch różnych nośnikach, z jedną kopią przechowywaną offsite. ● Immutable Storage: Wykorzystanie storage'u zabezpieczonego przed atakami ransomware (tzw. Immutable Storage), który jest odporny na modyfikacje i kasowanie, zapewnia dodatkowy poziom ochrony. Podsumowanie Proponowane rozwiązanie obejmuje wdrożenie scentralizowanego systemu backupu i monitoringu, z naciskiem na ochronę endpointów, geolokalizację usług oraz zabezpieczenie łańcucha dostaw. Zastosowanie polskich rozwiązań technologicznych oraz regularne backupowanie skrzynek pocztowych przyczyni się do zwiększenia bezpieczeństwa danych i ochrony przed cyberzagrożeniami. Wszystkie działania są zgodne z obowiązującą ustawą o KSC i mają na celu podniesienie poziomu cyberbezpieczeństwa na poziomie krajowym. Centralna chmura obliczeniowa, zgodna z regułą 3-2-1, z wykorzystaniem technologii Immutable Storage, dodatkowo wzmocni ochronę przed współczesnymi zagrożeniami, takimi jak ransomware. Słowniczek Pojęć A ● AirGap: Metoda zabezpieczania danych poprzez fizyczne oddzielenie kopii zapasowej od systemów produkcyjnych, co chroni przed atakami ransomware. B ● Backup: Tworzenie kopii zapasowych danych, które można wykorzystać do przywrócenia systemów po awarii lub utracie danych. ● Backup and Disaster Recovery (Odzyskiwanie po Awarii): Procedury i technologie umożliwiające szybkie odzyskanie danych i przywrócenie funkcjonowania systemów po awarii. C ● Centralizacja Usług: Proces konsolidacji zarządzania usługami IT w jednym, scentralizowanym systemie, co zwiększa efektywność i bezpieczeństwo.	

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

		● Chmura Obliczeniowa: Model dostarczania usług IT, w którym zasoby (np. serwery, storage, aplikacje) są dostarczane przez internet jako usługi na żądanie. D ● Data Migration (Migracja Danych): Proces przenoszenia danych między różnymi systemami, platformami lub lokalizacjami. E ● Endpoint Protection (Ochrona Endpointów): Zabezpieczanie urządzeń końcowych (np. komputerów, smartfonów) przed zagrożeniami cybernetycznymi. ● Edge Protection (Ochrona Brzegowa): Mechanizmy zabezpieczające urządzenia końcowe, obejmujące wykrywanie anomalii, ochronę danych wrażliwych oraz wykrywanie zagrożeń (Threat Hunting). G ● Geolokalizacja Usług: Określenie fizycznej lokalizacji, gdzie przechowywane i przetwarzane są dane, co ma znaczenie dla zgodności z lokalnymi regulacjami prawnymi. I ● Immutable Storage: Typ storage'u odporny na modyfikacje i usunięcie, chroniący dane przed atakami ransomware. K ● Kontrola Dostępu: Zasady i mechanizmy regulujące, kto i w jaki sposób może uzyskiwać dostęp do danych lub systemów informatycznych. ● Kopia Zapasowa: Zobacz "Backup". L ● Lokalni Dostawcy Rozwiązań: Firmy oferujące produkty i usługi IT, które są w 100% własnością krajowego kapitału, tworzące oprogramowanie i przechowujące dane w kraju. M Monitoring: Proces ciągłego nadzorowania systemów IT w celu wykrywania i reagowania na potencjalne problemy i zagrożenia. P ● Protected Data (Ochrona Danych): Zabezpieczenie danych przed nieautoryzowanym dostępem, utratą lub kradzieżą poprzez stosowanie polityk dostępu i technologii szyfrowania. R ● Reguła 3-2-1: Zasada tworzenia kopii zapasowych, która zaleca przechowywanie trzech kopii danych na dwóch różnych nośnikach, z jedną kopią przechowywaną offsite. ● Repozytoria Kodów: Bezpieczne miejsca do przechowywania i zarządzania kodem źródłowym. S ● S3 (Simple Storage Service): Usługa przechowywania danych w chmurze, umożliwiająca skalowalne i bezpieczne przechowywanie danych.	

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			● Storage Blokowy: Rodzaj pamięci masowej, gdzie dane są przechowywane w blokach, które mogą być adresowane i zarządzane indywidualnie. T ● Threat Hunting (Wykrywanie Zagrożeń): Proaktywny proces poszukiwania potencjalnych zagrożeń w systemach IT przed ich uruchomieniem i wyrządzeniem szkód. Z Zabezpieczenie Łańcucha Dostaw: Proces zapewnienia, że wszystkie elementy łańcucha dostaw IT są bezpieczne i nie niosą ze sobą ryzyka wprowadzenia zagrożeń do systemu. Podsumowanie Słowniczek ten obejmuje kluczowe terminy związane z proponowanym rozwiązaniem backupowym i zabezpieczeniami, które są istotne dla zrozumienia i implementacji skutecznych mechanizmów ochrony danych w kontekście krajowego systemu cyberbezpieczeństwa (KSC).	
121.	Związek Pracodawców Klastry Polskie	Ogólna	W nawiązaniu do opublikowanego dnia 24 kwietnia 2024 roku projektu nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (sygnatura DP.MC.WL.0211.16.2024; zwanej dalej „Projektem Legislacji”) pragniemy wyrazić nasz niepokój związany z brakiem zaangażowania klastrow (klastrow przemysłowych, klastrow innowacyjnych) w proces konsultacji tego projektu. Jako organizacja reprezentująca interesy klastrow, chcielibyśmy brać udział w dyskusjach nad tą nowelizacją. Prosimy o uwzględnienie naszej organizacji, jako podmiotu biorącego również udział w konsultacjach projektu. W związku z powyższym, zwracamy się z formalnym wnioskiem o wydłużenie terminu konsultacji publicznych o kolejne 30 dni. Przedłużenie procesu konsultacyjnego pozwoli na przeprowadzenie wewnętrznej dyskusji oraz zgromadzenie i analizę stanowisk naszych członków, co z kolei umożliwi przedstawienie kompleksowego stanowiska wobec Projektu Legislacji. Związek Pracodawców Klastry Polskie zrzesza poprzez należące do niego klastry ponad 4000 przedsiębiorstw, które zatrudniają ponad 700 tysięcy pracowników. Klastry i ich przedsiębiorstwa operują przede wszystkim w innowacyjnych i wysoce technologicznych branżach przemysłu i usług. Są także wymieniane przez Komisję Europejską jako organizacje odpowiedzialne za wdrażanie gospodarki cyfrowej zwłaszcza do małych i średnich przedsiębiorstw. Jesteśmy, więc organizacją, która powinna być uwzględniana w procesie konsultacji taka ważnego z punktu widzenia digitalizacji projektu. Zanim przedstawimy ostateczne stanowisko, już dziś zwracamy uwagę na pewne elementy projektu, np.: wprowadzenie podsektora urządzeń elektrycznych i podsektora maszyn do kategorii podmiotów kluczowych, zamiast do podmiotów ważnych jak określono w Załączniku II do Dyrektywy o Cyberbezpieczeństwie, wydaje nam się niepotrzebne, a nawet ryzykowne dla przedsiębiorstw. Generuje to znaczące koszty dla polskich przedsiębiorców. Te dodatkowe obciążenia finansowe mogą negatywnie wpłynąć na konkurencyjność polskich firm.	Wyjaśnienie uwagi Każdy mógł się wypowiedzieć w ramach konsultacji publicznych. Projekt był dostępny na stronach Rządowego Centrum Legislacji.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			Dodatkowo jednym z efektów Projektu Legislacji będzie usuwanie z polskiego rynku azjatyckich dostawców z siedmioletnim okresem dostawczym, co obejmuje również podmioty będące dostawcami podstawowych urządzeń wykorzystywanych w rozproszonej energetyce, takich jak panele fotowoltaiczne, inwertery, turbiny, mikroturbiny, baterie do magazynowania energii, pompy ciepła, systemy kolektorów słonecznych, systemy biogazowe., okablowanie. Podstawowe parametry inwestycyjne w OZE zakładały co najmniej piętnastoletnie lub dłuższe okresy amortyzacji. Dlatego mamy zastrzeżenia do blokowania i usuwania z polskiego rynku takich dostawców w sektorze energetycznym. Projekt Legislacji nie przewiduje również żadnych odszkodowań dla podmiotów zobowiązanych do wymiany urządzeń, tak więc koszty zostaną przeniesione na przedsiębiorców. Zwracamy uwagę, że powinna zostać opublikowana tabela zgodności z prawem europejskim, nawet biorąc pod uwagę pośpiech legislacyjny wynikający z napiętego kalendarza zakładającego wejście w życie przepisów jeszcze w październiku tego roku. Jeszcze raz apelujemy o dokładne i rzetelne przemyślenie oraz dostosowanie zakresu mechanizmu wykluczenia dostawców w ramach Projektu Legislacji do rzeczywistych potrzeb. Uważamy i wnioskujemy o to, aby analiza skutków regulacji była wynikiem analizy danych rzeczywistych, a tego rodzaju dane można pozyskać od organizacji przedsiębiorców, co wymaga z jednej strony czasu, ale daje gwarancje podejmowania decyzji racjonalnych i prawidłowo oszacowanych kosztów ich wdrażania. Prosimy o uwzględnienie naszego wniosku o włączenie Związku Pracodawców Klastry Polskie do procesu konsultacji społecznych Ustawy oraz przedłużenie czasu na wnoszenie uwag w ramach konsultacji.	
122.	Związek Przedsiębiorców i Pracodawców	Uwaga ogólna	● Związek Przedsiębiorców i Pracodawców z zadowoleniem przyjmuje rozpoczęcie konsultacji dotyczących długo wyczekiwanego projektu nowelizacji ustawy o Krajowym Systemie Cyberbezpieczeństwa. ● Wiele badań i analiz wskazuje, że w obszarze cyberbezpieczeństwa Polska zajmuje stosunkowo wysoką pozycję. W rankingu NCSI, który wymienia kraje mające najlepsze na świecie rozwiązania gwarantujące systemom IT bezpieczeństwo, zajmujemy 11 miejsce. Choć nie zaliczamy się do grona światowych liderów, to nasz kraj postrzegany jest jako relatywnie bezpieczny cyfrowo. Nie oznacza to jednak, że brakuje nam w tym obszarze wyzwań. W ostatnich latach doświadczyliśmy wielu cybernetycznych incydentów, uderzających nie tylko w instytucje publiczne, ale również firmy obsługujące krytyczną infrastrukturę. Co więcej, napięcia geopolityczne, a zwłaszcza konflikt na Ukrainie, zwiększają ryzyko ataków hakerskich na Polskę. ● W dobie rosnącej liczby cyberataków i zagrożeń w sieci aktualizacja przepisów jest niezbędna do skutecznego reagowania na nowe formy ataków. W tym kontekście, jedną z priorytetowych kwestii będzie uchwalenie nowelizacji ustawy o Krajowym Systemie Cyberbezpieczeństwa. Zapewni ona lepszą zgodność polskiego systemu cyberbezpieczeństwa z unijnymi standardami oraz dyrektywami (m.in. NIS2 oraz CER), istotną dla międzynarodowej współpracy i wymiany informacji o	Wyjaśnienie uwagi Dziękujemy za pozytywne odniesienie.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			występujących zagrożeniach. Dodatkowo udoskonalenie ustawy pozwoli na lepszą ochronę krytycznej infrastruktury narodowej, która coraz częściej staje się celem zaawansowanych ataków. • Cieszymy się z decyzji o przeprowadzeniu szerokich konsultacji projektu nowelizacji ustawy o Krajowym Systemie Cyberbezpieczeństwa i popieramy jej jak najszybsze przebiegnięcie. Pragniemy zwrócić jednak uwagę na m.in. na potrzebę doprecyzowania niektórych przepisów w kontekście dyrektywy NIS2, kwestię dostawców sprzętu wysokiego ryzyka oraz Oceny Skutków Regulacji. Podsumowując Związek Przedsiębiorców i Pracodawców z zadowoleniem przyjmuje rozpoczęcie konsultacji nad projektem nowelizacji ustawy o Krajowym Systemie Cyberbezpieczeństwa. Popieramy szybkie wprowadzenie zmian, które zwiększą zgodność polskiego systemu z unijnymi standardami oraz zapewnią skuteczną ochronę infrastruktury krytycznej. Jednocześnie zwracamy uwagę na konieczność doprecyzowania przepisów dotyczących kar, odpowiedzialności zarządzających oraz terminów wycofania sprzętu wysokiego ryzyka. Sugerujemy również uwzględnienie rzeczywistych kosztów implementacji oraz dostosowanie wymogów do praktycznych możliwości przedsiębiorców.	
123.	Związek Cyfrowa Polska	Uwaga ogólna	W imieniu Związku Cyfrowa Polska, branżowej organizacji pracodawców, która zrzesza branżę nowoczesnych technologii, przesyłam nasze stanowisko do <i>projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)</i>. Na wstępie chciałbym podkreślić, że oceniamy bardzo pozytywnie ogólny cel projektu (.in.. implementację dyrektywy, tzw. NIS2) i większość zaproponowanych rozwiązań, w tym odwołania do 5G toolbox w zakresie Dostawców Wysokiego Ryzyka, zwłaszcza w zakresie kryteriów technicznych jak i nietechnicznych ich oceny. W tym miejscu polecamy uwadze raport Strand Consult¹³ dotyczący dostawców do europejskich operatorów. Co więcej uważamy, że niezwłoczne przyjęcie proponowanych przepisów jest niezbędne ze względu na skalę cyberzagrożeń, zwłaszcza w kontekście geopolitycznej sytuacji Polski. Postulujemy więc o jak najszybsze procedowanie przedmiotowego projektu. Pragniemy jednak zwrócić uwagę na fakt, że niektóre przepisy wymagają doprecyzowania, bowiem w wersji poddanej konsultacjom - w wielu przypadkach - wykraczają poza intencje unijnych prawodawców tworząc nadregulację. Pozostawienie ustawy w aktualnym brzmieniu może pociągnąć za sobą szereg negatywnych konsekwencji dla systemu cyberbezpieczeństwa oraz otoczenia gospodarczego, a także rodzi ryzyko stworzenia aktu niezgodnego z prawem Unii Europejskiej. Poniżej chcielibyśmy się odnieść do kilku kluczowych zagadnień.	Uwaga uwzględniona Wymogi projektu zostaną złagodzone.

¹³ <https://strandconsult.dk/there-are-many-myths-about-china-and-its-technology-suppliers-the-eu-published-a-report-you-should-read/>

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

124.	Związek Cyfrowa Polska	Uwaga ogólna	Dyrektywa NIS2 zakłada, że państwa członkowskie mogą wymagać od podmiotów kluczowych i ważnych używania określonych produktów ICT, usług ICT i procesów ICT, opracowanych przez podmiot kluczowy lub ważny, albo pozyskanych od stron trzecich, które są certyfikowane w ramach europejskich schematów certyfikacji cyberbezpieczeństwa przyjętych zgodnie z artykułem 49 rozporządzenia (UE) 2019/881. Tymczasem projekt implementacji nie zobowiązuje podmiotów kluczowych lub ważnych do korzystania z konkretnych produktów ICT. Równocześnie pojawia się upoważnienie dla rządu w zakresie wydawania rozporządzeń określających konkretne wymagania dla systemów zarządzania informacją dla różnych rodzajów działalności prowadzonych przez podmioty ważne lub kluczowe.	Wyjaśnienie uwagi Należy zauważyć, że pierwszy z europejskich programów certyfikacji wejdzie w życie dopiero w lutym 2025 r., co oznacza, że pierwsze produkty certyfikowane zgodnie z nim mogą najwcześniej pojawić się w drugiej połowie 2025 r. Obecnie nie ma takich produktów w związku z czym niezasadne jest wprowadzanie obowiązku ich używania. Należy podkreślić, że dyrektywa NIS2 nie wymaga wprowadzenia obowiązków używania certyfikowanych produktów, usług i procesów, a jedynie tworzy taką możliwość. Wykorzystanie tej kompetencji będzie rozważane dopiero gdy już na rynku będzie wystarczającą liczba produktów, usług i procesów, które posiadają odpowiednie certyfikaty.
125.	Konfederacja Lewiatan	Uwaga ogólna	W imieniu Konfederacji Lewiatan niniejszym zgłaszamy uwagi do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw, opublikowanego do konsultacji publicznych. W pierwszej kolejności odnotowujemy, że część uwag zgłaszanych w toku poprzednich prac nad ustawą znalazła swoje odzwierciedlenie w nowym tekście nowelizacji, mimo, że w ramach wcześniejszych prac uwagi te nie były uwzględniane. Odbieramy to jako zjawisko pozytywne. W szczególności, że część z tych kwestii dotyczy właśnie dialogu między stroną publiczną, a prywatną w ramach stosowania środków władczych w ramach krajowego systemu cyberbezpieczeństwa. W zakresie sektora telekomunikacyjnego, zauważamy także utrzymanie dotychczasowych przepisów działu VIIA ustawy Prawo telekomunikacyjne (w ustawie wprowadzającej PKE) do czasu wdrożenia NIS2. To również uznajemy za istotną poprawę wobec stanu wcześniejszego.	Wyjaśnienie uwagi Dziękujemy za pozytywne odniesienie.
126.	Konfederacja Lewiatan	Uwaga ogólna	W drugiej kolejności dziękujemy za określenie 30-dniowego terminu konsultacji. Zabiegaliśmy o wydłużenie tego terminu, ale przyjmujemy argumenty dot. opóźnień w pracach nad wdrożeniem NIS2 na poziomie krajowym. Zauważamy jednak, że zakres projektu i jego skutków jest ogromny, co spowodowało, że skala wpływu na sektor telekomunikacyjny i teleinformatyczny nie mogła zostać w pełni oszacowana. Dokładając należytej staranności przy analizie projektu napotkaliśmy na liczne wątpliwości natury	Wyjaśnienie uwagi Ministerstwo Cyfryzacji jest otwarte na spotkania.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			interpretacyjnej, a potencjalnie także kwestie wymagające poprawek oraz zwiększenia proporcjonalności. Zakładamy, że w pozostałych sektorach objętych nowymi przepisami sytuacja jest podobna. Dlatego naszym ogólnym postulatem jest, aby po dokonaniu analizy zgłaszanych uwag zorganizowana zostało spotkanie (lub seria spotkań) w ramach konsultacji społecznych, w toku których ze strony Ministerstwa Cyfryzacji przedstawione zostałyby wyjaśnienia dotyczące praktycznych aspektów wdrażania projektowanych przepisów. Spotkania takie powinny odbyć się jeszcze przed skierowaniem projektu pod obrady komitetów Rady Ministrów. Uważamy, że jest to niezwykle ważne dla zapewnienia właściwego, merytorycznego przebiegu konsultacji oraz wyjaśnienia wszelkich wątpliwości interpretacyjnych. Dla objętych nowymi regulacjami firm jest to niezwykle istotne, aby właściwie planować przyszłe wdrożenia, w tym ich czaso- i kosztochłonność - które już teraz widać, że będą bardzo poważne.	
127.	Konfederacja Lewiatan	Uwaga ogólna	Po trzecie – co wynika z doświadczeń z prac nad poprzednimi wersjami projektu – wnioskujemy, aby w przypadku wprowadzania istotnych zmian mających wpływ na prawa i obowiązki regulowanych podmiotów, organizowane były także dodatkowe rundy konsultacyjne. Niestety bowiem wielokrotnie byliśmy zaskakiwani wprowadzaniem do projektu całych nowych rozdziałów, które nie były przedmiotem pierwotnych konsultacji, a w sposób fundamentalny oddziaływały – często negatywnie – na sektor telekomunikacyjny. Czwartą kwestią, która zauważamy w ramach uwag ogólnych, jest brak aktów wykonawczych do ustawy, a także brak aktów wykonawczych do samej dyrektywy NIS2. Powoduje to, że wiele kwestii jest wciąż niejasnych i nie jest tym samym możliwe dokonanie właściwej oceny wpływu regulacji na poszczególne typy działalności objętej nowymi przepisami. Z tego względu postulujemy jak najszybsze opublikowanie projektów aktów wykonawczych do wstępnych chociaż konsultacji oraz wstrzymanie dalszych prac nad projektowaną ustawą do czasu ich przeprowadzenia. Ponadto, w naszej ocenie głębszego wyjaśnienia i przedstawienia praktycznych wytycznych wymagają relacje między NIS2 i DORA. Dotyczy to szczególnie podmiotów, które są jednocześnie regulowane w obu reżimach. Z jednej bowiem strony w art. 8i projektu ustawy wyłącza się stosowanie wobec podmiotów podlegających pod DORA rozdziału 3, ponieważ odpowiednie obowiązki należy wdrażać na bazie rozporządzenia DORA stosowanego bezpośrednio. Z drugiej jednak strony, przyjmuje się podejście wyrażone wyraźnie w uzasadnieniu: <i>Dyrektywa NIS 2 odeszła od wdrażania środków zapewniających bezpieczeństwo systemów informacyjnych tylko w zakresie świadczonych usług kluczowych. Podmiot ma dbać o bezpieczeństwo wszystkich swoich systemów wykorzystywanych do prowadzenia swojej działalności</i>. Przy tym podejściu, wyjaśnienia wymaga w jaki sposób np. podmiot kluczowy NIS2 (który miałby wdrożyć obowiązki we wszystkich swoich systemach), ma wdrażać obowiązki z NIS2 w swoich systemach służących także do działalności objętej rozporządzeniem DORA (a więc teoretycznie wyłączonej)?	Wyjaśnienie uwagi Akty wykonawcze do dyrektywy NIS2 zostały przygotowane przez Komisję Europejską. Rozporządzenia dotyczące szczegółów systemu zarządzania bezpieczeństwem informacji przewidziane przez projekt ustawy mają charakter fakultatywny. Będą wydawane w ramach identyfikowanych potrzeb. Jesteśmy otwarci na robocze spotkania w trakcie procesu legislacyjnego.
128.	Konfederacja Lewiatan	Uwaga ogólna	Już na wstępie pragniemy także podkreślić konieczność głębokiej zmiany filozofii tego projektu, aby przyniósł on korzyści zarówno dla cyberbezpieczeństwa, jak i konkurencyjności polskich firm.	Wyjaśnienie uwagi Nie można zgodzić się z tą opinią .

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

		Doceniamy prace skoncentrowane na szybkiej implementacji dyrektywy NIS2. Niemniej zaproponowana treść przepisów, najbardziej restrykcyjna w porównaniu z innymi państwami członkowskimi w zakresie transpozycji dyrektywy NIS2. <u>Warto zauważyć, że nadmierne regulacje mogą prowadzić do odwrotnych skutków niż zamierzone.</u> Zamiast poprawiać bezpieczeństwo, mogą one skłaniać firmy do minimalizowania inwestycji w innowacje technologiczne oraz rozwój swoich systemów bezpieczeństwa, obawiając się wysokich kosztów i skomplikowanych procedur. W efekcie, może to paradoksalnie zwiększyć ryzyko cyberzagrożeń, zamiast je zredukować. Ponadto, takie obciążenia mogą odstraszać potencjalnych inwestorów, którzy będą wybierać państwa o bardziej przyjaznym środowisku regulacyjnym. Zasadne wydaje się zatem przyjęcie <u>bardziej zrównoważonego podejścia, które nie tylko spełnia wymagania dyrektywy NIS2, ale również wspiera konkurencyjność i rozwój gospodarczy.</u> Wprowadzenie elastyczniejszych, mniej obciążających przepisów, które jednak zapewniają odpowiedni poziom bezpieczeństwa, przyniesie korzyści zarówno dla sektora prywatnego, jak i dla ogólnego poziomu cyberbezpieczeństwa w Polsce. Projekt ustawy niesie ze sobą ogromne wyzwania i przekrojowo dotyka znacznej części polskich przedsiębiorców. W naszej ocenie projekt ustawy nie wyważa odpowiednio potrzeby zapewnienia państwu realnych narzędzi nadzoru i kontroli w obszarze cyberbezpieczeństwa z poszanowaniem i ochroną przedsiębiorczości oraz praw jednostki. Niestety, wiele elementów budzi głębokie wątpliwości z tego punktu widzenia. <u>Przedsiębiorcy wyrażają swoje głębokie niezadowolenie, ponieważ projekt powtarza błędy poprzednich nowelizacji i dodatkowo rozszerza restrykcyjne regulacje na wszystkie 18 sektorów objętych dyrektywą NIS2, co stanowi ewenement w Unii Europejskiej.</u> To podejście jest postrzegane jako nadmiernie obciążające dla polskich firm, zwiększając koszty i czasochłonność zgodności z przepisami i podkreślić należy, że spowoduje znaczne obniżenie atrakcyjności Polski, jako miejsca krajowych i zagranicznych inwestycji. Projekt ustawy nie zawiera nawet rzetelnie przeprowadzonej Oceny Skutków Regulacji, tak jak gdyby liczne obowiązki związane z cyberbezpieczeństwem miałyby pozostać bez wpływu na koszty prowadzenia działalności gospodarczej. Szczególne zastrzeżenia budzi postępowanie w sprawie uznania dostawcy za dostawcę wysokiego ryzyka (nie wynikające bezpośrednio z dyrektywy NIS2), które, spowoduje wykluczenie wielu dostawców z każdego z osiemnastu sektorów w Polsce, podczas ci sami dostawcy będą mogli bez przeszkód działać w innych krajach Unii Europejskiej). <u>Zdaniem części firm zrzeszonych w Lewiatanie proponowana procedura uznania dostawcy za dostawcę wysokiego ryzyka nie jest zgodna z dyrektywą NIS2 i może być uznana za dyskryminującą, skupiając się bardziej na kryteriach politycznych niż technicznych, a zwłaszcza na państwie pochodzenia dostawców spoza Unii Europejskiej lub NATO.</u> Niepokojące jest także, że władza nad tym procesem zostanie skupiona w zakresie kompetencji jednego ministra, który na podstawie niejawnych postępowań będzie mógł dowolnie wykluczać dostawców i ich rozwiązania z każdego sektora polskiej gospodarki. Taka koncentracja władzy budzi obawy o brak przejrzystości i potencjalne nadużycia, co może negatywnie	Postępowanie w sprawie uznania za dostawcę wysokiego ryzyka ma na celu zabezpieczenie polskiej gospodarki i polskiego społeczeństwa przed dostawcą sprzętu lub oprogramowania, który stwarza poważne zagrożenie dla bezpieczeństwa państwa, obronności, bezpieczeństwa i porządku publicznego lub zdrowia i życia ludzi. W ramach postępowania administracyjnego będą brane pod uwagę zarówno aspekty techniczne związane z dostarczaniem przez dostawcę sprzętem i oprogramowaniem jak również aspekty nietechniczne związane z dostawcą. Dzięki temu zostanie zidentyfikowany pełen obraz zagrożeń jakie stwarza dostawca sprzętu lub oprogramowania. Postępowanie umożliwia badanie dostawcy sprzętu lub oprogramowania dla wszystkich sektorów gospodarki wskazanych w ustawie. Jest to wskazane z uwagi na to, że każdy podmiot kluczowy i podmiot ważny musi dbać o bezpieczeństwo łańcuchów dostaw. Podmioty kluczowe i podmioty ważne mają istotny charakter dla funkcjonowania współczesnej gospodarki i społeczeństwa informacyjnego. Postępowanie będzie mogło być skontrolowane przez niezależny sąd administracyjny, co zapewni ochronę praw dostawcy.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			wpływać na konkurencyjność i innowacyjność polskiej gospodarki. Ponadto, możliwość arbitralnego wykluczania dostawców bez jasnych i przejrzystych kryteriów może prowadzić do zmniejszenia zaufania inwestorów zagranicznych oraz do destabilizacji rynku technologicznego w Polsce.	
129.	Konfederacja Lewiatan	Uwaga ogólna	Oczekujemy poważnych zmian w tekście projektowanych przepisów, które będą bardziej uwzględniać rzeczywiste potrzeby i możliwości polskiego rynku, przy jednoczesnym zachowaniu wysokiego poziomu cyberbezpieczeństwa, a także uwzględnia podejście innych krajów Unii Europejskiej. Istotne jest, aby nowe przepisy nie tylko spełniały wymogi dyrektywy NIS2, ale także wspierały rozwój gospodarczy i konkurencyjność polskich przedsiębiorstw. Izba nie neguje potrzeby i konieczności ochrony interesów Rzeczypospolitej Polskiej, jednak zwraca uwagę, że przyjęte rozwiązania powinny być proporcjonalne i dostosowane do specyfiki, a także uwzględniać skutki społeczne i ekonomiczne. <u>Dlatego wszelkie środki powinny być stosowane w odniesieniu do elementów krytycznych infrastruktury oraz związku z cechami konkretnego podmiotu kluczowego lub ważnego (podmiotu krajowego systemu cyberbezpieczeństwa).</u> <u>Jednocześnie część z firm zrzeszonych w Konfederacji Lewiatan nie widzi potrzeby zmian w treści projektu ustawy w zakresie odnoszącym się do procedury uznania danego przedsiębiorcy za dostawcę wysokiego ryzyka. Przedsiębiorcy Ci zwracają uwagę na to, że władze polskie, które odpowiadają za szeroko pojęte bezpieczeństwo państwa, muszą dysponować odpowiednimi narzędziami ograniczania realnych zagrożeń naszego bezpieczeństwa.</u> Implementacja dyrektywy NIS2 sama w sobie jest znaczącym wyzwaniem i prawdziwą rewolucją w obszarze cyberbezpieczeństwa. Wobec tak ambitnego zadania warto zastanowić się, czy czas na wprowadzanie dodatkowo restrykcyjnych przepisów, które wykraczają poza wymagania NIS2. Bardziej efektywne byłoby przyjęcie przepisów optymalnych, zgodnych z zasadą harmonizacji, a ewentualne korekty wprowadzać w zależności od sytuacji, co pozwoli na bardziej płynne dostosowanie do nowych regulacji. W kontekście samego zakresu nowelizacji należy także zwrócić uwagę, że sam projekt jest obszerniejszy, jeśli chodzi o treść i zawartość, niż sama ustawa o krajowym systemie cyberbezpieczeństwa. Zgodnie z § 84 Zasad techniki prawodawczej¹⁴ <u>Jeżeli zmiany wprowadzane w ustawie miałyby być liczne albo miałyby naruszać konstrukcję lub spójność ustawy albo gdy ustawa była już poprzednio wielokrotnie nowelizowana, opracowuje się projekt nowej ustawy.</u> Ponadto pomimo relatywnie krótkiego, gdyż 6-letniego okresu obowiązywania, ustawa o krajowym systemie cyberbezpieczeństwa, była już wielokrotnie, bo aż 9 razy nowelizowana i ukazały się już 3 teksty jednolite. Przepis § 84 Zasad techniki prawodawczej wymienia alternatywnie trzy przyczyny, co oznacza, że zaistnienie tylko jednej z nich uzasadnia konieczność przygotowania nowej ustawy. W przypadku tej propozycji nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa zachodzą dwie z trzech przyczyn wymienionych przez ten przepis, co uzasadnia przygotowanie nowej ustawy. Apelujemy także o poszanowanie procesu legislacyjnego oraz o przeprowadzenie szerokich konsultacji, tak by uniknąć powtórzenia wadliwych rozwiązań zawartych	Wyjaśnienie uwagi Celem projektodawcy jest aby nowe przepisy stanowiły kontynuację rozwiązań zawartych w obecnie obowiązujących przepisach ustawy o krajowym systemie cyberbezpieczeństwa. Wiele rozwiązań zawartych w tej ustawie stanowi rozwinięcie już funkcjonujących instytucji. Dla osiągnięcia tego celu najlepsza będzie nowelizacja obecnie obowiązującej ustawy.

¹⁴ Rozporządzenie z 20 czerwca 2002 r. Prezesa Rady Ministrów w sprawie „Zasad techniki prawodawczej” (t.j. Dz.U. z 2016 r. poz. 283)

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			w projekcie ustawy poprzedniego Rządu. Ważne jest, aby nowe przepisy były oparte na solidnych podstawach prawnych i uwzględniały rzeczywiste potrzeby oraz możliwości polskich przedsiębiorstw. Apelujemy również o <u>przeprowadzenie rzetelnej oceny skutków regulacji oraz analizy wpływu nowych obowiązków na koszty prowadzenia działalności w Polsce</u> . Przedsiębiorcy już teraz borykają się z wieloma wyzwaniami, a nadmierne obciążenia regulacyjne mogą dodatkowo pogorszyć ich sytuację. Z tego powodu, konieczne jest, aby proces legislacyjny był przeprowadzany w sposób transparentny, z uwzględnieniem opinii wszystkich zainteresowanych stron, co pozwoli na wypracowanie przepisów, które będą zarówno skuteczne, jak i sprawiedliwe.	
130.	Konfederacja Lewiatan	Uwaga ogólna	KL dostrzega znaczne potencjalne koszty oraz ryzyko nadregulacji związane z proponowanymi zmianami w ustawie o krajowym systemie cyberbezpieczeństwa. Obecny projekt ustawy wprowadza wiele kwestii wymagających dogłębnych konsultacji z różnymi sektorami gospodarki, również ze względu na szeroki zakres oddziaływania dyrektywy NIS2. Izba podkreśla, że szczególnie istotne jest unikanie tzw. "gold platingu", który prowadzi do niepotrzebnego obciążenia polskich przedsiębiorstw ponad wymagania dyrektywy NIS2, szczególnie w kontekście obecnych wyzwań makroekonomicznych, takich jak wzrost cen energii, inflacja oraz obciążenia podatkowe. Proponowane regulacje wprowadzają znaczne obciążenia finansowe i operacyjne dla polskich firm, co może negatywnie wpłynąć na ich konkurencyjność oraz stabilność ekonomiczną. W związku z tym, Izba wyraża nadzieję na zorganizowanie konferencji uzgodnieniowej oraz warsztatów, które umożliwią szczegółowe omówienie i dopracowanie tych zmian z uwzględnieniem opinii i doświadczeń poszczególnych sektorów. Takie podejście pozwoli na wypracowanie bardziej zrównoważonych i efektywnych rozwiązań, które będą adekwatnie chronić bezpieczeństwo cybernetyczne kraju, nie powodując jednocześnie nadmiernych obciążeń dla przedsiębiorców.	Wyjaśnienie uwagi Wymogi projektu zostaną złagodzone.
131.	Konfederacja Lewiatan	Uwaga ogólna	Proponowane uprawnienia ministra ds. informatyzacji dają mu znaczny wpływ na całą polską gospodarkę, co budzi obawy o nadmierne kompetencje i potencjalne konflikty z Konstytucją RP. Szczególnie w sytuacji, gdy Minister Cyfryzacji jest organem jednoosobowym o charakterze politycznym. Minister będzie mógł usuwać z polskiego rynku dowolnego dostawcę (poprzez zakaz korzystania z jego rozwiązań), w drodze rekomendacji decydować o losach wszystkich zamówień publicznych, wydając polecenia zabezpieczające ograniczać i w praktyce zamykać działalność gospodarczą. Prerogatywy te są niespotykane w dotychczasowej legislacji – a powody tak silnych uprawnień nieznane. Takie uprawnienia mogą prowadzić do nieproporcjonalnej kontroli, co wymaga ponownej oceny, aby zapewnić zgodność z zasadami konstytucyjnymi, a w szczególności z prawami obywatelskimi.	Wyjaśnienie uwagi Decyzje ministra właściwego do spraw informatyzacji będą podlegały kontroli sądu administracyjnego. Decyzje te dotyczą szczególnych i nadzwyczajnych sytuacji, gdy bezpieczeństwo państwa jest zagrożone. Przed wydaniem decyzji minister będzie zasięgał opinii Kolegium do Spraw Cyberbezpieczeństwa czy też zespołu do spraw incydentów krytycznych.
132.	Konfederacja Lewiatan	Uwaga ogólna	Projekt ustawy nakłada dodatkowe obowiązki na sektory, które nie są objęte dyrektywą NIS2, takie jak wszystkie jednostki samorządu terytorialnego, sektor farmaceutyczny, w tym apteki i instytucje edukacyjne. Rozszerzenie zakresu na te podmioty jest nieuzasadnione i prowadzi do zbędnych obciążeń finansowych i administracyjnych. W szczególności dyrektywa NIS2 nie obejmuje w pełni	Uwaga częściowo uwzględniona W art. 8 ust. 1 zostaną uwzględnione koszty prowadzenia działalności. Wyjaśnienie uwagi

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			sektora farmaceutycznego, jednak projekt ustawy klasyfikuje różne podmioty w tym sektorze jako kluczowe, co jest nadmierne i wprowadza niepotrzebne obciążenia regulacyjne. Analiza rozwiązań zawartych w projekcie ustawy prowadzi również do konkluzji, że projektodawca przyjął rozwiązania jak najmniej proporcjonalne i nie uwzględniające specyfiki poszczególnych sektorów. W proponowanych przepisach nowelizacji nigdzie nie proponuje się podejścia opartego na kosztach. Artykuł 21 ust. 1 Dyrektywy NIS2 zobowiązuje państwa członkowskie do zapewnienia, że podmioty kluczowe i ważne wdrażają odpowiednie i proporcjonalne środki techniczne, operacyjne oraz organizacyjne. Artykuł 8 ust. 1 pkt 2 projektu ustawy, który ma na celu implementację tych wymagań, nie zawiera odniesienia do kosztów wdrożenia jako kryterium oceny proporcjonalności środków. Stanowi to znaczącą różnicę w stosunku do dyrektywy, która podkreśla potrzebę uwzględniania tych kosztów w ocenie proporcjonalności środków zarządzania ryzykiem.	Dyrektywa NIS2 umożliwia zachowanie w systemie dotychczasowych operatorów usług kluczowych. Apteki już na gruncie obecnej ustawy KSC mogą być i są uznawane za operatorów usług kluczowych. Jednostki samorządu terytorialnego od 2012 r. mają obowiązek wdrożenia systemu zarządzania bezpieczeństwem informacji w systemach teleinformatycznych służących do realizacji zadań publicznych.																																																	
133.	Konfederacja Lewiatan	Uwaga ogólna	Potencjalna nadregulacja na tle innych państw członkowskich UE Poniżej przedstawiono analizę poszczególnych implementacji dyrektywy NIS2 w niektórych krajach UE w zakresie stosowania nietechnicznych kryteriów oceny dostawców w łańcuchu dostaw. <table><tr><th>Kraj</th><th>Status legislacji</th><th>Procedura DWR</th><th>Ocena nietechniczna w łańcuchach dostaw</th><th>Objęcie samorządu lokalnego</th><th>Objęcie instytucji edukacyjnych</th><th>Liczba podmiotów w</th></tr><tr><td>Belgia</td><td>Ukończona</td><td>Nie</td><td>Nie</td><td>Nie</td><td>Nie</td><td>2K+</td></tr><tr><td>Węgry</td><td>Ukończona</td><td>Nie</td><td>Nie</td><td>Nie</td><td>Nie</td><td>N/D</td></tr><tr><td>Chorwacja</td><td>Ukończona</td><td>Nie</td><td>Nie</td><td>Tak</td><td>Tak</td><td>N/D</td></tr><tr><td>Niemcy</td><td>Przegląd rządowy</td><td>Nie</td><td>W trakcie dyskusji</td><td>Nie</td><td>Nie</td><td>35K+</td></tr><tr><td>Francja</td><td>Przegląd rządowy</td><td>Nie</td><td>Nie</td><td>Tak (ograniczone do 1% gmin)</td><td>Tak (ograniczone do funkcji badawczych)</td><td>15K+</td></tr><tr><td>Austria</td><td>Konsultacje publiczne</td><td>Nie</td><td>Nie</td><td>Nie</td><td>Nie</td><td>4K+</td></tr></table>	Kraj	Status legislacji	Procedura DWR	Ocena nietechniczna w łańcuchach dostaw	Objęcie samorządu lokalnego	Objęcie instytucji edukacyjnych	Liczba podmiotów w	Belgia	Ukończona	Nie	Nie	Nie	Nie	2K+	Węgry	Ukończona	Nie	Nie	Nie	Nie	N/D	Chorwacja	Ukończona	Nie	Nie	Tak	Tak	N/D	Niemcy	Przegląd rządowy	Nie	W trakcie dyskusji	Nie	Nie	35K+	Francja	Przegląd rządowy	Nie	Nie	Tak (ograniczone do 1% gmin)	Tak (ograniczone do funkcji badawczych)	15K+	Austria	Konsultacje publiczne	Nie	Nie	Nie	Nie	4K+	Wyjaśnienie uwagi Tak jak wskazywaliśmy w zał. nr 1 do OSR, w Europie są rozwiązania dotyczące dostawcy wysokiego ryzyka.
Kraj	Status legislacji	Procedura DWR	Ocena nietechniczna w łańcuchach dostaw	Objęcie samorządu lokalnego	Objęcie instytucji edukacyjnych	Liczba podmiotów w																																															
Belgia	Ukończona	Nie	Nie	Nie	Nie	2K+																																															
Węgry	Ukończona	Nie	Nie	Nie	Nie	N/D																																															
Chorwacja	Ukończona	Nie	Nie	Tak	Tak	N/D																																															
Niemcy	Przegląd rządowy	Nie	W trakcie dyskusji	Nie	Nie	35K+																																															
Francja	Przegląd rządowy	Nie	Nie	Tak (ograniczone do 1% gmin)	Tak (ograniczone do funkcji badawczych)	15K+																																															
Austria	Konsultacje publiczne	Nie	Nie	Nie	Nie	4K+																																															

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			Finlandia	Konsultacje publiczne	Nie	Nie	Nie	Nie	N/D	
			Szwecja	Przegląd rządowy	Nie	Nie	Tak	Ograniczone do uniwersytetów	N/D	
		Implementacja dyrektywy NIS2 w krajach UE różni się znacząco pod względem liczby podmiotów objętych regulacjami. W Belgii, z populacją około 11,5 miliona i PKB wynoszącym 500 miliardów USD, dyrektywa obejmuje ponad 2,000 podmiotów. W Niemczech, liczących 83 miliony mieszkańców i z PKB około 4 bilionów USD, regulacje dotyczą ponad 35,000 podmiotów. We Francji, z populacją 67 milionów i PKB wynoszącym około 3 biliony USD, dyrektywa obejmuje ponad 15,000 podmiotów. Austria, mająca około 9 milionów mieszkańców i PKB wynoszący 480 miliardów USD, ma ponad 4,000 podmiotów objętych dyrektywą. Polska, z populacją 38 milionów i PKB wynoszącym 740 miliardów USD, przyjęła szerokie podejście, obejmując około 38,000 podmiotów. Mimo że Polska jest znacznie mniejszym krajem i rynkiem niż Niemcy, to szerokie podejście skutkuje znacznymi wyzwaniami regulacyjnymi i kosztami dla polskich przedsiębiorców. Szerokie podejście Polski do implementacji dyrektywy NIS2 może prowadzić do dużych obciążeń administracyjnych i finansowych dla polskich firm, które muszą spełniać liczne wymagania związane z bezpieczeństwem sieci i informacji. Dla porównania, Niemcy z większą populacją i znacznie wyższym PKB mają mniej podmiotów objętych dyrektywą, co wskazuje na bardziej wyważone podejście. W rezultacie polskie firmy mogą być zmuszone do poniesienia większych kosztów dostosowania się do nowych regulacji, co może wpłynąć na ich konkurencyjność na rynku europejskim. Podsumowując, Polska stoi przed wyzwaniem skutecznego wdrożenia dyrektywy NIS2 w sposób, który zapewni wysoki poziom bezpieczeństwa, ale jednocześnie nie zahamuje rozwoju gospodarczego i innowacji. Wymaga to strategicznego podejścia oraz wsparcia dla przedsiębiorców w adaptacji do nowych wymogów. Obecnie trwają prace nad implementacją Dyrektywy NIS2 w Czechach, w których główne elementy proponowanej oceny obejmują ocenę dostawców w czterech kluczowych sektorach: telekomunikacja, rząd, energia i transport. W telekomunikacji szczególną uwagę poświęca się funkcjom krytycznym. Brak jest jednak standardów oceny ryzyka dostawców opartych na kraju pochodzenia. Krajowa Agencja Bezpieczeństwa Cybernetycznego (NOUGHKIB) ma możliwość oceny ryzyka dostawców na podstawie zagrożeń dla bezpieczeństwa Czech lub porządku publicznego. Projekt ustawy o cyberbezpieczeństwie spotkał się z krytyką Rady Legislacyjnej Rządu (LRV), która zażądała jego modyfikacji. Problemy dotyczą m.in. szerokiego mandatu agencji oraz braku jasnych podstaw prawnych i ograniczeń dla wydawanych dekrétów. Natomiast Polska zamierza zastosować procedury oceny dostawców wysokiego ryzyka dla wszystkich 18 sektorów objętych dyrektywą								

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			NIS2, w przeciwieństwie do Czech, które skupiają się tylko na czterech sektorach. Polski plan obejmuje każdą kategorię urządzeń i oprogramowania.	
134.	Konfederacja Lewiatan	Uwaga ogólna	Procedury dla dostawców wysokiego ryzyka Za całkowicie nieproporcjonalne uważamy objęcie procedurą dla dostawców wysokiego ryzyka wszystkich osiemnastu sektorów, co stanowi duży krok wstecz, w stosunku do, i tak powszechnie krytykowanego, przedłożenia poprzedniego Rządu. Co więcej, również sama analiza przeprowadzona przez Ministerstwo Cyfryzacji dołączona do OSR prowadzi do wniosku, że projektodawca proponuje unikalne w całej Unii Europejskiej rozwiązanie, zgodnie z którym procedura wykluczenia dostawcy obejmie wszystkie osiemnaście sektorów. Proponowana procedura uznania dostawcy za dostawcę wysokiego ryzyka nie jest zgodna z dyrektywą NIS2 i może być uznana za dyskryminującą, skupiając się bardziej na kryteriach politycznych niż technicznych. Procedura ta może prowadzić do znaczących skutków ekonomicznych, w tym wzrostu cen i zakłóceń rynkowych. Taka procedura, umocowana właściwie w arbitralnej decyzji ministra ds. informatyzacji, w oparciu o niejawną opinię Kolegium ds. Cyberbezpieczeństwa budzi poważne zastrzeżenia z punktu widzenia zasady praworządności. Izba nie neguje potrzeby i konieczności ochrony interesów Rzeczypospolitej Polskiej, jednak zwraca uwagę, że przyjęte rozwiązania powinny być proporcjonalne i dostosowane do specyfiki, a także uwzględniać skutki społeczne i ekonomiczne. Dlatego wszelkie środki powinny być stosowane w odniesieniu do elementów krytycznych infrastruktury oraz związku z cechami konkretnego podmiotu kluczowego lub ważnego (podmiotu krajowego systemu cyberbezpieczeństwa).	Wyjaśnienie uwagi Dostawca wysokiego ryzyka może dostarczać sprzęt nie tylko dla przedsiębiorców telekomunikacyjnych, ale i dla pozostałych sektorów gospodarki. Poza tym zgodnie z dyrektywą NIS2 wszystkie podmioty kluczowe i podmioty ważne powinny zarządzać bezpieczeństwem łańcuchów dostaw.
135.	Konfederacja Lewiatan	Uwaga ogólna	Elastyczność w zakresie funkcji krytycznych i infrastruktury Aby ustawa nadążała za rozwojem technologii i dynamiką zagrożeń w cyberbezpieczeństwie, środki cyberbezpieczeństwa oraz zakres infrastruktury krytycznej muszą być łatwo dostosowywane. Wzorem Niemiec oraz Finlandii, funkcje krytyczne oraz infrastruktura krytyczna powinny być regulowane w aktach wykonawczych przez odpowiednie organy ds. cyberbezpieczeństwa dla każdego sektora, a nie sztywno określone w ustawie. Uważamy, że załącznik nr 3 powinien zostać usunięty, a oceny takich funkcji prowadzone przez Grupę Współpracy we współpracy z Komisją Europejską i ENISA, a nie przez ministra ds. informatyzacji.	Wyjaśnienie uwagi Z uwagi na krytyczne znaczenie tej regulacji postanowiono zachować załącznik nr 3 na poziomie ustawy.
136.	Konfederacja Lewiatan	Uwaga ogólna	Natychmiastowa wykonalność poleceń zabezpieczających bez możliwości odwołania się narusza podstawowe zasady prawne. Te polecenia mogą prowadzić do znacznych przerw w działalności oraz obciążeń finansowych dla podmiotów, które muszą się do nich dostosować, bez przewidzianego odszkodowania. W wyniku poszerzenia zakresu jego obowiązywania – polecenia zabezpieczające może w zasadzie w każdej chwili sparaliżować działalność danego podmiotu, włączonego w system cyberbezpieczeństwa.	Wyjaśnienie uwagi Polecenie zabezpieczające będzie dotyczyło szczególnej sytuacji wystąpienia incydentu krytycznego. To narzędzie ma uchronić podmioty przed incydemem krytycznym a nie go pogłębić.
137.	Konfederacja Lewiatan	Uwaga Ogólna	Konfederacja Lewiatan zdecydowanie rekomenduje ponowne rozważenie proponowanych zmian, aby zrównoważyć potrzeby w zakresie cyberbezpieczeństwa z praktycznymi realiami poszczególnych sektorów. Zapewnienie elastyczności w regulacji funkcji krytycznych i infrastruktury krytycznej	Wyjaśnienie uwagi Jesteśmy otwarci na rozmowy.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			pomoże uniknąć nadmiernych regulacji i związanych z nimi kosztów. Ponadto, kompetencje ministra ds. informatyzacji powinny zostać dokładnie przeanalizowane, aby zapobiec nadmiernej kontroli i zapewnić, że regulacje będą efektywne i proporcjonalne. Izba liczy na dalsze konsultacje i współpracę, aby dopracować przepisy w sposób wspierający zarówno cyberbezpieczeństwo, jak i stabilność ekonomiczną. Poniżej przedstawiono szczegółowe uwagi podzielone na dziesięć kluczowych obszarów.	
138.	Związku Pracodawców Technologii Cyfrowych Lewiatan	Uwaga ogólna	Stoimy na stanowisku, że projekt ustawy, który ma dotyczyć bezpośrednio ponad 38 tysięcy podmiotów, a pośrednio (dostawcy podmiotów kluczowych lub ważnych) kolejnych kilkudziesięciu tysięcy musi być bardzo solidnie przedyskutowany w szerokim gronie. Co więcej, w wielu krajach UE już dzisiaj rządy komunikują, że nie zdołają dotrzymać terminów przewidzianych w Dyrektywie, a oficjalna strona postępów wdrożenia wykazuje, że jedynym krajem, który ma proces za sobą jest Chorwacja. https://eur-lex.europa.eu/legal-content/EN/NIM/?uri=CELEX:32022L2555&qid=1715785064589 Dlatego też apelujemy, aby natychmiast rozpocząć kolejny etap konsultacji. Ze swojej strony deklarujemy gotowość do spotkania i przedstawienia w drodze dialogu przygotowane przez nas uwagi. Powinno to znakomicie skrócić czas związany z przygotowaniem kolejnych wersji.	Wyjaśnienie uwagi Ministerstwo Cyfryzacji zawsze jest chętne na spotkania robocze.
139.	Związku Pracodawców Technologii Cyfrowych Lewiatan	Uwaga ogólna	Ustawa o krajowym systemie cyberbezpieczeństwa jest w sposób nierozzerwalny połączona z wieloma innymi aktami prawnymi, które podlegają aktualnie nowelizacji. Wiele z nich nie zostało jeszcze formalnie opublikowanych, niektóre nie są przygotowywane w Ministerstwie Cyfryzacji – a to oznacza konieczność z jednej strony bardzo starannej koordynacji i synchronizacji pojęć, wymagań i procesów. Brak takiej analizy i odpowiednich zapisów będzie skutkował zwiększeniem poziomu prawnej niepewności, a w rezultacie finalnie nie przyczyni się do podniesienia cyberbezpieczeństwa Polski. Część zauważonych problemów przekazujemy dalej w uwagach szczegółowych. Wskazujemy na co najmniej następujące dokumenty, które właśnie podlegają zmianom: Ustawa o informatyzacji – 9 maja 2024 https://www.gov.pl/web/premier/projekt-ustawy-o-zmianie-ustawy-o-informatyzacji-dzialalnosci-podmiotow-realizujacych-zadania-publiczne Rozporządzenie KRI – 10 maja 2024 https://www.gov.pl/web/premier/projekt-rozporzadzenia-rady-ministrow-w-sprawie-krajowych-ram-interoperacyjnosci-minimalnych-wymagan-dla-rejestrow-publicznych-wymagan-dla-systemow-teleinformatycznych-oraz-wymiany-informacji-w-postaci-elektronicznej Ustawa o krajowym systemie certyfikacji cyberbezpieczeństwa – 2 maja 2024 https://www.gov.pl/web/premier/projekt-ustawy-o-krajowym-systemie-certyfikacji-cyberbezpieczenstwa Uchwała WIIP https://www.gov.pl/web/premier/projekt-uchwaly-rady-ministrow-zmieniajacej-uchwale-w-sprawie-inicjatywy-wspolna-infrastruktura-informatyczna-panstwa5 Projekt ustawy o zarządzaniu kryzysowym, infrastrukturze krytycznej i podmiotach krytycznych – w przygotowaniu	Wyjaśnienie uwagi Będziemy dążyć do uspoijnienia przepisów.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			Projekt ustawy o zmianie niektórych ustaw w związku z zapewnieniem operacyjnej odporności cyfrowej sektora finansowego (akty wdrażające DORA) https://legislacja.rcl.gov.pl/projekt/12384252/katalog/13053510#13053510 Warto przy tym zaznaczyć, że do tego projektu organizacje społeczne przesłały uwagi liczące po co najmniej kilkanaście stron. ale także trzeba uwzględnić co najmniej Ustawa o działaniach antyterrorystycznych, wprowadzającą stopnie alarmowe Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (sejm.gov.pl) oraz Rozporządzenie Prezesa Rady Ministrów z dnia 25 lipca 2016 r. w sprawie zakresu przedsięwzięć wykonywanych w poszczególnych stopniach alarmowych i stopniach alarmowych CRP Rozporządzenie Prezesa Rady Ministrów z dnia 25 lipca 2016 r. w sprawie zakresu przedsięwzięć wykonywanych w poszczególnych stopniach alarmowych i stopniach alarmowych CRP (sejm.gov.pl) patrz także: motyw (88) Dyrektywy NIS2 Rozporządzenie European Health Data Spaces, które najprawdopodobniej zostanie opublikowane do czasu uchwalenia nowelizacji uksc, a którego znaczenie dla sektora ochrony zdrowia jest równe znaczeniu DORA dla sektora finansowego https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2022/0140(COD)&l=en Rozporządzenie AI Act, którego publikacja jest planowana w najbliższych dniach https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2021/0106(COD)&l=en wdrożeniem w Polsce Aktu w sprawie danych (Data Act), który będzie miał ogromne znaczenie dla cyberbezpieczeństwa podmiotów kluczowych i ważnych wykorzystujących dane nieosobowe, a które będzie egzekwowalny od 12 września 2025 https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32023R2854 W szczególności chcemy tutaj zwrócić uwagę na współzależności pomiędzy Dyrektywami CER oraz NIS2, gdzie ta pierwsza odsyła zadania z cyberbezpieczeństwa do drugiej. Jednak należy zwrócić uwagę, że obszary ochrony w infrastrukturze krytycznej inne niż teleinformatyka są również w wielkim stopniu ucyfrowione. A to oznacza konieczność zgrania kompetencji i decyzyjności dla różnych regulatorów odpowiedzialnych za bezpieczeństwo. Innym elementem jest oczywiście odesłanie transpozycji NIS2 do prawa dla określonego segmentu np. DORA czy EHDS, zwłaszcza że granice wcale nie są tak twarde. Przykładowo Zakład Ubezpieczeń Społecznych podlega DORA, jednak jako podmiot sektora finansów publicznych i realizujący zadania publiczne będzie miał nakładane dodatkowe wymagania. Każda sprzeczność, a nawet tylko niejasność przepisów będzie prowadziła do problemów.	
140.	Związku Pracodawców Technologii	Uwaga ogólna	Oszacowanie kosztów wdrożenia w OSR Naszym zdaniem brakuje realnego oszacowania kosztów wdrożenia ustawy przez podmioty kluczowe i ważne. Wstępna ocena samej pracy papierowej związanej z przygotowaniem do realizacji zadań kierownika podmiotu kluczowego lub ważnego wymienionych w art. 8d (pomijając punkt 4) czyli	Wyjaśnienie uwagi Bardzo trudno jest oszacować koszty wdrożenia ustawy z uwagi na liczbę

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

	Cyfrowych Lewiatan		szkolenia) będzie kosztowała średnio przynajmniej dziesięć tysięcy złotych. Podkreślamy, że jest to bardzo konserwatywne wyliczenie, ponieważ w podmiotach powyżej 250 pracowników i dodatkowo nadzorowanych innymi przepisami taki proces przygotowawczy będzie kosztował nawet kilkaset tysięcy złotych. Jeśli nawet pominiemy podmioty sektora publicznego, które mają otrzymać dodatkowe wsparcie w wysokości ok. 1,5 mld złotych pochodzących z KPO to koszt dla pozostałych przedsiębiorstw będzie wynosił przynajmniej 100 milionów złotych. Chcemy dobitnie podkreślić, że nie są to kwoty wydane na podniesienie cyberbezpieczeństwa, ale na papierologię. Takie informacje i uczciwa kalkulacja powinna znaleźć się w OSR. W optymalnym przypadku razem z informacją w jaki sposób rząd zamierza ograniczyć wydatki na takie działania.	podmiotów oraz zróżnicowaną wielkość a także brak danych.
141.	Związku Pracodawców Technologii Cyfrowych Lewiatan	Uwaga ogólna	Koncentracja na systemie sprawozdawczym cyberbezpieczeństwa. Brak zasadniczych elementów cyberbezpieczeństwa w treści ustawy. Wydaje się, że projekt ustawy zbyt koncentruje się na części formalnej i sprawozdawczej. Szczegółowo opisywane są procedury, a nawet zasady naliczania kary pieniężnej jakiej może podlegać kierownik podmiotu kluczowego lub ważnego w proporcji do wynagrodzenia „obliczanego według zasad obowiązujących przy ustalaniu ekwiwalentu pieniężnego za urlop” (art. 73a), a jednak zasadniczym celem jest podniesienie poziomu cyberbezpieczeństwa, a nie „sprawozdawczości w cyberbezpieczeństwie”. Należy przy tym zauważyć, że zasady cyberbezpieczeństwa są podane w sposób bardzo ogólny w artykule 8, zaś bez jednoczesnej analizy aktów wykonawczych, o których mówi art. 8a trudno cokolwiek powiedzieć. Apelujemy o jak najszybsze przedstawienie projektów rozporządzeń, o których mówi ten artykuł, także w kontekście zmian innych aktów prawnych, o których mówiliśmy powyżej. W szczególności chcemy zwrócić uwagę na brak w treści ustawy zagadnień zapisanych w motywie (89) Dyrektywy NIS2 takich jak: • Zasada Zerowego Zaufania (Zero Trust) • Segmentacja sieci • Zarządzanie tożsamością i dostępem Uważamy za właściwe, aby te zapisy znalazły się – podobnie jak zapisy dotyczące aktualizacji oprogramowania - w ustawie.	Wyjaśnienie uwagi Wskazane w motywie 89 zagadnienia zgodnie z Dyrektywą stanowią elementy cyberhigieny, do której odnosi się także art. 8 projektu. Rozporządzenia będą miały charakter fakultatywny, ponieważ każdy sektor ma swoje odrębne uwarunkowania i wprowadzenie tych samych szczegółowych wytycznych SZBI dla podmiotów jest niezasadne.
142.	Związku Pracodawców Technologii Cyfrowych Lewiatan	Uwaga ogólna	Obecność outsourcingu informatycznego lub wykorzystania chmury obliczeniowej, w tym świadczonego z zagranicy Wydaje się, że przy projektowaniu ustawy przewidziano tylko jeden rodzaj przetwarzania w jednym rodzaju podmiotów. Zapisy są dopasowane do sytuacji, w której podmiot nadzorowany jest podmiotem działającym wyłącznie na terenie Polski i niebędącym częścią żadnej grupy przedsiębiorstw oraz przetwarzającym swoje dane wyłącznie w infrastrukturze własnej na terenie Polski.	Wyjaśnienie uwagi W takich przypadkach polski organ właściwy do spraw cyberbezpieczeństwa będzie mógł się zwrócić o pomoc do organu innego państwa członkowskiego UE, jeżeli podmiot świadczy usługi na terenie UE.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			Poniżej przedstawić chcemy – na przykładzie kilku scenariuszy związanych ze sprawowaniem nadzoru opisanych w art. 53a – 53d – jak najbardziej realne scenariusze: • Polski podmiot kluczowy/ważny będący częścią grupy międzynarodowej przetwarza dane w infrastrukturze grupy poza Polską • Polski podmiot kluczowy/ważny przetwarza u polskiego dostawcy chmury (centrum przetwarzania danych znajduje się w Polsce) współdzieląc zasoby tego dostawcy • Polski podmiot kluczowy przetwarza u dostawcy chmury w CPD poza Polską • Europejski podmiot kluczowy przetwarza u dostawcy chmury spoza Polski, ale w CPD znajdującym się na terenie Polski • Polski podmiot korzysta z outsourcingu informatycznego świadczonego poza Polską przez podmiot ważny (w Polsce, zgodnie z uksc taki podmiot zakwalifikowany byłby jako podmiot kluczowy) • Polski podmiot kluczowy sektora finansowego (podlegający DORA) wykorzystuje kluczowego zewnętrznego dostawcę ICT wyznaczonego przez Europejskie Urzędy Nadzoru (patrz art. 31-32 DORA) Oczywiście w tym przypadku należy także rozważyć elementy związane ze sprawowaniem nadzoru zwłaszcza opisanymi w art. 53d. Czy urzędnik monitorujący uda się za granicę aby bez przepustki poruszać się po terenie podmiotu kluczowego i przeprowadzać oględziny urządzeń, nośników i systemów informacyjnych? Czy urzędnik monitorujący z innego kraju UE będzie mógł wkroczyć bez przepustki na teren CPD na terenie Polski i dokonywać oględzin? Jak takie oględziny związane z prewencyjną kontrolą podmiotu X będą wyglądały u dostawcy chmury obliczeniowej, gdzie przetwarzają także podmioty Y i Z? A może także podmiot U, który nie jest polskim podmiotem? Wreszcie jak wygląda odpowiedzialność w przypadku kiedy urzędnik monitorujący dokonując oględzin doprowadzi do incydentu bezpieczeństwa, zwłaszcza kiedy przetwarzanie będzie miało miejsce w infrastrukturze innego podmiotu, a incydent dotyczy podmiotu trzeciego, niebędącego przedmiotem kontroli? Uważamy, że projekt uksc powinien być bardzo dokładnie przejrany pod kątem różnych scenariuszy przetwarzania, tak aby oddawał rzeczywistość technologiczną, a także relacje nadzoru opisane w innych aktach prawnych powiązanych z Dyrektywą NIS 2 (Dyrektywa CER, DORA, EHDS, CRA). Patrz także uwagi do art. 10, do art. 33 ust. 9 oraz art. 53d	
143.	Związku Pracodawców Technologii Cyfrowych Lewiatan	Uwaga ogólna	Postulujemy wykorzystywać w całej ustawie jednolitą nomenklaturę z wykorzystaniem zdefiniowanych pojęć „produkt ICT”, „proces ICT” i „usługa ICT” (art. 1 pkt 11h-11j). W tekście ustawy często używa się tych pojęć, niekiedy nawet nimi zastępuje pojęcia z aktualnej wersji ustawy, jednak pojawiają się ciągle równoległe określenia „sprzętu i oprogramowania” (przykład: art. 8, nawet sąsiadują ze sobą w pkt 4)	Wyjaśnienie uwagi Relacje między pojęciami produkt ICT, usługa ICT oraz proces ICT, a pojęciem sprzętu i oprogramowania zostały precyzyjnie określone w ustawie. W efekcie użycie tych pojęć nie powoduje wątpliwości interpretacyjnych.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

144.	Polska Izba Informatyki i Telekomunikacji	Art. 1	Nowelizacja w art. 1 ust. 8 projektu (art. 5 uksc) znacząco rozszerza zakres podmiotowy dotychczasowej regulacji, nakładając nowe obowiązki na wiele podmiotów, które dotychczas jej nie podlegały np. podmioty z sektorów infrastruktury cyfrowej, zarządzania usługami ICT, a także usług cyfrowych. Wskazania te nie przewidują żadnych wyłączeń dla przypadków świadczenia tych usług przez jedną ze spółek z grupy kapitałowej wyłącznie na rzecz innych spółek z tej samej grupy. Jednocześnie taki sposób organizacji działalności IT w polskich grupach kapitałowych jest powszechny i sprzyja ich profesjonalizacji oraz jakości - pozwala to na utrzymanie wysokiego poziomu kwalifikacji specjalistów zatrudnianych przez jeden podmiot z grupy, specjalizujących się w zarządzaniu poszczególnymi systemami ICT, w tym cyberbezpieczeństwem. Objęcie podmiotów świadczących usługi ICT i cyberbezpieczeństwa wyłącznie na rzecz swoich grup kapitałowych jest sprzeczne z celem regulacji i może spowodować znaczące pogorszenie poziomu cyberbezpieczeństwa polskich przedsiębiorstw. Wysokie koszty dostosowania do wymogów regulacyjnych, będą zachęcały przedsiębiorców do likwidacji wewnętrznych usług ICT poprzez likwidację centrów kompetencyjnych i przenoszenie zadań związanych z zarządzaniem systemami ICT i cyberbezpieczeństwa do każdego z podmiotów w grupie kapitałowej. Spowoduje, to że zamiast wysoko kompetentnych fachowców specjalizujących się w poszczególnych obszarach cyberbezpieczeństwa i ICT, będą zatrudniani niewyspecjalizowani pracownicy, których zakres zadań będzie nadmiernie szeroki, a zagadnienia dot. cyberbezpieczeństwa będą tylko jednym z wielu ich obowiązków. W związku z tym, w naszej opinii, wszystkie definicje dodawane w projektowanym art. 2, dotyczące dostawców usług (od pkt 4b do pkt 4i) powinny zostać zmodyfikowane w taki sposób, żeby odnosiły się tylko do podmiotów, które świadczą wskazane usługi w sposób publicznie dostępny. Ewentualnie powinno zostać dodane wyłączenie, które wskaże, że w zakres definicji świadczenia usług nie będą wchodziły usługi świadczone na rzecz jednostek powiązanych z dostawcą w rozumieniu ustawy o rachunkowości z dnia 29 września 1994 r. Podobny problem dotyczy wskazania jako podmiotów kluczowych przedsiębiorców telekomunikacyjnych oraz podmiot świadczących usługi komunikacji interpersonalnej niewykorzystujące numerów. Przy zaproponowanych szerokich definicjach przedsiębiorcy komunikacji elektronicznej oraz przedsiębiorcy telekomunikacyjnego polska ustawa implementująca wychodzi znacząco ponad wskazania zawarte w NIS 2, która wskazuje w swoim Załączniku I jako sektory kluczowe jedynie dostawców publicznych sieci łączności elektronicznej oraz dostawców publicznie dostępnych usług łączności elektronicznej. Tutaj również współpraca w ramach Grupy powoduje, że zgodnie z definicją europejską, nawet jeżeli jedno z przedsiębiorstw osiąga status średniego przedsiębiorcy, wpływa on na pozostałe podmioty. Tym samym nawet jeżeli działalność telekomunikacyjna niektórych podmiotów grupie jest marginalna – muszą one wdrożyć stosowne obowiązki. Aby zapewnić zgodność z wprowadzaną dyrektywą należy w szczególności zmodyfikować zaproponowaną definicję przedsiębiorcy telekomunikacyjnego w ten sposób, że powinna ona oznaczać jedynie przedsiębiorcę telekomunikacyjnego w rozumieniu art. 2 pkt 27	Wyjaśnienie uwagi Dyrektywa NIS2 nie rozróżnia grup kapitałowych.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne, który świadczy publicznie dostępne usługi telekomunikacyjne. Dodatkowo, postulujemy, aby wielkość przedsiębiorstwa określać na podstawie jego przychodów bezpośrednio z działalności telekomunikacyjnej a nie całości przez nie generowanych.	
145.	Polska Izba Informatyki i Telekomunikacji	Art. 2	W celu zwiększenia komunikatywności ustawy postulujemy sformułowanie definicji użytych w niej pojęć, w taki sposób, by nie ograniczały się one do odsyłania czytelnika do konkretnych jednostek redakcyjnych w aktach unijnych, w których zawarte są inne definicje. O ile jest możliwe dokonanie tego w sposób nieprowadzący do zniekształcenia znaczenia poszczególnych pojęć, proponujemy powtórzenie definicji unijnych w ustawie. Za niepożądane należy uznać zmuszanie adresatów norm ustawowych do odtwarzania ich treści poprzez odwoływanie się do innych aktów prawnych. Jednocześnie proponujemy przemyślenie zastąpienia terminu „ICT” bardziej poprawnym terminem „teleinformatyka” (i konsekwentnie „procesu ICT” - „procesem teleinformatycznym”, „produktu ICT” - „produktem teleinformatycznym” itd.).	Uwaga nieuwzględniona W przypadku definicji pochodzących z aktów prawa unijnego bezpośrednio stosowalnych nie możemy ich powtarzać tylko odwołać się do przepisów.
146.	Polska Izba Informatyki i Telekomunikacji	Art. 2	Art. 2 pkt 3c – bezpieczeństwo systemów informacyjnych Nowa definicja bezpieczeństwa systemów informacyjnych określa je jako: odporność systemów informacyjnych na zdarzenia naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy. Odpowiednia definicja w dyrektywy NIS2 wskazuje natomiast, że <i>bezpieczeństwo sieci i systemów informatycznych</i> oznacza odporność sieci i systemów informatycznych, przy danym poziomie zaufania, na wszelkie zdarzenia, które mogą naruszyć dostępność, autentyczność, integralność lub poufność przechowywanych, przekazywanych lub przetwarzanych danych lub usług oferowanych przez te sieci i systemy informatyczne lub dostępnych za ich pośrednictwem Różnica polega w szczególności na pominięciu w krajowej definicji zwrotu „przy danym poziomie zaufania”. Zmieniono także kolejność wylistowania atrybutów bezpieczeństwa. W pierwszej kolejności wnosimy o wyjaśnienie dla dokonania takich modyfikacji wobec dyrektywy NIS2, szczególnie, że w samym uzasadnieniu wskazano, że <i>Wprowadzone zmiany zapewnią spójność siatki pojęciowej wykorzystywanych we wszystkich krajach Unii Europejskiej</i> . Pominięcie w definicji stwierdzenia „na danym poziomie pewności” zmienia istotę tego wymagania i może nie pozostawać bez wpływu na zakres obowiązków dostawcy usług, a w konsekwencji może również wpłynąć na zakres jego odpowiedzialności. Z tego względu wnioskujemy o uzupełnienie tego braku.	Uwaga nieuwzględniona W przypadku definicji pochodzących z aktów prawa unijnego bezpośrednio stosowalnych nie możemy ich powtarzać tylko odwołać się do przepisów.
147.	Polska Izba Informatyki i Telekomunikacji	Art. 2	Dyrektywa NIS2 nie definiuje terminu „organu zarządzającego”, a jedynie wykorzystuje go w ramach trzech odniesień, które dotyczą wymagań w zakresie zarządzania. Tymczasem w projekcie przedstawionym przez Ministerstwo Cyfryzacji (art. 2 pkt 8a) określenie „organ zarządzający” zostało zastąpione terminem „kierownik jednostki” z bezpośrednim odwołaniem interpretacyjnym do art. 3 pkt 6 ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2023 r. poz. 120, 295 i 1598), co sprawia, że przepisy interpretacji mają swoje zastosowanie nie tylko wobec członków	Uwaga nieuwzględniona Odwołanie do kierownika jednostki ma zapewnić klarowne wskazanie kogo dotyczą obowiązki z zakresu cyberbezpieczeństwa w podmiocie.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			zarządu danego podmiotu, ale także osób odpowiedzialnych (w danym momencie) za zarządzanie tym podmiotem. Wydaje się, że nie było to intencją twórców Dyrektywy.	
148.	Polska Izba Informatyki i Telekomunikacji	Art. 2	Art. 2 pkt 11e - potencjalne zdarzenie dla cyberbezpieczeństwa <i>11e) potencjalne zdarzenie dla cyberbezpieczeństwa – zdarzenie, które może mieć niekorzystny wpływ na bezpieczeństwo systemów informacyjnych</i> Zauważamy, że definicja jest odmienna od definicji zawartej w NIS2. W szczególności pominięto w niej wskazanie, że jest to zdarzenie „któremu udało się jednak zapobiec lub które jednak nie wystąpiło;”.	Uwaga uwzględniona
149.	Polska Izba Informatyki i Telekomunikacji	Art. 2	Art. 2 pkt 12 - definicja ryzyka <i>12) ryzyko - kombinację prawdopodobieństwa wystąpienia zdarzenia niepożądanego i jego konsekwencji;</i> Zauważamy, że aktualna definicja używa niezdefiniowanego pojęcia „zdarzenia niepożądanego”. Jest też odmienna od definicji ryzyka z NIS2 używającej pojęć zdefiniowanych: „ryzyko” oznacza możliwość wystąpienia strat lub zakłóceń spowodowanych incydem, wyrażoną jako wypadkową wielkości takiej straty lub takich zakłóceń oraz prawdopodobieństwo wystąpienia takiego incydemu;	Wyjaśnienie uwagi Definicja ryzyka pochodzi z obecnej ustawy KSC i chcemy ją zachować dla zapewnienia ciągłości.
150.	Polska Izba Informatyki i Telekomunikacji	Art. 2	Art. 2 pkt 14 – system informacyjny W definicji systemu informacyjnego dodawane jest sformułowanie „urządzenie lub grupę połączonych urządzeń elektrycznych lub elektronicznych i oprogramowania zaprogramowanych w celu przetwarzania danych”. W uzasadnieniu wskazano, że intencją jest przesądzenie objęcia definicją systemów OT. Taka redakcja powoduje jednak, że jako system informacyjny może być klasyfikowany także pojedyncze urządzenie, jak np. laptop czy telefon, które wydają się same w sobie nie wyczerpywać pojęcia „systemu”. Wnosimy o ponowne rozważenie tej kwestii.	Wyjaśnienie uwagi NIS2 odnosi się także do samego urządzenia: „‘network and information system’ means: (a) an electronic communications network as defined in Article 2, point (1), of Directive (EU) 2018/1972; (b) any device or group of interconnected or related devices, one or more of which, pursuant to a programme, carry out automatic processing of digital data;
151.	Akademia Górniczo-Hutnicza	Art. 2	Art. 2 pkt 3c – bezpieczeństwo systemów informacyjnych Nowa definicja bezpieczeństwa systemów informacyjnych określa je jako: odporność systemów informacyjnych na zdarzenia naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy. Odpowiednia definicja w dyrektywy NIS2 wskazuje natomiast, że <i>bezpieczeństwo sieci i systemów informatycznych</i> ” oznacza odporność sieci i systemów informatycznych, przy danym poziomie zaufania, na wszelkie zdarzenia, które mogą naruszyć dostępność, autentyczność, integralność lub	Uwaga uwzględniona Stworzony zostanie sektor, w którym będą zarówno organizacje badawcze jak i uczelnie publiczne.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			<i>poufność przechowywanych, przekazywanych lub przetwarzanych danych lub usług oferowanych przez te sieci i systemy informatyczne lub dostępnych za ich pośrednictwem</i> Różnica polega w szczególności na pominięciu w krajowej definicji zwrotu „przy danym poziomie zaufania”. Zmieniono także kolejność wylistowania atrybutów bezpieczeństwa. W pierwszej kolejności wnosimy o wyjaśnienie dla dokonania takich modyfikacji wobec dyrektywy NIS2, szczególnie, że w samym uzasadnieniu wskazano, że <i>Wprowadzone zmiany zapewnią spójność siatki pojęciowej wykorzystywanych we wszystkich krajach Unii Europejskiej.</i> Pominięcie w definicji stwierdzenia „na danym poziomie pewności” zmienia istotę tego wymagania i może nie pozostawać bez wpływu na zakres obowiązków dostawcy usług, a w konsekwencji może również wpłynąć na zakres jego odpowiedzialności. Z tego względu wnioskujemy o uzupełnienie tego braku.	
152.	Amerykańska Izba Handlowa w Polsce	Art. 2	Zgodnie z definicją zawartą w art. 1 pkt 2 lit. e projektu, poważny incydent to incydent, który wpływa na inne podmioty powodując szkodę materialną lub niematerialną. Stanowi to rozbieżność z art. 23 ust. 3 lit. b dyrektywy NIS2, zgodnie z którym incydent poważny to taki, który „wpłynął lub jest w stanie wpłynąć na inne osoby fizyczne lub prawne, powodując znaczne szkody majątkowe i niemajątkowe”;	Uwaga uwzględniona Definicja incydentu poważnego zostanie poprawiona.
153.	Amerykańska Izba Handlowa w Polsce	Art. 2	Zgodnie z definicją zawartą w art. 1 pkt 2 lit. m projektu, który wprowadza do uksc art. 2 pkt 20, poważne zagrożenie cybernetyczne to zagrożenie cybernetyczne, które ze względu na swoje cechy techniczne może mieć poważny wpływ na bezpieczeństwo systemów informatycznych powodując szkodę materialną lub niematerialną. Stanowi to rozbieżność z art. 6 pkt 11 dyrektywy NIS 2, który znaczne zagrożenie cybernetyczne definiuje jako takie, które w szczególności może wywrzeć znaczący wpływ na sieć i systemy informatyczne danego podmiotu lub użytkowników, korzystających z usług tego podmiotu, powodując i znaczne szkody majątkowe lub niemajątkowe;	Uwaga uwzględniona Definicja zostanie poprawiona.
154.	Amerykańska Izba Handlowa w Polsce	Art. 2	Dyrektywa NIS 2 nie definiuje terminu „organu zarządzającego”, a jedynie wykorzystuje go w ramach trzech odniesień, które dotyczą wymagań w zakresie zarządzania. Tymczasem we wprowadzanym przez projekt art. 2 pkt 8a ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (dalej: uksc) określenie „organ zarządzający” zostało zastąpione terminem “kierownik jednostki” z bezpośrednim odwołaniem interpretacyjnym do art. 3 pkt 6 ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2023 r. poz. 120, 295 i 1598), co sprawia, że przepisy oparte na wprowadzonej definicji mają swoje zastosowanie nie tylko wobec członków zarządu danego podmiotu, ale także nadmiernie rozszerzają swój zakres stosowania również na osoby odpowiedzialne (w danym momencie) za zarządzanie tym podmiotem.⁹	Wyjaśnienie uwagi Zdaniem projektodawcy istnieje konieczność doprecyzowania pojęcia organu zarządzającego z dyrektywy NIS2. Wprowadzono odwołanie do pojęcia kierownika jednostki z ustawy o rachunkowości, aby objąć wszystkie osoby faktycznie zarządzające danym podmiotem.
155.	Osoba fizyczna	Art. 2	1. Art.2 (słownik pojęć stosowany w ustawie) Zapisy zawierają wiele wskazanie lub odwołanie do wielu bytów organizacyjnych, procesowych, technicznych itp., które nie zostały zdefiniowane, co powoduje brak zrozumienia lub niewłaściwe zrozumienie ich sensu i natury, jak też natury przepisów ustawy i wprowadzanych rozwiązań, w związku czym:	Wyjaśnienie uwagi Definicja ryzyka jest wzorowana na definicji ryzyka z ustawy o ochronie informacji niejawnych. Zakresowo obejmuje ona definicję ryzyka ujętą w NIS2.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			1.1. Pojęcia dotyczące ryzyka - Stosowane w ustawie uKSC2 definicje pojęć dotyczących ryzyka są niedookreślone, szczególnie w kontekście cyberbezpieczeństwa, brakuje wyjaśnienia pojęć, które pojawiają się w zapisach ustawy, np. analiza ryzyka zdaje się, że jest miejscami zamiennie stosowana z szacowaniem ryzyka, co zmienia kontekst i zakres wymaganych działań. Należy przyjąć, że analiza ryzyka jest podprocesem w procesie szacowania ryzyka, a szacowanie jest podprocesem w procesie zarządzania ryzykiem (re. def. 13). Proponuję wprowadzić szereg pojęć dotyczących ryzyka, wprowadzonych zapisami, lecz nie wyjaśnionych: 1.1.1. ryzyko – zgodnie z ISO 27005, ISO 31000 1.1.2. ryzyko w zakresie cyberbezpieczeństwa (stosowane) lub ryzyko cyberbezpieczeństwa – definicja ryzyka odniesiona do cyberbezpieczeństwa, 1.1.3. analiza ryzyka – zgodnie z ISO 27005, ISO 31000, 1.1.4. analiza ryzyka cyberbezpieczeństwa – definicja analizy ryzyka odniesiona do cyberbezpieczeństwa, 1.1.5. szacowanie ryzyka cyberbezpieczeństwa - definicja szacowania ryzyka odniesiona do cyberbezpieczeństwa, 1.1.6. poziom ryzyka - zgodnie z ISO 27005, ISO 31000 1.1.7. poziom ryzyka cyberbezpieczeństwa - definicja poziomu ryzyka odniesiona do cyberbezpieczeństwa, 1.1.8. zarządzanie ryzykiem cyberbezpieczeństwa – definicja zarządzania ryzykiem odniesiona do cyberbezpieczeństwa, 1.1.9. dynamiczna analiza ryzyka lub, co bardziej właściwe, dynamiczne szacowanie ryzyka (ref. Art. 26 ust.3, art. 44 ust.1b),	Naszym zdaniem nie ma potrzeby definiowania tych pojęć należy je rozumieć przez pryzmat znaczenia słownikowego, ew. poprzez wiedzę specjalistyczną.
156.	Związku Pracodawców Technologii Cyfrowych Lewiatan	Art. 2	Definicja dostawcy chmury (art. 2 pkt 4e) Uwaga 1: Dyrektywa NIS2 wprowadza definicję usług chmurowych (art. 6 p. 30), natomiast dostawca chmury (dostawca usług chmurowych) nie jest dalej definiowany. Wydaje się to właściwym podejściem. Uwaga 2: Rekomendujemy określenie „dostawca chmury” lub „dostawca chmury obliczeniowej”, ponieważ de facto zamawiający korzystają z predefiniowanych i prekonfigurowanych produktów, którymi samodzielnie zarządzają, używają i dostosowują przy minimalnym udziale dostawcy. Oferta chmurowa jako model jest podobna do oprogramowania z półki, w odróżnieniu od oferty outsourcingu, która jest bliższa oprogramowaniu tworzonemu na zamówienie, co wymaga bezpośredniego i dedykowanego zaangażowania usługodawcy. Widać to również w przypadku zamówień publicznych, w których dochodzi do dostawy produktów chmurowych. Uwaga 3: Rekomendujemy dokonaniu ujednolicenia pojęć związanych z chmurą obliczeniową w uksc, ustawie o informatyzacji, Rozporządzeniu Krajowe Ramy Informatyzacji oraz uchwale WIIP, a także innych aktach prawnych takich jak ustawa o obszarach morskich Rzeczypospolitej (patrz art. 2	Uwaga częściowo uwzględniona Dyrektywa NIS2 odrębnie definiuje „podmiot” (entity) i daną usługę. W nowelizacji zostało to połączone, zważywszy, że załącznik do NIS2 wskazuje na rodzaje podmiotów, a nie usługi. Wprowadzone zostanie pojęcie dostawcy chmury obliczeniowej.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			projektu uksc). Będzie to dotyczyło także kolejnych planowanych aktów prawnych oraz rekomendacji jak np. ustawa wdrażająca dyrektywę CER, nadchodzące wdrożenia Data Act i AI Act, czy oczekiwane zmiany w komunikacie chmurowym KNF.	
157.	Związku Pracodawców Technologii Cyfrowych Lewiatan	Art. 2	Definicja dostawcy usługi ośrodka przetwarzania danych (art. 2 pkt 4g) Uwaga 1: definicja w Dyrektywie NIS2 mówi o usłudze ośrodka przetwarzania danych, a nie o dostawcy. Proponujemy pozostawienie tego jak najbliższej wersji oryginalnej. Uwaga 2: Proponujemy określenie „centrum przetwarzania danych”, które przyjęło się już w nomenklaturze, np. ustawa dot. budowy Krajowego Centrum Przetwarzania Danych Uwaga 3: Definicja w projekcie posługuje się pojęciem „scentralizowanego hostingu”, które nigdzie nie jest zdefiniowane. Czy to oznacza, że prawodawca świadomie ogranicza działanie uksc tylko do tych podmiotów, które świadczą usługę „scentralizowanego hostingu”, a nie dotyczy to wszelkich innych form wykorzystywania centrów przetwarzania danych?	Uwaga częściowo uwzględniona Dyrektywa NIS2 odrębnie definiuje „podmiot” (entity) i daną usługę. W nowelizacji zostało to połączone, zważywszy, że załącznik do NIS2 wskazuje na rodzaje podmiotów, a nie usługi. Wprowadzone zostanie pojęcie centrum przetwarzania danych, a nie ośrodka przetwarzania danych.
158.	CyberMadeinPoland	Art. 2	W Art.1 niniejszej ustawy w odniesieniu do art.2 zmienianej ustawy w dodanym punkcie 3 c) zawierającym definicję bezpieczeństwa systemów informatycznych proponuje się pozostawić jedynie trzy kardynalne atrybuty bezpieczeństwa (poufność, integralność, dostępność) wykreślając atrybut pomocniczy „autentyczność” jako zawierający się zgodnie z definicją ISO w atrybucie „integralność”	Uwaga nieuwzględniona Podtrzymujemy odniesienie się do autentyczności.
159.	CyberMadeinPoland	Art. 2	W dodanym punkcie 11 b) zawierającym definicję podmiotu publicznego wskazano błędnie tytuł ustawy („ustawa w sektorze administracji publicznej” nie istnieje)	Wyjaśnienie uwagi To nie jest odwołanie do ustawy tylko odwołanie do załącznika nr 1 w ustawie.
160.	CyberMadeinPoland	Art. 2	Art. 2 p. 4h, 4i - doprecyzowanie definicji, ponieważ w obecnej postaci są dla nas niezrozumiałe oraz w szczególności mogą wykluczać podmioty, które de facto świadczą usługi z zakresu cyberbezpieczeństwa, ale nie dostarczają produktów ICT. Warto również doprecyzować czy chodzi tylko o dostawców dla podmiotów kluczowych. Zgodnie z przedstawioną definicją, dostawcą usług zarządzanych w zakresie cyberbezpieczeństwa jest też osoba prowadząca JDG i staje się ona podmiotem kluczowym	Wyjaśnienie uwagi Nie możemy doprecyzować, że chodzi tylko o dostawców MSP/MSSP dla podmiotów kluczowych, ponieważ sama dyrektywa NIS2 tego nie zawęża. W przypadku MSSP – tak, chodzi o podmioty świadczące usługi z zakresu cyberbezpieczeństwa. Natomiast możliwe jest wyłączenie z zakresu podmiotowego mikroprzedsiębiorców.
161.	CyberMadeinPoland	Art. 2	Art. 2 p. 11f) - doprecyzowanie sformułowania “niewykorzystującej numerów” - jeśli chodzi o numery telefonu, to warto uwzględnić komunikatory, które bazują również na numerach telefonów ale nie są telefonią komórkową.	Wyjaśnienie uwagi Pojęcie to pochodzi z dyrektywy 2018/1972 ustanawiającej Europejski Kodeks Łączności Elektronicznej. Chodzi o usługi komunikacji elektronicznej niewykorzystującej numerów - OTT-1 –

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

				czyli usługi, które są pewną konkurencją dla tradycyjnej telekomunikacji jak poczta elektroniczna czy komunikatory internetowe.
162.	CyberMadeinPoland	Art. 2	Dodatkowo pytanie dot. definicji dostawcy usług zarządzalnych cyberbezpieczeństwa: Dostawca usług zarządzanych, który świadczy usługi związane z zarządzaniem ryzykiem w zakresie cyberbezpieczeństwa lub zapewnia pomoc dla tych działań;" Czym jest zapewnienie pomocy dla tych działań? Jeśli dostarczamy platformę CyberSecurity Awarness, a produkt ten jest konfigurowany samodzielnie przez klienta to czy świadczenie wsparcia technicznego dla tego produktu jest „pomocą” wedle wskazanej definicji? Czy systemy klasy ITAM albo HelpDesk i wsparcie techniczne do takich produktów również wpisuje się w ramy tej definicji? Te produkty są wykorzystywane w procesie analizy ryzyka (inwentaryzacja aktywów) oraz zarządzania incydem (odpowiednia konfiguracja, dokumentacja i obsługa incydentu).	Wyjaśnienie uwagi Usługi typu HelpDesk należy kwalifikować jako usługę dostawcy usług zarządzanych ICT (Managed Services Providers, MSP). Usługa wsparcia technicznego mieści się w pojęciu MSP.
163.	Związek Pracodawców Technologii Cyfrowych Lewiatan	Art. 2	Definicje dostawcy usług zarządzanych i dostawcy usług zarządzanych w zakresie cyberbezpieczeństwa (art. 2 pkt 4h oraz 4i) Czy każde przedsiębiorstwo świadczące usługi supportu technicznego (także darmowe) staje się dostawcą usług zarządzanych, a jeśli w jakikolwiek sposób taka usługa dotyczy elementów związanych z cyberbezpieczeństwem to staje się dostawcą usług zarządzanych w zakresie cyberbezpieczeństwa? Jak działa ustawa w sytuacji kiedy taki support techniczny jest outsourcowany do podmiotu trzeciego? Czy to oznacza, że podmiot trzeci powinien być uświadomiony przez dostawcę produktu ICT, że staje się dostawcą usług zarządzanych? Jak działa ustawa jeśli podmiot świadczący usługi supportu technicznego jest podmiotem zagranicznym? W przypadku szczególnym, np. wsparcia technicznego na najwyższym poziomie, takiego supportu mogą udzielać osoby spoza Unii Europejskiej. Definicje te stają się szczególnie istotne w świetle art. 8h, jeśli dostawca produktu ICT lub usługi ICT dla podmiotu kluczowego/ważnego także jest podmiotem kluczowym/ważnym. W szczególności zapisy umów suportowych mogą wykluczać niektóre działania obu stron, które zostały zapisane w art. 8h	Wyjaśnienie uwagi Każde przedsiębiorstwo świadczące usługi wsparcia technicznego IT będzie Managed Services Providers. Dotyczy to także sytuacji, gdy usługi te są outsourcowane do podmiotu trzeciego. Zgodnie z NIS2 podmiot spoza UE działający na terenie UE musi wyznaczyć swojego przedstawiciela na terytorium UE.
164.	CyberMadeinPoland	Art. 2	Ad. “pytanie dot. definicji dostawcy usług zarządzalnych cyberbezpieczeństwa” - czy wsparcie w postaci doradztwa w zakresie wyboru metodyki oceny analizy ryzyka oraz jej przeprowadzenia oraz innego rodzaju doradztwo (np. przy wdrożeniu NIS 2) jest kwalifikowane jako usługa zarządzalna cyberbezpieczeństwa? Ad. „Spełnienie wymogów norm PN-EN ISO/IEC 27001 oraz PN-EN ISO/IEC 22301 jest równoznaczne ze spełnieniem wymogów z tego artykułu.” - czy spełnienie wymogów musi być potwierdzone certyfikatem, czy wystarczy, że system jest wdrożony i działa wg. deklaracji podmiotu.	Wyjaśnienie uwagi Zostanie wprowadzony przepis, zgodnie z którym usługi konsultingowe nie wchodzą w zakres pojęcia dostawcy usług zarządzanych w zakresie cyberbezpieczeństwa.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

165.	Federacja Przedsiębiorców Polskich	Art. 2	W art. 2 po punkcie 14 dodaje się punkt 14a w brzmieniu: <i>funkcje krytyczne – oznaczają funkcje zawarte w wykazie kategorii funkcji oraz komponentów krytycznych dla bezpieczeństwa sieci i usług których mowa w art. 67c ust. 2, które są krytyczne dla bezpieczeństwa produktów ICT, usług ICT i procesów ICT;</i> Wskazane w decyzji zakresy produktów ICT, rodzaje usług ICT lub konkretne procesy ICT o funkcjach krytycznych, pochodzące od dostawcy wysokiego ryzyka, zagrażające bezpieczeństwu kluczowych podmiotów w Polsce, będą musiały być wycofane z tych podmiotów. Produkty, usługi i procesy o funkcjach krytycznych, które zostaną wskazane do wycofania, będą precyzyjnie określone, co pozwoli na minimalizację zakresu wycofania i w konsekwencji znacząco ograniczy koszty społeczne i gospodarcze takiej decyzji. Wycofane z eksploatacji będą musiały być tylko wskazane produkty, usługi i procesy o funkcjach krytycznych, a nie wszystkie, co ograniczy znacząco koszty społeczne i gospodarcze takiej decyzji. Brak precyzyjnej definicji „funkcji krytycznych” w ustawie KSC stanowi poważne niedoprecyzowanie, które może prowadzić do niejasności interpretacyjnych oraz problemów praktycznych w procesie wycofywania zagrożonych produktów, usług i procesów. Dotychczasowa wersja ustawy KSC zawiera słowniczek pojęć używanych w tej ustawie, jednak brakowało w nim kluczowego terminu, jakim są „funkcje krytyczne”. Koniecznym więc było zdefiniowanie określenia „funkcje krytyczne” poprzez dodanie w art. 2 tej ustawy kolejnego punktu z tą definicją. Brak precyzyjnej definicji „funkcji krytycznych” w ustawie KSC stanowi poważne niedoprecyzowanie, które może prowadzić do niejasności interpretacyjnych oraz problemów praktycznych w procesie wycofywania zagrożonych produktów, usług i procesów. Dotychczasowa wersja ustawy KSC zawiera słowniczek pojęć używanych w tej ustawie, jednDefinicja „funkcji krytycznych” pozwoli na precyzyjne określenie, które produkty, usługi i procesy ICT są kluczowe dla bezpieczeństwa sieci i usług, a tym samym będą podlegały szczególnym procedurom oceny i ewentualnego wycofania. Takie podejście umożliwi skoncentrowanie działań na elementach, które rzeczywiście mają krytyczne znaczenie dla bezpieczeństwa narodowego, minimalizując jednocześnie niepotrzebne obciążenia dla podmiotów gospodarczych. nWprowadzenie definicji „funkcji krytycznych” jest również zgodne z zaleceniami międzynarodowymi i praktykami stosowanymi w innych krajach, które dążą do zwiększenia poziomu cyberbezpieczeństwa poprzez identyfikację i ochronę kluczowych elementów infrastruktury ICT. Przykładem mogą być rekomendacje zawarte w dokumencie przygotowanym przez Network and Information System Cooperation Group („NISCG”) oraz raport „Cybersecurity of 5G networks EU Toolbox of risk mitigating measures”, które wskazują na potrzebę precyzyjnego określenia krytycznych aktywów („key assets”) i dostosowania środków zaradczych do zidentyfikowanych zagrożeń. Dodatkowo, wprowadzenie definicji „funkcji krytycznych” w ustawie KSC przyczyni się do zwiększenia transparentności i przewidywalności działań administracyjnych, co jest istotne z punktu widzenia zarówno bezpieczeństwa narodowego, jak i praw podmiotów gospodarczych. Transparentność w procesie identyfikacji i oceny funkcji krytycznych oraz podejmowania decyzji o wycofaniu produktów, usług i procesów ICT będzie sprzyjać budowaniu zaufania w relacjach między	Uwaga nieuwzględniona Zaproponowana definicja nie wnosi dodatkowej wartości normatywnej względem proponowanego załącznika nr 3.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			administracją publiczną a podmiotami gospodarczymi, co jest kluczowe dla skutecznego zarządzania ryzykiem w obszarze cyberbezpieczeństwa. Konieczność wprowadzenia tej definicji wynika także z dynamicznego rozwoju technologicznego oraz coraz bardziej złożonego charakteru zagrożeń cyberbezpieczeństwa, które wymagają elastycznego i dobrze zdefiniowanego podejścia do ochrony kluczowych elementów infrastruktury ICT. Definicja „funkcji krytycznych” w ustawie KSC stanowi zatem niezbędny krok w kierunku kompleksowego i efektywnego systemu zarządzania ryzykiem w obszarze cyberbezpieczeństwa w Polsce.	
166.	FORYTEK&P ARTNERZY	Art. 2	Szanowni Państwo, chciałbym w ramach konsultacji zwrócić Państwa uwagę na fakt, że w projekcie ustawy definicja „podmiotu świadczącego usługi rejestracji nazw domen” jest wadliwa. Zgodnie z projektem, definicja ma brzmieć następująco: <i>„podmiot świadczący usługi rejestracji nazw domen – rejestratora lub agenta działającego w imieniu rejestratorów, w tym dostawcę lub odsprzedańcę usług w zakresie rejestracji prywatności lub serwerów proxy”</i> Jest to zasadniczo zbieżne z polską wersją językową Dyrektywy NIS 2. Zwracam natomiast uwagę, że w angielskiej wersji językowej dyrektywy NIS 2, definicja brzmi następująco: ‘entity providing domain name registration services’ means a registrar or an agent acting on behalf of registrars, <u>such as a privacy or proxy registration service provider or reseller;</u> Z powyższego wynika, że w projekcie ustawy (oraz polskiej wersji językowej Dyrektywy NIS 2) wadliwie odniesiono się do usług serwerów proxy, które nie mają wprost związku z rejestracją domen. Usługi proxy oraz privacy, o których mowa w projekcie ustawy i Dyrektywie NIS 2 to usługi świadczone przez podmioty oferujące ochronę danych Abonenta w bazie Whois (https://www.icann.org/resources/pages/privacy-proxy-registration-2013-03-22-en/) Definicje branżowe tych usług wypracowane przez ICANN są następujące: Privacy Services – Privacy services allow a domain name holder (registrant) to be listed as the registrant of record but with alternate, valid contact information (such as a mail-forwarding service address) published in place of the registrant's home address. Proxy Services – Proxy services allow a domain name to keep certain identity and contact details from appearing in public Whois information. The proxy service becomes the registered name holder of record, and its identity and contact information is displayed in Whois data. To w mojej ocenie świadczy o tym, że powyższa definicja wymaga podyfikacji, tak aby w odpowiedni sposób oddawała istotę usług privacy oraz proxy.	Uwaga uwzględniona Przepis zostanie zmieniony.
167.	Fundacja Bezpieczna Cyberprzestrzeń	Art. 2	Proponuje się przepisać definicje wskazywane w odnośnikach do innych aktów prawnych (tam gdzie jest to uzasadnione i nie spowoduje znacznego zwiększenia treści ustawy) np. definicji cyberbezpieczeństwa, cyberzagrożeń, procesu ICT, produktu ICT, usługi ICT i innych. Ułatwi to znakomicie pracę z treścią ustawy i wykluczy możliwość błędnej interpretacji przepisów.	Uwaga nieuwzględniona Projekt posługuje się odesłaniami dynamicznymi do przepisów, które mogą się zmienić. Dlatego nie możemy tego zrobić.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

168.	Fundacja Bezpieczna Cyberprzestrzeń	Art. 2	Art. 1 pkt 2 lit a, zmiana pkt. 3c – proponuje się zachować spójność z nową definicją cyberbezpieczeństwa (działania niezbędne do ochrony sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób przed cyberzagrożeniami), poprzez nadanie punktowi 3c następującego brzmienia: „bezpieczeństwo sieci i systemów informacyjnych – odporność sieci i systemów informacyjnych na zdarzenia naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy;”. Zmiana musi być konsekwentnie powtarzana we wszystkich przepisach odwołujących się lub powtarzających tę definicję np. art. 2 pkt 11e i dalsze.	Uwaga nieuwzględniona Obecna ustawa KSC od 2018 r. odnosi się do pojęcia systemu informacyjnego. Proponowana zmiana byłaby dużą zmianą definicyjną.
169.	Osoba fizyczna	Art. 2	Różna interpretacja definicji (Tryb dokonany i tryb przypuszczający). Projekt ustawy <i>d) pkt 5 otrzymuje brzmienie:</i> „5) incydent – zdarzenie, które ma lub może mieć niekorzystny wpływ na bezpieczeństwo systemów informacyjnych;”, <i>e) pkt 7 i 8 otrzymują brzmienie:</i> „7) incydent poważny – incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi przez podmiot kluczowy lub podmiot ważny, straty finansowe dla tego podmiotu lub wpływa na inne osoby fizyczne, osoby prawne, jednostki organizacyjnej nieposiadające osobowości prawnej poprzez wywołanie szkody materialnej lub niematerialnej Dyrektywa „incydent” oznacza zdarzenie naruszające dostępność, autentyczność, integralność lub poufność przechowywanych, przekazywanych lub przetwarzanych danych lub usług oferowanych przez sieci i systemy informatyczne lub dostępnych za ich pośrednictwem; Uzasadnienie. Wg. Projektu zdarzenia, które nie wywołały wpływu, natomiast mogłyby mieć wpływ są incydentami. Takich zdarzeń w systemach jest setki. Biorąc pod uwagę zapisy Projektu zapis o zgłaszaniu w art. 11: <i>a) w ust. 1:</i> – wprowadzenie do wyliczenia otrzymuje brzmienie: „Podmiot kluczowy i podmiot ważny:”, – w pkt 2 po wyrazie „właściwemu” dodaje się wyrazy „CSIRT sektorowemu”, – pkt 4 otrzymuje brzmienie: „4) zgłasza wczesne ostrzeżenie o incydencie poważnym niezwłocznie, nie później niż w ciągu 24 godzin od momentu jego wykrycia, do właściwego CSIRT sektorowego;”, – po pkt 4 dodaje się pkt 4a–4 c w brzmieniu: „4a) zgłasza incydent poważny niezwłocznie, nie później niż w ciągu 72 godzin od momentu jego wykrycia, do właściwego CSIRT sektorowego;	Uwaga nieuwzględniona Definicja incydentu obowiązuje od 2018 r. i istnieje już ugruntowana praktyka związana z jej stosowaniem. Intencją tej definicji było to, aby zbierane a potem raportowane do CSIRT były zdarzenia potencjalne, dzięki czemu CSIRT może ostrzec pozostałe podmioty o zagrożeniu.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			4b) przekazuje, na wniosek właściwego CSIRT sektorowego, sprawozdanie okresowe z obsługi incydentu poważnego; Może dojść do zgłaszania setek zdarzeń, które nie wywołały wpływu ale mogły i zostały zakwalifikowane jako incydent. Rekomenduje aby Incydent i incydent poważny były w trybie dokonany natomiast to co mogło spowodować zakwalifikować (w trybie przypuszczającym) jako cyberzagrożenie, które jest zdefiniowane „cyberzagrożenie” oznacza wszelkie potencjalne okoliczności, zdarzenie lub działanie, które mogą wyrządzić szkodę, spowodować zakłócenia lub w inny sposób niekorzystnie wpłynąć w przypadku sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób; Trudno też jest rozróżnić incydent od definicji potencjalne zdarzenie dla cyberbezpieczeństwa, które oznacza zdarzenie, które może mieć niekorzystny wpływ na bezpieczeństwo systemów informacyjnych.	
170.	Fundacja Open Allies	Art. 2	Fundacja zwraca uwagę na niezgodność definicji incydentu z odpowiadającą definicją w dyrektywie NIS2. Być może jest to pozostałość po poprzednich wersjach nowelizacji UKSC, przygotowanych jeszcze przed publikacją dyrektywy NIS2. Definicja „incydentu” w Projekcie uwzględnia nie tylko zaistniałe zdarzenia mające wpływ na bezpieczeństwo systemów informatycznych, lecz również te zdarzenia, które tylko mogą mieć wpływ na to bezpieczeństwo. Z kolei dyrektywa NIS2 wskazuje, że „incydent” oznacza zdarzenie naruszające dostępność itd., a nie mogące naruszać dostępność itd. Wnosimy o dostosowanie definicji incydentu w nowelizacji UKSC do postanowień dyrektywy NIS2, poprzez ograniczenie definicji “incydentu” wyłącznie do zaistniałych zdarzenia mające wpływ na bezpieczeństwo. Na marginesie można zauważyć, że definicja „incydentu” w Projekcie, w związku ze zbyt szerokim zakresem, obejmuje także np. „cyberzagrożenie” lub „potencjalne zdarzenie dla cyberbezpieczeństwa”, również definiowane (odpowiednio w rozporządzeniu 2019/881 lub w dyrektywie NIS2). Ustawodawca europejski celowo rozróżnił zdarzenia – na te, które mają wpływ na cyberbezpieczeństwo oraz te, które tylko mogą mieć wpływ. Zmiana definicji incydentu i doprowadzenie do zgodności z NIS2 prowadzi do konieczności zmian w definicji „incydentu poważnego”. Rozróżnienie jest istotne np. przy prowadzonych przez podmioty kluczowe analizach incydentów oraz obowiązkach zgłoszenia incydentów do właściwych CSIRT.	Uwaga nieuwzględniona Definicja incydentu obowiązuje od 2018 r. i istnieje już ugruntowana praktyka związana z jej stosowaniem. Intencją tej definicji było to, aby zbierane a potem raportowane do CSIRT były zdarzenia potencjalne, dzięki czemu CSIRT może ostrzec pozostałe podmioty o zagrożeniu.
171.	Fundacja Open Allies	Art. 2	Open Allies zwraca się o modyfikację postanowień art. 8 ust. 1 pkt 5 lit. b nowelizowanej UKSC. Ze wskazanego przepisu można wnioskować o obowiązku wdrożenia systemu zarządzania bezpieczeństwem informacji polegającym m.in. na regularnym przeprowadzaniu aktualizacji oprogramowania – z uwzględnieniem analizy wpływu aktualizacji na bezpieczeństwo świadczonej usługi oraz poziomu krytyczności poszczególnych aktualizacji. Naszym zdaniem wyjątki od przedmiotowego obowiązku powinny być rozszerzone. U dużych przedsiębiorców liczne systemy informacyjne są ze sobą wzajemnie powiązane. Przeprowadzanie	Wyjaśnienie uwagi Podzielamy zdanie Fundacji jednakże wskazujemy, że już obecne brzmienie przepisu uwzględnia tę okoliczność, bowiem przed aktualizacją ma być przeprowadzona analiza wpływu

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			aktualizacji powinno uwzględniać tę okoliczność, wobec czego nie zawsze przeprowadzenie niezwłocznej aktualizacji będzie najefektywniejszym rozwiązaniem z punktu widzenia nie tylko ciągłości świadczenia usług, ale również cyberbezpieczeństwa. Aktualizacje powinny być przeprowadzane w terminie uzasadnionym strukturą systemów informatycznych oraz mieć na uwadze ciągłość świadczenia usług. Wnosimy, aby art. 8 ust. 1 pkt 5 lit. b otrzymał następującą treść: „ <i>regularne przeprowadzanie aktualizacji oprogramowania, stosownie do zaleceń producenta, z uwzględnieniem analizy wpływu aktualizacji na bezpieczeństwo świadczonej usługi, wpływu aktualizacji na funkcjonowanie wszystkich systemów informatycznych w organizacji, zachowanie ciągłości świadczonych usług oraz poziomu krytyczności poszczególnych aktualizacji.</i> ”	aktualizacji na bezpieczeństwo świadczonej usługi.
172.	Fundacja Open Allies	Art. 2	Zwracamy się o dostosowanie przepisów dot. norm ISO do dyrektywy NIS2. W pierwszej kolejności, dyrektywa NIS2 w żadnym miejscu nie wskazuje, że uwzględnienie norm ISO oznacza spełnienie wymagań kierowanych do podmiotów kluczowych i podmiotów ważnych. Dyrektywa wskazuje, że m.in. Państwa Członkowskie powinny wspierać „ <i>dostosowanie do norm międzynarodowych i istniejących dobrych praktyk branżowych w dziedzinie zarządzania ryzykiem w cyberbezpieczeństwie</i> ”. Wspieranie nie oznacza miękkiego zobowiązania podmiotów kluczowych oraz podmiotów ważnych do stosowania konkretnych norm. Zwracamy się również o doprecyzowanie intencji projektodawcy przez wyraźne wskazanie, że w art. 8 ust. 2 nowelizowanej UKSC chodzi o materialne zapewnienie systemu zarządzania bezpieczeństwem informacji, z uwzględnieniem wymagań określonych w Polskiej Normie PN-EN ISO/IEC 27001 oraz PN-EN ISO/IEC 22301. Rozwijając ten wątek, zwracamy uwagę na art. 10 ust. 3 pkt 1 nowelizowanej UKSC. Zdajemy sobie sprawę, że przepis został przeniesiony z obecnie obowiązującego rozporządzenia Rady Ministrów, zatem wynika z implementacji uprzednich regulacji unijnych. Z punktu widzenia branży telekomunikacyjnej: dopiero teraz obejmie przedsiębiorców telekomunikacyjnych. Zwracamy uwagę, że, ponownie wbrew dyrektywie, zobowiązuje się podmioty kluczowe oraz podmioty ważne do stosowania konkretnej normy ISO. Naszym zdaniem taka regulacja nie powinna mieć miejsca na gruncie przepisów ustawowych. W przypadku pozostawienia przez Projektodawcę przedmiotowych przepisów, zwracamy się o doprecyzowanie, czy (nowe) sformułowanie „ <i>lub normy jej równoważnej</i> ” może oznaczać np. wersję angielską normy.	Wyjaśnienie uwagi Pod wpływem różnych uwag zmieniono koncepcję – wprowadzone zostanie mapowanie standardów przez ministra.
173.	ISAC-Kolej	Art. 2	„3d) bezpieczeństwo technologii operacyjnych - odporność przemysłowych systemów automatyki i sterowania na zdarzenia, które nie są częścią oczekiwanego działania systemu lub usługi, które powodują lub mogą spowodować zakłócenia lub obniżenie jakości usługi świadczonej przez te systemy” Po uwzględnieniu uwagi i wprowadzeniu nowego terminu w treści projektu ustawy, wyrazy „bezpieczeństwo systemów informacyjnych” należy zastąpić przez „bezpieczeństwo systemów informacyjnych i technologii operacyjnych” (w odpowiednim przypadku i kontekście) np. „systemu informacyjnego i technologii operacyjnych wykorzystywanych do świadczenia usługi”, itd.	Uwaga nieuwzględniona Proponuje się pozostawić definicję bezpieczeństwa systemów informacyjnych. System informacyjny w rozumieniu ustawy to jest również system OT. Definicja np. produktu ICT pomimo użycia w definiendum skrótu ‘ICT’ odnosi się do elementu systemu

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			Pojęcia „bezpieczeństwo systemów informacyjnych”, „proces ICT”, „produkt ICT” oraz „usługa ICT” nie „konsumują” w całości systemów, które są użytkowane w podmiotach kluczowych jako krytyczne. Systemy IT i ich bezpieczeństwo (bezpieczeństwo systemów informacyjnych) służą do przetwarzania i przesyłania danych w celu usprawnienia procesów i komunikacji w organizacji. Natomiast systemy OT (technologie operacyjne) obejmuje sprzęt i oprogramowanie wykorzystywane w środowiskach produkcyjnych i przemysłowych, w celu poprawy wydajności produkcji i bezpieczeństwa operacyjnego.	informacyjnego, w tym także systemu OT.
174.	ISAC-Kolej	Art. 2	„8a) ISAC – centrum wymiany i analizy informacji na temat podatności, cyberzagrożeń i incydentów funkcjonujące w danym sektorze lub podsektorze w celu wspierania podmiotów krajowego systemu cyberbezpieczeństwa” Pkt 8a) zmienić jako 8b) Zapisy, o których mowa w art. 8h ust. 1 – 6 sankcjonują tak naprawdę zasady działania struktury ISAC powołanych w danym sektorze lub podsektorze. Stąd warto w projekcie ustawy formalnie usankcjonować funkcjonowanie tych struktur do powołania których zachęcają m.in. CSIRT poziomu krajowego oraz NASK-PIB.	Uwaga nieuwzględniona Zaproponowana definicja pomija podstawową kwestię – formę prawną ISAC. W obecnej wersji projektu odwołano się do porozumień ws. wymiany informacji. W takiej formie funkcjonują polskie ISACi. Podkreślić należy, że w polskiej praktyce ISAC nie jest podmiotem, nie jest jednostką organizacyjną, nie może być podmiotem praw i obowiązków. Teoretycznie byłaby możliwość utworzenia nowej formy prawnej dedykowanej dla ISAC – np. coś na wzór stowarzyszenia zwykłego z uproszczoną rachunkowością, aby ISAC mógł, jako podmiot prawa i pracodawca, np. zatrudnić analityków. Natomiast zdaniem MC należy najpierw wykorzystywać obecne formy zrzeszeń – np. fundacja czy stowarzyszenie. Na ten moment brak jest jednoznacznego stanowiska polskich ISAC czy powinny mieć nadaną podmiotowość prawną, chociażby jako ułomną osobę prawną. MC jest jednak gotów do rozmów.
175.	ISAC-Kolej	Art. 2	„11) podatność” oznacza słabość, wrażliwość lub wadę produktów ICT lub usług ICT, które to cechy mogą zostać wykorzystane w wyniku cyberzagrożenia;” Ewentualnie, tak jak w przypadku pojęć „proces ICT”, „produkt ICT” i „usługa ICT” odwołać się do art. 6 pkt 15 dyrektywy 2022/2555	Wyjaśnienie uwagi Zdaniem MC zaproponowana definicja (odniesienie się do właściwości) obejmuje „słabość, wrażliwość lub wadę”.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			Proponowana definicja wskazana została w art. 6 pkt 15 dyrektywy NIS2 i bardziej dokładnie oraz szerzej określa pojęcie podatności niż definicja wskazana w projekcie ustawy (podatność – właściwość produktu ICT lub usługi ICT, które mogą być wykorzystane przez cyberzagrożenie)	
176.	ISAC-Kolej	Art. 2	„14a) technologia operacyjna - oznacza sprzęt i oprogramowanie, które wykrywają lub powodują zmiany poprzez bezpośrednie urządzeń przemysłowych, aktywów, procesów i zdarzeń nadzorujących procesy fizyczne obejmuje przemysłowe systemy sterowania, programowalne sterowniki logiczne, rozproszone systemy sterowania oraz systemy nadzoru i gromadzenia danych”. Wprowadzone w projekcie ustawy pojęcie „system informacyjny” odnosi się bardziej do technologii IT (information technology) i nie pokrywa zastosowania ustawy do technologii OT (operational technology), które obejmują sprzęt i oprogramowanie wykorzystywane w środowiskach produkcyjnych i przemysłowych, w celu poprawy wydajności produkcji i bezpieczeństwa operacyjnego.	Uwaga nieuwzględniona Definicja systemu informacyjnego obejmuje systemy OT.
177.	ISAC-Kolej	Art. 2	„21) „ISAC działający na zasadach określonych w art. 8h” ISAC powołany formalnie w danym sektorze lub podsektorze i działający na zasadach zgodnie zapisami art. 8h) powinien elementem krajowego systemu cyberbezpieczeństwa.	Uwaga nieuwzględniona w zw. z nieuwzględnieniem uwagi do definicji ISAC.
178.	ISSA Polska	Art. 2	Niespójne i nadmiarowe definicje, <i>Incydent, potencjalne zdarzenie dla cyberbezpieczeństwa</i> Jest to definicja, która odbiega od określonej w art. 6 pkt. 6 NIS2. Biorąc pod uwagę, że do projektu wprowadzono pojęcie potencjalnego zdarzenia dla cyberbezpieczeństwa (czyli zdarzenia, które może mieć niekorzystny wpływ na bezpieczeństwo systemów informacyjnych), utrzymanie definicji incydentu we wskazanym zakresie zwiększa obciążenie podmiotów kluczowych i ważnych w zakresie obsługi incydentu poza zakres wynikający z ram unijnych. Projektodawca, zaproponował definicję “incydentu” oraz formułując ją nadmiarowo z punktu widzenia definicji potencjalnego zdarzenia i faktu, że potencjalny skutek (który zgodnie z NIS2 musi być jednak realny a nie jedynie możliwy) pojawia się w art. 23 ust. 3 NIS2 dopiero w ramach definicji “incydentu poważnego” nadmiarowo. Użycie frazy “może mieć” oznacza rozszerzenie zrozumienia pojęcia incydent o “zdarzenia cyberbezpieczeństwa”, czyli potencjalne incydenty. W aktualnym brzmieniu rodzi potrzebę podejmowania działań nie proporcjonalnych do potrzeb dla obsługi “zdarzeń” czyli potencjalnych incydentów. Ponadto definicja “incydent” jest niespójna z definicją w Dyrektywie NIS2, a zgodnie z obecną w projekcie definicji “incydent” - następuje zbieżność w opisie z definicją “potencjalnego zdarzenia dla cyberbezpieczeństwa”. Proponujemy w związku z tym wprowadzenie następującej definicji incydentu: “incydent – zdarzenie, które ma niekorzystny wpływ na bezpieczeństwo systemów informacyjnych”. <i>Podatność</i> Definicja “podatności” również odnosi się do usług co może być trudne do interpretacji. Proponujemy w związku z tym uproszczenie definicji podatności:	Uwaga nieuwzględniona Definicja incydentu obowiązuje od 2018 r. i istnieje już ugruntowana praktyka związana z jej stosowaniem. Intencją tej definicji było to, aby zbierane a potem raportowane do CSIRT były zdarzenia potencjalne, dzięki czemu CSIRT może ostrzec pozostałe podmioty o zagrożeniu. Dyrektywa NIS2 wskazuje, że podatność może dotyczyć także usługi. Definicja systemu informacyjnego obejmuje systemy OT.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			“podatność - właściwość systemu informacyjnego lub jego elementu, która może być wykorzystana przez zagrożenie cyberbezpieczeństwa.” W art. 8 pkt 1 (3) występuje błędny zapis “zbieranie informacji o cyberzagrożeniach i podatnościach na incydenty systemu informacyjnego wykorzystywanego do świadczenia usługi”. Zwrot podatność na incydenty powinien być zastąpiony “podatnością systemów teleinformatycznych wspierających usług kluczowe i ważne”. <i>Produkt ICT, usługa ICT</i> Brak zdefiniowania rozwiązań klasy OT (Operation Technology) i IoT (Internet of Things). Zgodnie z definicją “produkt ICT” i “usługa ICT” nie uwzględniają wyżej wymienionych klas rozwiązań. Dodatkowo w zmianach do art. 226 ust. 1 pkt. 19 prawa zamówień publicznych wprowadzono pojęcie „typu produktu”, który można oczywiście wyłożyć w oparciu o inne przepisy dotyczące zgodności wyrobów, ale nie jest określony w ustawie o KSC.	
179.	ISSA Polska	Art. 2	Niespójne i nadmiarowe definicje <i>Incydent, potencjalne zdarzenie dla cyberbezpieczeństwa</i> Projektodawca, zaproponował definicję “incydentu” oraz “incydentu poważnego” nadmiarowo. Użycie frazy “może mieć” oznacza rozszerzenie zrozumienia pojęcia incydent o “zdarzenia cyberbezpieczeństwa”, czyli potencjalne incydenty. W aktualnym brzmieniu rodzi potrzebę podejmowania działań nie proporcjonalnych do potrzeb dla obsługi “zdarzeń” czyli potencjalnych incydentów. Ponadto definicja “incydent” jest niespójna z definicją w Dyrektywie NIS2, a zgodnie z obecną w projekcie definicji “incydent” - następuje zbieżność w opisie z definicją “potencjalnego zdarzenia dla cyberbezpieczeństwa”. Proponujemy w związku z tym wprowadzenie następującej definicji incydentu: “incydent – zdarzenie, które ma niekorzystny wpływ na bezpieczeństwo systemów informacyjnych”. Definicja “podatności” również odnosi się do usług co może być trudne do interpretacji. Proponujemy w związku z tym uproszczenie definicji podatności: “podatność - właściwość systemu informacyjnego lub jego elementu, która może być wykorzystana przez zagrożenie cyberbezpieczeństwa.” W art. 8 pkt 1 (3) występuje błędny zapis “zbieranie informacji o cyberzagrożeniach i podatnościach na incydenty systemu informacyjnego wykorzystywanego do świadczenia usługi”. Zwrot podatność na incydenty powinien być zastąpiony “podatnością systemów teleinformatycznych wspierających usług kluczowe i ważne”. <i>Produkt ICT, usługa ICT</i> Brak zdefiniowania rozwiązań klasy OT (Operation Technology) i IoT (Internet of Things). Zgodnie z definicją “produkt ICT” i “usługa ICT” nie uwzględniają wyżej wymienionych klas rozwiązań, czytając zapisy literalnie. Zapis: “urządzenie lub grupę połączonych urządzeń elektrycznych lub elektronicznych i oprogramowania zaprogramowanych w celu przetwarzania danych – wraz z danymi przetworzonymi w postaci elektronicznej;”, zapis może powodować	Uwaga nieuwzględniona Definicja incydentu obowiązuje od 2018 r. i istnieje już ugruntowana praktyka związana z jej stosowaniem . Intencją tej definicji było to, aby zbierane a potem raportowane do CSIRT były zdarzenia potencjalne, dzięki czemu CSIRT może ostrzec pozostałe podmioty o zagrożeniu. Dyrektywa NIS2 wskazuje, że podatność może dotyczyć także usługi. Definicja systemu informacyjnego obejmuje systemy OT.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			niejasne rozumienie systemu, łącznik “lub”.	
180.	ISACA	Art. 2	incydent – zdarzenie, które ma lub może mieć niekorzystny wpływ na bezpieczeństwo systemów informacyjnych; zastosować brzmienie z NIS2 "Wprowadzona definicja ma błąd logiczny (wyróżniony kolorem) i jest mniej precyzyjna w odniesieniu do definicji z Dyrektywy (nie odnosi się do celów bezpieczeństwa) [NIS2 art. 6 pkt 1] „incydent” oznacza zdarzenie naruszające dostępność, autentyczność, integralność lub poufność przechowywanych, przekazywanych lub przetwarzanych danych lub usług oferowanych przez sieci i systemy informatyczne lub dostępnych za ich pośrednictwem;"	Wyjaśnienie uwagi Definicja incydentu odnosi się także do atrybutów cyberbezpieczeństwa, ponieważ odnosi się do bezpieczeństwa systemów informacyjnych, które zawierają atrybuty cyberbezpieczeństwa.
181.	ISACA	Art. 2	Podatność – właściwość produktu ICT lub usługi ICT, które mogą być wykorzystane przez cyberzagrożenie; zastosować brzmienie z NIS2 "Definicja w Dyrektywie jest bardziej precyzyjna [NIS2 (art. 6 pkt 15)] „podatność” oznacza słabość, wrażliwość lub wadę produktów ICT lub usług ICT, które to cechy mogą zostać wykorzystane w wyniku cyberzagrożenia;"	Wyjaśnienie uwagi Zdaniem MC zaproponowana definicja (odniesienie się do właściwości) obejmuje „słabość, wrażliwość lub wadę.”
182.	ISACA	Art. 2	Ryzyko – kombinację prawdopodobieństwa wystąpienia zdarzenia niepożądanego i jego konsekwencji; zastosować brzmienie z NIS2 "Podana definicja jest błędna - podaje definicję miary ryzyka, a nie ryzyka. Poprawna merytorycznie jest definicja z Dyrektywy [NIS2 (art. 6 pkt 9)] „ryzyko” oznacza możliwość wystąpienia strat lub zakłóceń spowodowanych incydem, wyrażoną jako wypadkową wielkości takiej straty lub takich zakłóceń oraz prawdopodobieństwo wystąpienia takiego incydentu;"	Uwaga nieuwzględniona Naszym zdaniem definicja ryzyka z KSC obejmuje zakres definicji ryzyka z NIS2.
183.	ISACA	Art. 2	"system informacyjny – oznacza to: a) system teleinformatyczny o którym mowa w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2024 r. poz. 307) lub b) urządzenie lub grupę połączonych urządzeń elektrycznych lub elektronicznych i oprogramowania zaprogramowanych w celu przetwarzania danych – wraz z danymi przetwarzanymi w postaci elektronicznej;" zastosować brzmienie z NIS2 "Wprowadzona definicja jest istotnie różna znaczeniowo od definicji zawartej w Dyrektywie [NIS2 art. 6 pkt 1] „sieci i systemy informatyczne” oznaczają: a) sieć łączności elektronicznej zdefiniowaną w art. 2 pkt 1 dyrektywy (UE) 2018/1972 {ustanawiająca Europejski kodeks łączności elektronicznej}; b) urządzenie lub grupę wzajemnie połączonych lub powiązanych urządzeń, z których co najmniej jedno, na podstawie programu, automatycznie przetwarza dane cyfrowe; lub c) dane cyfrowe przechowywane, przetwarzane, pobierane lub przekazywane przez elementy określone w lit. a) i b) w celu ich eksploatacji, użycia, ochrony i utrzymania;"	Wyjaśnienie uwagi Zaproponowana definicja obejmuje sieci telekomunikacyjne, systemy informatyczne oraz systemy automatyki przemysłowej.
184.	Związek Pracodawców Technologii	Art. 2	Definicja incydentu, incydentu poważnego oraz potencjalnego zdarzenia dla cyberbezpieczeństwa (art. 2 odpowiednio pkt. 5, 7, 8 oraz 11e) Rekomendujemy pozostanie przy definicjach takich jak zapisane w Dyrektywie NIS2. Przykład: definicja „potencjalnego zdarzenia w cyberbezpieczeństwie” użyta w projekcie niewiele odbiega od	Wyjaśnienie uwagi Jest pewna różnica między definicją incydentu a potencjalnego zdarzenia dla

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

	Cyfrowych Lewiatan		definicji incydentu. Czy taki zabieg był celowy? Proponujemy powrót do definicji z Dyrektywy: „potencjalne zdarzenie dla cyberbezpieczeństwa” oznacza zdarzenie, które mogło naruszyć dostępność, autentyczność, integralność lub poufność przechowywanych, przekazywanych lub przetwarzanych danych lub usług oferowanych przez sieci i systemy informatyczne lub dostępnych za ich pośrednictwem, któremu udało się jednak zapobiec lub które jednak nie wystąpiło;	cyberbezpieczeństwa – to drugie nie wystąpiło lub udało się mu zapobiec.
185.	Związek Pracodawców Technologii Cyfrowych Lewiatan	Art. 2	Definicja podatności (art. 2 pkt 11) Proponowana definicja jest wierną kopią zapisu Dyrektywy NIS2. Mając jednak na uwadze definicję procesu ICT jaka jest przeniesiona do NIS2 z ROZPORZĄDZENIA PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2019/881 („proces ICT” oznacza zestaw czynności wykonywanych w celu projektowania, rozwijania, dostarczania lub utrzymywania produktów ICT lub usług ICT;) rekomendujemy poszerzenie jej także o procesy ICT. Przykładem takiego procesu może być nadzór nad procesem uczenia się modeli sztucznej inteligencji i w efekcie podatność wykorzystywanego systemu.	Wyjaśnienie uwagi Postanowiliśmy pozostawić tutaj wierne wdrożenie dyrektywy NIS2 i przyjmując, że podatność dotyczy tylko usługi/produktu ICT.
186.	Związek Pracodawców Technologii Cyfrowych Lewiatan	Art. 2	Definicja podmiotu krytycznego (art. 2 pkt 11c) Definicja powinna być tożsama/zgodna z definicją przyjętą w nieznanym nam projekcie ustawy o zarządzaniu kryzysowym, infrastrukturze krytycznej i podmiotach krytycznych (transpozycji dyrektywy CER)	Wyjaśnienie uwagi Będziemy dążyć do uspoźnienia projektów.
187.	Związek Pracodawców Technologii Cyfrowych Lewiatan	Art. 2	Definicje przedsiębiorcy komunikacji elektronicznej i przedsiębiorcy telekomunikacyjnego (art. 2 pkt 11f i 11g) Postulujemy tożsamość definicji z aktualnie procedowany Prawem Komunikacji Elektronicznej.	Uwaga uwzględniona
188.	Związek Pracodawców Technologii Cyfrowych Lewiatan	Art. 2	Definicja systemu informacyjnego (art. 2 pkt 14) Rekomendujemy przygotowanie jednej i jednolitej definicji systemu informacyjnego i wykorzystanie jej we wszystkich ustawach (patrz uwaga nr 2). To oznacza oczywiście także m.in. nowelizację definicji systemu teleinformatycznego w ustawie o informatyzacji, z której wykorzystano definicję w aktualnym projekcie.	Uwaga wyjaśniona Wpis projektu do wykazu prac legislacyjnych Rady Ministrów nie obejmuje swoim zakresem zmian w ustawie o informatyzacji.
189.	ISACA	Art. 2	Znaczące cyberzagrożenie – cyberzagrożenie, które przez swoje właściwości techniczne może mieć poważny wpływ na bezpieczeństwo systemów informacyjnych poprzez wywołanie szkody materialnej lub niematerialnej zastosować brzmienie z NIS2 "Wprowadzona definicja jest różna (znaczące vs. poważne) - nie jest jasne czy są to różne cyberzagrożenia (wyróżniono różnice) - definicja w Dyrektywie jest bardziej precyzyjna.i ma znacznie szerszy zakres stosowania (sieci, użytkownicy, podmiot) [NIS2 (art. 6 pkt 11)] „poważne cyberzagrożenie” oznacza cyberzagrożenie, co do którego można założyć w oparciu o jego charakterystykę techniczną, że może wyrzucić znaczący wpływ na sieć i systemy informatyczne danego podmiotu lub użytkowników, korzystających z usług tego podmiotu, powodując i znaczne szkody majątkowe lub niemajątkowe;"	Uwaga uwzględniona Przepis zostanie zmieniony.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

190.	ISACA	Art. 2	Potencjalne zdarzenie dla cyberbezpieczeństwa – zdarzenie, które może mieć niekorzystny wpływ na bezpieczeństwo systemów informacyjnych; zastosować brzmienie z NIS2 "Wprowadzona definicja jest mniej precyzyjna w odniesieniu do definicji z Dyrektywy (nie odnosi się do celów bezpieczeństwa) [NIS2 art. 6 pkt 1] „potencjalne zdarzenie dla cyberbezpieczeństwa” oznacza zdarzenie, które mogło naruszyć dostępność, autentyczność, integralność lub poufność przechowywanych, przekazywanych lub przetwarzanych danych lub usług oferowanych przez sieci i systemy informatyczne lub dostępnych za ich pośrednictwem, któremu udało się jednak zapobiec lub które jednak nie wystąpiło"	Uwaga częściowo uwzględniona Przepis zostanie zmieniony przy zachowaniu odwołania do bezpieczeństwa systemów informacyjnych.
191.	ISACA	Art. 2	"bezpieczeństwo systemów informacyjnych – odporność systemów informacyjnych na zdarzenia naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy; "zastosować brzmienie z NIS2 "Wprowadzona definicja jest istotnie różna znaczeniowo od definicji zawartej w Dyrektywie, w szczególności pomija wyróżnione słowa mające istotne znaczenie [NIS2 art. 6 pkt 1] „bezpieczeństwo sieci i systemów informatycznych” oznacza odporność sieci i systemów informatycznych, przy danym poziomie zaufania, na wszelkie zdarzenia, które mogą naruszyć dostępność, autentyczność, integralność lub poufność przechowywanych, przekazywanych lub przetwarzanych danych lub usług oferowanych przez te sieci i systemy informatyczne lub dostępnych za ich pośrednictwem;	Wyjaśnienie uwagi Definicja bezpieczeństwa systemów informacyjnych odnosi się do systemów informacyjnych, w ramach których znajdują się i systemy automatyki przemysłowej, sieci telekomunikacyjne czy wewnętrzne sieci i systemy danego podmiotu.
192.	KGHM Polska Miedź S.A.	Art. 1 pkt 2 lit. j ustawy zmieniającej , w zakresie pkt 11f	Projektowana definicja „przedsiębiorcy komunikacji elektronicznej”, pod którym rozumie się „przedsiębiorcę telekomunikacyjnego lub podmiot świadczący usługę komunikacji interpersonalnej niewykorzystującej numerów” jest odmienna od definicji zawartej w rządowym projekcie ustawy - Prawo komunikacji elektronicznej (dalej: „projekt nr UC7”, „PKE”) w art. 2 pkt 39 (cyt. „przedsiębiorca komunikacji elektronicznej – przedsiębiorcę telekomunikacyjnego lub podmiot świadczący publicznie dostępną usługę komunikacji interpersonalnej niewykorzystującą numerów”). Definicja „usługa łączności interpersonalnej” ujęta w projekcie nr UC7 zawiera wyłączenie potencjalnie wpływające na finalną klasyfikację podmiotu zgodnie z proponowaną definicją w pkt 11 f). Adekwatnie do treści uwagi proponujemy zastosowanie jednej, spójnej definicji oraz utrzymanie publicznie dostępnego rejestru przedsiębiorców/dostawców usług komunikacji elektronicznej uznanych za podmioty kluczowe. Każdy podmiot świadczący usługi komunikacji elektronicznej na terenie RP i uznany za podmiot kluczowy powinien być ujęty w ww. rejestrze i podlegać łącznie pod rygor ustaw: Prawo komunikacji elektronicznej oraz o Krajowym Systemie Cyberbezpieczeństwa (dalej: „KSC”). W zał. nr 1 do projektu (nr UC32) wskazano jako podmioty kluczowe w sektorze Infrastruktura cyfrowa podsektor „Komunikacja Elektroniczna”, a w nim: „Przedsiębiorcę telekomunikacyjnego” oraz „Podmiot świadczący usługę komunikacji interpersonalnej niewykorzystującą numerów”. eW rozumieniu projektodawcy, zastosowanie precyzyjnej definicji w przypadku „podmiotu kluczowego” jakim będą „dostawcy usług komunikacji elektronicznej” jest	Uwaga uwzględniona Zostanie wprowadzone odniesienie do ustawy – Prawo komunikacji elektronicznej.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			istotnym elementem skuteczności KSC. Rządowy projekt ustawy - Prawo Komunikacji Elektronicznej nr UC7, wniesiony do Sejmu RP w dniu 21.05.2024, posługuje się inaczej brzmiącą definicją. Jednoznaczne wskazanie podmiotu kluczowego oferującego usługi w zakresie komunikacji elektronicznej powinno być realizowane analogicznie jak w przypadku przedsiębiorców telekomunikacyjnych, z zastosowaniem adekwatnej definicji. Usługi świadczone przez podmioty posiadające status przedsiębiorców telekomunikacyjnych oraz przedsiębiorców komunikacji elektronicznej wykorzystywane między innymi przez inne podmioty kluczowe charakteryzować się powinny gwarantowanym poziomem zapewnienia cyberbezpieczeństwa, czemu w rozumieniu projektodawcy służy nowelizacja KSC.u Należy zwrócić też uwagę, że definicja „usługa łączności interpersonalnej” ujęta w Dyrektywie 2018/1972 oraz rządowym projekcie nr UC7 zawiera wyłączenie usług, w których interpersonalna i interaktywna komunikacja stanowi <u>wyłącznie funkcję podrzędną</u> względem innej usługi podstawowej – co przy specyficznej interpretacji mogłoby prowadzić do wyłączenia podmiotu świadczącego taką usługę z obowiązków ujętych w KSC.	
193.	PTI	Art. 2	1. W odniesieniu do art. 2 zmienianej ustawy w dodanym punkcie 3c) zawierającym definicję bezpieczeństwa systemów informatycznych proponuje się pozostawić jedynie trzy kardynalne atrybuty bezpieczeństwa (poufność, integralność, dostępność) wykreślając atrybut pomocniczy „autentyczność” jako zawierający się zgodnie z definicją ISO w atrybucie „integralność”	Wyjaśnienie uwagi Proponuje się pozostawienie tego atrybutu i przez to podkreślenie, że pochodzenie danych powinno być takie jak jest deklarowane.
194.	PTI	Art. 2	Art. 1 pkt 1) lit c) – w dodanej definicji 4b): „dostawca sieci dostarczania treści – osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, która dostarcza sieci rozproszonych geograficznie serwerów służących zapewnieniu wysokiej i łatwej dostępności treści i usług cyfrowych lub ich szybkiego dostarczania na rzecz użytkowników internetu w imieniu dostawców treści i usług;” jest niegrammatyczna, przez co niezrozumiała Proponuje się zmianę: „dostawca sieci dostarczania treści – osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, która dostarcza treści i usługi cyfrowe do sieci rozproszonych geograficznie serwerów służących zapewnieniu wysokiej i łatwej dostępności tych treści i usług lub ich szybkiego dostarczania na rzecz użytkowników internetu w imieniu dostawców treści i usług”	Uwaga uwzględniona Przepis zostanie zmieniony.
195.	PTI	Art. 2	Definicja 4e): „dostawca usług chmurowych – osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, która świadczy usługi umożliwiające dostęp do skalowalnego i elastycznego zbioru zasobów obliczeniowych do ~~wspólnego~~ wykorzystywania przez wielu użytkowników” jest nieprecyzyjna. Użytkownicy nie korzystają z zasobów „wspólnie”. Sugeruje się wykreślić słowo „wspólnego”	Wyjaśnienie uwagi Art. 6 pkt 30 Dyrektywy NIS2 wskazuje: ‘cloud computing service’ means a digital service that enables on-demand administration and broad remote access to a scalable and elastic pool of shareable computing resources, including where such resources are distributed across several locations;

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

				Co zostało przetłumaczone jako: „usługa chmurowa” oznacza usługę cyfrową umożliwiającą administrowanie na żądanie skalowalnym i elastycznym zbiorem zasobów obliczeniowych do wspólnego wykorzystywania oraz szeroki dostęp zdalny do tego zbioru, w tym również gdy takie zasoby są rozproszone w kilku lokalizacjach; Także zdaniem projektodawcy wyraz “wspólnie” powinien pozostać, aby zapewnić zgodność z dyrektywą.
196.	PTI	Art. 2	Definicja 4h): „dostawca usług zarządzanych – osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, która świadczy usługi związane z instalacją, eksploatacją lub konserwacją produktów ICT, usług ICT, procesów ICT lub systemów informacyjnych poprzez wsparcie lub aktywną administrację przeprowadzane u usługobiorcy lub zdalnie;” zawiera kilka nieścisłości: 1) system informacyjny może składać się z produktów ICT lub procesów ICT; system(y) informacyjne realizuje(a) usługi ICT; 2) „poprzez wsparcie lub aktywną administrację” – pojęcia z „wsparcie”, a w szczególności „aktywna administracja” są niezrozumiałe 3) „u usługobiorcy lub zdalnie” – zdalnie też jest „u usługobiorcy”. Sugeruje się następujące zmiany: „dostawca usług zarządzanych – osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, która świadczy usługi związane z instalacją, eksploatacją lub konserwacją ~~produktów ICT, usług ICT, procesów ICT lub~~ systemów informacyjnych ~~poprzez wsparcie lub aktywną administrację~~ przeprowadzane u usługobiorcy, na miejscu lub zdalnie”	Uwaga częściowo uwzględniona Art. 6 pkt 39 dyrektywy NIS2 wskazuje: 39) „dostawca usług zarządzanych” oznacza podmiot, który świadczy usługi związane z instalacją, eksploatacją lub konserwacją produktów, sieci, infrastruktury, aplikacji ICT lub innych sieci i systemów informatycznych lub z zarządzaniem nimi, poprzez pomoc lub aktywną administrację prowadzoną u klientów lub zdalnie; W propozycji ustawy wyrazy <i>produktów ICT, usług ICT, procesów ICT lub systemów informacyjnych</i> ma odzwierciedlać produktów, sieci, infrastruktury, aplikacji ICT lub innych sieci i systemów informatycznych z definicji z NIS2. Definicja zostanie uzupełniona o wskazanie, że wsparcie jest przeprowadzane także na miejscu u usługobiorcy.
197.	PTI	Art. 2	Definicja 4i) „dostawca usług zarządzanych w zakresie cyberbezpieczeństwa – dostawca usług zarządzanych, który świadczy usługi związane z zarządzaniem ryzykiem w zakresie cyberbezpieczeństwa lub zapewnia pomoc dla tych działań;” jest nieprecyzyjna i niekompletna	Uwaga uwzględniona

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			Definicja zarządzanych usług bezpieczeństwa (managed security services) została wprowadzona do poprawki do Rozporządzenia EU 2019/881 (akt o cyberbezpieczeństwie w następującym brzmieniu: <i>„managed security service’ means a service consisting of carrying out, or providing assistance for, activities relating to cybersecurity risk management, including incident response, penetration testing, security audits and consultancy”</i>) Dodatkowo, zarządzane usługi bezpieczeństwa nie są podzbiorem usług zarządzanych, stąd nie można zastosować „dostawca usług zarządzanych”, bo reguła podstawienia definicji daje w wyniku nonsens. Sugeruje się powtórzenie definicji z poprawki do CSA w KSC: <i>„dostawca zarządzanych usług bezpieczeństwa - osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, która świadczy usługi polegające na realizacji lub wsparciu dla realizacji działań związanych z zarządzaniem ryzykiem w cyberbezpieczeństwie, w tym reakcja na incydenty, testy penetracyjne, audyty bezpieczeństwa oraz konsultacje”</i>	Zostanie wprowadzona zmiana definicji zgodnie z propozycją, jednakże z wyłączeniem konsultacji.
198.	Osoba fizyczna	Art. 2	Chciałabym zwrócić uwagę, że w przypadku testów penetracyjnych i podobnych usług z zakresu cyberbezpieczeństwa mogą być one wykonywane przez ekspertów, specjalistów, którzy działają samodzielnie jako freelancerzy. Usługi takie mogą być wykonywane formalnie jako JDG. Ponieważ ustawa ma obejmować wszystkie podmioty z branży cyberbezpieczeństwa, niezależnie od ich wielkości, wpadać do tych przepisów będą również freelancerzy i niezależni konsultanci. Moim zdaniem w takim przypadku przewidziane przez ustawę obowiązki są nadmierne i nieadekwatne. Proszę o przewidzenie takiego wariantu i wyłączenie niezależnych konsultantów z wymagań ustawy lub dostosowanie (złagodzenie) tych wymagań w przypadku samodzielnych ekspertów, działających np. na JDG i niezatrudniających nikogo dodatkowego. Będę wdzięczna (i myślę, że nie tylko ja) za uwzględnienie powyższych uwag w przygotowywanej nowelizacji.	Uwaga uwzględniona Z zakresu dostawcy usług zarządzanych w zakresie cyberbezpieczeństwa wyłączeni zostaną mikroprzedsiębiorcy.
199.	PTI	Art. 2	lit i) Definicja: „11) <i>podatność – właściwość produktu ICT lub usługi ICT, które mogą być wykorzystane przez cyberzagrożenie;</i>”, jest niepoprawna. Nie każda właściwość produktu lub usługi (a nawet ogromna większość) nie powoduje podatności Sugeruje się zmianę „właściwość” na „słabość” – jak od wielu lat definiuje się chociażby z normach związanych z ISO/IEC 27001	Wyjaśnienie uwagi Definicja ta nie odnosi się do każdej właściwości produktu ICT lub usługi ICT, a jedynie do tych mogących być wykorzystane przez cyberzagrożenia.
200.	PTI	Art. 2	lit i) Definicja 11e): „potencjalne zdarzenie dla cyberbezpieczeństwa – zdarzenie, które może mieć niekorzystny wpływ na bezpieczeństwo systemów informacyjnych; – definicja w konflikcie z definicją incydentu i po prostu niepotrzebna, wystarczy użyć „potencjalny incydent” co oznacza: „potencjalne zdarzenie, które ma, lub może mieć niekorzystny wpływ na system informacyjny” Sugeruje się wykreślenie definicji	Wyjaśnienie uwagi Definicja ta jest wymagana przez Dyrektywę NIS2. Wiąże się z nią obowiązki w zakresie raportowania do zdarzeń do ENISA.
201.	PTI	Art. 2	W dodanym punkcie 11b) zawierającym definicję podmiotu publicznego wskazano błędnie tytuł ustawy („ustawa w sektorze administracji publicznej” nie istnieje). Należy wskazać prawidłowy tytuł ustawy którą Autor miał na myśli	Wyjaśnienie uwagi To nie jest odwołanie do innej ustawy tylko odwołanie do załącznika w ustawie.
202.	PTI	Art. 2	Art. 2 pkt 14 podpunkt b) zmienianej ustawy otrzymuje brzmienie:	Wyjaśnienie uwagi

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

		<i>b) urządzenie lub grupę połączonych urządzeń elektrycznych lub elektronicznych i oprogramowania zaprogramowanych w celu przetwarzania danych</i> <i>– wraz z danymi przetwarzanymi w postaci elektronicznej;”</i> Określenie „oprogramowania zaprogramowanego” stanowi tautologię. Całość zapisu jest niezrozumiała. Zaprogramowane (czyli posiadające zdolność do wykonania sekwencji działań zależnych od poprzedniego stanu – teoria automatów – maszyna Turinga) może być dowolne urządzenie posiadające zdolność wykonywania kolejnych działań, zależnych, lub niezależnych od poprzedniego stanu. W dokumencie „UZASADNIENIE” podano: „– „<i>W ten sposób projektodawca chce przeciąć wątpliwości co do tego czy systemy OT mieszczą się w ramach obecnej definicji systemu informacyjnego czy nie</i>”. Wskazać należy, że taka wątpliwość nigdy nie istniała, bo każde urządzenie elektromechaniczne spełniające warunki wskazane w teorii automatów jest systemem informatycznym, gdyż jego działanie zależy od przetwarzanej informacji Proponuje się zapis: <i>b) teleinformatyczny system sterujący lub monitorujący czasu rzeczywistego;</i> Biorąc pod uwagę, że przedmiotem regulacji są urządzenia elektryczne (elektroniczne stanowią ich odmianę- na ogół niskonapięciową, poza elementami mocy – tyrystory, triaki, czy tranzystory wysokonapięciowe), zapis – <i>wraz z danymi przetwarzanymi w postaci elektrycznej</i> – jest niepotrzebny	Pojawiająca się u niektórych z podmiotów wątpliwość co do zastosowania obecnej definicji systemu informacyjnego do systemów OT wzięła się z tego, że definicja systemu informacyjnego odwołuje się do definicji systemu teleinformatycznego, o którym mowa w art. 3 pkt 3 ustawy z 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne. Systemem teleinformatycznym w rozumieniu powołanego przepisu jest zaś zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu przepisów ustawy z 16 lipca 2004 r. – Prawo telekomunikacyjne. Telekomunikacyjne urządzenie końcowe według art. 2 pkt 43 Pt, do którego odsyła definicja z ustawy o informatyzacji, to „urządzenie telekomunikacyjne przeznaczone do podłączenia bezpośrednio lub pośrednio do zakończeń sieci”. Zakończenie sieci, w rozumieniu art. 2 pkt 52 ustawy Pt, stanowi fizyczny punkt, w którym abonent otrzymuje dostęp do publicznej sieci telekomunikacyjnej; w przypadku sieci stosujących komutację, lub przekierowywanie, zakończenie sieci identyfikuje się za pomocą konkretnego adresu sieciowego, który może być

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

				przypisany do numeru lub nazwy abonenta. Stąd niektóre podmioty uznawały, że oprogramowanie typu SCADA nie mieści się w definicji systemu informacyjnego, ponieważ nie są podłączone do publicznych sieci telekomunikacyjnych.
203.	PIPC	Art. 1 pkt 2 lit. j) ustawy zmieniającej , w zakresie pkt 11f)	Projektowana definicja „przedsiębiorcy komunikacji elektronicznej”, pod którym rozumie się „przedsiębiorcę telekomunikacyjnego lub podmiot świadczący usługę komunikacji interpersonalnej niewykorzystującej numerów” jest odmienna od definicji zawartej w rządowym projekcie ustawy - Prawo komunikacji elektronicznej (dalej: „projekt nr UC7”, „PKE”) w art. 2 pkt 39 (cyt. „przedsiębiorca komunikacji elektronicznej – przedsiębiorcę telekomunikacyjnego lub podmiot świadczący <u>publicznie dostępną</u> usługę komunikacji interpersonalnej niewykorzystującą numerów”). Definicja „usługa łączności interpersonalnej” ujęta w projekcie nr UC7 zawiera wyłączenie potencjalnie wpływające na finalną klasyfikację podmiotu zgodnie z proponowaną definicją w pkt 11 f). Adekwatnie do treści uwagi proponujemy zastosowanie jednej, spójnej definicji oraz utrzymanie publicznie dostępnego rejestru przedsiębiorców / dostawców usług komunikacji elektronicznej uznanych za podmioty kluczowe. Każdy podmiot świadczący usługi komunikacji elektronicznej na terenie RP i uznany za podmiot kluczowy powinien być ujęty w ww. rejestrze i podlegać łącznie pod rygor ustaw: Prawo komunikacji elektronicznej oraz o Krajowym Systemie Cyberbezpieczeństwa (dalej: „KSC”). W zał. nr 1 do projektu (nr UC32) wskazano jako podmioty kluczowe w sektorze Infrastruktura cyfrowa podsektor „Komunikacja Elektroniczna”, a w nim: „Przedsiębiorcę telekomunikacyjnego” oraz „Podmiot świadczący usługę komunikacji interpersonalnej niewykorzystującą numerów”. W rozumieniu projektodawcy, zastosowanie precyzyjnej definicji w przypadku „podmiotu kluczowego” jakim będą „dostawcy usług komunikacji elektronicznej” jest istotnym elementem skuteczności KSC. Rządowy projekt ustawy - Prawo Komunikacji Elektronicznej nr UC7, wniesiony do Sejmu RP w dniu 21.05.2024, posługuje się inaczej brzmiącą definicją. Jednoznaczne wskazanie podmiotu kluczowego oferującego usługi w zakresie komunikacji elektronicznej powinno być realizowane analogicznie jak w przypadku przedsiębiorców telekomunikacyjnych, z zastosowaniem adekwatnej definicji. Usługi świadczone przez podmioty posiadające status przedsiębiorców telekomunikacyjnych oraz przedsiębiorców komunikacji elektronicznej wykorzystywane między innymi przez inne podmioty kluczowe charakteryzować się powinny gwarantowanym poziomem zapewnienia cyberbezpieczeństwa, czemu w rozumieniu projektodawcy służy nowelizacja KSC.	Uwaga uwzględniona Zostanie wprowadzone odwołanie do PKE.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			Należy zwrócić też uwagę, że definicja „usługa łączności interpersonalnej” ujęta w Dyrektywie 2018/1972 oraz rządowym projekcie nr UC7 zawiera wyłączenie usług, w których interpersonalna i interaktywna komunikacja stanowi <u>wyłącznie funkcję podrzędną</u> względem innej usługi podstawowej – co przy specyficznej interpretacji mogłoby prowadzić do wyłączenia podmiotu świadczącego taką usługę z obowiązków ujętych w KSC.	
204.	Związek Pracodawców Polska Miedź	Art. 1 pkt 2 lit. j) ustawy zmieniającej, w zakresie pkt 11f)	Projektowana definicja „przedsiębiorcy komunikacji elektronicznej”, pod którym rozumie się „przedsiębiorcę telekomunikacyjnego lub podmiot świadczący usługę komunikacji interpersonalnej niewykorzystującej numerów” jest odmienna od definicji zawartej w rządowym projekcie ustawy - Prawo komunikacji elektronicznej (dalej: „projekt nr UC7”, „PKE”) w art. 2 pkt 39 (cyt. „przedsiębiorca komunikacji elektronicznej – przedsiębiorcę telekomunikacyjnego lub podmiot świadczący <u>publicznie dostępną</u> usługę komunikacji interpersonalnej niewykorzystującą numerów”). Definicja „usługa łączności interpersonalnej” ujęta w projekcie nr UC7 zawiera wyłączenie potencjalnie wpływające na finalną klasyfikację podmiotu zgodnie z proponowaną definicją w pkt 11 f). Adekwatnie do treści uwagi proponujemy zastosowanie jednej, spójnej definicji oraz utrzymanie publicznie dostępnego rejestru przedsiębiorców / dostawców usług komunikacji elektronicznej uznanych za podmioty kluczowe. Każdy podmiot świadczący usługi komunikacji elektronicznej na terenie RP i uznany za podmiot kluczowy powinien być ujęty w ww. rejestrze i podlegać łącznie pod rygor ustaw: Prawo komunikacji elektronicznej oraz o Krajowym Systemie Cyberbezpieczeństwa (dalej: „KSC”). W zał. nr 1 do projektu (nr UC32) wskazano jako podmioty kluczowe w sektorze Infrastruktura cyfrowa podsektor „Komunikacja Elektroniczna”, a w nim: „Przedsiębiorcę telekomunikacyjnego” oraz „Podmiot świadczący usługę komunikacji interpersonalnej niewykorzystującą numerów”. eW rozumieniu projektodawcy, zastosowanie precyzyjnej definicji w przypadku „podmiotu kluczowego” jakim będą „dostawcy usług komunikacji elektronicznej” jest istotnym elementem skuteczności KSC. Rządowy projekt ustawy - Prawo Komunikacji Elektronicznej nr UC7, wniesiony do Sejmu RP w dniu 21.05.2024, posługuje się inaczej brzmiącą definicją. Jednoznaczne wskazanie podmiotu kluczowego oferującego usługi w zakresie komunikacji elektronicznej powinno być realizowane analogicznie jak w przypadku przedsiębiorców telekomunikacyjnych, z zastosowaniem adekwatnej definicji. Usługi świadczone przez podmioty posiadające status przedsiębiorców telekomunikacyjnych oraz przedsiębiorców komunikacji elektronicznej wykorzystywane między innymi przez inne podmioty kluczowe charakteryzować się powinny gwarantowanym poziomem zapewnienia cyberbezpieczeństwa, czemu w rozumieniu projektodawcy służy nowelizacja KSC.u Należy zwrócić też uwagę, że definicja „usługa łączności interpersonalnej” ujęta w Dyrektywie 2018/1972 oraz rządowym projekcie nr UC7 zawiera wyłączenie usług, w których interpersonalna i interaktywna komunikacja stanowi <u>wyłącznie funkcję podrzędną</u> względem innej usługi podstawowej	Uwaga uwzględniona Zostanie wprowadzone odwołanie do PKE.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			– co przy specyficznej interpretacji mogłoby prowadzić do wyłączenia podmiotu świadczącego taką usługę z obowiązków ujętych w KSC.	
205.	ISAA Polska	Art. 2	Brak spójności z projektem ustawy – Prawo Komunikacji Elektronicznej Projekt nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa („ustawa KSC”) wykazuje brak spójności terminologicznej z równolegle procedowaną ustawą – Prawo komunikacji elektronicznej. W projekcie nowelizacji nadal występują odniesienia do ustawy – Prawo telekomunikacyjne, które ma zostać wkrótce uchylone. Dodatkowo, projekt wykorzystuje terminologię specyficzną dla projektu ustawy Prawo Komunikacji Elektronicznej, taką jak <i>"Podmiot świadczący usługę komunikacji interpersonalnej niewykorzystującej numerów"</i> . Ta niespójność terminologiczna może prowadzić do poważnych problemów interpretacyjnych, które z kolei wpłyną na efektywność i skuteczność stosowania przepisów nowelizacji. Proponujemy przeprowadzenie rewizji terminologicznej projektu nowelizacji w celu zapewnienia jego zgodności z aktualnym stanem prawnym i uniknięcia przyszłych problemów implementacyjnych.	Uwaga uwzględniona Zostanie wprowadzone odwołanie do PKE.
206.	KGHM Polska Miedź S.A.	Art. 2 pkt 5	Definicja incydentu w brzmieniu: „zdarzenie, które ma lub może mieć niekorzystny wpływ na bezpieczeństwo systemów informacyjnych”, w szczególności z uwagi na proponowaną definicję systemu informacyjnego, wydaje się niepełna. Dodatkowo przy przyjęciu założenia, że uznaje się za spełnienie wymagań art. 8 w sytuacji wdrożenia rozwiązań opartych o wymienione normy, należy przyjąć pogląd że definicja incydentu powinna pozostawać spójna z tymi normami. Również rządowy projekt ustawy nr UC7 odwołuje się do KSC w kwestii tzw. „incydentu telekomunikacyjnego”, który nie wpisuje się w ww. definicję. 5) incydent – zdarzenie, które ma lub może mieć niekorzystny wpływ na bezpieczeństwo systemów informacyjnych, produktu ICT, usługi ICT lub procesu ICT, zdarzenie, które stanowi naruszenie lub bezpośrednie zagrożenie naruszenia zasad bezpieczeństwa, procedur bezpieczeństwa lub zasad dopuszczalnego użytkowania oraz każde zdarzenie, które stwarza znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagraża bezpieczeństwu informacji. Spójne określenie definicji „incydentu” w ustawach KSC i PKE, a w przypadku stosowania odwołania do norm branżowych również z zapewnieniem zgodności z ich brzmieniem jest kluczowe dla zapewnienia właściwej identyfikacji zagrożeń, zdarzeń i ich obsługi. Spójne rozumienie definicji incydentu przez wszystkie podmioty zobowiązane do ich wykrywania i ograniczania sprzyja właściwej identyfikacji ryzyk i zagrożeń a przez to właściwemu doborowi zabezpieczeń technicznych i organizacyjnych wymienionych w art. 8.	Wyjaśnienie uwagi Definicja incydentu jest już przyjęta od kilku lat i zamierzamy ją podtrzymać. Odwołuje się ona do definicji bezpieczeństwa systemów informacyjnych, gdzie wymieniono atrybuty bezpieczeństwa informacji. Będziemy dążyć do uspoźnienia projektów KSC i PKE.
207.	PIKE	Art. 2	Definicja ‘incydentu’ stanowi nadregulację w porównaniu z dyrektywą NIS2, zgodnie z którą „incydent” oznacza zdarzenie naruszające dostępność, autentyczność, integralność lub poufność przechowywanych, przekazywanych lub przetwarzanych danych lub usług oferowanych przez sieci i systemy informatyczne lub dostępnych za ich pośrednictwem. Ponadto, zakres definicji incydentu jest problematyczny także ze względu na to, że incydemtem ma być także zdarzenie nie tylko “mające”, lecz również “mogące mieć niekorzystny wpływ” na bezpieczeństwo. Pojawia się problem rozdzielenia zakresu definicji incydentu oraz definicji ‘cyberzagrożenia’ i ‘podatności’.	Wyjaśnienie uwagi Definicja incydentu jest już przyjęta od kilku lat i zamierzamy ją podtrzymać. Odwołuje się ona do definicji bezpieczeństwa systemów informacyjnych, gdzie wymieniono atrybuty bezpieczeństwa informacji.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

208.	PIPC	Art. 2 pkt 5	Definicja incydentu w brzmieniu: „zdarzenie, które ma lub może mieć niekorzystny wpływ na bezpieczeństwo systemów informacyjnych”, w szczególności z uwagi na proponowaną definicję systemu informacyjnego, wydaje się niepełna. Dodatkowo przy przyjęciu założenia, że uznaje się za spełnienie wymagań art. 8 w sytuacji wdrożenia rozwiązań opartych o wymienione normy, należy przyjąć pogląd, że definicja incydentu powinna pozostawać spójna z tymi normami. Również rządowy projekt ustawy nr UC7 odwołuje się do KSC w kwestii tzw. „incydentu telekomunikacyjnego”, który nie wpisuje się w ww. definicję. 5) incydent – zdarzenie, które ma lub może mieć niekorzystny wpływ na bezpieczeństwo systemów informacyjnych, produktu ICT, usługi ICT lub procesu ICT, zdarzenie, które stanowi naruszenie lub bezpośrednie zagrożenie naruszenia zasad bezpieczeństwa, procedur bezpieczeństwa lub zasad dopuszczalnego użytkowania oraz każde zdarzenie, które stwarza znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagraża bezpieczeństwu informacji. Spójne określenie definicji „incydentu” w ustawach KSC i PKE, a w przypadku stosowania odwołania do norm branżowych również z zapewnieniem zgodności z ich brzmieniem jest kluczowe dla zapewnienia właściwej identyfikacji zagrożeń, zdarzeń i ich obsługi. Spójne rozumienie definicji incydentu przez wszystkie podmioty zobowiązana do ich wykrywania i ograniczania sprzyja właściwej identyfikacji ryzyk i zagrożeń a przez to właściwemu doborowi zabezpieczeń technicznych i organizacyjnych wymienionych w art. 8.	Wyjaśnienie uwagi Definicja incydentu jest już przyjęta od kilku lat i zamierzamy ją podtrzymać. Odwołuje się ona do definicji bezpieczeństwa systemów informacyjnych, gdzie wymieniono atrybuty bezpieczeństwa informacji. Będziemy dążyć do uspoźnienia projektów KSC i PKE.
209.	Związek Pracodawców Polska Miedź	Art. 2 pkt 5	Definicja incydentu w brzmieniu: „zdarzenie, które ma lub może mieć niekorzystny wpływ na bezpieczeństwo systemów informacyjnych”, w szczególności z uwagi na proponowaną definicję systemu informacyjnego, wydaje się niepełna. Dodatkowo przy przyjęciu założenia, że uznaje się za spełnienie wymagań art. 8 w sytuacji wdrożenia rozwiązań opartych o wymienione normy, należy przyjąć pogląd że definicja incydentu powinna pozostawać spójna z tymi normami. Również rządowy projekt ustawy nr UC7 odwołuje się do KSC w kwestii tzw. „incydentu telekomunikacyjnego”, który nie wpisuje się w ww. definicję. 5) incydent – zdarzenie, które ma lub może mieć niekorzystny wpływ na bezpieczeństwo systemów informacyjnych, produktu ICT, usługi ICT lub procesu ICT, zdarzenie, które stanowi naruszenie lub bezpośrednie zagrożenie naruszenia zasad bezpieczeństwa, procedur bezpieczeństwa lub zasad dopuszczalnego użytkowania oraz każde zdarzenie, które stwarza znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagraża bezpieczeństwu informacji. Spójne określenie definicji „incydentu” w ustawach KSC i PKE, a w przypadku stosowania odwołania do norm branżowych również z zapewnieniem zgodności z ich brzmieniem jest kluczowe dla zapewnienia właściwej identyfikacji zagrożeń, zdarzeń i ich obsługi. Spójne rozumienie definicji incydentu przez wszystkie podmioty zobowiązana do ich wykrywania i ograniczania sprzyja właściwej identyfikacji ryzyk i zagrożeń a przez to właściwemu doborowi zabezpieczeń technicznych i organizacyjnych wymienionych w art. 8.	Wyjaśnienie uwagi Definicja incydentu jest już przyjęta od kilku lat i zamierzamy ją podtrzymać. Odwołuje się ona do definicji bezpieczeństwa systemów informacyjnych, gdzie wymieniono atrybuty bezpieczeństwa informacji. Będziemy dążyć do uspoźnienia projektów KSC i PKE.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

210.	Krzysztof Rożko i Wspólnicy Kancelaria Prawna sp. k.	Art. 2	UWAGA ZGŁOSZONA W RAMACH ZGŁOSZENIA LOBBINGOWEGO Projekt ustawy o zmianie niektórych ustaw w związku z zapewnieniem operacyjnej odporności cyfrowej sektora finansowego (która na celu umożliwienie stosowania przepisów rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniającej rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (dalej odpowiednio „projekt ustawy wdrażającej DORA”, „Rozporządzenie 2022/2554”), przewiduje już dodanie w art. 2 pkt 11a)-c) w ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (dalej „uKSC”) o odmiennej jednakże treści.2W związku z powyższym, postulujemy koordynację pracy nad obydwo aktami prawnymi i w rezultacie dostosowanie numeracji w art. 2 uKSC.	Wyjaśnienie uwagi Dziękujemy za uwagę, trwają prace robocze pomiędzy Ministerstwem Cyfryzacji a Ministerstwem Finansów w celu uzgodnienia obydwu projektów.
211.	Krzysztof Rożko i Wspólnicy Kancelaria Prawna sp. k.	Art. 2	UWAGA ZGŁOSZONA W RAMACH ZGŁOSZENIA LOBBINGOWEGO Zwracamy uwagę, że zarówno w art. 1 pkt 2 lit. m) projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (dalej „projekt nowelizacji uKSC”), jak również projekt ustawy wdrażającej DORA przewiduje dodanie do uKSC w art. 2 pkt.20 uKSC, zawierającego definicję znaczącego cyberzagrożenia. Projekty przepisów, które przewidują wprowadzenie wskazanej definicji poprzez projekt ustawy wdrażającej DORA oraz poprzez nowelizację uKSC, w istocie dotyczą jednak różnych pojęć. W projekcie ustawy wdrażającej DORA, co zrozumiałe, posłużono się odwołaniem do definicji znaczącego cyberzagrożenia zawartej w treści Rozporządzenia 2022/2554, natomiast w nowelizacji uKSC zdecydowano się na wprowadzenie autonomicznej definicji tego pojęcia bazującej jednak na definicji „poważnego cyberzagrożenia” zawartej w art. 6 pkt 11 dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 („Dyrektywa 2022/2555”). Pomimo, że brzmienie wskazanych wyżej definicji, tj. „znaczącego cyberzagrożenia” na gruncie Rozporządzenia 2022/2554 oraz „poważnego cyberzagrożenia” zdefiniowanego w Dyrektywie 2022/2555, może wydawać się zbliżone, to szczegółowa analiza ich treści prowadzi do wniosku, że zakres obydwu definicji jest różny. Wobec powyższego proponujemy rozróżnienie rzeczonych pojęć na gruncie przepisów krajowych, tj. UKSC, poprzez odrębne zdefiniowanie: 1) „Znaczącego cyberzagrożenia związanego z ICT” – przez odwołanie do art. 3 pkt 13 Rozporządzenia 2022/2554, 2) „Poważnego cyberzagrożenia” – poprzez zastąpienie pojęcia „znaczącego cyberzagrożenia”, którym posłużono się w art. 1 pkt 2) lit. m nowelizacji uKSC, pojęciem „poważnego cyberzagrożenia”.	Wyjaśnienie uwagi Dziękujemy za uwagę, trwają prace robocze pomiędzy Ministerstwem Cyfryzacji a Ministerstwem Finansów w celu uzgodnienia obydwu projektów.
212.	Konfederacja Lewiatan	Art. 2 i art. 15	Projektowany art. 2 pkt 8a – odesłanie do ustawy o rachunkowości powinno dotyczyć art. 3 ust. 1 pkt 6, a nie art. 3 pkt 6, ponieważ ta jednostka redakcyjna jest podzielona na ustępy.	Uwaga uwzględniona Przepisy zostaną zmienione.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			W dotychczasowym art. 15 ust. 6 pozostało sformułowanie „operator usługi kluczowej”.	
213.	Osoba fizyczna	Art. 2	Pojęcia dotyczące bezpieczeństwa – Zastosowano w ustawie uKSC2 pojęcie „bezpieczeństwo systemów informacyjnych” (ref. 3c), zdefiniowane poprzez „odporność”, co nie zostało wyjaśnione. Poza tym „bezpieczeństwo systemów informacyjnych” jest charakteryzowane jako odporność na naruszenie atrybutów bezpieczeństwa danych lub usług systemów, a nie odnosi się do odporności na naruszenie atrybutów bezpieczeństwa samych systemów. Należy też zwrócić uwagę, że „bezpieczeństwo systemów informacyjnych” to synonim „cyberbezpieczeństwa”, pomimo że w ustawie zastosowano inną jego definicję. Zastosowano w ustawie również niezdefiniowane pojęcia „bezpieczeństwo cyberprzestrzeni” i „bezpieczeństwo technologii informacyjnej”, które zostały wprowadzone w nieznanym i niewyjaśnionym kontekście, co wymaga weryfikacji ich zastosowania i wprowadzenia ich definicji. Proponuję wprowadzić szereg pojęć dotyczących bezpieczeństwa, wprowadzonych zapisami, lecz nie wyjaśnionych: 1.1.1. bezpieczeństwo systemów informacyjnych – odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność tych systemów informacyjnych i realizowanych przez nie usług oraz naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych (ref. 3c), 1.1.2. odporność - (ref. 3c) 1.1.3. odporność systemów informacyjnych – (ref. 3c) 1.1.4. cyberodporność – (ref. Art. 69 ust.2 p.9) 1.1.5. bezpieczeństwo cyberprzestrzeni – proponuję zweryfikować intencję zastosowania tego pojęcia, w przypadku zasadności, wprowadzić stosowną definicję uwzględniającą definicję cyberprzestrzeni (ref. Art. 39a), 1.1.6. bezpieczeństwo technologii informacyjnej - proponuję zweryfikować intencję zastosowania tego pojęcia, w przypadku zasadności, wprowadzić stosowną definicję. Być może intencją było bezpieczeństwo systemów informacyjnych lub produktów ICT, usług ICT i procesów ICT, wtedy proponuję odpowiednio skorygować zapisy (ref. Art. 45 ust.1 p.9), 1.1.7. poziom bezpieczeństwa systemów informacyjnych – (ref. Art. 67a), 1.1.8. poziom bezpieczeństwa cyberprzestrzeni - (ref. Art. 39a)	Wyjaśnienie uwagi Bezpieczeństwo systemów informacyjnych nie jest synonimem cyberbezpieczeństwa z uwagi na odmienne potraktowanie tych pojęć w prawie unijnym. Cyberbezpieczeństwo zostało zdefiniowane w art. 2 pkt 1 rozporządzenia (UE) 2019/881 Cybersecurity act jako: „cyberbezpieczeństwo” oznacza działania niezbędne do ochrony sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób przed cyberzagrożeniami; W dyrektywie NIS2 wprowadzono z kolei Art. 6 pkt 2 „bezpieczeństwo sieci i systemów informatycznych” oznacza odporność sieci i systemów informatycznych, przy danym poziomie zaufania, na wszelkie zdarzenia, które mogą naruszyć dostępność, autentyczność, integralność lub poufność przechowywanych, przekazywanych lub przetwarzanych danych lub usług oferowanych przez te sieci i systemy informatyczne lub dostępnych za ich pośrednictwem; Skoro prawo unijne rozróżnia te dwa pojęcia tak też musi je rozróżnić prawodawca krajowy. Odporność; odporność systemów informacyjnych, poziom bezpieczeństwa systemów informacyjnych należy rozumieć zgodnie z definicją słownikową.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

214.	Osoba fizyczna	Art. 2	Pojęcia dotyczące cyberbezpieczeństwa - Zastosowano w ustawie uKSC2 definicję pojęcia „cyberbezpieczeństwo” poprzez odwołanie do rozporządzenia PE i RE 2019/881 bez przywołania treści definicji. Definicja źródłowa brzmi: „działania niezbędne do ochrony sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób przed zagrożeniami”. Zastosowanie powyższej definicji wprowadza: 1) nowe pojęcie – „sieci i systemy informatyczne”, które wymaga ulokowania w ramach definicji uKSC2, i które jest niespójne z zastosowanym w uKSC2 pojęciem „systemu informacyjnego”, który intencjonalnie zdaje się być zamiennikiem sformułowania „sieci i systemy informatyczne”, 2) pojmowanie cyberbezpieczeństwa jako realizowanych działań, bez uwzględnienie skutku w postaci jakiegoś akceptowalnego poziomu bezpieczeństwa sieci i systemów informatycznych/systemów informacyjnych. Należy zwrócić uwagę, że działania podejmowane dla ochrony obiektu mogą być scharakteryzowane jako zapewnianie bezpieczeństwa lub zarządzanie bezpieczeństwem prowadzącym do uzyskania określonego poziomu bezpieczeństwa obiektu, nie zaś bezpośrednio samym jego bezpieczeństwem. W tym kontekście cyberbezpieczeństwo, należy potraktować jako bezpieczeństwo systemów cybernetycznych, tutaj rozumianych jako informatycznych (teleinformatycznych) i należy rozumieć jako odpowiedni poziom bezpieczeństwa sieci i systemów informatycznych. Rozumienie to, dla jakiejś formy spójności z def. Rozporządzenia 2019/881 można rozszerzyć o realizację działań prowadzących do bezpieczeństwa. Proponuję zmodyfikować przyjętą definicję cyberbezpieczeństwa, np.: 1.1.1. 1) cyberbezpieczeństwo – bezpieczeństwo sieci i systemów informatycznych oraz ich użytkowników (lub adekwatnie – bezpieczeństwo systemów informacyjnych oraz ich użytkowników), albo alternatywnie: 2) cyberbezpieczeństwo – działania oraz rozwiązania organizacyjne i techniczne zapewniające ochronę i odpowiedni poziom bezpieczeństwa sieci i systemów informatycznych oraz ich użytkowników przed cyberzagrożeniami (lub adekwatnie – działania oraz rozwiązania organizacyjne i techniczne zapewniające ochronę i odpowiedni poziom bezpieczeństwa systemów informacyjnych oraz ich użytkowników przed cyberzagrożeniami).	Wyjaśnienie uwagi W przypadku definicji cyberbezpieczeństwa prawodawca krajowy nie może jej transponować w innym brzmieniu. Definicja ta pochodzi z unijnego aktu o cyberbezpieczeństwie, który jest aktem bezpośrednio stosowalnym w Unii Europejskiej zgodnie z zasadą pierwszeństwa prawa unijnego. Jakkolwiek transpozycja tego pojęcia do polskiego prawa przez inne sformułowanie skutkowałaby ryzykiem naruszenia traktatów unijnych.
215.	Osoba fizyczna	Art. 2	Pojęcia dotyczące systemów informacyjnych – Zastosowano w ustawie uKSC2 pojęcie „system informacyjny”. Można przyjąć, że jest to intencjonalne zastosowanie, jako zamiennika stosowanego w NIS2 pojęcia „sieci i systemy informatyczne”. Należy zwrócić uwagę, że zakres definicji NIS2 obejmuje sieci i systemy informatyczne oraz dane, a zakres definicji systemu informacyjnego uKSC2 obejmuje system teleinformatyczny (zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego) oraz grupę połączonych urządzeń i oprogramowania zaprogramowanych w celu przetwarzania danych i dane. Jak widać, definicja pojęcia zawiera 2 zdublowane charakterystyki	Wyjaśnienie uwagi Definicja systemu informacyjnego obejmuje sieć telekomunikacyjną Cyberprzestrzeń została zdefiniowana w m.in. ustawie o stanie wyjątkowym. Sieć telekomunikacyjna jest zdefiniowana w Prawie telekomunikacyjnym/Prawie komunikacji elektronicznej.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			systemu, natomiast nie zawiera elementu sieci telekomunikacyjnej. W związku z czym definicja pojęcia „system informacyjny” powinna zostać 1) zredukowana w aktualnej treści i 2) rozszerzona o sieć telekomunikacyjną (np. środki komunikacji elektronicznej – środki komunikacji elektronicznej w rozumieniu art. 2 pkt 5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną; sieć telekomunikacyjna – systemy transmisyjne oraz urządzenia komutacyjne lub przekierowujące, a także inne zasoby, w tym nieaktywne elementy sieci, które umożliwiają nadawanie, odbiór lub transmisję sygnałów za pomocą przewodów, fal radiowych, optycznych lub innych środków wykorzystujących energię elektromagnetyczną, niezależnie od ich rodzaju – ustawa PT, art. 2 p.35), dla zapewnienia pełnego zakresu funkcjonalnego i strukturalnego systemu informacyjnego oraz dla możliwości identyfikowania systemu przedsiębiorców telekomunikacyjnych. Proponuję zmodyfikować przyjętą definicję systemu informacyjnego oraz wprowadzić nowe pojęcie, wprowadzone zapisami, lecz nie wyjaśnione: 1.1.1. „system informacyjny” – zmodyfikowane pojęcie, adresujące w zakresie system informatyczny, sieć i dane (ref. 14), 1.1.2. „cyberprzestrzeń” – sieć połączonych systemów informacyjnych, 1.1.3. „sieć telekomunikacyjna” – systemy transmisyjne oraz urządzenia komutacyjne lub przekierowujące, a także inne zasoby, w tym nieaktywne elementy sieci, które umożliwiają nadawanie, odbiór lub transmisję sygnałów za pomocą przewodów, fal radiowych, optycznych lub innych środków wykorzystujących energię elektromagnetyczną, niezależnie od ich rodzaju (ref. ustawa PT, art. 2 p.35), 1.1.4. „krytyczna infrastruktura informatyczna” - proponuję wprowadzić definicję tego pojęcia (ref. Art. 72b ust.2 p.6).	W art. 72 odeszliśmy od pojęcia krytycznej infrastruktury informatycznej.
216.	Osoba fizyczna	Art. 2	Pojęcia dotyczące ICT – Zastosowano w ustawie uKSC2 pojęcia „sprzęt i oprogramowanie” oraz „produkty ICT, usługi ICT i procesy ICT”, które często stosowane są zamiennie, zdaje się nierozważnie i niezasadnie. Zdaje się, że zwrot „sprzęt i oprogramowanie” służy do określania rodzaju dostawcy – „dostawca sprzętu i oprogramowania”, natomiast konkretne produkty tegoż sprzętu i oprogramowania są określane jako „produkty ICT, usługi ICT i procesy ICT”. W tekście uKSC2 jednorazowo pojawiło się pojęcie „technologii informacyjnej” w kontekście „bezpieczeństwa technologii informacyjnej” - być może intencją było bezpieczeństwo „systemów informacyjnych” lub „produktów ICT, usług ICT i procesów ICT” (ref. Art. 45 ust.1 p.9). Proponuję przyjąć jednoznaczne rozumienie tych pojęć i ich jednoznaczne stosowanie w całym dokumencie, co wymaga stosownych korekt. Proponuję wprowadzić pojęcie „sprzęt i oprogramowanie”.	Wyjaśnienie uwagi Przyjęta siatka pojęciowa wynika z obowiązujących przepisów prawa europejskiego w tym obszarze i służy to zapewnieniu spójności przepisów krajowych z europejskimi.
217.	Osoba fizyczna	Art. 2	Pojęcia dotyczące zdarzeń i incydentów – Zastosowano w ustawie uKSC2 pojęcia wraz z wyjaśnieniami: cyberzagrożenie, znaczące cyberzagrożenie (w tekście pojawia się poważne cyberzagrożenie, definicja NIS2 jest niespójna z definicją uKSC2), incydent, incydent poważny, incydent krytyczny, incydent w cyberbezpieczeństwie na dużą skalę, obsługa incydentu. Pojęcie	Uwaga częściowo uwzględniona Definicja poważnego cyberzagrożenia została zmieniona.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			„incydent” jest zdefiniowane jako zdarzenie, które ma lub może mieć niekorzystny wpływ. Jest to dotychczasowa definicja, przyjęta z ISO 27001. Należy zwrócić uwagę, że incydent jest zdarzeniem zaistniałym mającym niekorzystne skutki, w przeciwnym razie powinno być traktowane jako zdarzenie dla cyberbezpieczeństwa. Takie podejście jest zastosowane w NIS2, w związku z czym proponuję przyjąć definicję NIS2 dla incydentu i potencjalnego zdarzenia dla cyberbezpieczeństwa. Zastosowano w tekście również pojęcia, które nie zostały wyjaśnione definicyjnie. Proponuję zmodyfikować przyjętą definicję incydentu oraz wprowadzić nowe pojęcia, wprowadzone zapisami, lecz nie wyjaśnione: 1.1.1. „incydent” – zdarzenie, które ma niekorzystny wpływ na bezpieczeństwo systemów informacyjnych, 1.1.2. „potencjalne zdarzenie dla cyberbezpieczeństwa” – proponuję przyjąć definicję NIS2, 1.1.3. „skoordynowane zarządzanie incydentami” - (ref. Art. 27b ust.2 p.7), 1.1.4. <u>poważne/znaczące cyberzagrożenie – proponuję przyjąć definicję NIS2</u>	
218.	Osoba fizyczna	Art. 2	Pojęcia dotyczące sytuacji kryzysowych i zarządzania kryzysowego w cyberbezpieczeństwie – Zastosowano w ustawie uKSC2 pojęcia dotyczące sytuacji kryzysowych i zarządzania kryzysowego w cyberbezpieczeństwie bez sformułowania ich definicji. Zastosowano pojęcie „sytuacja kryzysowa w cyberbezpieczeństwie”, należy ustalić intencje jego zastosowania, czy może chodzi o sytuacje kryzysowe w bezpieczeństwie systemów informacyjnych (ref. art. 62a ust.6 p.5). Proponuję wprowadzić nowe pojęcia, wprowadzone zapisami, lecz nie wyjaśnione: 1.1.1. „sytuacja kryzysowa w cyberbezpieczeństwie” - (ref. art. 62a ust.6 p.5), 1.1.2. „zarządzanie kryzysowe w cyberbezpieczeństwie” - (ref. Art. 72b ust.2 p.7), 1.1.3. „zarządzanie kryzysowe w cyberbezpieczeństwie na dużą skalę” – (ref. Art. 72b ust.2 p.7), 1.1.4. „skoordynowane zarządzanie kryzysowe w cyberbezpieczeństwie” - (ref. Art. 72b ust.2 p.7), 1.1.5. „skoordynowane zarządzanie kryzysowe w cyberbezpieczeństwie na dużą skalę” – (ref. Art. 72b ust.2 p.7).	Uwaga nieuwzględniona Naszym zdaniem nie ma potrzeby definiowania tych pojęć. Zarządzanie kryzysowe jest zdefiniowane w ustawie o zarządzaniu kryzysowym.
219.	Osoba fizyczna	Art. 2	Pojęcie usługi – Zastosowano w ustawie uKSC2 wielokrotnie pojęcie usługi świadczonej przez podmioty kluczowe i ważne oraz wielokrotne i wielokontekstowe odniesienia do niej, do relacji usług różnych podmiotów, zależności usług od systemu informacyjnego, ciągłości i jakości usługi, jednak nie została ona zdefiniowana. Usługi podmiotów powinny być zdefiniowane dla jasnego i konkretnego rozumienia i realizacji wielu zapisów ustawy i całego KSC. Nie zaś tylko na potrzeby systemu S46, bo to nie wyjaśni sensu organizacji KSC. Wprowadzony art. 21a uszczegóławia pojęcie usługi podmiotu publicznego, co jest uzasadnieniem do sprecyzowania tego pojęcia dla wszystkich podmiotów. Proponuję, żeby definiowanie usług zostało przeprowadzone w odniesieniu do sektorów i podsektorów oraz rodzajów podmiotów, wskazanych w Załącznikach NIS2 i uKSC2, z rodzajów podmiotów można wyprowadzić rodzaje działalności, a te zidentyfikować i powiązać z kodami	Wyjaśnienie uwagi Pojęcie usługi należy rozumieć słownikowo.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			działalności określonymi w PKD/EKD, a następnie wyprowadzić z nich usługi. Katalog usług KSC jest aktualnie zdefiniowany w rozporządzeniu do UKSC, proponuję go rozszerzyć do pełnego zakresu, pokrywającego pełny zbiór rodzajów działalności podmiotów z Zał. 1 i 1 NIS2/uKSC2. Proponuję wprowadzić nowe pojęcie, wprowadzone zapisami, lecz nie wyjaśnione: 1.1.1. „usługa podmiotu kluczowego i podmiotu ważnego” – proponuję, żeby definicja obejmowała usługę, jak wywiedzione powyżej, łącznie z procesami niezbędnymi do jej realizacji i systemem informacyjnym, od którego zależne jest świadczenie usługi.	
220.	Osoba fizyczna	Art. 2	Zastosowano w ustawie definicje pojęć poprzez odwołanie do rozporządzenia PE i RE 2019/881 bez przywołania treści definicji. Przyjmując, że utrwalona została praktyka przywoływania innych regulacji, zasadnym i ekonomicznym byłoby zaprezentowanie źródłowych zapisów choćby w przypisie. Jeśli choćby tysiąc osób zainteresowanych przepisami uKSC jednocześnie będzie szukać treści źródłowej przez 1 godz., to łącznie wszystkim zajmie to 1 tys. godzin, co stanowi ponad półroczny etatowy wymiar pracy pojedynczej osoby. Zdajemy sobie sprawę, że osób zainteresowanych nowelizacją uKSC są setki tysięcy, więc takie praktyki eliminują dożywno kilkadziesiąt osób z rynku pracy. Proponuję przy każdym odwołaniu do definicji w innej regulacji, choćby w przypisie przywoływać tekst źródłowy.	Uwaga nieuwzględniona Zgodnie z zasadami techniki prawodawczej nie kopiuje się norm prawnych z innych aktów prawnych, ale odwołuje się do nich.
221.	PGE SA	Art. 2	Podczas przeglądu naszą uwagę zwracają niekonsekwencje w definicjach (art. 2 ustawy), co prowadzi do niejednoznaczności, które w przyszłości mogą przełożyć się na rozbieżności interpretacyjne w trakcie audytów. Podobne rozbieżności w wykładni zmienionych przepisów mogą mieć miejsce w trakcie ewentualnych sporów sądowych. Niejednoznaczności dotyczą w szczególności definicji: <i>bezpieczeństwo systemów informacyjnych</i>, <i>cyberbezpieczeństwo</i>, <i>system teleinformatyczny</i>. Ponadto, w trakcie analizy przepisów projektu zwracają uwagę takie rozbieżności jak: - <i>bezpieczeństwo systemów informacyjnych</i> definiowane jest jako własność aktywa, natomiast <i>cyberbezpieczeństwo</i> definiowane jest jako działanie. - pkt 11) definicja podatności odnosi się tylko do ICT - ustawa nie powinna odwoływać się tylko do ICT, nie wskazując na OT. - pkt 11h) proces ICT, 11i) produkt ICT, 11j) usługa ICT – jak powyżej, odwołanie jest tylko do ICT. - pkt 14) rozumienie pojęcia <i>system informacyjny</i> - należałoby zastosować spójnie do definicji wprowadzonych w punktach 11h, 11i, 11j. Wtedy te definicje obejmą również produkty, usługi i procesy w systemach z obszaru OT. Nie proponujemy własnych definicji, niemniej prosimy o weryfikację wprowadzonych i zmienianych definicji i logiczne ułożenie definicji w sposób eliminujący rozbieżności.	Wyjaśnienie uwagi Definicje cyberbezpieczeństwa oraz bezpieczeństwa systemów wynikają z odrębnego potraktowania tych pojęć na gruncie prawa unijnego. Definicja systemu informacyjnego ma za zadanie objąć także systemy OT.
222.	Fundacja Bezpieczna Cyberprzestrzeń	Art. 2	art. 1 pkt 2 lit. c, treść pkt. 4i – proponuje się nadać definicji następujące brzmienie: „4i. dostawca usług zarządzanych w zakresie cyberbezpieczeństwa – dostawca usług zarządzanych, który świadczy usługi z zakresu cyberbezpieczeństwa lub zapewnia pomoc dla tych działań”. Proponowane w nowelizacji brzmienie może powodować błędną interpretację, ograniczającą możliwość skorzystania ze wsparcia podmiotów zewnętrznych jedynie w sprawach związanych z wąskim rozumieniem zarządzania ryzykiem (tym bardziej, że brzmienie art. 1 pkt 19 nie uwzględnia	Wyjaśnienie uwagi Dyrektywa szeroko traktuje pojęcie środków zarządzania ryzykiem, ujmując w nich także np. obsługę incydentów. Art. 14 ust. 1 zostanie przywrócony.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			ryzyka „w zakresie cyberbezpieczeństwa”). Ponadto proponowane powyżej brzmienie będzie podobne do zastosowanego w art 14 ust. 1 nowelizowanej ustawy, do którego dostawcy usług kluczowych i podmioty świadczące usługi z zakresu cyberbezpieczeństwa się przyzwyczaiły i stosowały w opracowanych dokumentach.	
223.	Fundacja Bezpieczna Cyberprzestrzeń	Art. 2	Art. 1 pkt 2 lit. e, treść pkt. 8 – taka definicja incydentu w cyberbezpieczeństwie na dużą skalę nie uwzględnia sytuacji, w których incydent poważny nie przekroczy zdolności reagowania państwa, a będzie miał wpływ na wiele podmiotów ważnych i kluczowych (lub sytuacji wielu incydentów poważnych jednocześnie). W praktyce tak zdefiniowany incydent w cyberbezpieczeństwie na dużą skalę będzie dotyczył jedynie zdarzeń mających charakter międzynarodowy i w istocie będzie wymagał skoordynowanej reakcji wspólnotowej lub sojuszniczej (NATO). Ponadto obecna definicja incydentu krytycznego uwzględnia „znaczną szkodę dla interesów międzynarodowych” RP, zatem niejako zawarte są w niej przesłanki definicji incydentu w cyberbezpieczeństwie na dużą skalę. W związku z powyższym proponuje się rezygnację z tej definicji lub powiązanie jej z wejściami do standardowych procedur operacyjnych z Krajowego Planu Zarządzania Kryzysowego w zakresie cyberzagrożeń np.: „incydent w cyberbezpieczeństwie na dużą skalę – sytuacja szczególnego zagrożenia konstytucyjnego ustroju państwa, bezpieczeństwa obywateli lub porządku publicznego spowodowana działaniami w cyberprzestrzeni, które nie może być usunięte poprzez użycie dostępnych środków reagowania” lub „ incydent w cyberbezpieczeństwie na dużą skalę – incydent lub seria incydentów skutkująca wystąpieniem lub wysokim prawdopodobieństwem wystąpienia incydentu krytycznego”.	Wyjaśnienie uwagi Tak, definicja incydentu w cyberbezpieczeństwie na dużą skalę to kwalifikowana postać incydentu krytycznego, który przekracza możliwości państwa lub wywiera znaczące skutki w 2 lub więcej państwach EU. Jest to też zgodne z pojęciem z dyrektywy NIS2 „7) „incydent w cyberbezpieczeństwie na dużą skalę” oznacza incydent, który powoduje zakłócenia na poziomie przekraczającym zdolność państwa członkowskiego do reagowania na ten incydent lub który wywiera znaczące skutki w co najmniej dwóch państwach członkowskich;”.
224.	Fundacja Bezpieczna Cyberprzestrzeń	Art. 2	Art. 1 pkt 2 lit. m, treść pkt 20 – jaki jest cel wprowadzenia tej definicji? W ustawie wykorzystywane jest ono jedynie w celu informacyjnym. Lepszym rozwiązaniem wydaje się by umożliwić podmiotom kluczowym i ważnym informowanie użytkowników o każdym rodzaju zagrożenia, wymagającego od nich podjęcia działań prewencyjnych (zapobiegawczych). Organom właściwym natomiast umożliwić nakazanie informowania o wszelkiego rodzaju cyberzagrożeniach (art. 53 ust. 5 lit. 4). W opinii FBC ograniczy to próby interpretowania co jest znaczącym cyberzagrożeniem, a co nim nie jest. W związku z powyższym proponuje się usunąć punkt 20.n	Wyjaśnienie uwagi Definicja znaczącego cyberzagrożenia wdraża art. 6 pkt 11 dyrektywy NIS2 czyli „11) „poważne cyberzagrożenie” oznacza cyberzagrożenie, co do którego można założyć w oparciu o jego charakterystykę techniczną, że może wywrzeć znaczący wpływ na sieć i systemy informatyczne danego podmiotu lub użytkowników, korzystających z usług tego podmiotu, powodując i znaczne szkody majątkowe lub niemajątkowe;”. Jest to dalej powiązane z art. 23 ust. 2 dyrektywy NIS2. Art. 9 projektu nakazuje podmiotowi kluczowemu i ważnemu informowanie o bieżących cyberzagrożeniach – basic cyberawareness. Natomiast nie można

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

				tutaj przesadzić, ponieważ informowanie o każdym cyberzagrożeniu stanowiło by niepotrzebne obciążenie działów bezpieczeństwa oraz znużyłoby odbiorców tych informacji, co byłoby kontrproduktywne.
225.	Międzynarodowego Centrum Bezpieczeństwa Chemicznego	Art. 2	Dodanie definicji kwalifikacji zawodowych Propozycja zapisu: W art. 2 [Objaśnienie pojęć] dodaje się punkt definiujący kwalifikacje zawodowe: „<i>kwalifikacje zawodowe w zakresie niezawodności i cyberbezpieczeństwa w przemyśle – zestaw efektów uczenia się wymaganych do zarządzania ryzykiem, identyfikacji zagrożeń, analizy incydentów oraz wdrażania polityki bezpieczeństwa w systemach przemysłowych, zgodnie z normami prawnymi i branżowymi standardami.</i>” Uzasadnienie: Ustanowienie jednoznacznej definicji kwalifikacji zawodowych pozwoli na jasne określenie wymagań dla specjalistów odpowiedzialnych za cyberbezpieczeństwo w przemyśle. Zgodnie z art. 11 Dyrektywy NIS 2, CSIRT promują przyjmowanie i stosowanie wspólnych lub znormalizowanych praktyk, systemów klasyfikacji i systematyki związanych z: a) procedurami obsługi incydentu; b) zarządzaniem kryzysowym; oraz c) skoordynowanym ujawnianiem podatności podkreśla znaczenie wdrażania środków zarządzania ryzykiem cyberbezpieczeństwa. Dlatego kwalifikacje zawodowe są kluczowe dla skutecznej realizacji tych zadań. m	Uwaga nieuwzględniona Kwestia ta wykracza poza dyrektywę NIS2.
226.	Rada Bezpieczeństwa Biznesowego Grupy MiSOT	Art. 2	Art 2 pkt 4f KSC: „dostawca usług DNS - podmiot, który świadczy dostępne publicznie rekurencyjne usługi rozpoznawania nazw domen na rzecz użytkowników końcowych internetu lub autorytatywne usługi rozpoznawania nazw domen do użytku osób trzecich, z wyjątkiem głównych serwerów nazw” Uzasadnienie: Z uwagi na znaczenie słowa “publiczny” w języku polskim prosimy o takie doprecyzowanie tego punktu, aby wskazywał on rzeczywiście na serwery dostępne dla wszystkich. Słowo “publiczny” odnosi się również w swojej definicji do zamkniętych grup lub społeczności, a to powoduje, że każdy serwer DNS zostanie objęty tą definicją. Pragniemy również zwrócić uwagę, że serwery autorytatywne DNS są często używane przez operatorów i do potrzeb technicznych. Wygodnego oznaczania urządzeń sieciowych. Wskazują wtedy co prawda na adresy z klas prywatnych, ale są autorytatywne w rozumieniu definicji takiego serwera. Tu też prosilibyśmy aby dokonano bezpiecznej zmiany w tym zakresie, aby właśnie takie serwery wykluczyć z tej definicji.	Uwaga uwzględniona Przepis zostanie zmodyfikowany – wprowadzimy odniesienie, że chodzi o usługi DNS dostępne dla ogółu użytkowników.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

227.	Stowarzyszenie Bezpieczeństwo Informacji w Telekomunikacji	Art. 2	W całej ustawie ujednolicić pojęcie: „Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego”. Pojęcie „incydent bezpieczeństwa komputerowego” nie jest zdefiniowany ani w ustawie o Krajowym systemie cyberbezpieczeństwa ani w projekcie ustawy o zmianie ustawy o KSC. Proponuje się zmienić tę definicję i nadać jej brzmienie: „Zespół Reagowania na Incydenty Bezpieczeństwa Systemu Informacyjnego”. Zdefiniowane w uKSC pojęcia „incydentów” odnoszą się do systemów informacyjnych.	Uwaga nieuwzględniona Pojęcie Zespołów Reagowania na Incydenty Bezpieczeństwa Komputerowego jest już stosowane od wdrożenia dyrektywy NIS i jest rozpoznawalne. Nie ma potrzeby jego zmiany.
228.	Stowarzyszenie Bezpieczeństwo Informacji w Telekomunikacji	Art. 2	Art. 2 pkt 11 f i 5 ust. 2 pkt 3 (oraz w tekście Projektu) do czasu opublikowania ustawy PKE nie używać pojęć „przedsiębiorca komunikacji elektronicznej” Użycie takiego pojęcia może skutkować trudnościami w zrozumieniu przepisów. Po uchwaleniu uPKE konieczna będzie nowelizacja ustawy o KSC.	Wyjaśnienie uwagi Projektodawca zdaje sobie sprawę z relacji przedmiotowego projektu z PKE. Po wejściu w życie PKE projekt zostanie dostosowany do nowej siatki pojęciowej.
229.	ZBP	Art. 2 pkt 3a	3a) centrum wymiany i analiz informacji - podmiot, o którym mowa w art. 4 ust. 1 pkt 59 ustawy z dnia ustawy z 29 sierpnia 1997 r. – Prawo Bankowe Wprowadzenie do ustawy pojęcia wprowadzonego w związku z proponowanymi zmianami w ustawie – Prawo Bankowe.	Uwaga nieuwzględniona Nie przewiduje się zmian w Prawie bankowym.
230.	Konfederacja Lewiatan	Art. 2 pkt 3c	Nowa definicja bezpieczeństwa systemów informacyjnych określa je jako: <i>odporność systemów informacyjnych na zdarzenia naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy.</i> Odpowiednia definicja w dyrektywy NIS2 wskazuje natomiast, że <i>bezpieczeństwo sieci i systemów informatycznych</i> ” oznacza <i>odporność sieci i systemów informatycznych, przy danym poziomie zaufania, na wszelkie zdarzenia, które mogą naruszyć dostępność, autentyczność, integralność lub poufność przechowywanych, przekazywanych lub przetwarzanych danych lub usług oferowanych przez te sieci i systemy informatyczne lub dostępnych za ich pośrednictwem</i> Różnica polega w szczególności na pominięciu w krajowej definicji zwrotu „przy danym poziomie zaufania”. Zmieniono także kolejność wylistowania atrybutów bezpieczeństwa. W pierwszej kolejności wnosimy o wyjaśnienie dla dokonania takich modyfikacji wobec dyrektywy NIS2, szczególnie, że w samym uzasadnieniu wskazano, że <i>Wprowadzone zmiany zapewnią spójność siatki pojęciowej wykorzystywanych we wszystkich krajach Unii Europejskiej.</i> Pominięcie w definicji stwierdzenia „na danym poziomie pewności” zmienia istotę tego wymagania i może nie pozostawać bez wpływu na zakres obowiązków dostawcy usług, a w konsekwencji może również wpłynąć na zakres jego odpowiedzialności. Z tego względu wnioskujemy o uzupełnienie tego braku.	Uwaga uwzględniona Przepis zostanie zmieniony.
231.	Konfederacja Lewiatan	Art. 2 pkt 4b	Jednostka redakcyjna: art. 2 pkt 4b) projektu KSC Jednostka redakcyjna NIS2: art. 6 pkt 32) Uwaga: Definicja dostawcy sieci dostarczania treści (CDN) mówi o "osobie fizycznej, osobie prawnej albo jednostce organizacyjnej nieposiadającej osobowości prawnej, która dostarcza sieci rozproszonych geograficznie serwerów służących zapewnieniu wysokiej i łatwej dostępności treści i	Uwaga uwzględniona Zostanie wprowadzone wyłączenie że nie dotyczy to przedsiębiorców komunikacji elektronicznej.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			usług cyfrowych lub ich szybkiego dostarczania na rzecz użytkowników internetu w imieniu dostawców treści i usług". Istnieją kluczowe elementy tej definicji, które mogą umożliwić zaliczenie operatorów telekomunikacyjnych do kategorii dostawców CDN: a) "<i>Dostarcza sieci rozproszonych geograficznie serwerów</i>" - operator telekomunikacyjny zazwyczaj zarządza rozległą infrastrukturą sieciową, która obejmuje serwery i inne urządzenia telekomunikacyjne rozmieszczone geograficznie w różnych lokalizacjach, aby zapewnić pokrycie sieci i usług na dużą skalę. Choć głównym celem jest zapewnienie dostępu do sieci, infrastruktura ta technicznie spełnia kryterium "sieci rozproszonych geograficznie serwerów". b) "<i>Służących zapewnieniu wysokiej i łatwej dostępności treści i usług cyfrowych lub ich szybkiego dostarczania</i>" - w ramach swojej działalności operator telekomunikacyjny często oferuje usługi, które zapewniają dostęp do cyfrowych treści i usług (np. dostęp do internetu, usługi streamingowe, hosting). Infrastruktura ta jest kluczowa w utrzymaniu wysokiej dostępności i wydajności dostarczania tych usług, co jest zgodne z rolą CDN w kontekście szybkiego dostarczania treści. c) "<i>Na rzecz użytkowników internetu w imieniu dostawców treści i usług</i>" - operator telekomunikacyjny świadczy usługi, które umożliwiają dostarczanie treści od dostawców treści do użytkowników końcowych. Operator działa jako kluczowe ogniwo w łańcuchu dostarczania treści od producentów do konsumentów. Zaproponowana definicja może prowadzić do wniosku, że operator telekomunikacyjny spełnia niektóre z kluczowych kryteriów definiujących dostawcę CDN. Definicja jest na tyle szeroka, że technicznie obejmuje działalność operatora telekomunikacyjnego w kontekście zarządzania i dystrybucji cyfrowych treści i usług. Wprowadzona w projekcie nowelizacji definicja dostawcy sieci dostarczania treści (CDN) jest niezwykle szeroka, co może prowadzić do niezamierzonych konsekwencji. Zgodnie z proponowanym art. 2 pkt 4b, każdy podmiot świadczący usługi CDN, niezależnie od stopnia technicznego zaangażowania w proces ich tworzenia, może zostać uznany za podmiot kluczowy. Taka sytuacja stawia pod znakiem zapytania m.in. status dostawców treści rozrywkowych, takich jak platformy VOD, które z założenia nie zajmują się zarządzaniem infrastrukturą krytyczną. Klasyfikacja tych podmiotów jako kluczowych nałoży na nie obowiązki typowe dla sektora ochrony infrastruktury krytycznej, takie jak rygorystyczne wymogi bezpieczeństwa czy obowiązkowe audyty, co może być nieadekwatne do charakteru ich działalności. Zaleca się dokładniejsze określenie kryteriów klasyfikacji dostawców CDN, by ograniczyć tę definicję tylko do tych podmiotów, które faktycznie odpowiadają za kluczowe aspekty infrastruktury krytycznej, unikając nadmiernego obciążenia podmiotów, których główna działalność nie wiąże się bezpośrednio z zagrożeniami dla cyberbezpieczeństwa.	
232.	ISACA	Art. 2 pkt 4b	Ryzyko nieadekwatnego zakwalifikowania dostawców sieci CDN jako podmiotów kluczowych Wprowadzona w projekcie nowelizacji definicja dostawcy sieci dostarczania treści (CDN) jest niezwykle szeroka, co może prowadzić do niezamierzonych	Uwaga uwzględniona Zostanie wprowadzone wyłączenie, że nie dotyczy to przedsiębiorców komunikacji elektronicznej.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			konsekwencji. Zgodnie z proponowanym art. 2 pkt 4b, każdy podmiot świadczący usługi CDN, niezależnie od stopnia technicznego zaangażowania w proces ich tworzenia, może zostać uznany za podmiot kluczowy. Taka sytuacja stawia pod znakiem zapytania m.in. status dostawców treści rozrywkowych, takich jak platformy VOD, które z założenia nie zajmują się zarządzaniem infrastrukturą krytyczną. Klasyfikacja tych podmiotów jako kluczowych nałoży na nie obowiązki typowe dla sektora ochrony infrastruktury krytycznej, takie jak rygorystyczne wymogi bezpieczeństwa czy obowiązkowe audyty, co może być nieadekwatne do charakteru ich działalności. Zaleca się dokładniejsze określenie kryteriów klasyfikacji dostawców CDN, by ograniczyć tę definicję tylko do tych podmiotów, które faktycznie odpowiadają za kluczowe aspekty infrastruktury krytycznej, unikając nadmiernego obciążenia podmiotów, których główna działalność nie powoduje bezpośrednio zagrożeń dla bezpieczeństwa państwa.	
233.	Konfederacja Lewiatan	Art. 2 pkt 4d	Jednostka redakcyjna: art. 2 pkt 4d) projektu KSC Jednostka redakcyjna NIS2: art. 6 pkt 28) Uwaga: Nie ma konieczności tworzenia autonomicznej definicji dostawy internetowej platformy handlowej, ponieważ jest już ona zdefiniowana w art. 2 pkt 9 ustawy o prawach konsumenta. Z tego samego założenia wychodzi ustawodawca europejski, odsyłając w tym zakresie do postanowień Dyrektywy 2005/29/WE. W tym przypadku nie ma potrzeby stosowania § 146 ust. 1 pkt 4) Zasad techniki prawodawczej, ponieważ nie ma potrzeby ustalania nowego znaczenia danego określenia.	Uwaga uwzględniona Przepis zostanie zmieniony.
234.	ZBP	Art. 2 pkt 5	incydent – zdarzenie, które ma lub może mieć niekorzystny wpływ na bezpieczeństwo systemów informacyjnych Incydent - każde zdarzenie, które ma rzeczywisty niekorzystny wpływ na bezpieczeństwo systemów informacyjnych; Obecne brzmienie propozycji powoduje że wszelkie zmiany wynikające z potrzeb poprawy systemów w przedsiębiorstwie (zauważone luki czy podatności nawet mitygowane w inny sposób) będą traktowane jako incydent ze względu na potencjalny wpływ na bezpieczeństwo. W związku z powyższym, proponujemy aby jako incydent kwalifikowane były wyłącznie zdarzenia, które wykazują rzeczywisty wpływ na bezpieczeństwo systemów.	Uwaga nieuwzględniona Definicja incydentu obowiązuje od 2018 r. i istnieje już ugruntowana praktyka związana z jej stosowaniem. Intencją tej definicji było to, aby zbierane a potem raportowane do CSIRT były zdarzenia potencjalne, dzięki czemu CSIRT może ostrzec pozostałe podmioty o zagrożeniu.
235.	Konfederacja Lewiatan	Art. 2 pkt 5	Jednostka redakcyjna: art. 2 pkt 5) projektu KSC Jednostka redakcyjna NIS2: art. 6 pkt 6) Uwaga: Zgodnie z art. 6 pkt 6) NIS2, incydent oznacza zdarzenie naruszające dostępność, autentyczność, integralność lub poufność przechowywanych, przekazywanych lub przetwarzanych danych lub usług oferowanych przez sieci i systemy informatyczne lub dostępnych za ich pośrednictwem. Natomiast projektodawca proponuje definicję, zgodnie z którą incydent to zdarzenie, które ma lub może mieć niekorzystny wpływ na bezpieczeństwo systemów informacyjnych. Proponowana definicja jest na tyle ogólna, że potencjalnie każde zdarzenie, które w jakikolwiek sposób wpłynie lub mogłoby wpłynąć na systemy informacyjne, może być uznane za incydent. To	Uwaga nieuwzględniona Definicja incydentu obowiązuje od 2018 r. i istnieje już ugruntowana praktyka związana z jej stosowaniem. Intencją tej definicji było to, aby zbierane a potem raportowane do CSIRT były zdarzenia potencjalne, dzięki czemu CSIRT może ostrzec pozostałe podmioty o zagrożeniu.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			proceeds to a situation, in which it is difficult to distinguish real incidents from events. Lack of clear criteria regarding this, what exactly constitutes a breach of security, may hinder effective management of incidents. Organizations and bodies responsible for cybersecurity may have difficulties with definition, which events require reporting and what actions should be taken. Definition, which may cover almost every event, also increases the risk of excessive burden of the organization with the obligation of reporting. It may lead to a too large number of reports, which burdens both reporting entities, as well as supervisory bodies, and it may also divert attention from more critical threats. Therefore, it is necessary to adapt the definition of an incident in the project to NIS2 standards, to ensure clarity and precision in the scope of reporting obligations and effective management of incidents.	
236.	Związek Cyfrowa Polska	Art. 2 pkt 7	Zgodnie z art. 2 pkt 7 projektu, poważny incydent jest opisany między innymi jako incydent, który wpływa na inne podmioty powodując szkodę materialną lub niematerialną (w porównaniu z definicją w art. 23 ust. 3 lit. b dyrektywy NIS2, projekt nie zawiera odniesienia do „znacznej” szkody oraz do incydentu, który nie tylko wpływa, ale również „może wpływać” na osoby).	Uwaga uwzględniona Definicja poważnego incydentu zostanie poprawiona poprzez uwzględnienie znacznej szkody oraz możliwości wpływu na osoby.
237.	Konfederacja Lewiatan	Art. 2 pkt 7	Definicja incydentu poważnego niezgodna z NIS2, skutkująca znaczącym rozszerzeniem zakresu regulacji Jednostka redakcyjna: art. 2 pkt 7) projektu KSC Jednostka redakcyjna NIS2: art. 23 ust. 2 Uwaga: Projektodawca proponuje rozszerzenie definicji incydentu poważnego, określonego w art. 23 ust. 2 dyrektywy NIS2. Zgodnie z NIS2, incydent uznaje się za poważny, jeżeli ma on poważne skutki operacyjne lub finansowe dla danego podmiotu oraz jeśli wpływa na inne osoby fizyczne lub prawne, powodując znaczne szkody majątkowe lub niemajątkowe. Wprowadzona definicja poszerza zakres, obejmując nie tylko skutki operacyjne i finansowe, ale również poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi (art. 2 pkt 7 projektu KSC). Nowe sformułowanie, jakim jest "poważne obniżenie jakości", wprowadza większą subiektywność i może być trudne do jednoznacznego określenia. Taka zmiana w definicji daje możliwość klasyfikacji szerokiej gamy zdarzeń jako incydentów poważnych, nawet jeśli ich wpływ nie jest bezpośrednio porównywalny z tym, co przewiduje dyrektywa NIS2. Przyjęcie takiej definicji może prowadzić do nadregulacji, zwiększając obciążenia dla przedsiębiorców, którzy będą zobowiązani do zgłaszania nawet mniejszych awarii technicznych. Choć takie incydenty mogą wpływać na jakość usługi, niekoniecznie prowadzą one do poważnych zakłóceń operacyjnych czy znaczących strat finansowych. Może to skutkować nieproporcjonalnym zwiększeniem liczby zgłoszeń, co obciąży zarówno przedsiębiorców, jak i organy nadzorujące, potencjalnie odwracając ich uwagę od rzeczywistych incydentów. Dlatego konieczne jest dostosowanie definicji incydentu poważnego w polskim projekcie do standardów NIS2, aby uniknąć nadmiernych obciążeń i skupić się na rzeczywistych zagrożeniach.	Wyjaśnienie uwagi To jest skonkretyzowanie poważnych skutków operacyjnych w sposób, który sprawia, że definicja jest znacznie bardziej precyzyjna. Ułatwi to podmiotom klasyfikowanie tych incydentów i zapobieganie różnemu podejściu do definiowania „dotkliwych zakłóceń operacyjnych usług”. Należy podkreślić, że inaczej formułowane są przepisy prawa europejskiego a inaczej prawa krajowego, a implementacja dyrektyw nie oznacza prostego przepisywania przepisów dyrektywy

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

238.	Konfederacja Lewiatan	Art. 2 pkt 8a	Szeroka odpowiedzialność kierowników podmiotów kluczowych lub podmiotów ważnych, niewymagana przez NIS2 Jednostka redakcyjna: art. 2 pkt 8a) projektu KSC Jednostka redakcyjna NIS2: art. 20 ust. 2 Uwaga: W art. 2 pkt 8a) projektu KSC proponuje się zdefiniowanie kierownika podmiotu kluczowego lub podmiotu ważnego poprzez odesłanie do przepisów art. 3 pkt 6) ustawy o rachunkowości. Odesłanie jest błędne, gdyż powinno odsyłać do art. 3 ust. 1 pkt 6 ustawy o rachunkowości. Definicja ta posiada istotne znaczenie pod kątem obowiązków kierowników oraz zasad ich odpowiedzialności. Zastosowanie bardzo szerokiej definicji z ustawy o rachunkowości skutkuje tym, że odpowiedzialność o charakterze penalnym, zamiast być ściśle ograniczona, obejmuje wszystkie osoby odpowiedzialne za zarządzanie danym podmiotem, nawet w sytuacji, gdy z okoliczności prawnych lub faktycznych wynika, że nie są one w ogóle odpowiedzialne za kwestie cyberbezpieczeństwa. W tym zakresie projektodawca powinien raczej zastosować konstrukcję prawną znaną z ustawy – Prawo telekomunikacyjne, tj. wykorzystanie pojęcia "osoba kierująca przedsiębiorstwem" (tak art. 209 ust. 2 ustawy – Prawo telekomunikacyjne). Takie podejście będzie również bardziej adekwatne w stosunku do terminu "organ zarządzający podmiotem kluczowym i podmiotem ważnym", do którego odwołuje się art. 20 ust. 1 i 2 NIS2. Ponadto, odesłanie może być nieadekwatne, ponieważ nie wszystkie podmioty stosują ustawę o rachunkowości. Na marginesie również budzi wątpliwości odesłanie akurat do tej ustawy, w kontekście materii regulowanej projektem KSC. W związku z powyższym, zaleca się zrewidowanie definicji kierownika podmiotu kluczowego lub podmiotu ważnego w projekcie KSC, aby odpowiedzialność była precyzyjnie określona i adekwatna do zakresu obowiązków związanych z cyberbezpieczeństwem.	Uwaga częściowo uwzględniona W zakresie odesłania do ustawy o rachunkowości to zostanie to poprawione. Wprowadzenie definicji kierownika podmiotu odnoszącej się do ustawy o rachunkowości pozwoli na jednoznaczne przypisanie odpowiedzialności za cyberbezpieczeństwo organom zarządczym danego podmiotu.
239.	Związek Cyfrowa Polska	Aart. 2 pkt 8a, art. 8c-8e, art. 73a	Dyrektywa NIS2 nie definiuje terminu „organu zarządzającego”, a jedynie wykorzystuje go w ramach trzech odniesień, które dotyczą wymagań w zakresie zarządzania. Tymczasem w projekcie przedstawionym przez Ministerstwo Cyfryzacji (art. 2 pkt 8a) określenie “organ zarządzający” zostało zastąpione terminem “kierownik jednostki” z bezpośrednim odwołaniem interpretacyjnym do art. 3 pkt 6 ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2023 r. poz. 120, 295 i 1598), co sprawia, że przepisy interpretacji mają swoje zastosowanie nie tylko wobec członków zarządu danego podmiotu, ale także osób odpowiedzialnych (w danym momencie) za zarządzanie tym podmiotem. Państwa członkowskie zapewniają w NIS2, że organy zarządzające podmiotów kluczowych i ważnych zatwierdzają środki zarządzania ryzykiem cyberbezpieczeństwa podjęte przez te podmioty w celu przestrzegania artykułu 21, nadzorują ich wdrażanie oraz mogą ponosić odpowiedzialność za naruszenia tego artykułu przez te podmioty. Polski projekt implementacji określa obowiązki szefów podmiotów kluczowych i ważnych (art. 8c do 8e) oraz zasady związane z karami finansowymi, które mogą być na nich nałożone (art. 73a). Kara może być nałożona w dwóch przypadkach: a. jeśli szef jednostki nie wypełnił swoich obowiązków wynikających z polskiej implementacji NIS2, wymienionych w art. 73a projektu, lub	Wyjaśnienie uwagi Wprowadzenie definicji kierownika podmiotu odnoszącej się do ustawy o rachunkowości pozwoli na jednoznaczne przypisanie odpowiedzialności za cyberbezpieczeństwo organom zarządczym danego podmiotu. Kary zgodnie z NIS2 mają być dotkliwe i skuteczne.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			b. jeśli podmiot kluczowy ub ważny nie wypełnił swoich obowiązków wynikających z projektu implementacji NIS2, wymienionych w art. 73 krajowego projektu implementacji. Kwota kary nie może przekroczyć 600% wynagrodzenia otrzymanego przez ukaraną osobę, obliczonego zgodnie z zasadami dotyczącymi ustalania ekwiwalentu pieniężnego za urlop. Takie uszczegółowienie w sposób istotny odbiega od zasad określonych w dyrektywie. Kara taka powinna uwzględniać zdolność finansową szefa jednostki.	
240.	ZBP	Art. 2 pkt 11a	platforma sieci usług społecznościowych – usługę świadczoną drogą elektroniczną w rozumieniu przepisów ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2020 r. poz. 344), która umożliwia użytkownikom końcowym łączenie się z innymi osobami oraz komunikowanie się i wymianę, udostępnianie i odkrywanie treści za pomocą wielu urządzeń platforma sieci usług społecznościowych – usługę świadczoną drogą elektroniczną w rozumieniu przepisów ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2020 r. poz. 344), która umożliwia użytkownikom końcowym łączenie się z innymi osobami oraz komunikowanie się lub wymianę, udostępnianie lub odkrywanie treści za pomocą wielu urządzeń Proponujemy weryfikację powyższego i np. zastąpienie niektórych „i” przez „lub”. Dzięki tego rodzaju zmianie możliwe będzie uwzględnienie w ramach definicji szeregu różnych rozwiązań technologicznych.	Uwaga nieuwzględniona Dyrektywa posługuje się tutaj spójnikiem „i” dlatego nie możemy go zastąpić spójnikiem lub.
241.	Konfederacja Lewiatan	Art. 2 pkt 11	Jednostka redakcyjna: w art. 2 pkt 12 <i>12) ryzyko - kombinację prawdopodobieństwa wystąpienia zdarzenia niepożądanego i jego konsekwencji;</i> Zauważamy, że aktualna definicja używa niezdefiniowanego pojęcia „zdarzenia niepożądanego”. Jest też odmienna od definicji ryzyka z NIS2 używającej pojęć zdefiniowanych: <i>„„ryzyko” oznacza możliwość wystąpienia strat lub zakłóceń spowodowanych incydem, wyrażoną jako wypadkową wielkości takiej straty lub takich zakłóceń oraz prawdopodobieństwo wystąpienia takiego incydentu;”</i>	Uwaga nieuwzględniona Obecna definicja ryzyka jest obecna w ustawie od kilku lat oraz w innych ustawach, np. w ustawie o ochronie informacji niejawnych i istnieje już ugruntowana praktyka związana z jej stosowaniem.
242.	Konfederacja Lewiatan	Art. 2 pkt 11c	Definicja podmiotu krytycznego Jednostka redakcyjna: art. 2 pkt 11c) projektu KSC Jednostka redakcyjna NIS2: art. 2 ust. 5 Uwaga: Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557, podobnie jak każda inna dyrektywa, co do zasady obowiązuje tylko państwa członkowskie. Z tej przyczyny nieprawidłowym może być odsyłanie do definicji podmiotu krytycznego w art. 2 pkt 1 dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE. Szczególnie, gdy zgodnie z art. 7 ust. 8 projektu KSC informację o wyznaczeniu takiemu podmiotowi przekazuje ministrowi właściwemu do spraw informatyzacji dyrektor Rządowego Centrum Bezpieczeństwa. Aby uniknąć nieprawidłowości i zapewnić jasność przepisów, zaleca się sformułowanie definicji podmiotu krytycznego bezpośrednio w ustawie KSC, zamiast odsyłania do definicji zawartej w dyrektywie. W ten sposób	Wyjaśnienie uwagi Projekt zostanie uspojniony z projektem ustawy wdrażającej dyrektywę CER.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			zapewni się, że definicja jest w pełni zrozumiała i zgodna z krajowymi regulacjami oraz praktykami. Ustawa może odsyłać do dyrektywy, ale należy pamiętać, że dyrektywy jako takie nie mają bezpośredniego zastosowania w prawie krajowym – wymagają transpozycji, czyli wdrożenia poprzez krajowe akty prawne.	
243.	Konfederacja Lewiatan	Art. 2 pkt 11e	<u>10. Potencjalne zdarzenie dla cyberbezpieczeństwa</u> Jednostka redakcyjna: Art. 2 pkt 11e - potencjalne zdarzenie dla cyberbezpieczeństwa Jednostka redakcyjna NIS2: art. 6 pkt 5) <i>11e) potencjalne zdarzenie dla cyberbezpieczeństwa – zdarzenie, które może mieć niekorzystny wpływ na bezpieczeństwo systemów informacyjnych</i> Zauważamy, że definicja jest odmienna od definicji zawartej w NIS2. W szczególności pominięto w niej wskazanie, że jest to zdarzenie „któremu udało się jednak zapobiec lub które jednak nie wystąpiło;”. Art. 6 pkt 5 NIS2 skupia się na konkretnych aspektach bezpieczeństwa danych i systemów informatycznych, takich jak dostępność, autentyczność, integralność i poufność. Uwzględnia zdarzenia, które mogły naruszyć te aspekty, ale którym udało się zapobiec lub które ostatecznie nie wystąpiły. Natomiast propozycja projektodawcy jest bardziej ogólna i obejmuje każde zdarzenie, które może mieć negatywny wpływ na bezpieczeństwo systemów informacyjnych. Nie ogranicza się do konkretnych aspektów bezpieczeństwa danych, co otwiera możliwość interpretacji każdego zdarzenia jako potencjalnego zagrożenia. Szerokie i nieprecyzyjne określenie "potencjalne zdarzenie" może prowadzić do nadmiernego obciążenia organizacji obowiązkiem raportowania nawet mało znaczących zdarzeń. To z kolei może prowadzić do zwiększenia biurokracji i rozmycia uwagi od rzeczywiście istotnych zagrożeń. Podmioty kluczowe i ważne mogą borykać się z problemem ustalenia, które zdarzenia faktycznie stanowią zagrożenie wymagające zgłoszenia, co może prowadzić do przeciążenia systemów raportowania i rozproszenia uwagi od zagrożeń wymagających natychmiastowej interwencji.	Uwaga uwzględniona Przepis zostanie zmieniony.
244.	Konfederacja Lewiatan	Art. 11g	Brak dostosowania przepisów do projektu ustawy Prawo Komunikacji Elektronicznej przyjęte przez Radę Ministrów 7.05.2024 Jednostka redakcyjna: art. 2 pkt 11g) projektu KSC; art. 5 projektu ustawy, Jednostka redakcyjna NIS2: nie dotyczy Uwaga: 7 maja 2024 r. Rada Ministrów przyjęła projekt ustawy Prawo komunikacji elektronicznej. Niemniej, opublikowana wersja projektu KSC zakłada odwołanie się do obowiązującej ustawy – Prawo telekomunikacyjne, która zostanie uchylona przez ustawę wdrażającą Prawo komunikacji elektronicznej. Na tym etapie brak odwołania do Prawa komunikacji elektronicznej uniemożliwia całościową analizę proponowanych przepisów z uwzględnieniem stanu prawnego po wejściu w życie ustawy – Prawo komunikacji elektronicznej (planowane po 1 stycznia 2025 r.).	Wyjaśnienie uwagi Projektodawca zdaje sobie sprawę z relacji przedmiotowego projektu z PKE. Po wejściu w życie PKE projekt zostanie dostosowany do nowej siatki pojęciowej.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

245.	Konfederacja Lewiatan	Art. 14	System informacyjny. Jednostka redakcyjna: Art. 2 pkt 14 – system informacyjny Jednostka redakcyjna NIS2: art. 6 pkt 1) W art. 2 pkt 14) projektu KSC projektodawca definiuje system teleinformatyczny jako: a) system teleinformatyczny, o którym mowa w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2024 r. poz. 307) lub b) urządzenie lub grupę połączonych urządzeń elektrycznych lub elektronicznych i oprogramowania zaprogramowanych w celu przetwarzania danych – wraz z danymi przetwarzanymi w postaci elektronicznej. W definicji systemu informacyjnego dodawane jest sformułowanie „urządzenie lub grupę połączonych urządzeń elektrycznych lub elektronicznych i oprogramowania zaprogramowanych w celu przetwarzania danych”. W uzasadnieniu wskazano, że intencją jest przesądzenie objęcia definicją systemów OT. Taka redakcja powoduje jednak, że jako system informacyjny może być klasyfikowany także pojedyncze urządzenie, jak np. laptop czy telefon, które wydają się same w sobie nie wyczerpywać pojęcia „systemu”. Wnosimy o ponowne rozważenie tej kwestii.	Uwaga nieuwzględniona Definicja została celowo zaprojektowana jako szeroka, aby objąć wszystkie rozwiązania techniczne u podmiotów ksc.
246.	Związek Cyfrowa Polska	Art. 2 pkt 20	Zgodnie z art. 2 pkt 20 projektu poważne zagrożenie cybernetyczne to zagrożenie cybernetyczne, które ze względu na swoje cechy techniczne może mieć poważny wpływ na bezpieczeństwo systemów informatycznych powodując szkodę materialną lub niematerialną (w porównaniu z definicją w art. 6 (11) dyrektywy NIS2, polski projekt nie zawiera odniesienia do „znacznej” szkody). Projekt jedynie przewiduje, że rząd wyda rozporządzenie określające progi uznania incydentu za poważny incydent, z uwzględnieniem sektorów i podsektorów.o	Uwaga uwzględniona Definicja poważnego cyberzagrożenia zostanie zmieniona.
247.	Morskie Centrum Cyberbezpieczeństwa Akademia Marynarki Wojennej w Gdyni	Art. 3a	Działania w ramach obsługi incydentów Cel główny KSC został zdefiniowany w art. 3, lecz cel obsługi incydentów w art. 3a jest przedstawiony w formie szczątkowej. Proponujemy rozbudowanie artykułu o kolejne kwestie: Art. 3a W ramach obsługi incydentów podmiot krajowego systemu cyberbezpieczeństwa może w szczególności podejmować działania w celu: 1) wykrywania źródła lub dokonywania analizy ruchu sieciowego powodujących wystąpienie incydentu zakłócającego świadczenie przez ten podmiot usług; 2) modyfikacji procesu świadczenia usług do czasu zakończenia obsługi incydentu; 3) <u>ułatwionego zakupu produktów lub usług niezbędnych do przywrócenie sposobu świadczenia usługi w podstawowy sposób;</u> 4) <u>ułatwionego skorzystania ze wsparcia ekspertów dających rękojmię zachowania w poufności przekazywanych informacji.</u>	Wyjaśnienie uwagi Zdaniem Ministerstwa Cyfryzacji modyfikacja procesu świadczenia usług już mieści się w ramach ogólnej definicji incydentu. W zakresie propozycji punktu 3 oraz 4 – kwestie te wykraczają poza zakres przedmiotowy przepisu. Ułatwiony zakup – ogólne zasady są tutaj regulowane przez kodeks cywilny, ewentualnie ustawy – Prawo zamówień publicznych. Podmiot obsługujący incydent nadal musi mieścić w ramach wyznaczonych przez te przepisy. Z uwagi nie wynika w jaki sposób podmiot obsługujący incydent

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

				miałby sobie ułatwić zakup produktów. Z drugiej strony nie ulega wątpliwości, że w trakcie obsługi incydentu może zajść potrzeba zakupu dodatkowego sprzętu/oprogramowania albo skorzystania z usług zewnętrznych ekspertów.
248.	Stowarzyszenie Absolwentów Studiów Cyberbezpieczeństwa MBA	Art. 3a	Brak wymuszenia realizowania środków niezbędnych do ustalenia przyczyny incydentu Na podstawie projektowanego art. 3a ustawy KSC podmiot nie jest zobligowany do ustalenia przyczyny zaistnienia incydentu. W myśl projektu podmiot może dokonać działań działania w celu wykrywania źródła lub dokonywania analizy ruchu sieciowego powodujących wystąpienie incydentu zakłócającego świadczenie. Działania te powinny być obligatoryjnie wykonywane. Jest to niezbędne, ponieważ tylko po ich wykonaniu ich (działania informatyki śledczej) można ustalić na wektor ataku oraz tylko działania te umożliwiają wdrożenie odpowiednich działań mitygujących środków zapobiegawczych. W tym zakresie, jeżeli atakujący za pomocą złośliwego kodu dokona przełamania zabezpieczeń, to tylko analiza tego kodu jest w stanie wskazać potencjalne skutki działania atakującego. W związku z tym proponujemy zmianę brzmienia przepis art. 3a z “podmiot krajowego systemu cyberbezpieczeństwa może w szczególności podejmować działania w celu wykrywania źródła lub dokonywania analizy ruchu sieciowego” na “podmiot krajowego systemu cyberbezpieczeństwa jest zobowiązany podjąć działania informatyki śledczej oraz dokonać analizy ruchu sieciowego w celu ustalenia źródła ataków”.	Wyjaśnienie uwagi Zadania z zakresu informatyki śledczej mieszczą się w ramach obecnej definicji obsługi incydentu.
249.	ISSA Polska	Art. 3a	Brak wymuszenia realizowania środków niezbędnych do ustalenia przyczyny incydentu W ramach zapisu art. 3A podmiot nie jest zobligowany do ustalenia przyczyny zaistnienia incydentu. W myśl projektu podmiot może dokonać działań działania w celu wykrywania źródła lub dokonywania analizy ruchu sieciowego powodujących wystąpienie incydentu zakłócającego świadczenie. Działania te powinny być obligatoryjnie wykonywane. Jest to niezbędne, ponieważ po wykonaniu ich (działania Forensic) można ustalić na wektor ataku oraz działania te umożliwiają wdrożenie odpowiednich działań mitygujących. W tym zakresie, jeżeli atakujący za pomocą złośliwego kodu dokona przełamania zabezpieczeń, to tylko analiza tego kodu jest w stanie wskazać potencjalne skutki działania atakującego.	Wyjaśnienie uwagi Zgodnie z definicją obsługi incydentu obejmuje ona 10) obsługa incydentu - czynności umożliwiające wykrywanie, rejestrowanie, analizowanie, klasyfikowanie, priorytetyzację, podejmowanie działań naprawczych i ograniczenie skutków incydentu; Aby wykonać te działania należy ustalić przyczynę incydentu.
250.	Konfederacja Lewiatan	Art. 3a	Niejasne uprawnienia podmiotów krajowego systemu cyberbezpieczeństwa w zakresie dokonywania analizy ruchu sieciowego w kontekście tajemnicy telekomunikacyjnej (a także tajemnicy korespondencji). Jednostka redakcyjna: art. 3a projektu KSC Jednostka redakcyjna NIS2: art. 21 ust. 2 pkt b) „Art. 3a. W ramach obsługi incydentów podmiot krajowego systemu cyberbezpieczeństwa może w szczególności podejmować działania w celu wykrywania źródła lub dokonywania analizy ruchu	Wyjaśnienie uwagi Czasowe ograniczenie ruchu z adresów IP jest już możliwe na podstawie obecnych przepisów, ale chcieliśmy to wprost wskazać w uzasadnieniu, aby nie było wątpliwości. Uzasadnienie zostanie doprecyzowane w tym zakresie. Nie

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			sieciowego powodujących wystąpienie incydentu zakłócającego świadczenie przez ten podmiot usług.”; W uzasadnieniu wskazano, że „Przepisy ustawy przesądzają, że w ramach obsługi incydentu dotknięty nim podmiot może wykrywać źródło ataku oraz czasowo ograniczyć ruch sieciowy z adresów IP lub adresów URL. Uprawnienia te są niezbędne dla zapewnienia skutecznej reakcji na incydent, a w praktyce sprawiają one problemy praktyczne. Wykrycie źródła ataku często jest niezbędne do jego powstrzymania i przywrócenia normalnego funkcjonowania systemów. Równocześnie te działania mogą prowadzić do ewentualnego naruszenia uprawnień innych podmiotów. Do tej pory istniały wątpliwości na ile takie działania mogą być podejmowane. W związku z tym konieczne jest wprowadzenie wyraźnej podstawy prawnej do takich działań.” Zaproponowany zapis naszym zdaniem zakreśla węższy zakres uprawnień niż ten, o którym mowa w uzasadnieniu. W szczególności pominięto słowo „ataku” co jednak można uznać za zabieg celowy. Co jednak istotniejsze, projektowany przepis nie zawiera przywołanego w uzasadnieniu uprawnienia do „czasowego ograniczania ruchu sieciowego z adresów IP lub adresów URL”. Jeśli więc cel określony w uzasadnieniu miałby zostać osiągnięty, przepis należy rozszerzyć. Uwaga. Dodatkowo art. 3a projektu KSC proponuje, aby podmioty krajowego systemu cyberbezpieczeństwa mogły podejmować działania w celu wykrywania źródła lub dokonywania analizy ruchu sieciowego powodującego wystąpienie incydentu zakłócającego świadczenie przez ten podmiot usług. Niemniej, przepis ten jest zbyt ogólny i nie określa jednoznacznie zakresu uprawnień tych podmiotów. Brak precyzyjnego ograniczenia tych uprawnień może prowadzić do kolizji z normami zawartymi w art. 159 ustawy – Prawo telekomunikacyjne, który chroni tajemnicę telekomunikacyjną, obejmującą m.in. treść indywidualnych komunikatów oraz dane transmisyjne i lokalizacyjne. Szerokie i nieokreślone uprawnienia mogą prowadzić do naruszenia tajemnicy telekomunikacyjnej i korespondencji, co jest niedopuszczalne. Z uwagi na powyższe, przepis art. 3a projektu KSC powinien zostać doprecyzowany, aby jasno określał granice uprawnień podmiotów krajowego systemu cyberbezpieczeństwa w zakresie analizy ruchu sieciowego. Poza powyższym, zauważamy, że wraz z uchYLENIEM RZDZ. VIIA uPT usunięty zostanie także przepis art. 175c przewidujący szczególne uprawnienia przedsiębiorców telekomunikacyjnych w zakresie podejmowania proporcjonalnych i uzasadnionych środków mających na celu zapewnienie bezpieczeństwa i integralności sieci, usług oraz przekazu komunikatów związanych ze świadczonymi usługami, w tym: 1) eliminacji przekazu komunikatu, który zagraża bezpieczeństwu sieci lub usług; 2) przerwanie lub ograniczenie świadczenia usługi telekomunikacyjnej na zakończeniu sieci, z którego następuje wysyłanie komunikatów zagrażających bezpieczeństwu sieci lub usług. Wnosimy o rozważenie utrzymania tego uprawnienia w projektowanym brzmieniu uKSC	chodzi tu o analizę treści danej korespondencji, ale jedynie o dane niezbędne do zabezpieczenia swoich systemów. Użycie sformułowania obsługa incydentu zapewnia spójność i jest niezbędne dla realnego wykorzystania tego przepisu. Należy podkreślić, że w momencie wykrycia incydentu dany podmiot może nie wiedzieć czy ma do czynienia z atakiem czy też jest to np. skutek błędu lub awarii. Dlatego sformułowanie to jest poprawne.
251.	Polska Izba Informatyki i	Art. 3a	Art. 3a – uprawnienia podmiotu krajowego systemu cyberbezpieczeństwa.	Wyjaśnienie uwagi

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

	Telekomunikacji		„Art. 3a. W ramach obsługi incydentów podmiot krajowego systemu cyberbezpieczeństwa może w szczególności podejmować działania w celu wykrywania źródła lub dokonywania analizy ruchu sieciowego powodujących wystąpienie incydentu zakłócającego świadczenie przez ten podmiot usług.”; W uzasadnieniu wskazano, że „Przepisy ustawy przesądzają, że w ramach obsługi incydentu dotknięty nim podmiot może wykrywać źródło ataku oraz czasowo ograniczyć ruch sieciowy z adresów IP lub adresów URL. Uprawnienia te są niezbędne dla zapewnienia skutecznej reakcji na incydent, a w praktyce sprawiają one problemy praktyczne. Wykrycie źródła ataku często jest niezbędne do jego powstrzymania i przywrócenia normalnego funkcjonowania systemów. Równocześnie te działania mogą prowadzić do ewentualnego naruszenia uprawnień innych podmiotów. Do tej pory istniały wątpliwości na ile takie działania mogą być podejmowane. W związku z tym konieczne jest wprowadzenie wyraźnej podstawy prawnej do takich działań.” Zaproponowany zapis naszym zdaniem zakreśla węższy zakres uprawnień niż ten, o którym mowa w uzasadnieniu. W szczególności pominięto słowo „ataku” co jednak można uznać za zabieg celowy. Co jednak istotniejsze, projektowany przepis nie zawiera przywołanego w uzasadnieniu uprawnienia do „czasowego ograniczania ruchu sieciowego z adresów IP lub adresów URL”. Jeśli więc cel określony w uzasadnieniu miałby zostać osiągnięty, przepis należy rozszerzyć. Poza powyższym, zauważamy, że wraz z uchYLENIEM rozdz. VIIA ustawy Prawo telekomunikacyjne usunięty zostanie także przepis art. 175c, przewidujący szczególne uprawnienia przedsiębiorców telekomunikacyjnych w zakresie podejmowania proporcjonalnych i uzasadnionych środków mających na celu zapewnienie bezpieczeństwa i integralności sieci, usług oraz przekazu komunikatów związanych ze świadczonymi usługami, w tym: 1) eliminacji przekazu komunikatu, który zagraża bezpieczeństwu sieci lub usług; 2) przerwanie lub ograniczenie świadczenia usługi telekomunikacyjnej na zakończeniu sieci, z którego następuje wysyłanie komunikatów zagrażających bezpieczeństwu sieci lub usług. Wnosimy o rozważenie utrzymania tego uprawnienia w projektowanym brzmieniu uksc.	Czasowe ograniczenie ruchu z adresów IP jest już możliwe na podstawie obecnych przepisów o obsłudze incydentu, ale chcieliśmy to wprost wskazać w uzasadnieniu, aby nie było wątpliwości. Uzasadnienie zostanie doprecyzowane w tym zakresie. Nie chodzi tu o analizę treści danej korespondencji, ale jedynie o dane niezbędne do zabezpieczenia swoich systemów. Użycie sformułowania obsługa incydentu zapewnia spójność i jest niezbędne dla realnego wykorzystania tego przepisu. Należy podkreślić, że w momencie wykrycia incydentu dany podmiot może nie wiedzieć czy ma do czynienia z atakiem czy też jest to np. skutek błędu lub awarii.
252.	ZBP	Art. 4 pkt 7	Uchylony 7) centrum wymiany i analiz informacji W opinii sektora bankowego, uzasadnione jest włączenie centrów wymiany i analiz informacji – tworzonych na podstawie zaproponowanych zmian w ustawie – Prawo Bankowe do katalogu podmiotów Krajowego Systemu Cyberbezpieczeństwa. Umożliwienie Centrum wymiany informacji z poszczególnymi CSIRT pozwoli na wzmocnienie zdolności sektora bankowego do zapobiegania zagrożeniom oraz prowadzenia obsługi incydentów. Włączenie centrów wymiany i analiz informacji do Krajowego Systemu Cyberbezpieczeństwa jest krokiem w kierunku zwiększenia bezpieczeństwa sektora bankowego oraz ochrony klientów. Umożliwi to lepszą koordynację działań na poziomie krajowym i międzynarodowym.	Wyjaśnienie uwagi Polskie ISACi mają postać porozumień i kwestie te są uregulowane w art. 8h ust. 5.
253.	ISACA	Art. 5	Podmiotem kluczowym jest: 3) niezależnie od wielkości podmiotu	Uwaga uwzględniona Przepis zostanie zmieniony.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			b) dostawca usług zarządzanych w zakresie cyberbezpieczeństwa"Doprecyzować zapis, aby wyłączyć z regulacji lub części definicji usługi mikroprzedsiębiorców, jeśli ich działania w ramach usługi nie mają znaczącego wpływu na cyberbezpieczeństwo. W połączeniu z definicją w art 2 pkt 4i "dostawca usług zarządzanych w zakresie cyberbezpieczeństwa – dostawca usług zarządzanych, który świadczy usługi związane z zarządzaniem ryzykiem w zakresie cyberbezpieczeństwa lub zapewnia pomoc dla tych działań" Zapis sprawia, że wszystkie osoby prowadzące JDG i świadczące usługi z obszaru cyberbezpieczeństwa (np. zatrudnieni w formule B2B) staną się podmiotami kluczowymi. Spowoduje to wypaczenie sensu regulacji i nałoży na wszystkie osoby zajmujące się cyberbezpieczeństwem jako mikroprzedsiębiorcy niewspółmierne obciążenia.	
254.	Izba Gospodarcza Wodociągi Polskie	Art. 5	Proponowany zapis dot. objęcia podmiotów kluczowych jest nieprecyzyjny. Podmiotem tym jest podmiot, który przewyższa wymogi dla średniego przedsiębiorstwa określone z art. 2 ust. 1 załącznika I do rozporządzenia Komisji (UE) nr 651/2014 z dnia 17 czerwca 2014 r. Zgodnie z treścią, do kategorii mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw („MŚP”) należą przedsiębiorstwa, które zatrudniają mniej niż 250 pracowników i których roczny obrót nie przekracza 50 milionów EUR, lub roczna suma bilansowa nie przekracza 43 milionów EUR. Izba wskazuje, że wiele przedsiębiorstw funkcjonujących w sektorach „woda pitna i ścieki” nie spełnia obu wymogów, ponieważ zatrudnia powyżej 250 osób, ale obrót nie przekracza 50 milionów EURO, a tym bardziej roczna suma bilansowa nie przekracza 43 milionów EUR.	Wyjaśnienie uwagi Aby być podmiotem kluczowym, poza wyjątkami, trzeba być dużym przedsiębiorcą. Jeśli podmiot zatrudnia powyżej 250 pracowników oraz jego roczny obrót nie przekracza 50 milionów EUR lub roczna suma bilansowa nie przekracza 43 milionów EUR to taki podmiot nie jest dużym przedsiębiorcą, a więc nie jest podmiotem kluczowym.
255.	Izba Gospodarcza Wodociągi Polskie	Art. 5	Zapisy powyższego artykułu są nieprecyzyjne, ponieważ podmiotem ważnym jest podmiot, który spełnia wymogi zgodne la średniego przedsiębiorstwa. Zgodnie z rozporządzeniem Komisji [UE] nr 651/2014 obejmie to podmioty, które zatrudniają od 51 do 250 osób, a obrót roczny lub suma bilansowa wynoszą powyżej 10 milionów EUR ale obrót nie przekracza 50 milionów EURO, a roczna suma bilansowa nie przekracza 43 milionów EUR. Również w tej sytuacji znajdują się przedsiębiorstwa, które spełniają wymóg zatrudnionych osób, a nie znajdują się w progach objętych zarówno obrotem, jak i sumą bilansową.	Wyjaśnienie uwagi Aby być podmiotem ważnym trzeba być, co do zasady, średnim przedsiębiorcą. Najistotniejszy jest tutaj próg bilansowy/obrotu. Jeśli podmiot zatrudnia 49 pracowników, ale jego obrót przekracza 10 milionów EUR, to jest to średnie przedsiębiorstwo. Jeśli przedsiębiorstwo ma 9 pracowników, ale jego roczny obrót przekracza 2 mln EUR to jest to małe przedsiębiorstwo a nie mikroprzedsiębiorstwo.
256.	Konfederacja Lewiatan	Art. 5 i załączniki 1 i2	Objęcie nowymi obowiązkami w zakresie cyberbezpieczeństwa podmiotów, które nie powinny zostać nimi objęte zgodnie z NIS2. Zakres stosowania określany wg GBER Jednostka redakcyjna: art. 5 projektu KSC; załącznik nr 1; załącznik nr 2 Jednostka redakcyjna NIS2: art. 3	Uwaga częściowo uwzględniona Sektory produkcji żywności, produkcji chemikaliów, produkcji ogółem zostaną przeniesione do sektorów ważnych. Jednostki samorządu terytorialnego od 2012 r. mają obowiązki w zakresie

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

		NIS2 wskazuje na dokonywania oceny wielkości przedsiębiorstwa na podstawie art. 2 załącznika do zalecenia 2003/361/WE natomiast projekt ustawy w art. 5 ust. 1 pkt 1, ust.2, odnosi się wprost do art. 2 załącznika 2 rozporządzenia GBER, ale już art. 5 ust. 1 pkt 2 odnosi się do całego GBER. W uzasadnieniu wyjaśniono, że wynika to z zasad techniki prawodawczej i konieczności odwołania się do obowiązujących przepisów prawnych. Wyjaśnienia wymaga czy dla oceny wielkości przedsiębiorstwa należy uwzględniać jedynie pułapy określone w art. 2 załącznika 2 GBER czy także pozostałe przepisy załącznika 2 GBER dot. powiązań między przedsiębiorstwami. Z uwagi na wprowadzenie w ust. 3 wyłączenia art. 3 ust. 4 załącznika GBER wydaje się, że intencją jest stosowanie wszystkich zapisów załącznika oprócz wyłączonych. Niezrozumiała jest jednocześnie wyżej wskazana różnica w sposobie odwołania do rozporządzenia GBER. W porównaniu z NIS2 projekt ustawy nakłada dodatkowe obowiązki na sektory, które nie muszą podlegać tak rygorystycznym regulacjom. Po pierwsze projekt ustawy klasyfikuje jako podmioty kluczowe podmioty ważne, zgodnie z dyrektywą NIS2, co wiąże się z podwyższeniem stopnia nadzoru nad tymi podmiotami. Takie działanie zostało podjęte w sektorach takich jak <u>produkcja, wytwarzanie i dystrybucja chemikaliów; produkcja, przetwarzanie i dystrybucja żywności; produkcja w tym podsektor produkcji wyrobów medycznych i wyrobów medycznych do diagnostyki in vitro, podsektor produkcji komputerów, wyrobów elektronicznych i optycznych, podsektor produkcji urządzeń elektrycznych, podsektor produkcji maszyn i urządzeń, gdzie indziej niesklasyfikowana, oraz podsektor produkcji pojazdów samochodowych, przyczep i naczep</u>. Nie można obciążać polskich przedsiębiorców dodatkowymi wymaganiami, co powoduje dalsze koszty, zwłaszcza w kontekście polityki energetycznej, wzrostu cen, inflacji oraz wzrostu obciążeń podatkowych. Po drugie dyrektywa NIS2 nie obejmuje co do zasady jednostek samorządu terytorialnego i instytucji edukacyjnych (brak obligatoryjności). Dyrektywa NIS2 nie nakłada obowiązku regulacji na jednostki samorządu terytorialnego oraz instytucje edukacyjne jako takie. Natomiast rządowy projekt ustawy rozszerza zakres podmiotów kluczowych o jednostki samorządu terytorialnego oraz instytucje edukacyjne prowadzące działalność badawczą, co odbiega od postanowień dyrektywy NIS2. W świetle przepisów dyrektywy, jednostki na poziomie regionalnym mogą zostać uznane za podmioty administracji publicznej tylko wtedy, gdy świadczą usługi o znaczącym wpływie społeczno-gospodarczym, co powinno być potwierdzone oceną ryzyka. Jednakże, projekt ustawy nie uwzględnia tego warunku, co prowadzi do nieuzasadnionych obciążeń dla jednostek samorządu terytorialnego oraz instytucji edukacyjnych, takich jak domy kultury czy muzea. Co więcej zgodnie z art. 2 ust. 5 dyrektywy NIS2, państwa członkowskie mogą zdecydować o włączeniu do zakresu dyrektywy lokalnych jednostek administracji publicznej lub instytucji edukacyjnych, pod warunkiem, że prowadzą one działalność badawczą o krytycznym znaczeniu. Jednakże, projekt ustawy krajowej generalizuje to rozszerzenie na wszystkie publiczne uczelnie i instytucje kulturalne, niezależnie od	wdrożenia systemu zarządzania bezpieczeństwem informacji w systemach teleinformatycznych służących realizacji zadań publicznych. Stąd zasadne jest, aby objąć je także wymogami ustawy. Apteki sektor farmaceutyczny jest już obecny w ustawie o ksc – a dyrektywa NIS2 pozwala na objęcie swoimi wymogami także operatorów usług kluczowych zidentyfikowanych przed wejściem w życie NIS2.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			charakteru ich działalności, co stoi w sprzeczności z intencją dyrektywy i generuje niepotrzebne koszty. Po trzecie Dyrektywa NIS2 nie obejmuje w całości sektora farmaceutycznego, w tym aptek: Projekt ustawy kwalifikuje jako podmioty kluczowe hurtownie farmaceutyczne, przedsiębiorców posiadających pozwolenie na dopuszczenie do obrotu produktu leczniczego, importerów i wytwórców produktów leczniczych/substancji czynnych, importerów równoległych, dystrybutorów substancji czynnej oraz apteki. Tymczasem, zgodnie z załącznikiem nr 1 do NIS2, status podmiotów kluczowych przysługuje tylko tym podmiotom, które prowadzą działalność badawczo-rozwojową w zakresie produktów leczniczych, podmiotom produkującym podstawowe substancje farmaceutyczne oraz leki i pozostałe wyroby farmaceutyczne, a także podmiotom produkującym wyroby medyczne uznane za mające krytyczne znaczenie podczas stanu zagrożenia zdrowia publicznego. Poniżej przedstawiono szczegółową informację w tym zakresie: Lista podmiotów, które nie zostały wskazane w załączniku I do Dyrektywy NIS2, a które umieszczono w załączniku nr 1 do projektu ustawy <u>co oznacza objęcie obowiązkami wynikającymi z ustawy podmiotów, które nie muszą pod nią podlegać</u>: 1) Sektor energia a. Jednostki organizacyjne podległe ministrowi właściwemu do spraw energii lub przez niego nadzorowane. b. Jednostki organizacyjne podległe ministrowi właściwemu do spraw gospodarki złożami kopalin lub przez niego nadzorowane. 2) Sektor bankowość i infrastruktura rynków finansowych a. Administratorzy kluczowych wskaźników referencyjnych. 3) Sektor ochrona zdrowia: a. Przedsiębiorca prowadzący działalność polegającą na prowadzeniu hurtowni farmaceutycznej w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne (Dz. U. z 2022 r. poz. 2301, 605, 650, 1859 i 1938). b. Przedsiębiorca lub podmiot prowadzący działalność gospodarczą w państwie członkowskim Unii Europejskiej lub państwie członkowskim Europejskiego Porozumienia o Wolnym Handlu (EFTA) - stronie umowy o Europejskim Obszarze Gospodarczym, który uzyskał pozwolenie na dopuszczenie do obrotu produktu leczniczego. c. Importer produktu leczniczego/substancji czynnej w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne. d. Wytwórca produktu leczniczego/substancji czynnej w rozumieniu ustawy z dnia 6 2001 r. – Prawo farmaceutyczne. e. Importer równoległy w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne. f. Dystrybutor substancji czynnej w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne.	

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

		g. Przedsiębiorca prowadzący działalność w formie apteki ogólnodostępnej w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne. 4) Sektor administracja publiczna: a. jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 1–6, 8 i 10–13 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych, w tym: ▪ jednostki samorządu terytorialnego oraz ich związki; ▪ związki metropolitalne; ▪ jednostki budżetowe; iv. samorządowe zakłady budżetowe ▪ uczelnie publiczne; ▪ Polska Akademia Nauk i tworzone przez nią jednostki organizacyjne; ▪ państwowe i samorządowe instytucje kultury; b. instytuty badawcze Lista podmiotów, które nie zostały wskazane w załączniku I do Dyrektywy NIS2, a które umieszczono w załączniku nr 1 do projektu ustawy zamiast w załączniku nr 2 do ustawy(<u>podwyższenie wymogów minimalnych wynikających z Dyrektywy NIS2, poprzez sklasyfikowanie niektórych sektorów jako podmiotów kluczowych, zamiast jako podmiotów ważnych</u>): 1. Sektor produkcja, wytwarzanie i dystrybucja chemikaliów a) Przedsiębiorstwo zajmujące się produkcją substancji oraz wytwarzaniem i dystrybucją substancji lub mieszanin, o których mowa w art. 3 pkt 9 i 14 rozporządzenia (WE) nr 1907/2006 Parlamentu Europejskiego i Rady. b) Przedsiębiorstwa zajmujące się wytwarzaniem z substancji lub mieszanin wyrobów o których mowa w art. 3 pkt 3 rozporządzenia (WE) nr 1907/2006 Parlamentu Europejskiego i Rady. 2. Sektor produkcja, przetwarzanie i dystrybucja żywności a) Przedsiębiorstwa spożywcze w rozumieniu art. 3 pkt 2 rozporządzenia (WE) nr 178/2002 Parlamentu Europejskiego i Rady, zajmujące się dystrybucją hurtową oraz przemysłowymi produkcją i przetwarzaniem. 3. Sektor produkcja: a) podsektor produkcja wyrobów medycznych i wyrobów medycznych do diagnostyki in vitro: • Podmioty produkujące wyroby medyczne w rozumieniu art. 2 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2017/745. • Podmioty produkujące wyroby medyczne do diagnostyki in vitro w rozumieniu art. 2 ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2017/746, z wyjątkiem podmiotów produkujących wyroby medyczne uznane za mające krytyczne znaczenie podczas danego stanu zagrożenia zdrowia publicznego. b) podsektor produkcja komputerów, wyrobów elektronicznych i optycznych	

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			- Przedsiębiorca prowadzący którykolwiek z rodzajów działalności gospodarczej, o których mowa w sekcji C dział 26 klasyfikacji NACE Rev. 2, ujętej w załączniku I do rozporządzenia (WE) nr 1893/2006 Parlamentu Europejskiego i Rady z dnia 20 grudnia 2006 r. w sprawie statystycznej klasyfikacji działalności gospodarczej NACE Rev. 2 i zmieniającego rozporządzenie Rady (EWG) nr 3037/90 oraz niektóre rozporządzenia WE w sprawie określonych dziedzin statystycznych (Dz. Urz. UE L 393 z 30.12.2006, str. 1, z późn. zm.). c) podsektor produkcja urządzeń elektrycznych - Przedsiębiorca prowadzący którykolwiek z rodzajów działalności gospodarczej, o których mowa w sekcji C dział 27 klasyfikacji NACE Rev. 2. d) podsektor produkcja maszyn i urządzeń, gdzie indziej niesklasyfikowana - Przedsiębiorca prowadzący którykolwiek z rodzajów działalności gospodarczej, o których mowa w sekcji C dział 28 klasyfikacji NACE Rev. 2. e) podsektor produkcja pojazdów samochodowych, przyczep i naczep - Przedsiębiorca prowadzący którykolwiek z rodzajów działalności gospodarczej, o których mowa w sekcji C dział 29 klasyfikacji NACE Rev. 2. f) podsektor produkcja pozostałego sprzętu transportowego - Przedsiębiorca prowadzący którykolwiek z rodzajów działalności gospodarczej, o których mowa w sekcji C dział 30 klasyfikacji NACE Rev. 2.	
257.	Konfederacja Lewiatan	Art. 5	W ramach projektowanej nowelizacji ustawy o Krajowym Systemie Cyberbezpieczeństwa, znacznemu poszerzeniu ulega krąg podmiotów, do których zastosowanie będą miały przepisy ustawy co nie znajduje uzasadnienia we wdrażanej dyrektywie NIS2. Zgodnie z dyrektywą NIS2 nowymi obowiązkami dotyczącymi cyberbezpieczeństwa miały zostać objęte jedynie podmioty, które świadczą usługi o charakterze publicznym. Przepisy nowelizacji ustawy o KSC, przy zaproponowanych szerokich definicjach przedsiębiorcy komunikacji elektronicznej oraz przedsiębiorcy telekomunikacyjnego wychodzą znacząco ponad wskazania zawarte w NIS 2, która wskazuje w swoim Załączniku I jako sektory kluczowe jedynie dostawców publicznych sieci łączności elektronicznej oraz dostawców publicznie dostępnych usług łączności elektronicznej. Definicje zaproponowane w nowelizowanej ustawie KSC powodują, że krąg podmiotów objętych ustawą jest znacznie szerszy i obejmuje również podmioty, których usługi nie mają charakteru publicznego, są świadczone okazjonalnie i jedynie np. dla podmiotów z grupy kapitałowej, do której należą. Nakładanie na takie podmioty nowych obowiązków związanych z dostosowaniem ich infrastruktury, koniecznością zaprojektowania nowych procesów czy zatrudnienia nowych osób jest całkowicie nieuzasadnione ekonomiczne i sprzeczne z wymogami dyrektywy NIS2. Zgodnie z proponowanym w nowelizacji art. 1 ust. 8 Podmiotem Kluczowym, do którego będą miały zastosowanie przepisy nowelizowanej ustawy są m.in. przedsiębiorcy komunikacji elektronicznej, którzy co najmniej spełniają wymogi dla średniego przedsiębiorcy. W zakresie definicji przedsiębiorcy komunikacji elektronicznej projekt nowelizacji ustawy posługuje się pojęciem	Uwaga nieuwzględniona Docelowo projekt KSC będzie posługiwał się pojęciem przedsiębiorcy komunikacji elektronicznej z PKE. Naszym zdaniem spółka zapewniająca np. telekomunikację dla portu/lotniska/kopalni itd. Również powinna być objęta wymaganiami z zakresu cyberbezpieczeństwa.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			zbieżnym z siatką pojęciową, którą posługuje się procedowany aktualnie w Sejmie projekt nowego Prawa Komunikacji Elektronicznej. Zgodnie z definicją przedsiębiorcy komunikacji elektronicznej, krąg ten obejmuje przedsiębiorcę telekomunikacyjnego, oraz podmiot świadczący usługi komunikacji interpersonalnej niewykorzystującej numerów. Wątpliwości budzi w szczególności interpretacja definicji przedsiębiorcy telekomunikacyjnego zawarta w nowelizowanej ustawie PKE, która obejmuje: podmioty, które wykonują działalność gospodarczą polegającą na dostarczaniu publicznych sieci telekomunikacyjnych, <i>świadczeniu powiązanych usług</i> lub świadczeniu publicznie dostępnych usług telekomunikacyjnych. Wśród wymienionych podmiotów znajduje się podmioty świadczące usługi powiązane, które zgodnie z literalnym brzmieniem definicji nie muszą mieć charakteru usługi publicznej – co jest sprzeczne z wytycznymi dyrektywy NIS2. W związku z tym, aby zapewnić zgodność z wprowadzaną dyrektywą NIS2, definicje dodawane projektowanym art. 2 dotyczące dostawców usług (od pkt 4b do pkt 4i) jak również definicje znajdujące się w procedowanym w Sejmie PKE, powinny zostać zmodyfikowane w taki sposób, żeby odnosiły się tylko do podmiotów, które świadczą wskazane usługi w sposób publicznie dostępny. Ewentualnie powinno zostać dodatkowe wyłączenie, które wskaże, że w zakres definicji świadczenia usług nie będą wchodziły usługi świadczone na rzecz jednostek powiązanych z dostawcą w rozumieniu Ustawy o rachunkowości z dnia 29 września 1994 r. Oczekiwany skutek można również uzyskać odpowiednio modyfikując propozycję definicji przedsiębiorcy telekomunikacyjnego zawartą w nowelizowanym PKE.	
258.	Konfederacja Lewiatan	Art. 5	Jednostka redakcyjna: art. 5 ust. 1 pkt 1 i 2 oraz ust. 2 pkt 1 ustawy KSC Jednostka redakcyjna NIS2: art. 2 ust. 1 Uwaga: Projekt nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa wprowadza problematyczne i niejasne kryteria klasyfikacji podmiotów kluczowych i ważnych, w tym odwołanie do art. 2 ust. 1 załącznika I do rozporządzenia Komisji (UE) nr 651/2014. Zastosowanie tego przepisu prowadzi do sytuacji, w której całe grupy kapitałowe lub holdingi mogą zostać zakwalifikowane jako podmioty objęte ustawą, niezależnie od rzeczywistej wielkości poszczególnych spółek, ich obrotów czy liczby zatrudnionych pracowników. Jest to podejście niewspółmierne. Kluczowym czynnikiem decydującym o zakwalifikowaniu przedsiębiorstwa jako podmiotu kluczowego lub ważnego staje się jedynie fakt przynależności do grupy kapitałowej, a nie rzeczywista działalność i wpływ na infrastrukturę krytyczną. Ignorowanie w projektowanej nowelizacji motywu (16) dyrektywy NIS2, który sugeruje konieczność analizy powiązań między przedsiębiorcami w celu uniknięcia niewłaściwego klasyfikowania podmiotów, jest poważnym zaniedbaniem. Podejście to może prowadzić do niewłaściwego alokowania zasobów na środki ochrony, które w rzeczywistości mogą nie przyczyniać się do zwiększenia poziomu bezpieczeństwa cybernetycznego. Takie rozwiązanie jest nie tylko absurdałne, ale też szkodliwe, gdyż obciąża firmy niepotrzebnymi kosztami i wymogami administracyjnymi, co jest sprzeczne z ideą efektywnej ochrony cyberbezpieczeństwa.	Uwaga uwzględniona Zostanie wprowadzone wyłączenie zgodne z motywem 16 dyrektywy NIS2.
259.	ISSAA Polska	Art.5	Nieuzasadnione włączenie całych grup kapitałowych jako podmiotów kluczowych i ważnych – art. 5 ust. 1 pkt 1 i 2 oraz ust. 2 pkt 1 ustawy KSC	Uwaga uwzględniona

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			NIS2 podzieliła podmioty na kluczowe (duże przedsiębiorstwa z załącznika 1) oraz ważne (średnie przedsiębiorstwa z załącznika 1 i co najmniej średnie z załącznika 2). Dodatkowo określiła podmioty, które bez względu na swoją wielkość, mogą być uznane za kluczowe. Projekt przesunął część podmiotów (m.in. producentów) z załącznika 2 do NIS2 do wykazu podmiotów kluczowych w załączniku nr 1 do projektu ustawy. Zgodnie z przepisami NIS2 państwo członkowskie może zmodyfikować katalog określony w tym akcie unijnym w dwóch przypadkach – jeżeli podmioty spełniają kryteria określone w art. 2 ust. 2 lit. b) – e) NIS2 (co implementuje art. 7c projektowanej ustawy) lub podmioty miały status operatora usługi kluczowej na gruncie poprzednich przepisów. W związku z tym można mieć wątpliwość czy postanowienia art. 5 ust. 1 pkt. 1) projektowanej ustawy nie pozostają w sprzeczności z przepisami art. 3 ust. 1 i 3 NIS2. Projekt nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa wprowadza problematyczne i niejasne kryteria klasyfikacji podmiotów kluczowych i ważnych, w tym odwołanie do art. 2 ust. 1 załącznika I do rozporządzenia Komisji (UE) nr 651/2014. Zastosowanie tego przepisu prowadzi do sytuacji, w której całe grupy kapitałowe lub holdingi mogą zostać zakwalifikowane jako podmioty objęte ustawą, niezależnie od rzeczywistej wielkości poszczególnych spółek, ich obrotów czy liczby zatrudnionych pracowników. Jest to podejście niewspółmierne. Kluczowym czynnikiem decydującym o zakwalifikowaniu przedsiębiorstwa jako podmiotu kluczowego lub ważnego staje się jedynie fakt przynależności do grupy kapitałowej, a nie rzeczywista działalność i wpływ na infrastrukturę krytyczną. Ignorowanie w projektowanej nowelizacji motywu (16) dyrektywy NIS2, który sugeruje konieczność analizy powiązań między przedsiębiorcami w celu uniknięcia niewłaściwego klasyfikowania podmiotów, jest poważnym zaniedbaniem. Podejście to może prowadzić do niewłaściwego alokowania zasobów na środki ochrony, które w rzeczywistości mogą nie przyczyniać się do zwiększenia poziomu bezpieczeństwa cybernetycznego. Proponujemy, żeby dokonać analizy zastosowanych w projekcie ustawy definicji pod kątem rynkowych warunków działalności przedsiębiorstw, uwzględniając podmioty świadczące usługi wyłącznie na rzecz jednostek powiązanych z dostawcą zgodnie z Ustawą o rachunkowości z dnia 29 września 1994 oraz podmioty, których działalność istotna z punktu widzenia ustawy stanowi marginalną część działalności grupy kapitałowej.	Zostanie wprowadzone wyłączenie zgodne z motywem 16 dyrektywy NIS2.
260.	Konfederacja Lewiatan	Art. 5	Zauważamy wykroczenie poza ramy dyrektywy NIS2 i nadmiarowe wobec niej zakwalifikowanie wszystkich dostawców usług zarządzanych w zakresie cyberbezpieczeństwa do kategorii podmiotów kluczowych niezależnie od ich wielkości. W uzasadnieniu wyjaśniono, że zabieg ten jest celowy i wynika z faktu, że takie podmioty świadczą usługi dla innych podmiotów. Wydaje się jednak, że włączenie wszystkich takich podmiotów byłoby bardziej proporcjonalne, gdyby było uzależnione od tego czy faktycznie świadczą usługi podmiotom KSC czy nie.	Uwaga częściowo uwzględniona Z zakresu podmiotowego ustawy zostaną wyłączeni dostawcy usług zarządzanych w zakresie cyberbezpieczeństwa będący mikroprzedsiębiorstwami.
261.	Konfederacja Lewiatan	Art. 5	Uwaga: Zgodnie z przepisami, przedsiębiorstwa, które przekroczą określone progi zatrudnienia lub obrotu, mają zaledwie 2 miesiące na dokonanie wpisu do tego wykazu, co może być szczególnie problematyczne. Taki krótki termin stawia sektor przed wyzwaniem szybkiego dostosowania się do	Uwaga częściowo uwzględniona Przesłanki badania statusu podmiotu kluczowego/ważnego będą się odbywać

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			nowych wymogów, nawet przed zamknięciem roku obrachunkowego i przed sporządzeniem sprawozdania finansowego. Dodatkowo, wymóg składania oświadczenia o statusie pod rygorem odpowiedzialności karnej (art. 5 ust. 10 ustawy KSC) zwiększa ryzyko dla przedsiębiorstw, które mogą nieświadomie naruszyć ten obowiązek. W efekcie, firmy są zmuszane do prowadzenia ciągłej i często skomplikowanej samooceny, aby uniknąć sankcji karnych za niezłożenie wymaganej deklaracji w odpowiednim terminie. Takie podejście nie tylko generuje dodatkowe, często nieuzasadnione obciążenia dla przedsiębiorstw, ale również potencjalnie odciąga zasoby, które mogłyby być wykorzystane na rzeczywiste wzmocnienie bezpieczeństwa cybernetycznego. Absurdalność tej sytuacji polega na tym, że zamiast faktycznego zwiększania bezpieczeństwa, projekt nowelizacji wprowadza mechanizmy, które skupiają się na spełnianiu formalnych wymogów, zamiast na rzeczywistym adresowaniu zagrożeń cybernetycznych.	na dzień sporządzenia sprawozdania finansowego. Wymóg podania prawidłowych danych pod rygorem odpowiedzialności karnej występuje przy wielu rejestrach publicznych.
262.	ISSA Polska	Art. 5	Nieproporcjonalny obowiązek rejestracji i rygorystyczne terminy samo rejestracji dla podmiotów kluczowych i ważnych (art. 5 ust. 3 ustawy KSC) Zgodnie z przepisami, w toku stosowania przepisów (po zakończeniu okresu przejściowego) przedsiębiorstwa, które przekroczą określone progi zatrudnienia lub obrotu, mają zaledwie 2 miesiące na dokonanie wpisu do tego wykazu, co może być szczególnie problematyczne. Taki krótki termin stawia sektor przed wyzwaniem szybkiego dostosowania się do nowych wymogów, nawet przed zamknięciem roku obrachunkowego i przed sporządzeniem sprawozdania finansowego. Dodatkowo, wymóg składania oświadczenia o statusie pod rygorem odpowiedzialności karnej (art. 5 ust. 10 ustawy KSC) zwiększa ryzyko dla przedsiębiorstw, które mogą nieświadomie naruszyć te skomplikowane regulacje. W efekcie, firmy są zmuszane do prowadzenia ciągłej i często skomplikowanej samooceny, aby uniknąć sankcji karnych za niezłożenie wymaganej deklaracji w odpowiednim terminie. Takie podejście nie tylko generuje dodatkowe, często nieuzasadnione obciążenia dla przedsiębiorstw, ale również potencjalnie odciąga zasoby, które mogłyby być wykorzystane na rzeczywiste wzmocnienie bezpieczeństwa cybernetycznego. Absurdalność tej sytuacji polega na tym, że zamiast faktycznego zwiększania bezpieczeństwa, projekt nowelizacji wprowadza mechanizmy, które skupiają się na spełnianiu formalnych wymogów, zamiast na rzeczywistym adresowaniu zagrożeń. Proponujemy wydłużenie czasu dokonania wpisu do wykazu oraz przyjęcie daty złożenia sprawozdania finansowego jako rozpoczęcia biegu terminu. Aktualne brzmienie projektowanych przepisów nie precyzuje również sytuacji, w których ten sam podmiot (zidentyfikowany w oparciu o jego indywidualizację zgodnie z przepisami prawa cywilnego i przepisów kodeksu spółek handlowych), będzie kwalifikował się do więcej niż jednego sektora lub podsektora. Zgodnie z art. 7 ust. 2 pkt. 2 ustawy o KSC w wykazie podmiotów kluczowych i ważnych znajduje się informacja do jakiego sektora i podsektora należy podmiot. Jest to pozycja wypełniana przez sam podmiot (chyba, że jest on przepisywany na podstawie decyzji o uznaniu za operatora usługi kluczowej lub danych z innego rejestru). Nie ma w przepisach odniesienia do	Uwaga częściowo uwzględniona Przesłanki badania statusu podmiotu kluczowego/ważnego będą się odbywać na dzień sporządzenia sprawozdania finansowego.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			sytuacji, kiedy podmiot prowadzi działalność w więcej niż jednym sektorze. Sytuacja taka ma miejsce w przypadku różnego rodzaju podmiotów, najczęściej w zakresie łączenia swojej podstawowej działalności (np. produkcyjnej) m.in. z działalnością w zakresie: 1. energetyki (stacje ładowania, odcinki sieci dystrybucyjnych czy małoskalowa działalność w zakresie obrotu – niepodlegająca wymogom unbundlingu), 2. transportu kolejowego (w zakresie zarządzania obiektami typu bocznicą kolejową lub posiadania licencji na wykonywanie przewozów), 3. wodociągowo-kanalizacyjnej, 4. gospodarowania odpadami. Rodzi to poważne trudności dla rynku, w kwestii ustalenia zarówno właściwego trybu zgłoszenia do rejestru (tym większe, jeżeli w harmonogramie opublikowanym zgodnie z art. 14 ust. 2 w zw. z art. 15 ust. 3 projektu, dla różnych sektorów będą różne terminy), a w zależności od sposobu skonstruowania formularza do samozgłoszenia, może oznaczać konieczność dokonania kilku odrębnych zgłoszeń do różnych sektorów (głównego i aktualizujących). W przypadku podmiotów, które do wykazu podmiotów kluczowych i ważnych zostaną wpisane z urzędu (zgodnie z art.), pojawi się wątpliwość dotycząca potrzeby i terminu aktualizacji wpisu w zakresie, jaki wykracza poza treść decyzji (taką sytuację może mieć np. ciepło, gdzie podział na dystrybucję, przesył i obrót w praktyce nie ma znaczenia, bo większość podmiotów na rynku łączy te działalności, a decyzje jakie uzyskiwały o uznaniu za operatora usługi kluczowej nie były wydawane jednolicie i mogą dotyczyć tylko niektórych z tych obszarów). Brak wywiązania się z obowiązków rejestrowych oznacza karę dla podmiotu, a brak aktualizacji wpisu – dla jego kierownika. Dolegliwość ta powinna być co najmniej ograniczona w okresie pierwszych 12 miesięcy od pełnego uruchomienia funkcjonalności systemu do samorejestracji, przez sformułowanie obowiązku odstąpienia od wymierzenia kary przez organ, jeżeli ma miejsce sytuacja opisana powyżej.	
263.	Amerykańska Izba Handlowa w Polsce	Art. 5	Projekt zakłada, że za podmiot kluczowy zostaną objęte określone podmioty bez względu na ich wielkość. Takie rozwiązanie może skutkować nadmiernym obciążeniem małych i mikroprzedsiębiorstw, które mogą nie być w stanie sprostać wymaganym standardom ze względu na swoje ograniczone zasoby finansowe i ludzkie. Konieczność dostosowania się do nowych przepisów może stanowić dla nich poważne wyzwanie – istotne jest zatem rozważenie modyfikacji zakresu podmiotowego regulacji, na przykład poprzez wyłączenie spod zakresu projektu mikro lub/i małych przedsiębiorców.	Wyjaśnienie uwagi W dużej mierze wynika to z samej dyrektywy NIS2. Przykładowo wszyscy przedsiębiorcy telekomunikacyjni podlegają obowiązkom z zakresu cyberbezpieczeństwa niezależnie od wielkości podmiotu.
264.	Fundacja Bezpieczna Cyberprzestrzeń	Art. 5	Art. 1 pkt 8, treść art. 5 ust 1 pkt 3 – wydaje się, że takie zdefiniowanie podmiotów kluczowych jest nadmiarowe. Na polskim rynku jest wiele podmiotów dostarczających usług w zakresie cyberbezpieczeństwa, które trudno uznać za podmioty kluczowe dla krajowego systemu cyberbezpieczeństwa np. usług konsultacyjnych czy cyber threat intelligence (często są to podmioty spoza RP). Proponuje się powiązać uznanie dostawcy usług zarządzanych w zakresie cyberbezpieczeństwa, jako podmiotów kluczowych z warunkami określonymi w art. 7c ust. 1 pkt 3 ustawy.	Uwaga częściowo uwzględniona Celem przepisu było uwzględnienie podmiotów świadczących usług typu SOC/CERT/CSIRT, które mają np. poniżej 50 pracowników. Zespoły te - wspierające inne podmioty w cyberbezpieczeństwie, powinny same

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

				mieć wdrożone proporcjonalne środki techniczne i organizacyjne z zakresu cyberbezpieczeństwa. Natomiast faktycznie uwzględnienie pojedynczych ekspertów-niezależnych doradców jest nadmiarowe. Z tego powodu z zakresu podmiotowego zostaną wyłączeni mikroprzedsiębiorcy.
265.	KWKR Konieczny Wierzbicki i Partnerzy S.K.A.	Art. 5	Ustawa implementująca obejmuje szeroką grupę podmiotów, w tym w szczególności w kontekście podmiotów będących elementami grupy spółek. W obecnym kształcie prowadzenie przez daną spółkę, będącą elementem grupy spółek, działalności ujętej w Załącznikach I lub II do ustawy, nawet na niewielką skalę i wyłącznie na wewnętrzne potrzeby grupy, powoduje podleganie pod uregulowania ustawy implementującej, jeżeli grupa spółek jako całość co najmniej spełnia wymogi dla średniego przedsiębiorstwa określone w art. 2 ust. 1 załącznika I do rozporządzenia Komisji (UE) nr 651/2014 z dnia 17 czerwca 2014 r. uznającego niektóre rodzaje pomocy za zgodne z rynkiem wewnętrznym w zastosowaniu art. 107 i 108 Traktatu (Dz. Urz. UE L 187 z 26.06.2014, str. 1), (zwane dalej „rozporządzeniem 651/2014/UE”), pomimo, że spełnienie tych wymogów (co do liczby zatrudnionych, przychodów) będzie jedynie w niewielkiej części związane z działalnością określoną w Załącznikach I lub II do ustawy.	Uwaga uwzględniona Zostanie dodany odpowiedni przepis w projekcie uwzględniający motyw 16 do dyrektywy NIS2.
266.	KWKR Konieczny Wierzbicki i Partnerzy S.K.A.	Art. 5	Ponadto, dostawcy usług zarządzanych w zakresie cyberbezpieczeństwa, zgodnie z proponowanym nowym brzmieniem art. 5 ust. 1 pkt. 3) uksc, będą podmiotem kluczowym niezależnie od wielkości podmiotu. Oznacza to, że podmiotami kluczowymi będą także mali i mikro przedsiębiorcy, w tym indywidualni przedsiębiorcy nie zatrudniający żadnych pracowników. W praktyce, na rynku usług zarządzanych w zakresie cyberbezpieczeństwa funkcjonuje wielu mikro przedsiębiorców, w tym indywidualnych specjalistów świadczących usługi np. w zakresie testów penetracyjnych. Takich mikro przedsiębiorców uregulowania ustawy implementującej dotkną w nieproporcjonalnie większym stopniu niż inne podmioty, dysponujące nieproporcjonalnie większymi środkami na wdrożenie obowiązków wynikających z ustawy (w szczególności obowiązków formalnych związanych z koniecznością wdrożenia systemu zarządzania bezpieczeństwem informacji, w tym posiadania odpowiednich polityk i procedur), co zapewne nie pozostanie bez wpływu na zamknięcie lub bardzo mocne ograniczenie dostępu do tego rynku dla tego typu podmiotów.	Uwaga częściowo uwzględniona Celem przepisu było uwzględnienie podmiotów świadczących usługi typu SOC/CERT/CSIRT, które mają np. poniżej 50 pracowników. Zespoły te - wspierające inne podmioty w cyberbezpieczeństwie, powinny same mieć wdrożone proporcjonalne środki techniczne i organizacyjne z zakresu cyberbezpieczeństwa. Natomiast faktycznie uwzględnienie pojedynczych ekspertów-niezależnych doradców jest nadmiarowe. Z tego powodu z zakresu podmiotowego zostaną wyłączeni mikroprzedsiębiorcy.
267.	Krzysztof Rożko i Wspólnicy	Art. 5	UWAGA ZGŁOSZONA W RAMACH ZGŁOSZENIA LOBBINGOWEGO Projekt nowelizacji uKSC, wymienia w art. 1 pkt 8) (wprowadzając zmianę do art. 5 ust. 6) uKSC CSIRT MON, CSIRT NASK lub CSIRT GOV jako właściwe do zwrócenia się w związku z obowiązkami podmiotu wynikającymi z ustawy. Projekt pomija możliwość zwrócenia się do podmiotu	Uwaga uwzględniona Przepis art. 5 ust. 6 zostanie zmieniony.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

	Kancelaria Prawna sp. k.		w związku z obowiązkami wynikającymi z ustawy przez CSIRT sektorowy. W art. 6 pkt 34) dyrektywa NIS 2 określa organ krajowy lub CSIRT jako mogące się zwrócić w związku z obowiązkami podmiotu przewidzianymi w niniejszej dyrektywie, co pozwala stwierdzić, że CSIRT sektorowe, również powinny być uprawnione do zwrócenia w związku z obowiązkami podmiotu wynikającymi z ustawy.	
268.	KIGEIT	Art. 5	Rozszerzenie regulacji KSC na różne sektory gospodarki, które obecnie nie podlegają pod przepisy KSC. Wprowadzane w ramach projektu KSC przeregulowanie (w porównaniu z regulacjami UE i innych krajów UE) w zakresie sektorów objętych nowymi przepisami. W ramach Projektu KSC wprowadzono, wychodzącą poza to co jest wymagane zgodnie z Dyrektywą NIS2, identyfikację jako podmioty kluczowe część sektorów, które w Dyrektywie NIS2 są kwalifikowane jako sektory ważne – m.in. sektor produkcji, wytwarzanie i dystrybucja chemikaliów, sektor produkcji, przetwarzania i dystrybucji żywności, sektor produkcji obejmujący m.in. podsektor produkcji wyrobów medycznych i wyrobów medycznych do diagnostyki in vitro czy urządzeń elektrycznych, sektor działalność w zakresie wydobywania kopalin. Dyrektywa NIS2 określa co prawda minimalny zakres harmonizacji, więc państwa członkowskie mogą przyjmować dalej idące regulacje, jednak biorąc pod uwagę konsekwencje zmiany, a więc możliwość stosowania wobec podmiotów kluczowych czynności nadzorczych prewencyjnych i następczych (wobec podmiotu ważnego tylko następcze), a także różnicę w pałapie możliwych do nałożenia sankcji na podmioty kluczowe i podmioty ważne, takie rozszerzenie powinno być dokładnie przeanalizowane i uargumentowane oraz wskazane powinno zostać co najmniej odniesienie jak w tym zakresie postępują inne państwa UE, ponieważ wydaje się, że polski Projekt KSC jako wdrożenie Dyrektywy NIS2, idzie najdalej w porównaniu z przepisami innych krajów UE. Zgodnie z szacunkowymi wskazaniem w OSR, które jak przyznaje sam Projektodawca - nie są dokładne i wystarczające, podmioty kluczowe i ważne zgodnie z Projektem KSC obejmują aż 38,5 tys. podmiotów (38 532). Porównując polskie szacunki oddziaływania implementacji Dyrektywy NIS2 z innymi krajami, gospodarki większe od polskiej wskazują na niższy zakres oddziaływania na podmioty objęte regulacjami, np. Niemcy – 35 tys. podmiotów, Hiszpania – 25 tys. podmiotów.	Uwaga częściowo uwzględniona Sektory produkcji, wytwarzanie i dystrybucja chemikaliów, sektor produkcji, przetwarzania i dystrybucji żywności, sektor produkcji obejmujący m.in. podsektor produkcji wyrobów medycznych i wyrobów medycznych do diagnostyki in vitro, czy urządzeń elektrycznych zostaną przeniesione do sektorów ważnych. Sektor wydobywania kopalin już obecnie występuje na gruncie obecnej ustawy o KSC a dyrektywa NIS2 pozwala na uznanie dotychczasowych operatorów usług kluczowych za podmioty kluczowe.
269.	Stowarzyszenie Bezpieczeństwo Informacji w Telekomunikacji	Art. 5	Definiując podmioty będące podmiotami kluczowymi lub podmiotami ważnymi proponuje się brać pod uwagę tylko część działalności tego podmiotu związanej z przedmiotem regulacji ustawy. Bardzo często przedsiębiorca prowadzi działalność w wielu dziedzinach, a dziedzina objęta ustawą (np. telekomunikacja jest tylko niewielką częścią takiej działalności). Przykład: Przedsiębiorstwo budowlane, którego obrót roczny z działalności budowlanej wynosi 100 mln. zł . 98% tej kwoty dotyczy działalności budowlanej a 2% działalności telekomunikacyjnej. W takim przypadku przedsiębiorca taki zgodnie z projektem uKSC zostanie zakwalifikowany jako podmiot kluczowy. Jeśli ten podmiot prowadziłby tylko działalność telekomunikacyjną zostałby zakwalifikowany jako podmiot ważny. Działalność budowlana nie jest objęta obowiązkiem wynikającym z ustawy o KSC. Ponadto proponuje się zrównać parametry na podstawie przedsiębiorców zalicza się do podmiotów kluczowych lub podmiotów ważnych. Przedsiębiorca komunikacji elektronicznej będący średnim	Wyjaśnienie uwagi Zgodnie z dyrektywą NIS2 wszyscy przedsiębiorcy telekomunikacyjni, bez względu na wielkość podlegają obowiązkowi z zakresu cyberbezpieczeństwa.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			przedsiębiorcą staje się podmiotem kluczowym, w przypadku gdy pozostali przedsiębiorcy wskazani w załączniku do projektu uKSC stają się podmiotami kluczowymi, gdy przekroczą poziom wymagany dla przedsiębiorcy średniego.	
270.	TVN S.A.	Art. 5	Definicja Podmiotu Kluczowego – art. 1 ust. 8 projektu (art. 5 UKSC) – zmiana zakresu podmiotowego projektowanej ustawy, objęcie ustawą jedynie podmiotów świadczących publicznie dostępne usługi W ramach analizy projektowanej nowelizacji ustawy o Krajowym Systemie Cyberbezpieczeństwa, pojawiają się wątpliwości związane ze znacznym poszerzeniu kręgu podmiotów, do których zastosowanie będą miały przepisy ustawy co jest sprzeczne z wytycznymi wdrażanej dyrektywy NIS2. Zgodnie z dyrektywą NIS2 nowymi obowiązkami dotyczącymi cyberbezpieczeństwa miały zostać objęte jedynie podmioty, które świadczą usługi o charakterze publicznym, jednak propozycja definicji zawarta w art. 1 ust. 8 projektu UKSC i odwołanie do nowej definicji przedsiębiorcy telekomunikacyjnego w procedowanym w Sejmie nowelizacji PKE, budzi wątpliwości czy nie obejmuje swym zakresem dużo szerszy krąg podmiotów, dla których działalność telekomunikacyjna jest jedynie poboczną i wspierającą ich podstawową działalność. Interpretacja nowych przepisów nowelizacji UKSC, przy zaproponowanych szerokich definicjach przedsiębiorcy komunikacji elektronicznej oraz przedsiębiorcy telekomunikacyjnego budzi poważne wątpliwości czy definicje te nie wychodzą znacząco ponad wskazania zawarte w dyrektywie NIS2, która wskazuje w swoim Załączniku I jako sektory kluczowe jedynie dostawców publicznych sieci łączności elektronicznej oraz dostawców publicznie dostępnych usług łączności elektronicznej. Definicje zaproponowane w nowelizowanej ustawie KSC budzą wątpliwości czy krąg podmiotów objętych ustawą nie jest znacznie szerszy i nie obejmuje również podmiotów, których usługi nie mają charakteru publicznego, są świadczone okazjonalnie i jedynie np. dla podmiotów z grupy kapitałowej, do której należą. Nakładanie na takie podmioty nowych obowiązków związanych z dostosowaniem ich infrastruktury, koniecznością zaprojektowania nowych procesów czy zatrudnienia nowych osób jest całkowicie nieuzasadnione ekonomiczne i sprzeczne z wymogami dyrektywy NIS2. Dlatego wydaje się niezbędnym, w celu uniknięcia wątpliwości doprecyzowanie kręgu podmiotów objętych UKSC. Zgodnie z proponowanym w nowelizacji UKSC art. 1 ust. 8 Podmiotem Kluczowym, do którego mają być stosowane przepisy nowelizowanej UKSC są m.in. przedsiębiorcy komunikacji elektronicznej, którzy co najmniej spełniają wymogi dla średniego przedsiębiorcy. W zakresie definicji przedsiębiorcy telekomunikacji elektronicznej projekt nowelizowanej ustawy odwołuje się natomiast do procedowanego aktualnie w Sejmie nowego Prawa Komunikacji Elektronicznej. Zgodnie z definicją przedsiębiorcy komunikacji elektronicznej, krąg ten obejmuje przedsiębiorcę telekomunikacyjnego, przedsiębiorcę komunikacji elektronicznej oraz usługi komunikacji interpersonalnej. Wątpliwości budzi w szczególności interpretacja definicji przedsiębiorcy telekomunikacyjnego zawarta w nowelizowanej ustawie PKE, która obejmuje: podmioty, które wykonują działalność gospodarczą polegającą na dostarczaniu publicznych sieci telekomunikacyjnych, świadczeniu powiązanych usług lub świadczeniu publicznie dostępnych usług telekomunikacyjnych. Wśród wymienionych podmiotów znajduje się podmioty świadczące usługi	Uwaga nieuwzględniona Docelowo projekt KSC będzie posługiwał się pojęciem przedsiębiorcy komunikacji elektronicznej z PKE. Naszym zdaniem spółka zapewniająca np. telekomunikację dla portu/lotniska/kopalni itd. również powinna być objęta wymaganiami z zakresu cyberbezpieczeństwa.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			powiązane, które zgodnie z literalnym brzmieniem definicji nie muszą mieć charakteru usługi publicznej – co jest sprzeczne z wytycznymi dyrektywy NIS2. Analizują proponowane modyfikacje stoimy na stanowisku, że „usługi powiązane” jako bezpośrednio związane z innymi usługami o publicznym charakterze również powinny być publiczne aby były objęte przepisami ustawy ale nie wynika to wprost z zapisu i w związku z powyższym budzi wątpliwości, co wobec sprzeczności tych wątpliwości z wytycznymi dyrektywy NIS2 – powinno zostać w naszej ocenie doprecyzowane. Definicja wprowadzona w taki sposób powoduje, że pojawiają się wątpliwości interpretacyjne czy nowe wymogi będą miały zastosowanie do wszystkich podmiotów posiadających status przedsiębiorcy telekomunikacyjnego co z pewnością nie było intencją unijnego ustawodawcy. Przy tak szerokiej interpretacji definicji przedsiębiorcy telekomunikacyjnego polska ustawa implementująca wychodziłaby znacząco ponad wskazania zawarte w dyrektywie NIS2, która wskazuje w swoim Załączniku I jako sektory kluczowe jedynie dostawców publicznych sieci łączności elektronicznej oraz dostawców publicznie dostępnych usług łączności elektronicznej. W celu zapewnienia pełnej zgodności z wprowadzaną dyrektywą NIS2 postulujemy w szczególności doprecyzowanie definicji poprzez zmodyfikowanie zaproponowanej definicji przedsiębiorcy telekomunikacyjnego w ten sposób, że powinna ona oznaczać jedynie przedsiębiorcę telekomunikacyjnego w rozumieniu art. 2 pkt 27 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne, który świadczy publicznie dostępne usługi telekomunikacyjne, z wyraźnym wyłączeniem innych usług typu „usługi powiązane” jeśli nie mają charakteru publicznego. Ewentualnie powinno zostać dodatkowe wyłączenie, które wskaże, że w zakres definicji świadczenia usług nie będą wchodziły usługi świadczone na rzecz jednostek powiązanych z dostawcą w rozumieniu Ustawy o rachunkowości z dnia 29 września 1994 r. Oczekiwany skutek można również uzyskać odpowiednio modyfikując propozycję definicji przedsiębiorcy telekomunikacyjnego zawartą w nowelizowanym PKE.	
271.	Polskie Stowarzyszenie Fotowoltaiki	Art. 5	Art. 5 ust 1 i 2 zawierają katalog podmiotów uznawanych odpowiednio za PK i PW. W Projekcie, podmioty będące dostawcami usług zarządzanych oraz dostawcami usług zarządzanych w zakresie cyberbezpieczeństwa zostały automatycznie uznane za PK niezależnie od ich wielkości. Podobna sytuacja zachodzi w odniesieniu do rejestrów nazw domen najwyższego poziomu (TLD)). Ogólny wpływ regulacji: Zastosowanie wymogów PK względem dostawców usług zarządzanych oraz dostawców usług zarządzanych w zakresie cyberbezpieczeństwa będzie miało miejsce niezależnie od ich wielkości. Wpływ na sektor energetyczny: Biorąc pod uwagę specyfikę sektora energetyki, dostawcy usług i sprzętu wykorzystywanego w energetyce mogą podlegać kwalifikacji jako dostawcy usług zarządzanych, w tym w zakresie cyberbezpieczeństwa. W rezultacie, niezależnie od ich wielkości, podmioty te będą podlegały obowiązkowi PK wynikającym z ustawy. Ponadto, jak zostało to opisane w dalszej części przedmiotowego zestawienia, katalog podmiotów uznawanych odpowiednio za PK i PW znacznie odbiega od tego, określonego w Dyrektywie NIS2 w zakresie, w jakim rozszerza katalog podmiotów	Uwaga częściowo uwzględniona Celem przepisu było uwzględnienie podmiotów świadczących usługi typu SOC/CERT/CSIRT, które mają np. poniżej 50 pracowników. Zespoły te - wspierające inne podmioty w cyberbezpieczeństwie, powinny same mieć wdrożone proporcjonalne środki techniczne i organizacyjne z zakresu cyberbezpieczeństwa. Natomiast faktycznie uwzględnienie pojedynczych ekspertów-niezależnych doradców jest nadmiarowe. Z tego powodu z zakresu

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			uznawanych za PK. Wkonsekwencji, przyjęcie takiej regulacji może skutkować powstaniem o wiele bardziej restrykcyjnego środowiska prawnego dla podmiotów z sektora energetycznego, w porównaniu do innych państw członkowskich UE, co z kolei może mieć wpływ na obniżenie efektywności operacyjnej kluczowych podmiotów z sektora energetycznego lub, w skrajnych wypadkach, zawieszenie działalności przez te podmioty na terenie kraju z uwagi na zbyt restrykcyjne wymogi prawne. [Nadregulacja względem Dyrektywy NIS2] Uznanie dostawców usług zarządzanych w zakresie cyberbezpieczeństwa za PW niezależnie od ich wielkości wykracza poza wymogi Dyrektywy NIS2. Rekomendacja: W celu zachowania minimalnego charakteru implementacji, rekomendowane jest stosowanie zasad ogólnych do kwalifikacji dostawców usług zarządzanych oraz dostawców usług zarządzanych w zakresie cyberbezpieczeństwa jako PW.	podmiotowego zostaną wyłączeni mikroprzedsiębiorcy.
272.	Związek Telewizji Kablowych Izba Gospodarcza	Art. 5	Punktem wyjścia do dalszych rozważań musi być kwestia, iż zakresem podmiotowym ustawy z dnia 5.07.2018 r. o krajowym systemie cyberbezpieczeństwa (tekst jedn. Dz. U. z 2023 r. poz. 913 z późn. zm.), zwanej dalej ustawą o KSC, zostają objęci także przedsiębiorcy telekomunikacyjni, o czym przesądza uchylene art. 1 ust. 2 pkt. 1 ustawy o KSC mocą regulacji art. 1 pkt. 1 lit. b projektu ustawy zmieniającej ustawę o KSC. Mimo iż taka perspektywa zachwytu nie wzbudza zdajemy sobie sprawę, iż taka konieczność wynika z faktu uchylenia z dniem 18.10.2024 r. dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6.07.2016 r. w sprawie środków na rzecz wysokiego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. U. UE.L.2016.194.1), zwanej dalej Dyrektywą NIS 1. na mocy regulacji art. 44 dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14.12.2022 r. w sprawie środków na rzecz wysokiego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniającej rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającą dyrektywę (UE) 2016/1148 (dyrektywa NIS 2)(Dz.U. UE.L.2022.333.80), zwanej dalej dyrektywą NIS 2. Należy bowiem zważyć, iż z jednej strony wedle regulacji art. 1 ust. 3 dyrektywy NIS 1 przepisy tejże dyrektywy dotyczące bezpieczeństwa i zgłaszania incydentów nie znajdowały zastosowania do przedsiębiorstw udostępniających publiczne sieci łączności lub świadczące publicznie dostępne usługi łączności elektronicznej, wobec czego rodzimy ustawodawca mógł wyłączyć spod regulacji ustawy o KSC przedsiębiorców telekomunikacyjnych, co też uczynił na mocy art. 1 ust. 2 pkt. 1 ustawy o KSC. Z kolei z drugiej strony należy wziąć pod uwagę, iż na mocy regulacji art. 41 ust. 1 dyrektywy NIS 2 przepisy prawa krajowego należy dostosować do wymogów tejże dyrektywy do dnia 17.10.2024 r. i stosować je począwszy od dnia 18.10.2024 r., zaś dostawcy publicznych sieci łączności elektronicznej oraz dostawcy publicznie dostępnych usług łączności elektronicznej zostali objęci	Uwaga częściowo uwzględniona Podtrzymujemy zasadność odwołania się do rozporządzenia GBER dotyczącego progów mikro, małych i średnich przedsiębiorstw. Odwołanie do polskiego Prawa przedsiębiorców mogłoby być uznane za niewystarczające wdrożenie dyrektywy NIS2. Odesłania do przepisów załącznika rozporządzenia GBER zostaną poprawione.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

		zakresem podmiotowym dyrektywy NIS 2 na mocy przepisu art. 2 ust. 1 i art. 2 ust. 2 lit. a (i) dyrektywy NIS 2. Mając zatem na uwadze powyżej przytoczone uwarunkowania prawne oraz regulację art. 288 zd.4 Traktatu o funkcjonowaniu Unii Europejskiej z dnia 25.03.1957 r. (Dz. U. z 2004 r. nr 90 poz. 864/2 z późn. zm.), zwanego dalej Traktatem o funkcjonowaniu Unii Europejskiej, nie budzi cienia wątpliwości, iż rozciągnięcie na przedsiębiorców telekomunikacyjnych zakresu podmiotowego ustawy o KSC zastrzeżeń natury prawnej budzić nie może. a/ błąd odesłania Przede wszystkim nie sposób się zgodzić z definiowaniem podmiotu kluczowego w oparciu o odesłanie do przekroczenia wymogów lub spełnienia wymogów średniego przedsiębiorcy przyjętych w rozporządzeniu Komisji (UE) nr 651/2014 z dnia 17.06.2014 r. uznającego niektóre rodzaje pomocy za zgodne z rynkiem wewnętrznym w zastosowaniu art. 107 i art. 108 Traktatu (Dz. U. UE.L.2014.187.1), zwanego dalej rozporządzeniem GBER[art. 5 ust. 1 pkt. 1 i pkt. 2 ustawy' o KSC w brzmieniu nadanym przez art. 1 pkt. 8 ustawy zmieniającej ustawę o KSC], oraz z definiowaniem podmiotu ważnego w oparciu o pojęcie mikro, małych i średnich przedsiębiorców przyjęte w rozporządzeniu GBER [art. 5 ust. 2 pkt. 1, pkt. 2, pkt. 3 ustawy o KSC w brzmieniu nadanym art. 1 pkt. 8 ustawy zmieniającej ustawę o KSC]. Prawodawca unijny w art. 2 ust. 1 dyrektywy NIS 2 przyjmuje, że przepisy dyrektywy NIS 2 stosuje się tak do podmiotów publicznych, jak i podmiotów prywatnych wskazanych w załączniku I lub II do dyrektywy, które kwalifikują się jako średnie przedsiębiorstwa na podstawie art. 2 załącznika do zalecenia Komisji 2003/361/WE z dnia 6.05.2003 r. dotyczące definicji mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw (Dz. U. UE. L 2003.124.36), zwanego dalej zaleceniem nr 2003/361/WE, lub które przekraczają pułapy dla średnich przedsiębiorstw określone w ust. 1 tego artykułu oraz które świadczą usługi lub prowadzą działalność w Unii. Do grona podmiotów kluczowych objętych dyrektywą NIS 2 zaliczono podmioty wskazane w załączniku I do dyrektywy przekraczające pułapy dla średnich przedsiębiorstw określone w art. 2 ust. 1 załącznika do zalecenia nr 2003/361/WE (art. 3 ust. 1 lit. a dyrektywy NIS 2), a także dostawców publicznych sieci łączności elektronicznej lub dostawców publicznie dostępnych usług łączności elektronicznej, które kwalifikują się jako średnie przedsiębiorstwa na podstawie art. 2 załącznika do zalecenia nr 2003/361/WE (art. 3 ust. 1 lit. c dyrektywy NIS 2). Dyrektywa NIS 2 przy określaniu jej zakresu podmiotowego oraz pojęcia podmiotów kluczowych nakazuje opierać się na wymogach zakreślonych dla średnich przedsiębiorstw w art. 2 zalecenia nr 2003/361/WE, a nie na pojęciu średniego przedsiębiorstwa przyjętym w art. 2 ust. 1 załącznika I do rozporządzenia GBER. Definiując zatem pojęcie podmiotu kluczowego w oparciu o spełnienie lub przekroczenie wymogów zakreślonych dla przedsiębiorstwa średniego określonych w art. 2 ust. 1 załącznika I do rozporządzenia GBER wydawać by się mogło, że projektodawca dopuszcza się obrazy art. 288 zd. 4 Traktatu o funkcjonowaniu Unii Europejskiej wiążącej państwo członkowskie co do rezultatu jaki ma	

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

		zostać osiągnięty wprowadzeniem stosownej regulacji wewnętrznej, gdyż odmiennie niż w dyrektywie NIS 2 opiera tak zakres podmiotowy stosowania dyrektywy, jak i pojęcie podmiotów kluczowych na wymogach stosowanych do przedsiębiorstwa średniego nie przyjętych jednakże w art. 2 załącznika do zalecenia nr 2003/361/WE, lecz na wymogach przyjętych dla przedsiębiorcy średniego w art. 2 ust. 1 załącznika I do rozporządzenia GBER. Mimo jednakże nieoparcia pojęcia podmiotu kluczowego na wymogach stawianych przedsiębiorstwu średniemu ujętych w art. 2 załącznika do zalecenia nr 2003/361/WE, z tego akurat powodu nie sposób byłoby stawiać projektodawcy zarzutu, natomiast zarzut dotyczy tego, że oparto się na wymogach stawianych przedsiębiorstwu średniemu w art. 2 ust. 1 załącznika I do rozporządzenia GBER, o czym za chwilę. Niezarzucalność bowiem braku oparcia pojęcia podmiotu kluczowego na pojęciu średniego przedsiębiorstwa w ujęciu art. 2 załącznika do zalecenia nr 2003/361/WE wynika z tego, iż jak słusznie wskazano na stronie 13 uzasadnienia projektu ustawy zmieniającej ustawę o KSC „<i>Zalecenie Komisji(UE) jest aktem prawa miękkiego i zgodnie z zasadami techniki prawodawczej nie odwołuje się do tego rodzaju aktów. Dlatego ustawa odwołuje się do progów średniego przedsiębiorstwa określonych w załączniku I do rozporządzenia Komisji (UE) nr 651/2014 z dnia 17 czerwca 2014 r. uznającego niektóre rodzaje pomocy za zgodne z rynkiem wewnętrznym w zastosowaniu art. 108 i 108 Traktatu (Dz. Urz. UE L 651/2014 z 26.06.2014 r.), „zwane dalej rozporządzeniem 651/2014/UE”, które jest identyczne z zaleceniem Komisji (UE).</i>”. Niemożliwość zastosowania wymogów przewidzianych w załączniku do zalecenia nr 2003/361/WE dla średniego przedsiębiorstwa wynika bowiem z niedopuszczalności dokonywania odesłania do postanowień innych aktów normatywnych niż postanowienia tej samej lub innej ustawy, postanowień ratyfikowanych przez Rzeczpospolitą Polską umowy międzynarodowej lub dających się bezpośrednio stosować aktów normatywnych ustanowionych przez organizacje międzynarodowe lub organy międzynarodowe [§ 22 ust. 1 w zw. z § 4 ust. 3 w zw. z § 4 ust. 2 załącznika do rozporządzenia Prezesa Rady Ministrów z dnia 20.06.2002 r. w sprawie „Zasad techniki prawodawczej” (tekst jedn. Dz. U. z 2016 r. poz. 283), zwanego dalej rozporządzeniem w sprawie zasad techniki prawodawczej]. Niewątpliwie bowiem zalecenie Komisji nr 2003/361/WE zgodnie z regulacją art. 288 zd. 7 Traktatu o funkcjonowaniu Unii Europejskiej nie jest aktem prawnym, którego postanowienia mogą być bezpośrednio stosowane, a zatem niedopuszczalne by było odsyłanie do wymogów stawianych średniemu przedsiębiorstwu w załączniku do tegoż zalecenia (§ 22 ust. 1 w zw. z § 4 ust. 3 w zw. z § 4 ust. 2 załącznika do rozporządzenia w sprawie techniki prawodawczej). Jest jeszcze jedna przyczyna, która i tak by uniemożliwiała skuteczne odesłanie przy pojęciu podmiotu kluczowego do wymogów stawianych średniemu przedsiębiorstwu w art. 2 załącznika do zalecenia nr 2003/361/WE, a mianowicie względ na to, że zalecenie, w tym i Komisji Europejskiej, nie posiada mocy wiążącej (art. 288 zd. 7 Traktatu o funkcjonowaniu Unii Europejskiej), bo	

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			doprawdy trudno byłoby stosować progi przewidziane dla średniego przedsiębiorstwa ustanowione w nieposiadającym mocy wiążącej akcie prawnym Unii Europejskiej. Natomiast względem na to, że rozporządzenie GBER jest aktem prawnym Unii Europejskiej stosowanym bezpośrednio w porządku prawnym każdego państwa członkowskiego Unii Europejskiej (art. 288 zd. 3 Traktatu o funkcjonowaniu Unii Europejskiej), jak i względem na to, że pojęcie średniego przedsiębiorstwa przyjęte w art. 2 ust. 1 załącznika I do tegoż rozporządzenia w swojej treści odpowiada pojęciu średniego przedsiębiorstwa przyjętemu w załączniku do zalecenia nr 2003/361/WE, mimo iż stanowi regulację wprost stosowaną w naszym kraju, co z formalnoprawnego punktu widzenia umożliwiałoby odesłanie do wymogów stawianych średniemu przedsiębiorstwu ujętych w art. 2 ust. 1 załącznika I do rozporządzenia GBER w świetle regulacji § 22 ust. 1 w zw. z § 4 ust. 3 w zw. z § 4 ust. 2 załącznika do rozporządzenia w sprawie techniki prawodawczej okazuje się jednakże niewystarczające, gdyż nie jest w przypadku odesłania obojętne do postanowień jakiego aktu normatywnego bezpośrednio stosowanego dokonujemy odesłania. 1 z tego właśnie powodu nie sposób zgodzić się z poglądem projektodawcy wyrażonym na stronie 13 uzasadnienia projektu ustawy zmieniającej ustawę o KSC „Zalecenie Komisji(UE) jest aktem prawa miękkiego i zgodnie z zasadami techniki prawodawczej nie odwołuje się do tego rodzaju aktów. Dlatego ustawa odwołuje się do progów średniego przedsiębiorstwa określonych w załączniku I do rozporządzenia Komisji (UE) nr 651/2014 z dnia 17 czerwca 2014 r. uznającego niektóre rodzaje pomocy za zgodne z rynkiem wewnętrznym w zastosowaniu art. 108 i 108 Traktatu (Dz. Urz. UE L 651/2014 z 26.06.2014 r.), „zwane dalej rozporządzeniem 651/2014/UE”, które jest identyczne z zaleceniem Komisji (UE). W tym przypadku nie jest możliwe odwołanie się do ustawy z dnia 6 marca 2018 r.~ Prawo przedsiębiorców, ponieważ jego przepisy nie odpowiadają ww. zaleceniu”. Jest bowiem dokładnie odwrotnie niż twierdzi projektodawca. To bowiem czy przepisy ustawy z dnia 6.,03.2018 r.- prawo przedsiębiorców (tekst jedn. Dz. U. z 2024 r. poz. 236 z późn. zm.), zwanej dalej prawem przedsiębiorców, są identyczne w swojej treści z treścią zalecenia Komisji nr 2003/361/WE jest prawnie irrelewantne z tego powodu, iż przedmiotowe zalecenie Komisji Europejskiej nie posiada mocy wiążącej (art. 288 zd. 7 Traktatu o funkcjonowaniu Unii Europejskiej), a zatem porównywanie wiążącej treści ustawy- prawo przedsiębiorców, co wynika z obowiązku przestrzegania prawa Rzeczypospolitej Polskiej przez każdego, w tym i przez projektodawcę na etapie przygotowywania projektu ustawy [art. 83 Konstytucja Rzeczypospolitej Polskiej z dnia 2.04.1997 r. (Dz. U. nr 78 poz. 483 z późn. zm.), zwanej dalej Konstytucją RP], z treścią niewiążącego zalecenia Komisji Europejskiej jest prawnie niedopuszczalne, skoro zalecenie Komisji nie posiada dla państwa polskiego, jak i dla innych krajów Unii Europejskich jakiegokolwiek znaczenia właśnie ze względu na niewiążącą moc tego aktu prawnego Unii Europejskiej (art. 288 zd. 7 Traktatu o funkcjonowaniu Unii Europejskiej). Co więcej w sytuacji, gdy dyrektywa NIS 2 nie definiuje pojęcia przedsiębiorstwa średniego zupełnie niezrozumiałe jest oparcie przez projektodawcę pułapów dla średniego przedsiębiorcy na regulacji art. 2 ust. 1 załącznika 1 do rozporządzenia GBER. gdyż regulacja przedmiotowego rozporządzenia	

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

		nie stanowi ani regulacji definiującej pojęcie średniego przedsiębiorstwa na potrzeby cyberbezpieczeństwa, gdyż tej definicji legalnej nie zawarto w akcie prawnym poświęconym problematyce cyberbezpieczeństwa, ani też nie stanowi chociażby regulacji ogólnej odnoszącej się do przedsiębiorców lub przedsiębiorstw unijnych, lecz jest regulacją poświęconą konkretnej sytuacji prawnej, a mianowicie uznaniu niektórych rodzajów pomocy publicznej za zgodną z rynkiem wewnętrznym w zastosowaniu art. 107 i art. 108 Traktatu o funkcjonowaniu Unii Europejskiej. Nie sposób bowiem dopatrzeć się jakiegokolwiek powiązania tematyki uznania pewnych rodzajów pomocy publicznej za zgodne z rynkiem wewnętrznym z problematyką cyberbezpieczeństwa. Trudno bowiem byłoby uznać z punktu widzenia konstytucyjnej zasady demokratycznego państwa prawnego (art. 2 w zw. z art. 8 Konstytucji RP) za trafną praktykę stosowania definicji legalnych stworzonych na potrzeby innej dziedziny lub gałęzi prawa, dla potrzeb zdefiniowania takiego samego pojęcia w akcie prawnym z zupełnie odmiennej dziedziny lub gałęzi prawa, a z taką właśnie sytuacją mamy do czynienia w omawianym przypadku. W sytuacji zatem, gdy ani przepisy wspólnotowe, ani też przepisy prawa krajowego z zakresu cyberbezpieczeństwa nie zawierają definicji legalnej przedsiębiorstwa/ przedsiębiorcy średniego, ani też wywodzonych z nich pojęć przedsiębiorstwa/ przedsiębiorcy małego i mikroprzedsiębiorcy, wówczas przed projektodawcą stoją dwie możliwości. Pierwsza zasadza się we wprowadzeniu na potrzeby projektowanej ustawy do słowniczka zawartego w ustawie o KSC własnej definicji średniego przedsiębiorcy, a także małego przedsiębiorcy i mikroprzedsiębiorcy przy określaniu pojęcia podmiotu kluczowego i podmiotu ważnego (§ 21 ust. 1 pkt. 2 załącznika do rozporządzenia w sprawie techniki prawodawczej), oczywiście przestrzegając w tym zakresie wymogów przyjętych w dyrektywie NIS 2. Nic zatem nie stoi na przeszkodzie, by projektodawca mimo braku mocy wiążącej przepisu art. 2 załącznika do zalecenia Komisji nr 2003/361/WE na potrzeby zdefiniowania w ustawie o KSC pojęć podmiotu kluczowego i podmiotu ważnego „zaadoptował” z art. 2 załącznika do zalecenia Komisji nr 2003/361/WE progi przyjęte dla przedsiębiorcy średniego, przedsiębiorcy małego oraz mikroprzedsiębiorcy jako elementy własnej (projektodawcy) definicji legalnej tych pojęć (podmiotu ważnego i podmiotu kluczowego). Druga z kolei możliwość, jaka zachodzi w sytuacji, gdy przepisy ogólne prawa wspólnotowego poświęcone przedsiębiorcom/ przedsiębiorstwom takie jak Traktat o funkcjonowaniu Unii Europejskiej, czy też Dyrektywa 2006/123/WE Parlamentu Europejskiego i Rady z dnia 12.12.2006 r. dotycząca usług rynku wewnętrznego (Dz. U.UE.L.2006.376.36), zwana dalej dyrektywa dotycząca usług rynku wewnętrznego, którą wdraża ustawa- prawo przedsiębiorców, nie przewidują definicji legalnej średniego przedsiębiorcy/przedsiębiorstwa, małego przedsiębiorcy/przedsiębiorstwa, mikroprzedsiębiorcy/ mikroprzedsiębiorstwa, wówczas definicje legalne podmiotów kluczowych oraz podmiotów ważnych wprowadzane do ustawy o KSC można oprzeć jedynie na odesłaniu do definicji legalnych średniego przedsiębiorcy, małego przedsiębiorcy, mikroprzedsiębiorcy zawartych w ustawie- prawo przedsiębiorców, co czyni stosowne odesłanie do innej ustawy (prawo	

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			przedsiębiorców) zgodnym z § 22 ust. 1 w zw. z § 4 ust. 3 in principio załącznika do rozporządzenia w sprawie techniki prawodawczej. Na zakończenie tej części rozważań zauważyć także należy, że w projektowanym art. 5 ust. 2 pkt. 2 i pkt. 3 ustawy o KSC określającym pojęcie podmiotu ważnego nieprawidłowe jest odesłanie do pojęcia małego przedsiębiorcy i mikroprzedsiębiorcy zawartym zdaniem projektodawcy w art. 2 ust. 1 załącznika I do rozporządzenia GBER albowiem pojęcie małego przedsiębiorcy zostało zawarte w art. 2 ust. 2 załącznika I do rozporządzenia GBER, zaś pojęcie mikroprzedsiębiorcy zostało zawarte w art. 2 ust. 3 załącznika do rozporządzenia GBER, a nie w art. 2 ust. 1 załącznika I do rozporządzenia GBER. Tego typu błąd odesłania świadczy o zwyczajnym niechlujstwie projektodawcy, który przygotowując projekt regulacji ustawowej nie raczył nawet dokładnie zapoznać się z treścią załącznika I do rozporządzenia GBER w oparciu o które chciałby określić zakres podmiotowy pojęcia podmiotów ważnych, a do regulacji którego to załącznika przecież odsyła.	
273.	Związek Telewizji Kablowych Izba Gospodarcza	Art. 5	Prawodawca wspólnotowy przewidział, iż jednym z kryteriów zaliczenia danego podmiotu do grupy podmiotów kluczowych lub podmiotów ważnych jest zaliczenie działalności danego podmiotu do sektorów gospodarki kluczowych (załącznik I do dyrektywy NIS 2 w zw. z art. 2 ust. 1 w zw. z art. 2 ust. 2 in principio w zw. z art. 3 ust. 1 lit. a w zw. z art. 3 ust. 1 lit. e dyrektywy NIS 2) lub sektorów gospodarki ważnych (załącznik II do dyrektywy NIS 2 w zw. z art. art. 2 ust. 1 w zw. z art. 2 ust. 2 in principio w zw. z art. 3 ust. 2 dyrektywy NIS 2). Oznacza to, iż będąc zobowiązanym do osiągnięcia rezultatu przewidzianego w dyrektywie NIS 2 (art. 288 zd. 4 Traktatu o funkcjonowaniu Unii Europejskiej) projektodawca powinien tak przygotować przepisy prawa wewnętrznego, by zakresem ustawy o KSC objąć tylko te podmioty kluczowe oraz tylko te podmioty ważne, które nakazuje państwu członkowskiemu ująć prawodawca unijny w dyrektywie NIS 2. Tymczasem polski prawodawca w projekcie ustawy zmieniającej ustawę o KSC poszerza listę sektorów gospodarki pozwalających na zaliczenie podmiotu do grupy podmiotów kluczowych, jednocześnie zawężając listę sektorów gospodarki pozwalających na zaliczenie podmiotu do grupy podmiotów ważnych. W przypadku podmiotów kluczowych projektodawca w stosunku do treści załącznika I do dyrektywy NIS 2 rozszerza zakres działalności o: 1/ sektor energetyka nazwany w załączniku nr 1 do projektu ustawy zmieniającej ustawę o KSC sektorem energii poszerza o podsektor wydobywania kopalin, mimo iż sektor energetyka załącznika I do dyrektywy NIS 2 podsektora wydobywania kopalin nie zalicza do usług kluczowych, 2/ wychodząc poza zamknięty zakres sektorów kluczowych objętych załącznikiem I do dyrektywy NIS 2 projektodawca w załączniku do projektu ustawy zmieniającej ustawę o KSC do sektorów kluczowych zalicza także: a/ produkcję, wytwarzanie i dystrybucję chemikaliów b/ produkcję, przetwarzanie i dystrybucję żywności,	Uwaga częściowo uwzględniona Sektory a/ produkcja, wytwarzanie i dystrybucja chemikaliów b/ produkcja, przetwarzanie i dystrybucja żywności, c/ produkcja zostaną przeniesione do sektorów ważnych. Sektor wydobywania kopalin pozostał ponieważ już obecnie istnieje taki sektor w ustawie o krajowym systemie cyberbezpieczeństwa. Dyrektywa NIS2 dopuszcza, aby państwa członkowskie uznały jako podmioty kluczowe dotychczas wyznaczonych operatorów usług kluczowych.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

		c/ produkcję, które to sektory prawodawca unijny zalicza w załączniku II do dyrektywy NIS 2 do sektorów ważnych, a nie kluczowych. Skutkuje to z kolei tym, że zakres sektorów ważnych zostaje przez projektodawcę w załączniku nr 2 do projektu ustawy zmieniającej ustawę o KSC zawężony w zestawieniu z załącznikiem II do dyrektywy NIS 2 właśnie o sektory: a/ produkcji, wytwarzania i dystrybucji chemikaliów b/ produkcji, przetwarzania i dystrybucji żywności, c/ produkcji. Pozbawiona jakiegokolwiek znaczenia prawnego dla zaliczenia do sektora kluczowego podsektora wydobywania kopalin jest ocena projektodawcy wskazująca na bardzo istotny wpływ wydobycia kopalin na funkcjonowanie innych podmiotów, zwłaszcza zaś z sektora energetyki, co zdaniem projektodawcy implikuje objęciem ich tymi samymi regułami co przedsiębiorstwa wytwarzające i przesyłające prąd (str. 91 uzasadnienia projektu ustawy zmieniającej ustawę o KSC). Gdyby bowiem prawodawca wspólnotowy podzielał pogląd polskiego projektodawcy to dałby temu wyraz poprzez zaliczenie podsektora wydobywania kopalin do sektora kluczowego, a tego w załączniku I do dyrektywy NIS 2 nie uczynił. Z kolei o przesunięciu 3 sektorów ważnych do grupy sektorów kluczowych nie może decydować uznanie podmiotów z tych sektorów za podmioty krytyczne w ramach dyrektywy CER oraz względ na zapewnienie spójności przepisów o cyberbezpieczeństwie i o zarządzaniu kryzysowym jak to argumentuje projektodawca (str. 91- str. 92 uzasadnienia projektu ustawy zmieniającej ustawę o KSC) albowiem prawodawca wspólnotowy tego rodzaju przekonaniu nie dał wyrazu, gdyż podmioty z sektorów: a/ produkcji, wytwarzania i dystrybucji chemikaliów b/ produkcji, przetwarzania i dystrybucji żywności, c/ produkcji. należące do grupy podmiotów krytycznych nie wyłączył z zakresu sektorów ważnych ujętych w załączniku II do dyrektywy NIS 2 i nie przeniósł ich do załącznika I do dyrektywy NIS 2 obejmującego sektory kluczowe, a wręcz przeciwnie uznał, iż brak jest podstaw przemawiających za zaliczeniem tych trzech sektorów do sektorów kluczowych objętych załącznikiem I do dyrektywy NIS 2 i zaliczył je w sposób wyraźny, nie budzący cienia wątpliwości do sektorów ważnych ujętych w załączniku II do dyrektywy NIS 2. Niewątpliwie zatem poszerzenie przez polskiego projektodawcę o 3 sektory gospodarki działalności zaliczonej w załączniku nr 1 do projektu ustawy zmieniającej ustawę o KSC w zestawieniu z załącznikiem I do dyrektywy NIS 2 oraz o podsektor wydobywania kopalin nieujęty w żadnym z załączników do dyrektywy NIS 2, przy jednoczesnym zawężeniu o te trzy sektory załącznika nr 2 do ustawy zmieniającej ustawę o KSC w zestawieniu z załącznikiem II do dyrektywy NIS 2 skutkuje tym, iż tego rodzaju „przesunięcia” między sektorami oraz „poszerzenie” sektora energetyka o	

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

		podsektor wydobywania kopalin dokonane przez polskiego projektodawcę nie prowadzi do osiągnięcia rezultatu zamierzonego w dyrektywie NIS 2 przez prawodawcę unijnego dotyczącego zakresu sektorów pozwalających do zaliczenia pewnych podmiotów do grupy podmiotów kluczowych oraz dotyczącego zakresu sektorów pozwalających na zaliczenie pewnych podmiotów do grupy podmiotów ważnych. Tego rodzaju „przesunięcie” działalności pomiędzy sektorami ważnymi i kluczowymi oraz „poszerzenie” sektora energetyka o sektor wydobywania kopalin, które proponuje nam projektodawca, a do dokonania którego projektodawca unijny nie upoważnia prawodawców w krajach członkowskich mocą zapisów dyrektywy NIS 2, z uwagi na nieosiągnięcie rezultatu przewidzianego w dyrektywie NIS 2 odnośnie zakresu podmiotowego podmiotów kluczowych i podmiotów ważnych nie może zostać skutecznie wdrożone jako sprzeczne z regulacją art. 288 zd. 4 Traktatu o funkcjonowaniu Unii Europejskiej, gdyż nie stanowi pełnej implementacji tejże dyrektywy w tymże zakresie do wewnętrznego porządku prawnego naszego kraju. Co więcej „przesunięcie” trzech sektorów gospodarki powyżej wskazanych z sektorów ważnych do sektorów kluczowych oraz „poszerzenie” sektora kluczowego energetyka o podsektor wydobywania kopalin nie może zostać uzasadnione wdrażaniem przez projektodawcę dyrektywy NIS 2, gdyż akurat w zakresie „poszerzenia” grupy podmiotów uznanych za kluczowe, przy jednoczesnym „zawężeniu” o te trzy sektory grupy podmiotów ważnych, oraz dodatkowe „poszerzenie” sektora energetyka zaliczonego do sektora kluczowego o podsektor wydobywania kopalin, nie znajduje oparcia w dyrektywie NIS 2, a zatem twierdzenie wyrażone przez projektodawcę, iż projekt ustawy zmieniającej ustawę o KSC stanowi wdrożenie dyrektywy NIS 2 (ust. 1 str. 1 Oceny Skutków Regulacji, zwanej dalej OSR. stanowiącej część uzasadnienia projektu ustawy zmieniającej ustawę o KSC), w odniesieniu do przedmiotowego „przesunięcia” i „poszerzenia” sektora kluczowego energetyka jest niezgodny z rzeczywistością, gdyż w tym akurat zakresie oparcia w dyrektywie NIS 2 nie znajduje i jest w tym zakresie sprzeczny z treścią załącznika I oraz załącznika II do dyrektywy NIS 2. Przesunięcie trzech sektorów gospodarki z sektorów ważnych do sektorów kluczowych zostaje dokonane przez projektodawcę na niekorzyść przedsiębiorców z sektorów: a/ produkcji, wytwarzania i dystrybucji chemikaliów, b/produkcji, przetwarzania i dystrybucji żywności, c/ produkcji, albowiem będąc przedsiębiorcami zaliczonymi do grupy podmiotów ważnych sprawowany wobec nich byłby przez organy właściwe do spraw cyberbezpieczeństwa jedynie nadzór o charakterze następczym (projektowane nowe brzmienie art. 53 ust. 3 pkt. 2 ustawy o KSC), gdy tymczasem zaliczenie tych przedsiębiorców do grupy podmiotów kluczowych skutkować będzie objęciem ich nadzorem ze strony organów właściwych do spraw cyberbezpieczeństwa poza nadzorem o charakterze następczym także nadzorem o charakterze prewencyjnym (projektowane nowe brzmienie art. 53 ust. 3 pkt. 1 ustawy o KSC), co zresztą projektodawca sam potwierdza na stronie 13 uzasadnienia projektu ustawy zmieniającej ustawę o KSC. Nieprawdziwe zatem okazuje się	

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			przekonanie wyrażone przez projektodawcę jakoby przesunięcie 3 sektorów z grupy sektorów ważnych do grupy sektorów kluczowych nie wiązało się z nałożeniem na te podmioty dodatkowych obowiązków (str. 92 uzasadnienia projektu ustawy zmieniającej ustawę o KSC). Jeszcze gorzej przedstawia się sytuacja przedsiębiorców zaliczonych do podsektora wydobywania kopalin albowiem wedle zamierzeń prawodawcy unijnego nie zostali oni zaliczenia ani do grupy sektorów kluczowych (załącznik I do dyrektywy NIS 2), ani też do grupy sektorów ważnych (załącznik II do dyrektywy NIS 2), tymczasem zaliczenie tego podsektora do sektorów kluczowych w załączniku nr 1 do projektu ustawy zmieniającej ustawę o KSC skutkować będzie nałożeniem na nich wszystkich obowiązków ustawowych nakładanych na podmioty kluczowe, czego prawodawca unijny wobec tej grupy podmiotów zajmujących się wydobywaniem kopalin nie przewidywał. W tym zatem zakresie także rezultat zamierzony w dyrektywnie NIS 2 nie zostaje osiągnięty naruszając wymóg przewidziany w art. 288 zd. 4 Traktatu o funkcjonowaniu Unii Europejskiej. Przedmiotowego zatem przesunięcia przedmiotowych 3 sektorów gospodarki powyżej opisanych z sektorów ważnych do sektorów kluczowych oraz wtłoczenie podsektora wydobywania kopalin do sektora kluczowego energetyka nie sposób zaaprobować.	
274.	Związek Telewizji Kablowych Izba Gospodarcza	Art. 5	W związku z omówionymi powyżej zarzutami dotyczącymi przyjętego w projekcie ustawy zmieniającej ustawę o KSC zakresu podmiotowego ustawy o KSC oraz wprowadzenia pojęć podmiotów kluczowych oraz podmiotów ważnych Związek Telewizji Kablowych w Polsce Izba Gospodarcza wnosi o wprowadzenie następujących zmian w art. 1 pkt. 8 projektu ustawy zmieniającej ustawę o KSC: a/ w art. 5 ust. 1 pkt. 1 ustawy o KSC słowa w brzmieniu „wymogi dla średniego przedsiębiorstwa określone w art. 2 ust. 1 załącznika I do rozporządzenia Komisji (UE) nr 651/2014 z dnia 17 czerwca 2014 r. uznającego niektóre rodzaje pomocy za zgodne z rynkiem wewnętrznym w zastosowaniu art. 107 i 108 Traktatu (Dz. Urz. UE L 187 z 26.06.2014, str. 1), zwanego dalej „rozporządzeniem 651/2014/UE”” zastąpić słowami w brzmieniu „wymogi dla średniego przedsiębiorcy określone w art. 7 ust. 1 pkt. 3 ustawy z dnia 6 marca 2018 r.~ prawo przedsiębiorców (tekst jedn. Dz. U. z 2024 r. poz. 236 z późn. zm.), zwanej dalej prawem przedsiębiorców” b/ w art. 5 ust. 1 pkt. 2 ustawy o KSC słowa w brzmieniu „rozporządzeniu 651/2014/UE” zastąpić słowami w brzmieniu „art. 7 ust. 1 pkt. 3 prawa przedsiębiorców”, c/ w art. 5 ust. 2 pkt. 1 ustawy o KSC słowa w brzmieniu „rozporządzeniu 651/2014/UE” zastąpić słowami w brzmieniu „art. 7 ust. 1 pkt. 3 prawa przedsiębiorców”, d/ w art. 5 ust. 2 pkt. 2 ustawy o KSC słowa w brzmieniu „mikro-, małym lub średnim przedsiębiorcą, o którym mowa w art. 2 ust. 1 załącznika I do rozporządzenia 651/2014/UE” zastąpić słowami w brzmieniu: „mikroprzedsiębiorcą, o którym mowa w art. 7 ust. 1 pkt. 1 prawa przedsiębiorców, małym przedsiębiorcą, o którym mowa w art. 7 ust. 1 pkt. 2 prawa przedsiębiorców lub średnim przedsiębiorcą, o którym mowa w art. 7 ust. 1 pkt. 3 prawa przedsiębiorców”, e/ w art. 5 ust. 2 pkt. 3 ustawy o KSC słowa w brzmieniu „mikro-, małym lub średnim przedsiębiorcą, o którym mowa art. 2 ust. 1 załącznika I do rozporządzenia 651/2014/UE” zastąpić	Uwaga częściowo uwzględniona Podtrzymujemy zasadność odwołania się do rozporządzenia GBER dotyczącego progów mikro, małych i średnich przedsiębiorstw. Odwołanie do polskiego Prawa przedsiębiorców mogłoby być uznane za niewystarczające wdrożenie dyrektywy NIS2. Odesłania do przepisów załącznika rozporządzenia GBER zostaną poprawione.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			słowa w brzmieniu: „mikroprzedsiębiorcą, o którym mowa w art. 7 ust. 1 pkt. 1 prawa przedsiębiorców, małym przedsiębiorcą, o którym mowa w art. 7 ust. 1 pkt. 2 prawa przedsiębiorców lub średnim przedsiębiorcą, o którym mowa w art. 7 ust. 1 pkt. 3 prawa przedsiębiorców”, fl art. 5 ust. 3 ustawy o KSC należy skreślić.	
275.	Związek Telewizji Kablowych Izba Gospodarcza	Art. 5	Regulacja art. 7 ust. 2 i ust. 5 ustawy o KSC to klasyczny przykład nadmiernej regulacji ustawowej, która mimo nałożenia na państwa członkowskie mocą regulacji art. 3 ust. 3 dyrektywy NIS 2 obowiązku założenia do 17.04.2025 r. wykazu podmiotów kluczowych i ważnych nie wymaga zbierania tak szczegółowych danych jak to uczyniono w projektowanym art. 7 ust. 2 ustawy o KSC. Co gorsza regulacja ta przewiduje obowiązek samorejestracji podmiotów ważnych i kluczowych w tymże wykazie, któremu uchybienie skutkuje odpowiedzialnością prawną z zastosowaniem wielu dolegliwych środków, w tym i kar pieniężnych. Z braku uprawnienia do zbierania tak szerokich danych od podmiotów kluczowych i ważnych doskonale zdaje sobie sprawę także sam projektodawca, który wskazuje że z uwagi na obciążające państwa członkowskie z mocy dyrektywy NIS 2 obowiązki przekazania do dnia 17.04.2025 r. do Unii Europejskiej informacji o liczbie podmiotów w poszczególnych sektorach zidentyfikowanych w danym państwie, a w przypadku sektora infrastruktury cyfrowej podanie w tymże terminie konkretnych podmiotów świadczących usługi wskazuje, że „Niezbędny jest więc mechanizm umożliwiający sprawną identyfikację podmiotów kluczowych i podmiotów ważnych. Aby ułatwić identyfikację podmiotów kluczowych i podmiotów ważnych wprowadzono obowiązek samorejestracji tych podmiotów. Rejestracja będzie dokonywała się w wykazie podmiotów kluczowych i ważnych, który będzie prowadzony przez ministra właściwego do spraw informatyzacji(str. 16 uzasadnienia projektu ustawy zmieniającej ustawę o KSC). Zważyć bowiem należy, że prawodawca unijny przewiduje, iż w celu ustanowienia wykazu podmiotów kluczowych i ważnych państwa członkowskie wymagają od tychże podmiotów przedłożenia co najmniej informacji obejmujących: nazwę podmiotu, adres i aktualne dane kontaktowe, w tym adresy poczty elektronicznej, zakresy adresów IP i numery telefonów, w stosownych przypadkach wskazania odpowiedniego sektora i podsektora kluczowego lub ważnego, a także w stosownych przypadkach wykazu państw członkowskich, w których podmioty te świadczą usługi objęte zakresem dyrektywy NIS 2 (art. 3 ust. 4 dyrektywy NIS 2). Przedmiotowe dane są wystarczające dla wykonania do dnia 17.04.2025 r. oraz w kolejnych dwuletnich okrasach czasu przez Ministra Cyfryzacji obowiązku przekazania informacji o liczbie podmiotów kluczowych i ważnych wymienionych w wykazie dla każdego sektora i podsektora do Komisji Europejskiej i Grupy Współpracy oraz informacji istotnych na temat liczby podmiotów kluczowych i ważnych wskazanych na podstawie art. 2 ust. 2 lit. b)-e) dyrektywy NIS 2, sektora i podsektora, o których mowa w załączniku I lub II do dyrektywy NIS 2 i do których podmioty te należą, rodzaju świadczonej przez nie usługi oraz przepisu spośród tych ustanowionych na podstawie art. 2 ust. 2 lit. b)-e) dyrektywy NIS 2, na podstawie którego zostały one wskazane do Komisji Europejskiej (art. 3 ust. 4 dyrektywy NIS 2).	Uwaga częściowo uwzględniona Podanie numeru NIP i REGON jest niezbędne do dokonania prawidłowej identyfikacji podmiotu. Natomiast adres do doręczeń elektronicznych minister właściwy do spraw informatyzacji może pozyskać z bazy adresów elektronicznych, co zostanie zmienione.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

		W zupełności zatem wystarczające będzie przekazanie do wykazu podmiotów kluczowych i ważnych informacji ujętych w projekcie art. 7 ust. 2 pkt. 1-3, 5, 9 i 14 ustawy o KSC, z wyłączeniem jednakże adresu do doręczeń elektronicznych, nawet jeżeli został nadany(projektowany art. 7 ust. 2 pkt. 4 ustawy o KSC), gdyż tego akurat wymogu nie umieszczono w art. 3 ust. 4 dyrektywy NIS 2. Tym samym całkowicie zbędne okazuje się podanie danych określonych w projektowanym art. 7 ust. 2 pkt. 4, 6-8,10-13.15-17 ustawy o KSC, jak i przekazywanie do tegoż wykazu przez Ministra Cyfryzacji danych określonych w projektowanym art. 7 ust. 2 pkt. 18-25 (projektowany art. 7 ust. 5 ustawy o KSC). Dziwić także musi propozycja zgłoszenia do wykazu numeru identyfikacji podatkowej (NIP), jeżeli został nadany oraz numeru identyfikacyjnego podmiotu publicznego w krajowym rejestrze urzędowym podmiotów gospodarki narodowej (REGON)[projektowany art. 7 ust. 2 pkt. 6 i pkt. 7 ustawy o KSC]. W przypadku bowiem przedsiębiorców, a oczywistym wręcz jest, że podmiot nie będący przedsiębiorcą inny niż podmiot publiczny nie będzie objęty zakresem podmiotowym ustawy o KSC, wpisanych w Krajowym Rejestrze Sądowym w Rejestrze Przedsiębiorców NIP i REGON podlegają wpisowi do tegoż rejestru urzędowego [art. 38 pkt. 1 lit. h i pkt. 3 ustawy z dnia 20.08.1997 r. o Krajowym Rejestrze Sadowym (tekst jedn. Dz. U. z 2023 r. poz. 685 z późn. zm.), zwanej dalej ustawą o KRS], zaś przedmiotowy rejestr urzędowy jest rejestrem jawnym, do którego każdemu jest zagwarantowany swobodny dostęp (art. 8 ust. 1 w zw. z art. 8 ust. 2 ustawy o KRS), wpisom dokonany w tym rejestrze przysługuje domniemanie prawdziwości (art. 17 ust. 1 ustawy o KRS), zaś nikt nie może zasłaniać się nieznaną wpisów dokonanych w Krajowym Rejestrze Sądowym- Rejestrze Przedsiębiorców poczynając od dnia ich ogłoszenia w Monitorze Sądowym i Gospodarczym (art. 15 ust. 1 ustawy o KRS). Z kolei w przypadku przedsiębiorcy będącego osobą fizyczną rejestrowanego w Centralnej Ewidencji i Informacji o Działalności Gospodarczej, zwanej dalej CEiDG, wpisowi do CEiDG podlegają NIP i REGON [art. 5 ust. 1 pkt. 4 i pkt. 3 ustawy z dnia 6.03.2018 r. o Centralnej Ewidencji i Informacji o Działalności Gospodarczej i Punkcie Informacji dla Przedsiębiorcy (tekst jedn. Dz. U. z 2022 r. poz. 541 z późn. zm.), zwanej dalej ustawą o CEiDG]. Wpisom dokonany w CEiDG także przysługuje domniemanie ich prawdziwości (art. 16 ust. 1 zd. 1 ustawy o CEiDG), zaś przedmiotowy rejestr urzędowy jest rejestrem jawnym, do którego każdemu zagwarantowany jest swobodny dostęp (art. 2 ust. 2 pkt. 2-4 ustawy o CEiDG). W tej zatem sytuacji, gdy minister właściwy do spraw informatyzacji bez problemu może uzyskać z Krajowego Rejestru Sądowego- Rejestru Przedsiębiorców lub z CEiDG informację o numerze NIP i numerze REGON przedsiębiorcy będącego podmiotem ważnym lub kluczowym doprawdy trudno zrozumieć wymaganie podania tych danych we wniosku o wpis do wykazu podmiotów kluczowych i ważnych. Należy podnieść, że mimo iż w art. 3 ust. 4 dyrektywy NIS 2 wskazano, że w celu ustanowienia wykazu podmiotów kluczowych i ważnych określono minimalną ilość informacji, które	

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			przedmiotowe podmioty mogą być zobowiązane do dostarczenia ministrowi właściwemu do spraw' informatyzacji, to jednakże wprowadzenie w projekcie art. 7 ust. 2 ustawy o KSC obowiązku zgłoszenia do wykazu o wiele większej liczby informacji pozostanie w sprzeczności z obowiązkiem zachowania zasady proporcjonalności i adekwatności przy opracowywaniu projektu aktu normatywnego określającego zasady podejmowania, wykonywania i zakończenia działalności gospodarczej (art. 67 in principio prawa przedsiębiorców), w tym zwłaszcza z: a/ obowiązkiem dążenia do nienakładania nowych obowiązków administracyjnych, a jeśli nie jest to możliwe z obowiązkiem dążenia do ich nakładania jedynie w stopniu koniecznym do osiągnięcia ich celów (art. 67 pkt. 1 prawa przedsiębiorców), b/ w przypadku implementacji prawa Unii Europejskiej obowiązkiem dążenia do nakładania wyłącznie obowiązków administracyjnych niezbędnych do osiągnięcia celów implementowanych przepisów (art. 67 pkt. 4 prawa przedsiębiorców), c/ obowiązkiem dążenia do ograniczenia obowiązków informacyjnych, zwłaszcza gdy wymagane informacje są przekazywane przez obowiązanych organom władzy publicznej na podstawie obowiązujących przepisów (art. 67 pkt. 2 prawa przedsiębiorców). W sytuacji, gdy prawodawca unijny wyraźnie wskazał w' art. 3 ust. 4 dyrektywy NIS 2, iż w celu ustanowienia wykazu podmiotów kluczowych i ważnych wystarczające będzie zgłoszenie przez te podmioty jedynie danych określonych w tym przepisie nałożenie na podmioty kluczowe i ważne obowiązku podania o wiele obszerniejszych danych niż wskazano w art. 3 ust. 4 dyrektywy NIS 2 pozostawać będzie w sprzeczności z dyrektywami stanowienia prawa dla przedsiębiorców wskazanymi w art. 67 in principio prawa przedsiębiorców oraz art. 67 pkt. 1, pkt. 2, pkt. 4 prawa przedsiębiorców. W zaistniałej zatem sytuacji wnioskujemy o wprowadzenie zmian art. 1 pkt. 10 projektu ustawy zmieniającej ustawę o KSC zasadzających się na: a/ w art. 7 ust. 2 ustawy o KSC wykreślenie punktów: 4, 6-8,10-13,15- 25, b/ w art. 7 ustawy o KSC skreślenie ust. 5.	
276.	Polska Izba Informatyki i Telekomunikacji	Art. 5	Art. 5 – zakres stosowania określany wg GBER NIS2 wskazuje na dokonywania oceny wielkości przedsiębiorstwa na podstawie art. 2 załącznika do zalecenia 2003/361/WE natomiast projekt ustawy w art. 5 ust. 1 pkt 1, ust.2 odnosi się wprost do art. 2 załącznika 2 rozporządzenia GBER, ale już art. 5 ust. 1 pkt 2 odnosi się do całego GBER. W uzasadnieniu wyjaśniono, że wynika to z zasad techniki prawodawczej i konieczności odwołania się do obowiązujących przepisów prawnych. Wyjaśnienia wymaga, czy dla oceny wielkości przedsiębiorstwa należy uwzględniać jedynie pułapy określone w art. 2 załącznika 2 GBER czy także pozostałe przepisy załącznika 2 GBER dot. powiązań między przedsiębiorstwami. Z uwagi na wprowadzenie w ust. 3 wyłączenia art. 3 ust. 4 załącznika GBER wydaje się, że intencją jest stosowanie wszystkich zapisów załącznika oprócz wyłączonych. Niezrozumiała jest jednocześnie wyżej wskazana różnica w sposobie odwołania do rozporządzenia GBER.	Wyjaśnienie uwagi Stosuje się cały zał. nr I GBER z wyłączeniem art. 3 ust. 4.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

277.	Polska Izba Informatyki i Telekomunikacji	Art. 5	Zauważamy wykrócenie poza ramy dyrektywy NIS2 i nadmiarowe wobec niej zakwalifikowanie wszystkich dostawców usług zarządzanych w zakresie cyberbezpieczeństwa do kategorii podmiotów kluczowych niezależnie od ich wielkości. W uzasadnieniu wyjaśniono, że zabieg ten jest celowy i wynika z faktu, że takie podmioty świadczą usługi dla innych podmiotów. Wydaje się jednak, że włączenie wszystkich takich podmiotów byłoby bardziej proporcjonalne, gdyby było uzależnione od tego, czy faktycznie świadczą usługi podmiotom ksc czy nie.	Uwaga częściowo uwzględniona Chcemy objąć SOC/CSIRT, które np. nie mają 50 pracowników, z wyłączeniem mikroprzedsiębiorców.
278.	Polska Izba Informatyki i Telekomunikacji	Art. 7	Przepis przewiduje obowiązek wpisu do wykazu przez podmiot kluczowy i ważny. Wnosimy o wyraźne rozstrzygnięcie sposobu w jaki powinny dokonywać wpisu podmioty, których działalność obejmuje kilka rodzajów usług kluczowych lub ważnych. Wnoskujemy o jak najszybsze udostępnienie testowej wersji systemu służącego do dokonywania zgłoszeń do rejestru. Sygnalizujemy również, że w zakresie niektórych punktów mogą wystąpić trudności w ich zgłoszeniu: np. pkt 12 (w dużych firmach nie istnieje jeden numer telefonu, inny niż infolinia), pkt 15 (nie każdy podmiot zawrze takie umowy), pkt 17 (nie każdy podmiot zawrze takie porozumienie).	Uwaga uwzględniona
279.	Polska Izba Informatyki i Telekomunikacji	Art. 7	Doprecyzowania lub wyjaśnienia wymaga forma oraz zakres danych, który ma być złożony we wniosku o wpis do wykazu przez przedsiębiorcę telekomunikacyjnego oraz inne podmioty wskazane w zmienianym art. 7 ust. 6. Zgodnie z brzmieniem projektowanego art. 7 ust. 6 zgodnie, z którym dane wskazane w art. 7 ust. 1 uzupełniane są przez ministra ds. informatyzacji na podstawie danych zawartych w rejestrach publicznych, lub przekazanych przez właściwe organy nadzorcze, jednocześnie zgodnie z art. 7 ust. 7 podmioty te uzupełniają dane w wykazie składając wniosek o zmianę wpisu w wykazie, pojawia się zatem wątpliwość, jakie dane powinny być wskazane przez przedsiębiorców telekomunikacyjnych we wniosku o wpis lub ewentualnie w wniosku o zmianę wpisu oraz jaki jest termin na dokonanie zmiany danych wpisanych przez ministra do spraw informatyzacji przez m.in. przedsiębiorców telekomunikacyjnych.	Uwaga uwzględniona Doprecyzujemy zakresy danych, które mają być uzupełnione.
280.	Polska Izba Informatyki i Telekomunikacji	Art. 7	Wyjaśnienia wymaga, w jakich okolicznościach Minister może wpisać określony podmiot z urzędu i czy podmiot może zaprzeczyć istnieniu podstaw do dokonania wpisu. Zastrzeżenie dot. rygoru kary pieniężnej wydaje się zbędne, w przypadku gdy projekt ustawy zawiera wydzielone przepisy dot. kar. Nie jest zupełnie jasna relacja tego przepisu do projektowanego art. 7a, który również mówi o wpisie do wykazu przez organ właściwy podmiotowi. Wątpliwości i niejasności budzi treść tego postanowienia w świetle postanowień ust. 6.	Wyjaśnienie uwagi Minister właściwy do spraw informatyzacji dokonuje wpisu z urzędu w oparciu o już istniejące rejestry/wykazy.
281.	Amerykańska Izba Handlowa	Art. 7	Do art. 7 ust. 2 pkt 15 uksc projekt wprowadza obowiązek zawarcia w wykazie podmiotów kluczowych i ważnych informacji o zawarciu przez dany podmiot umowy z dostawcą usług zarządzanych w zakresie cyberbezpieczeństwa na realizację zadań, o których mowa w art. 8 i art. 11 uksc, wraz z danymi tego dostawcy zawierające nazwę (firmę) dostawcy, siedzibę, adres, numer telefonu i adres poczty elektronicznej. Chociaż środek ten ma na celu zwiększenie nadzoru i zapewnienie przejrzystości w ekosystemie, to stoimy na stanowisku, że konieczne jest zachowanie szczególnej ostrożności w przetwarzaniu tych danych, ponieważ informacje o praktykach bezpieczeństwa i partnerstwach są szczególnie wrażliwe.	Wyjaśnienie uwagi Wykaz podmiotów kluczowych i podmiotów ważnych będzie miał odpowiednie zabezpieczenia zapewniające poufność przetwarzanych informacji. .

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

282.	Amerykańska Izba Handlowa	Art. 7	Przewidywana w art. 7 ust. 20 uksc w brzmieniu ustalonym projektem procedura wykreślenia podmiotu z rejestru podmiotów kluczowych i podmiotów ważnych powinna uwzględniać dodatkowy etap weryfikacji wniosków o wykreślenie. W obecnym brzmieniu przepisu organ właściwy do spraw cyberbezpieczeństwa rozpatruje wniosek samodzielnie – brak jest jednak wytycznych w odniesieniu do zakresu tego wniosku. Projekt nie przewiduje także żadnej procedury wyjaśniającej w odniesieniu do wniosku o wykreślenie z rejestru. W celu zapewnienia poprawności czynności wykreślenia z rejestru należy rozważyć nałożenie na wnioskodawcę obowiązku należytego uzasadnienia wniosku wraz z podaniem elementów tego uzasadnienia (w szczególności w odniesieniu do obowiązku wykazania, że wnioskodawca przestał spełniać przesłanki uznania za podmiot kluczowy lub podmiot ważny).	Uwaga uwzględniona
283.	CYBERMADEI NPOLAND	Art. 7	Art. 7. 1. Minister właściwy do spraw informatyzacji prowadzi wykaz podmiotów kluczowych i podmiotów ważnych. 2. Wykaz, o którym mowa w ust. 1, zawiera: 15) informację o zawarciu umowy z dostawcą usług zarządzanych w zakresie cyberbezpieczeństwa na realizację zadań, o których mowa w art. 8 i art. 11, wraz z danymi tego dostawcy zawierające nazwę (firmę) dostawcy, siedzibę, adres, numer telefonu, adres poczty elektronicznej; Uważam, że doprecyzowania wymaga aspekt w jakim zakresie odnosi się to do art. 8 i 11. Np. w przypadku: h) edukację z zakresu cyberbezpieczeństwa dla personelu podmiotu, w tym podstawowe zasady cyberhigieny. Czy kilkuosobowe firmy szkoleniowe zajmujące się zagadnieniami z cyberbezpieczeństwa będą zaliczane do podmiotów kluczowych np. jeśli świadczą usługi dla podmiotów kluczowych lub ważnych?	Wyjaśnienie uwagi Firmy szkoleniowe nie są MSSP i nie będą podlegały pod KSC.
284.	CYBERMADEI NPOLAND	Art. 7	Określenie poziomu domeny w art. 7 p.10.	Wyjaśnienie uwagi Należy podać całe nazwy domenowe, niezależnie czy to będzie domena pierwszego poziomu czy drugiego.
285.	CYBERMADEI NPOLAND	Art. 7	art. 7 p. 9. Zgłoszenie IP nie jest możliwe w wielu przypadkach (zmienne IP, adresy dostawców chmurowych).	Wyjaśnienie uwagi Podanie adresów IP wynika wprost z dyrektywy NIS2.
286.	CYBERMADEI NPOLAND	Art. 7	Art. 7 p. 11 oraz art. 9 - doprecyzowanie związku osób kontaktowych z podmiotem oraz przedstawienie alternatywy dla działalności jednoosobowych.	Uwaga uwzględniona W przypadku działalności jednoosobowych wymagana będzie tylko jedna osoba do kontaktu. Nie ma konieczności doprecyzowania związku – czy ma to być pracownik czy osoba na zleceniu.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

287.	Fundacja Bezpieczna Cyberprzestrzeń	Art. 7	Art. 1 pkt 10, treść art. 7 ust. 1 – proponuje się rozważenie czy do wykazu podmiotów kluczowych nie powinny mieć zastosowania przepisy o ochronie informacji niejawnych. Agregacja w jednym wykazie wszystkich informacji, o których mowa w art. 7 ust. 2 sprawia, że taki wykaz będzie zawierał dane wrażliwe z punktu widzenia bezpieczeństwa państwa. Aby utrzymać charakter wykazu bez jego klauzulowania proponuje się zmniejszenie ilości pozyskiwanych i gromadzonych danych np. zawartych w art. 7 ust. 2 pkt 9 i pkt 10, które mogą się zmieniać. Korzystanie z wykazu w postaci niejawnej jest uciążliwe.	Wyjaśnienie uwagi Zgodnie z art. 7 ust. 4 do wykazu podmiotów kluczowych i podmiotów ważnych nie będą stosowane przepisy ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej oraz ustawy z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego. Wykaz nie będzie miał charakteru niejawnego ale nie będzie on publiczny. Podanie zakresu adresów IP jest wymagane przez dyrektywę NIS2.
288.	Fundacja Bezpieczna Cyberprzestrzeń	Art. 7	Art. 1 pkt 10, treść art. 7 ust. 2 pkt 9 i pkt 10 – czy podawane zakresy adresacji oraz nazw domenowych mają mieć związek z główną działalnością podmiotu kluczowego czy odniesienie do konkretnego rodzaju działalności. W praktyce dostawców usług zarządzanych w zakresie cyberbezpieczeństwa często stosuje się domeny lub adresy IP wykorzystywane czasowo, na potrzeby konkretnych projektów/zleceń. Czy w takim przypadku również należy podawać takie adresy/domeny? Czy w takim przypadku należy wysyłać do ministra właściwego do spraw informatyzacji uzupełnienie danych?	Wyjaśnienie uwagi Zakresy adresacji mają dotyczyć mają dotyczyć głównej działalności.
289.	ISAC-Kolej	Art. 7	„17) informację o członkostwie w ISAC (sektorowym lub podsektorowym) oraz w związku z tym o zawarciu przez podmiot kluczowy lub podmiot ważny porozumienia, o którym mowa w art. 8h ust. 5” Zapisy, o których mowa w art. 8h ust. 1 – 6 sankcjonują tak naprawdę zasady działania struktury ISAC powołanych w danym sektorze lub podsektorze	Uwaga nieuwzględniona Takie brzmienie sugeruje, że ISAC jest podmiotem prawa, tymczasem w polskiej praktyce są to porozumienia.
290.	ISACA	Art. 7	"9) zakres adresów IP wykorzystywanych przez podmiot kluczowy lub podmiot ważny; 10) domeny internetowe wykorzystywane przez podmiot kluczowy lub podmiot ważny; "wykreślenie, zamiast tego wprowadzenie innego alternatywnego mechanizmu: Podmioty kluczowe i podmioty ważne przekazują dane dotyczące zakresu adresów IP oraz domen internetowych wykorzystywanych przez te podmioty za pomocą dedykowanych systemów informatycznych lub usług sieciowych udostępnianych przez właściwe CSIRT MON, CSIRT NASK, CSIRT GOV, lub CSIRT sektorowy. Dane te są aktualizowane przez podmioty bez zbędnej zwłoki, w przypadku każdej zmiany." "Dynamika zmian adresów IP i domen: W dzisiejszych dynamicznych środowiskach IT, adresy IP oraz domeny internetowe mogą często się zmieniać. Podmioty korzystające z chmury obliczeniowej, CDN (Content Delivery Network) oraz innych technologii mogą mieć często aktualizowane lub zmienne adresy IP i domeny. Utrzymanie aktualności tych danych w centralnym wykazie jest wyzwaniem administracyjnym i może prowadzić do nieścisłości oraz nieaktualności.	Wyjaśnienie uwagi Wymóg podawania zakresów adresów IP wynika z dyrektywy NIS2.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			Uzasadnienie dodania alternatywnego przepisu: 1. Przekazywanie danych za pomocą dedykowanych systemów informatycznych lub usług sieciowych (Web Service) umożliwi bieżącą aktualizację informacji o adresach IP i domenach internetowych, co zwiększa dokładność i aktualność tych danych. 2. Dostępność zautomatyzowanego systemu przekazywania danych zmniejsza obciążenie administracyjne związane z ręcznym aktualizowaniem centralnego wykazu i pozwala na bardziej efektywne zarządzanie informacjami przez podmioty kluczowe i ważne oraz zapewnia prawidłowe informacje dla CSIRT-ów."	
291.	KWKR Konieczny Wierzbicki i Partnerzy S.K.A.	Art. 7	W przypadku wpisania z urzędu podmiotów, o których mowa w art. 7 ust. 6 uksc po nowelizacji do wykazu podmiotów kluczowych i ważnych podmioty te mają 14 dni na uzupełnienie brakujących danych w wykazie (art. 7 ust. 16 uksc po nowelizacji). Wpisanie tych podmiotów z urzędu i zobowiązanie do uzupełnienia danych w terminie 14 dni powoduje, że w rzeczywistości te podmioty (w tym mikro i mali operatorzy telekomunikacyjni, mali i mikro dostawcy usług zarządzanych w zakresie cyberbezpieczeństwa) mają krótszy termin na realizację obowiązków ustawowych niż inne podmioty kluczowe i ważne, które na wpis do wykazu mają 2 miesiące (art. 7 ust. 3 uksc po nowelizacji). W terminie 14 dni podmioty, o których mowa w art. 7 ust. 6 Projektu, muszą m.in. wskazać: y- dane co najmniej 2 osób do kontaktu z podmiotami krajowego systemu cyberbezpieczeństwa zawierające: imię i nazwisko, numer telefonu oraz adres poczty elektronicznej, - oraz muszą rozpocząć korzystanie z systemu informatycznego, o którym mowa w art. 46 ust. 1 (art. 9 pkt 3 uksc po nowelizacji). W rezultacie obowiązki te musiałyby być realizowane de facto w krótszym czasie niż w przypadku pozostałych podmiotów kluczowych i ważnych. A przyśpieszony termin realizacji dotyczy także mikro i małych przedsiębiorstw, które co do zasady dysponują skromniejszymi środkami niż podmioty średnie i duże.	Uwaga uwzględniona Termin zostanie wydłużony.
292.	Konfederacja Lewiatan	Art. 7	Przepis przewiduje obowiązek wpisu do wykazu przez podmiot kluczowy i ważny. Wnosimy o wyraźne rozstrzygnięcie sposobu w jaki powinny dokonywać wpisu podmioty, których działalność obejmuje kilka rodzajów usług kluczowych lub ważnych. Wnioskujemy o jak najszybsze udostępnienie testowej wersji systemu służącego do dokonywania zgłoszeń do rejestru. Sygnalizujemy również, że w zakresie niektórych punktów mogą wystąpić trudności w ich zgłoszeniu: np. pkt 12 (w dużych firmach nie istnieje jeden numer telefonu, inny niż infolinia), pkt 15 (nie każdy podmiot zawrze takie umowy), pkt 17 (nie każdy podmiot zawrze takie porozumienie).	Wyjaśnienie uwagi Będą podejmowane działania szkoleniowe dot. systemu s46. W przypadku umów czy porozumień to informacja jest wymagana wtedy, gdy taka umowa/porozumienie została zawarta.
293.	Konfederacja Lewiatan	Art. 7	Jednostka redakcyjna: Art. 7 ust. 16 Wyjaśnienia wymaga, w jakich okolicznościach Minister może wpisać określony podmiot z urzędu i czy podmiot może zaprzeczyć istnieniu podstaw do dokonania wpisu. Zastrzeżenie dot. rygoru kary pieniężnej wydaje się zbędne, w przypadku, gdy projekt ustawy zawiera wydzielone przepisy dot. kar. Nie jest zupełnie jasna relacja tego przepisu do projektowanego art. 7a, który również mówi o wpisie do wykazu przez organ właściwy podmiotu.	Wyjaśnienie uwagi Wpis z urzędu dotyczy sytuacji, gdy już podmiot został ujęty w innych wykazach.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

294.	Osoba fizyczna	Art. 7	W projekcie ustawy napisano, że podmiot wpisany obecnie do rejestru Operatorów Usługi Kluczowej będzie z urzędu wpisany do rejestru podmiotów kluczowych. Powinno być również wprost napisane, że nie musi już podejmować żadnych czynności związanych z samorejestracją (jeśli nie będzie musiał).	Wyjaśnienie uwagi Kwestia ta jest uregulowana w przepisach dostosowujących.
295.	Osoba fizyczna	Art.7	Sektorowa przynależność. Zgodnie z projektem ustawy KSC art. 7 ust 3 oraz Art. 5 ust.1 <i>Podmiot kluczowy i podmiot ważny składa wniosek o wpis w wykazie, o którym mowa w ust. 1, w terminie 2 miesięcy od dnia spełnienia wymogów, o których mowa w art. 5 ust. 1 lub ust. 2</i> <i>„Art. 5. 1. Podmiotem kluczowym jest:</i> <i>1) osoba fizyczna, osoba prawna albo jednostka organizacyjna nieposiadająca osobowości prawnej wskazana w załączniku nr 1 i nr 2 do ustawy</i> Uzasadnienie: Jeżeli podmiot prowadzi działalność wskazaną w Załączniku nr 1 w obszarze „Rodzaj Podmiotu”, spełniający wpisane podstawy prawne, odpowiadające kilku sektorom to czy podlega pod różne sektory. ? Czy będzie zobowiązany do kilku zgłoszeń w różnych sektorach ? Do którego CSIRT'u Sektorowego będzie należał. Czy będzie zobowiązany zgłaszać incydenty, lub wczesne ostrzeżenia do wszystkich CSIRT'ów czy tylko do jednego. ?	Wyjaśnienie uwagi Podmiot może przynależeć do kilku sektorów. Zgłoszenie będzie jedno – system S46 prześle automatycznie zgłoszenie do właściwego CSIRT sektorowego.
296.	Polska Organizacja Handlu i Dystrybucji	Art. 7 ust. 6 pkt 1, art. 16 ust. 1 pkt 1 i art. 14 ust 1	zmiana terminu z 6 na 12 miesięcy	Uwaga nieuwzględniona termin 6 miesięcy pozostanie z uwagi na wdrożenie dyrektywy NIS2.
297.	Polska Organizacja Handlu i Dystrybucji	Art. 7 ust. 6 pkt 2, art. 16 ust. 1 pkt 2	zmiana terminu z 12 na 18 miesięcy	Uwaga uwzględniona Termin został wydłużony do 24 miesięcy.
298.	PGE SA	Art. 1 pkt 10, art. 7 ust. 2 pkt 9	Wnioskujemy o wykreślenie tego punktu lub określenie sposobu ochrony tych informacji w sposób szczególny. Informacje o adresacji IP stanowią powierzchnię ataku podmiotu przekazującego. ~~9) zakres adresów IP wykorzystywanych przez podmiot kluczowy lub podmiot ważny;~~	Uwaga nieuwzględniona Podanie zakresu adresów IP jest wymagane przez dyrektywę NIS2. Ponadto zgodnie z art. 7 ust. 4 do wykazu podmiotów kluczowych i podmiotów ważnych nie będą stosowane przepisy ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej oraz ustawy z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego. Informacje te nie będą publicznie dostępne.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

299.	PGE SA	Art. 7 ust. 13	Ustęp mówi o wniosku, ale nie określa, czy dotyczy wniosku o wpis, czy również wniosku o zmianę wpisu – proszę o doprecyzowanie.	Uwaga uwzględniona Chodzi także o wniosek o zmianę wniosku. Przepis zostanie przeredagowany.
300.	Polskie Stowarzyszenie Fotowoltaiki	Art. 7	PK i PW zobowiązany jest do złożenia wniosku o wpis w wykazie PK i PW („Wykaz”) w terminie 2 miesięcy od dnia spełnienia wymogów kwalifikacji jako którykolwiek z tych podmiotów. Złożenie wniosku o wpis, zmianę lub wykreślenie z wykazu wymaga m.in. złożenia oświadczenia o odpowiedzialności karnej za złożenie fałszywego oświadczenia. PK i PW zobowiązany jest do - aktualizacji informacji wskazanych w wykazie w terminie 14 dni od dnia ich zmiany; - złożenia wniosku o wykreślenie z Wykazu w razie przestał spełniać przesłanki uznania za PK lub PW. Wpis, zmiana wpisu oraz wykreślenie wpisu z Wykazu jest czynnością materialno-techniczną i ma charakter deklaratoryjny. Ogólny wpływ regulacji: Obowiązek dokonania samodzielnego wpisu do Wykazu wymaga przez podmioty gospodarcze dokonania: - samodzielnej analizy prowadzonej przez siebie działalności oraz - kwalifikacji jako PK lub PW. Realizacja obowiązków skutkuje obciążeniem podmiotów gospodarczych (również tych nieobjętych ustawą) dodatkowymi kosztami, powstającymi w szczególności z uwagi na wdrożenie odpowiednich procedur weryfikacji, monitorowania spełnienia przesłanek i obowiązku aktualizacji informacji, weryfikacji uznania za PK lub PW, analiz prawnych. Obowiązek aktualizacji informacji w terminie 14 dni wynika bezpośrednio z Dyrektywy NIS2. Wpływ na sektor energetyczny: Uwagi jw. – brak specyficznego wpływu na sektor energetyczny [Nadregulacja względem Dyrektywy NIS2] Zakres danych wymaganych na podstawie Projektu, które mają być ujęte w wykazie, istotnie wykracza poza zakres danych wymaganych na gruncie Dyrektywy NIS2, która w odniesieniu do poszczególnych kategorii informacji przewiduje, że muszą być one podawane jedynie „w stosownych przypadkach”. Projekt wymaga najpełniejszego zakresu danych od wszystkich PK i PW. [Niepełna implementacja Dyrektywy NIS2] Jednocześnie na marginesie wskazujemy, że art. 7 ust. 18 KSC wg Projektu nie przewiduje jednoznacznego obowiązku zmiany danych w wykazie w przypadku wygaśnięcia porozumień, o których mowa w art. 8h ust. 5 KSC wg Projektu, jak również Projekt nie wskazuje przypadków, w których PK i PW mają przekazywać informacje o wygaśnięciu porozumień, co wydaje się nie realizować wytycznych Dyrektywy NIS2. Art. 29 ust. 4 Dyrektywy NIS przewiduje bowiem, że PK i PW powiadamiają właściwe organy „w stosownych przypadkach, o wycofaniu się z takich mechanizmów, gdy wycofanie stanie się skuteczne.”	Wyjaśnienie uwagi Przepis nakazuje podmiotowi kluczowemu/ważnemu aktualizację danych w wykazie. Dane zawarte w wykazie mają na celu ułatwić identyfikację podmiotów oraz wsparcie w realizowaniu zadań CSIRT.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			Rekomendacja - ograniczenie zakresu wymaganych informacji do niezbędnego minimum, wyznaczonego przez Dyrektywę NIS2; - dostosowanie Projektu w celu implementacji postanowień art. 29 ust. 4 Dyrektywy NIS2.	
301.	STOWARZYSZENIE ABSOLWENTÓW STUDIÓW CYBERBEZPIECZEŃSTWA MBA	Art. 7	Niedoprecyzowany obowiązek rejestracji dla podmiotów kluczowych i ważnych Zgodnie z projektowanym art. 7 ust. 3 ustawy o krajowym systemie cyberbezpieczeństwa „Podmiot kluczowy i podmiot ważny składa wniosek o wpis w wykazie, o którym mowa w ust. 1, w terminie 2 miesięcy od dnia spełnienia wymogów, o których mowa w art. 5 ust. 1 lub ust. 2”. W toku stosowania przepisów (po zakończeniu okresu przejściowego) przedsiębiorstwa, które przekroczy określone progi zatrudnienia lub obrotu, mają zaledwie 2 miesiące na dokonanie wpisu do tego wykazu, co może być problematyczne. Krótki termin stawia sektor przed wyzwaniem szybkiego dostosowania się do nowych wymogów. Dodatkowo, wymóg składania oświadczenia o statusie pod rygorem odpowiedzialności karnej (projektowany art. 7 ust. 10 ustawy KSC) zwiększa ryzyko dla przedsiębiorstw, które mogą nieświadomie naruszyć te skomplikowane regulacje. W efekcie, podmioty są zmuszane do prowadzenia ciągłej i często skomplikowanej samooceny, aby uniknąć sankcji karnych za niezłożenie wymaganej deklaracji w odpowiednim terminie. Proponujemy wydłużenie terminu na dokonanie wpisu do wykazu do 6 miesięcy od dnia zatwierdzenia sprawozdania finansowego, a w razie jego niezatwierdzenia w terminie wynikającym z przepisów – od jego sporządzenia. Aktualne brzmienie projektowanych przepisów nie precyzuje również sytuacji, w których ten sam podmiot (zidentyfikowany w oparciu o jego indywidualizację zgodnie z przepisami prawa cywilnego i przepisów kodeksu spółek handlowych), będzie kwalifikował się do więcej niż jednego sektora lub podsektora. Zgodnie z art. 7 ust. 2 pkt. 2 ustawy o KSC w wykazie podmiotów kluczowych i ważnych znajduje się informacja do jakiego sektora i podsektora należy podmiot. Jest to pozycja wypełniana przez sam podmiot (chyba, że jest on przepisywany na podstawie decyzji o uznaniu za operatora usługi kluczowej lub danych z innego rejestru). Nie ma w przepisach odniesienia do sytuacji, kiedy podmiot prowadzi działalność w więcej niż jednym sektorze. Sytuacja taka ma miejsce w przypadku różnego rodzaju podmiotów, najczęściej w zakresie łączenia swojej podstawowej działalności (np. produkcyjnej) m.in. z działalnością w zakresie: 1. energetyki (stacje ładowania, odcinki sieci dystrybucyjnych czy małoskalowa działalność w zakresie obrotu – niepodlegająca wymogom unbundlingu), 2. transportu kolejowego (w zakresie zarządzania obiektami typu bocznica kolejowa lub posiadania licencji na wykonywanie przewozów), 3. wodociągowo-kanalizacyjnej, 4. gospodarowania odpadami. Rodzi to poważne trudności dla rynku, w kwestii ustalenia zarówno właściwego trybu zgłoszenia do rejestru (tym większe, jeżeli w harmonogramie opublikowanym zgodnie z art. 14 ust. 2 w zw. z art. 15	Uwaga częściowo uwzględniona Wykaz będzie wskazywał w jakich sektorach może się podmiot znajdować. Termin będzie się liczył od zatwierdzenia sprawozdania finansowego.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			ust. 3 projektu, dla różnych sektorów będą różne terminy), a w zależności od sposobu skonstruowania formularza do samozgłoszenia, może oznaczać konieczność dokonania kilku odrębnych zgłoszeń do różnych sektorów (głównego i aktualizujących). W przypadku podmiotów, które do wykazu podmiotów kluczowych i ważnych zostaną wpisane z urzędu, pojawi się wątpliwość dotycząca potrzeby i terminu aktualizacji wpisu w zakresie, jaki wykracza poza treść decyzji (taką sytuację może mieć np. ciepło, gdzie podział na dystrybucję, przesył i obrót w praktyce nie ma znaczenia, bo większość podmiotów na rynku łączy te działalności, a decyzje jakie uzyskiwały o uznaniu za operatora usługi kluczowej nie były wydawane jednolicie i mogą dotyczyć tylko niektórych z tych obszarów). Brak wywiązania się z obowiązków rejestrowych oznacza karę dla podmiotu, a brak aktualizacji wpisu – dla jego kierownika. Dolegliwość ta powinna być co najmniej ograniczona w okresie pierwszych 12 miesięcy od pełnego uruchomienia funkcjonalności systemu do samorejestracji, przez sformułowanie obowiązku odstąpienia od wymierzenia kary przez organ, jeżeli ma miejsce sytuacja opisana powyżej.	
302.	Stowarzyszenie Absolwentów Studiów Cyberbezpieczeństwa MBA	Art. 7	Podawanie adresacji IP do wykazu (projektowany art. 7 ust. 2 pkt 9) ustawy o KSC) Nie każdy podmiot wykorzystuje statyczną adresację IP. Przepis jest nieprecyzyjny, a ze względu na mnogość możliwości technicznej realizacji połączenia sieci (np. translacja adresów) wydaje się również nieegzekwowalny i nieuzasadniony z punktu widzenia krajowego systemu cyberbezpieczeństwa. Ponadto zapis: “zakres adresów IP wykorzystywanych przez podmiot kluczowy lub podmiot ważny” może prowadzić na potrzebę przekazania danych nadmiarowych np. adresacji wewnętrznej, która z definicji tak jak dokumentacja cyberbezpieczeństwa winna być chroniona. Zasadne jest doprecyzowanie przepisu art. 7 ust. 2 pkt 9) tak, aby uzyskał brzmienie: “publiczną adresację IP wykorzystywanych przez podmiot kluczowy lub podmiot ważny”.	Uwaga uwzględniona Kwestia podania adresów IP jest wymagana przez dyrektywę NIS2. Przepis zostanie zmieniony zgodnie z propozycją.
303.	ISSA Polska	Art. 7	Nie każdy podmiot wykorzystuje statyczną adresację IP. Zapis jest nieprecyzyjny, a ze względu na mnogość możliwości technicznej realizacji połączenia sieci (np. translacja adresów) wydaje się również nieegzekwowalny i nieuzasadniony z punktu widzenia krajowego systemu cyberbezpieczeństwa. Ponadto zapis: “zakres adresów IP wykorzystywanych przez podmiot kluczowy lub podmiot ważny” może prowadzić na potrzebę przekazania danych nadmiarowych np. adresacji wewnętrznej, która z definicji tak jak dokumentacja cyberbezpieczeństwa winna być chroniona. Prosimy o wyjaśnienie intencji i doprecyzowanie zapisu.	Wyjaśnienie uwagi Kwestia podania adresów IP jest wymagana przez dyrektywę NIS2.
304.	ZBP	Art. 7 ust. 3 oraz ust. 14 i 15	Podmiot kluczowy i podmiot ważny składa wniosek o wpis w wykazie, o którym mowa w ust. 1, w terminie 2 miesięcy od dnia spełnienia wymogów, o których mowa w art. 5 ust. 1 lub ust. 2 Dla zwiększenia czytelności ustawy – proponujemy opisanie wymogów w ramach następujących po sobie przepisów.	Uwaga uwzględniona Przepis zostanie przeredagowany.
305.	ZBP	Art. 7 ust. 7	Podmioty, o których mowa w ust. 6, uzupełniają dane w wykazie, o którym mowa w ust. 1, składając wnioski o zmianę wpisu w tym wykazie Uwaga ogólna	Uwaga uwzględniona Podmioty muszą złożyć uzupełnienie po uzyskaniu informacji o wpisie.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			Prosimy o doprecyzowanie, czy uzupełnienie danych w tym trybie powinno następować z własnej inicjatywy – obowiązkowo po uzyskaniu informacji o wpisie – jeśli tak – w jakim terminie powinno to nastąpić?	
306.	KGHM Polska Miedź S.A.	Art. 7a ust. 3 oraz przepisy powiązane	Proponujemy zmienić brzmienie sformułowania „adres do doręczeń elektronicznych” na „adres do doręczeń elektronicznych lub adres pocztowy siedziby podmiotu”. Adekwatnie do treści uwagi w odniesieniu do wszystkich wystąpień sformułowania w treści aktu. Propozycja uzupełnienia o alternatywne metody komunikacji w okresie przejściowym przed pełnym uruchomieniem e-doręczeń oraz w przypadkach, gdy ten kanał komunikacji pozostawałby niedostępny. Zgodnie z art. 6 ust. 1 pkt 3 ustawy o doręczeniach elektronicznych z dnia 18 listopada 2020 r. (t.j. Dz. U. z 2023 r. poz. 285 z późn. zm.), dopuszczono wskazanie w przepisie odrębnym innych sposobów doręczeń.	Uwaga nieuwzględniona W wykazie będzie także adres do korespondencji. Co do adresu do doręczeń elektronicznych to będzie on wpisany, jeżeli zostanie wpisany do bazy adresów elektronicznych.
307.	PIPC	Art. 7a ust. 3 oraz przepisy powiązane	Proponujemy zmienić brzmienie sformułowania „adres do doręczeń elektronicznych” na „adres do doręczeń elektronicznych lub adres pocztowy siedziby podmiotu”. Adekwatnie do treści uwagi w odniesieniu do wszystkich wystąpień sformułowania w treści aktu. Propozycja uzupełnienia o alternatywne metody komunikacji w okresie przejściowym przed pełnym uruchomieniem e-doręczeń oraz w przypadkach, gdy ten kanał komunikacji pozostawałby niedostępny. Zgodnie z art. 6 ust. 1 pkt 3 ustawy o doręczeniach elektronicznych z dnia 18 listopada 2020 r. (t.j. Dz. U. z 2023 r. poz. 285 z późn. zm.), dopuszczono wskazanie w przepisie odrębnym innych sposobów doręczeń.	Uwaga uwzględniona Zostanie wprowadzona zmiana w przepisie – dodana zostanie informacja – „jeśli został wpisany do bazy adresów elektronicznych”.
308.	Polskie Stowarzyszenie Fotowoltaiki	Art. 7a ust. 3 Art. 7b ust. 2 Art. 7c ust. 3(2)	Obowiązek: - uzupełnienia brakujących danych w Wykazie w terminie 14 dni od dnia otrzymania zawiadomienia, w razie wpisania do Wykazu przez organ właściwy do spraw cyberbezpieczeństwa z urzędu (uprawnienie takie przysługuje właściwemu organowi); - zmiany wpisu do wykazu w razie stwierdzenia, że dane w wykazie są niezgodne ze stanem faktycznym przez organ właściwy do spraw cyberbezpieczeństwa; - uzupełnienia brakujących danych w Wykazie w razie wydania decyzji przez organ właściwy do spraw cyberbezpieczeństwa o uznaniu za PK lub PW na podstawie art. 7c ust. 1 KSC wg Projektu. Ogólny wpływ regulacji: Zarówno w zakresie obowiązku uzupełnienia danych w wykazie w trybie przewidzianym w art. 7a ust. 3, jak i 7c ust. 3 pkt 2) KSC wg Projektu, 14-dniowy termin na uzupełnienie danych w wykazie jest terminem zbyt krótkim, nie znajdującym odzwierciedlenia w Dyrektywie NIS2. Sytuacja, w której dany podmiot uznawany jest za PK lub PW w drodze decyzji lub z uwagi na wpis do wykazu, jest sytuacją zbliżoną do tej, w której to dany podmiot samodzielnie dokonuje wpisu do Wykazu, po spełnieniu przesłanek uznania za PK lub PW. W tej ostatniej sytuacji, zgodnie z Projektem, PK lub PW ma 2 miesiące na złożenie wniosku o wpis w Wykazie. Tym samym, terminy 14 dni na uzupełnienie danych w wykazie są nieproporcjonalne i mogą być niewystarczające do realizacji tego obowiązku. Wpływ na sektor energetyczny	Uwaga uwzględniona Przepis zostanie zmieniony.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			Należy również zwrócić uwagę, że w trybie przewidzianym w art. 7c KSC wg Projektu, jako PW lub PK w drodze decyzji organu właściwego zaklasyfikowanych może zostać szereg mikro i małych przedsiębiorców świadczących usługi w sektorze energetycznym, w odniesieniu do których przekazanie wszystkich informacji wymaganych Projektem może wymagać większej ilości czasu. [Nadregulacja względem Dyrektywy NIS2] Różnicowanie sytuacji podmiotów, które dokonują samooceny i tych, względem których właściwy organ wydaje decyzję o wpisaniu do rejestru, jest nieuzasadnione i nie znajduje odzwierciedlenia w Dyrektywie NIS2. Rekomendacja: W przypadkach, o których mowa w art. 7a oraz 7c KSC wg Projektu, termin na uzupełnienie informacji w wykazie, powinien konsekwentnie wynosić 2 miesiące.	
309.	Związek Pracodawców Polska Miedź	Art. 7a ust. 3 oraz przepisy powiązane	Proponujemy zmienić brzmienie sformułowania „adres do doręczeń elektronicznych” na „adres do doręczeń elektronicznych lub adres pocztowy siedziby podmiotu”. Adekwatnie do treści uwagi w odniesieniu do wszystkich wystąpień sformułowania w treści aktu. Propozycja uzupełnienia o alternatywne metody komunikacji w okresie przejściowym przed pełnym uruchomieniem e-doręczeń oraz w przypadkach, gdy ten kanał komunikacji pozostawałby niedostępny. Zgodnie z art. 6 ust. 1 pkt 3 ustawy o doręczeniach elektronicznych z dnia 18 listopada 2020 r. (t.j. Dz. U. z 2023 r. poz. 285 z późn. zm.), dopuszczono wskazanie w przepisie odrębnym innych sposobów doręczeń.	Uwaga uwzględniona Zostanie wprowadzona zmiana w przepisie – dodana zostanie informacja – „jeśli został wpisany do bazy adresów elektronicznych”.
310.	KGHM Polska Miedź S.A.	Art. 7a ust. 4, Art. 7c	Rekomenduje się, aby działania organu właściwego miały formę decyzji administracyjnej, a nie jedynie innej czynności z zakresu administracji publicznej. Adekwatnie do treści uwagi Wpisanie lub odmowa wykreślenia podmiotu do/z wykazu niewątpliwie nakładać będzie na podmioty określone obowiązki prawne, w związku z czym rekomenduje się wskazanie, że będzie to dokonywane w drodze decyzji administracyjnej.	Uwaga nieuwzględniona Obowiązki z zakresu cyberbezpieczeństwa danego podmiotu będą wynikały wprost z przepisów ustawowych. Wpis do wykazu też będzie miał charakter deklaratoryjny. Obowiązek wpisu do wykazu będzie wynikał wprost z przepisów prawa. Organ właściwy do spraw cyberbezpieczeństwa będzie jedynie dokonywał czynności, której nie dokonał podmiot kluczowy/podmiot ważny. Nie jest możliwe, przy tak dużej liczbie podmiotów, aby organ właściwy do spraw cyberbezpieczeństwa w każdym przypadku przeprowadzał skomplikowane postępowanie administracyjne. Dlatego zdecydowano się na prostszą formułę <i>innej czynności z zakresu administracji publicznej</i> przy

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

				zapewnieniu również odwołania do sądu administracyjnego.
311.	PIPC	Art. 7a ust. 4, Art. 7c	Rekomenduje się, aby działania organu właściwego miały formę decyzji administracyjnej, a nie jedynie innej czynności z zakresu administracji publicznej. Adekwatnie do treści uwagi Wpisanie lub odmowa wykreślenia podmiotu do/z wykazu niewątpliwie nakładać będzie na podmioty określone obowiązki prawne, w związku z czym rekomendujemy wskazanie, że będzie to dokonywane w drodze decyzji administracyjnej.	Uwaga nieuwzględniona Obowiązki z zakresu cyberbezpieczeństwa danego podmiotu będą wynikały wprost z przepisów ustawowych. Wpis do wykazu też będzie miał charakter deklaratoryjny. Obowiązek wpisu do wykazu będzie wynikała wprost z przepisów prawa. Organ właściwy do spraw cyberbezpieczeństwa będzie jedynie dokonywał czynności, której nie dokonał podmiot kluczowy/podmiot ważny. Nie jest możliwe, przy tak dużej liczbie podmiotów, aby organ właściwy do spraw cyberbezpieczeństwa w każdym przypadku przeprowadzał skomplikowane postępowanie administracyjne. Dlatego zdecydowano się na prostszą formułę <i>innej czynności z zakresu administracji publicznej</i> przy zapewnieniu również odwołania do sądu administracyjnego.
312.	Związek Pracodawców Polska Miedź	Art. 7a ust. 4, Art. 7c	Rekomenduje się, aby działania organu właściwego miały formę decyzji administracyjnej, a nie jedynie innej czynności z zakresu administracji publicznej. Adekwatnie do treści uwagi Wpisanie lub odmowa wykreślenia podmiotu do/z wykazu niewątpliwie nakładać będzie na podmioty określone obowiązki prawne, w związku z czym rekomenduje się wskazanie, że będzie to dokonywane w drodze decyzji administracyjnej.	Uwaga nieuwzględniona Obowiązki z zakresu cyberbezpieczeństwa danego podmiotu będą wynikały wprost z przepisów ustawowych. Wpis do wykazu też będzie miał charakter deklaratoryjny. Obowiązek wpisu do wykazu będzie wynikała wprost z przepisów prawa. Organ właściwy do spraw cyberbezpieczeństwa będzie jedynie dokonywał czynności, której nie dokonał podmiot kluczowy/podmiot ważny. Nie jest możliwe, przy tak dużej liczbie podmiotów, aby organ właściwy do spraw cyberbezpieczeństwa w każdym przypadku przeprowadzał

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

				skomplikowane postępowanie administracyjne. Dlatego zdecydowano się na prostszą formułę innej czynności z zakresu administracji publicznej przy zapewnieniu również odwołania do sądu administracyjnego.
313.	KIKE	Art. 7c ust. 6	Izba postuluje wydłużenie w ustawie terminów wdrożenia obowiązków. Przede wszystkim zwracamy uwagę na terminy z art. 7c ust. 6 uKSC, gdzie nakazuje się wykonanie obowiązków z art. 8, 9, 10 i 11 uKSC w terminie 6 miesięcy od dnia wpisania do rejestru KSC. Izba wskazuje, że jest to termin zbyt krótki, zwłaszcza w zakresie przeprowadzenia w tym czasie audytu przez ponad 3 tysięcy przedsiębiorców telekomunikacyjnych z czego 2800 ma status MŚP. Co więcej, w tak krótkim terminie 6 miesięcy będzie niemożliwe dla wielu MŚP w sektorze telekomunikacyjnym uzyskanie certyfikatu zgodności z normą ISO 27001 i ISO 22301. W opinii Izby, konieczność wdrożenia obowiązków i audytów z uKSC w tak krótkim terminie nie ma uzasadnienia (zwłaszcza wobec podmiotów MŚP). W tym kontekście zwracam uwagę, że Projekt daje aż 18 miesięcy na wyznaczenie sektorowych CSIRT, sugerując, że wdrożenie regulacji uKSC nie jest pilne. Z tego względu Izba postuluje, aby termin wdrożenia obowiązków z Projektu wynosił 12 miesięcy od dnia wpisu do KSC (a przynajmniej wobec MŚP). Z kolei wspomniany już obowiązek przeprowadzenia pierwszego audytu z art. 7c uKSC powinien zostać ograniczony do podmiotów kluczowych. W przypadku nieprzychylenia się do tego postulatu, wnoszę o wydłużenie terminu wykonania tego audytu do 24 miesięcy od dnia wpisu do KSC. 7	Uwaga nieuwzględniona termin 6 miesięcy pozostanie z uwagi na wdrożenie dyrektywy NIS2
314.	TAURON Polska Energia S.A	Art. 7c ust. 6 pkt 1	Podmiot, wobec którego wydano decyzję, o której mowa w ust. 1: 1) realizuje obowiązki, o których mowa w rozdziale 3, w terminie 6 miesięcy. Praktyka pokazuje, że wdrożenie wymagań regulacji, w tym pośrednio wymagań norm ISO 27001 oraz ISO 22301 jest złożonym i czasochłonnym procesem, szczególnie dla podmiotu, który wcześniej nie był elementem Krajowego Systemu Cyberbezpieczeństwa. Termin 6 miesięcy wydaje się nierealny i skutkować będzie tworzeniem „papierowego” bezpieczeństwa. Proponowane brzmienie, uwzględniające powyższe : „Podmiot, wobec którego wydano decyzję, o której mowa w ust. 1: 1) realizuje obowiązki, o których mowa w rozdziale 3, w terminie 12 miesięcy,”	Uwaga nieuwzględniona termin 6 miesięcy pozostanie z uwagi na wdrożenie dyrektywy NIS2
315.	Polskie Stowarzyszenie Fotowoltaiki	Art. 7c	- Organ właściwy do spraw cyberbezpieczeństwa, w drodze decyzji, uznaje osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej za podmiot kluczowy lub podmiotważny; - Uprawnienie dotyczy uznania za PW lub PK mikro lub małych przedsiębiorców; - Decyzja podlega natychmiastowemu wykonaniu. Ogólny wpływ regulacji:	Uwaga nieuwzględniona Przepis stanowi bezpośrednie wdrożenie art. 2 ust. 2 lit. b-e dyrektywy NIS2.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			Biorąc pod uwagę kryteria przedstawione w ramach art. 7c KSC wg Projektu, na podstawie których organ właściwy ma prawo uznać danego mikro lub małego przedsiębiorcę za PW lub PK, należy wskazać, że istnieje poważne ryzyko nieadekwatnego przeregulowania mikro i małych przedsiębiorstw. Wskazane w art. 7c ust. 1 pkt 3) przesłanki mają charakter niezwykle nieostrej, generalny i ocenny, a przede wszystkim nie uwzględniają w należyty sposób kryteriów wskazanych w ramach motywu 7 Dyrektywy NIS2. W szczególności, kryteria te nie uwzględniają specyfiki usług mikro i małych przedsiębiorców, która może różnić się w zależności od poszczególnych sektorów. Wpływ na sektor energetyczny: Projektowana regulacja może doprowadzić do przeregulowania krajowych mikro i małych przedsiębiorców, poprzez nałożenie na nich niewspółmiernie szerokich i wymagających obowiązków, zarówno w kontekście ich wdrożenia jak i utrzymania. Obowiązki przewidziane w Rozdziale 3 KSC wg Projektu, w tym wdrożenie systemu zarządzania bezpieczeństwem informacji (,,SZBI”) projektowane było z myślą o średnich i dużych przedsiębiorstwach, które posiadają już pewne doświadczenie w zakresie wdrażania SZBI, jak również posiadają odpowiednie zasoby ludzkie i środki w celu wdrożenia tego typu wymagań. Jednocześnie, w ramach OSR brak jest oceny wpływu Projektu w zakresie omówionym powyżej, na konkurencyjność polskich firm z sektora energetycznego. Brak jakichkolwiek odniesień, choćby co do stosowania zasady proporcjonalności przewidzianej w Dyrektywie NIS2 w artykule 21, czy też nałożenia mniejszej liczby obowiązków, niż te przewidziane dla przedsiębiorstw przekraczających próg średnich, może prowadzić do istotnego utrudnienia prowadzenia działalności przez mikro i małe przedsiębiorstwa z sektora, wpływając negatywnie na konkurencyjność tych firm i ich zdolności do oferowania produktów niezbędnych do funkcjonowania całej branży, w ramach łańcucha dostaw. [Nadregulacja względem Dyrektywy NIS2] Projektowana zmiana stanowi nadregulację względem Dyrektywy NIS2 Rekomendacja: - uwzględnienie w ramach Projektu sektorowych kryteriów uznania mikro i małych przedsiębiorców za PK i PW, z uwzględnieniem specyfiki danego sektora (optymalnie podsektora) i opracowanie takich sektorowych kryteriów w oparciu o kryteria europejskie (o których mowa w motywie 20 Dyrektywy NIS2). Kryteria te powinny być możliwe do obiektywnej weryfikacji, jak również publicznie dostępne z odpowiednim wyprzedzeniem, w celu możliwości oceny ryzyka bycia uznanym za PW i PK przez mniejsze podmioty z branży. Dyskrecjonalne działanie organów krajowych w oparciu o nieostre kryteria uznania za PW i PK, może z wysokim prawdopodobieństwem doprowadzić do istotnego przeregulowania mikro i małych przedsiębiorstw na polskim rynku, a w konsekwencji doprowadzić do braku konkurencyjności tych podmiotów na rynku energetycznym względem zagranicznych podmiotów z UE i zwiększenia	

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			kosztów działalności szerszego kręgu podmiotów sektora energetycznego, z uwagi na istotny udział niektórych mikro i małych przedsiębiorstw w łańcuchach dostaw. - uwzględnienie w nakładanych obowiązkach wielkości podmiotu i innych kryteriów, które wskazane zostały w art. 21 Dyrektywy NIS2 jako niezbędne do uwzględnienia w trakcie oceny proporcjonalności nakładanych obowiązków w zakresie środków w celu zarządzania ryzykiem dla bezpieczeństwa sieci i systemów informatycznych - dokonanie oceny wpływu regulacji na konkurencyjność polskich firm z sektora energetycznego.	
316.	Polskie Stowarzyszenie Fotowoltaiki	Art. 7c ust. 6	Ogólny wpływ regulacji: Wdrożenie środków technicznych i organizacyjnych dot. cyberbezpieczeństwa oraz realizację pozostałych obowiązków określonych w ustawie może wymagać modyfikacji lub zupełnego wdrożenia skomplikowanych procesów biznesowych. W zależności od wielkości organizacji oraz sektora, termin 6 miesięcy może nie być wystarczający dla zachowania zgodności z wymogami ustawy. Wpływ na sektor energetyczny Mając na uwadze szeroki katalog nowych obowiązków nałożonych na PK i PW w rozdziale 3 KSC wg Projektu, 6-miesięczny termin wyznaczony przez projektodawcę na wdrażanie środków technicznych i organizacyjnych dot. cyberbezpieczeństwa jest co najmniej niewystarczający. Zważywszy, że sektor energetyczny odgrywa kluczową rolę z punktu widzenia planowania strategicznego oraz bezpieczeństwa państwa, wdrożenie SZBI powinno zostać dokonane w sposób profesjonalny, bez negatywnego wpływu na działalność biznesową takich podmiotów. Dodatkowo, biorąc pod uwagę wskazaną wwierszu powyżej możliwość objęcia regulacją mikro i małych przedsiębiorców, którzy nie posiadają doświadczeń w zakresie wdrażania złożonych SZBI, terminy te są tym bardziej nieadekwatne. [Nadregulacja względem Dyrektywy NIS2] Dyrektywa NIS2 nie określa terminów w jakich określone w niej obowiązki powinny zostać wdrożone przez podmioty podlegające automatycznej kwalifikacji jako PK lub PW, jak również w drodze decyzji organu właściwego ds. cyberbezpieczeństwa. Rekomendacja: - wydłużenie terminu realizacji obowiązków PK i PW w razie wydania decyzji o uznaniu za PK lub PW do co najmniej 12 miesięcy. Podmioty, które dotychczas są kwalifikowane jako operatorzy usług kluczowych i częściowo wdrożyły już niezbędne środki techniczne i organizacyjne związane się terminem 6 miesięcy na zrealizowanie obowiązków wynikających z Projektu (art. 16 ust. 1 KSC wg Projektu). Termin dla mikro i małych przedsiębiorców kwalifikowanych w jako PK lub PW w drodze decyzji powinien być odpowiednio wydłużony.	Uwaga nieuwzględniona termin 6 miesięcy pozostanie z uwagi na wdrożenie dyrektywy NIS2
317.	Polska Izba Informatyki i Telekomunikacji	Art. 8	Zwracamy uwagę, że aktualny projekt wprowadza niepotrzebną komplikację mapowania 10 środków zarządzania ryzykiem pogrupowaną w Art. 21.2.a-j Dyrektywy NIS2. Proponowana wersja spowoduje komplikację w mapowaniu dla przedsiębiorstw wielonarodowych, gdzie zachodzi konieczność porównania statusu w poszczególnych domenach. Np. w niemieckim projekcie ustawy	Uwaga uwzględniona Przepis zostanie dostosowany do treści dyrektywy NIS2.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

		NIS2 transpozycje Art 21.2. Dyrektywy zachowano w relacji 1 do 1 (por. paragraf 30 niemieckiego projektu transpozycji dyrektywy2). Proponujemy ujednolicenie zgodnie z Art. 21.2. Dyrektywy NIS2 poniższych praktyk, gdyż umożliwiają one zmapowanie na dobre praktyki i normy ISO. Aktualnie poprzestawiane są fragmenty Art 8.1.2 z porządkiem w Dyrektywie NIS2 oraz znajdują się w tych środkach wymagania nadmiarowe (np. „polityki tematyczne”) lub występują pominięcia (albo odrębne potraktowanie bezpieczeństwa zasobów ludzkich). Trudność i niejednoznaczność mapowania przedstawia poniższa tabela. Elementy pogrubione w lewej kolumnie tabeli nie występują w projekcie uksc.							
		<table><tr><td>Środki zarządzania ryzykiem (Art. 21.2 a-j Dyrektywy NIS2)</td><td>Środki zaproponowane w opiniowanym projekcie uksc</td></tr><tr><td>a) polityka analizy ryzyka i bezpieczeństwa systemów informatycznych</td><td>Art. 8.1.2)a) polityki szacowania ryzyka oraz bezpieczeństwa systemu informacyjnego, w tym polityki tematyczne, Polityki tematyczne są nadmiarowe (por uwaga nr 15 dot. Polityk tematycznych)</td></tr><tr><td>b) obsługa incydentu</td><td>Art. 8.1.4) zarządzanie incydentami;</td></tr></table>	Środki zarządzania ryzykiem (Art. 21.2 a-j Dyrektywy NIS2)	Środki zaproponowane w opiniowanym projekcie uksc	a) polityka analizy ryzyka i bezpieczeństwa systemów informatycznych	Art. 8.1.2)a) polityki szacowania ryzyka oraz bezpieczeństwa systemu informacyjnego, w tym polityki tematyczne, Polityki tematyczne są nadmiarowe (por uwaga nr 15 dot. Polityk tematycznych)	b) obsługa incydentu	Art. 8.1.4) zarządzanie incydentami;	
Środki zarządzania ryzykiem (Art. 21.2 a-j Dyrektywy NIS2)	Środki zaproponowane w opiniowanym projekcie uksc								
a) polityka analizy ryzyka i bezpieczeństwa systemów informatycznych	Art. 8.1.2)a) polityki szacowania ryzyka oraz bezpieczeństwa systemu informacyjnego, w tym polityki tematyczne, Polityki tematyczne są nadmiarowe (por uwaga nr 15 dot. Polityk tematycznych)								
b) obsługa incydentu	Art. 8.1.4) zarządzanie incydentami;								

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			c) ciągłość działania, np. zarządzanie kopiami zapasowymi i przywracanie normalnego działania po wystąpieniu sytuacji nadzwyczajnej, i zarządzanie kryzysowe	Art. 8.1.2) b) utrzymanie i bezpieczną eksploatację systemu informacyjnego, punkt ten pasuje i do ciągłości działania i do punktu 21.2e) z kolumny obok. Brakuje jasnego wskazania na zarządzanie kopiami zapasowymi co w kontekście zagrożeń ransoware jest kluczowe (back-up/kopia bezpieczeństwa off-line nie zainfekowana). Ponadto zidentyfikowano pominięcie wymagań dot. Zarządzania kryzysowego na poziomie podmiotów kluczowych i ważnych. Nieuzasadnione wydaje się zawężenie wdrożenia praktyk zarządzania kryzysowego do podmiotów z branży energetycznej (por. Art. 8b. Podmioty kluczowe z podsektora energii elektrycznej). Jako obowiązująca norma w tym zakresie może być zastosowana ISO/IEC 22361. Art. 8.1.2) e) wdrażanie, dokumentowanie i utrzymywanie planów działania umożliwiających ciągłe i niezakłócone świadczenie usługi oraz zapewniających poufność, integralność, dostępność i autentyczność informacji, oraz planów awaryjnych umożliwiających odtworzenie systemu informacyjnego po katastrofie, Proponujemy ujednolicenie zgodnie z Dyrektywą NIS2 oraz doprecyzowanie „sytuacji nadzwyczajnej” wg Dyrektywy NIS2) lub katastrofy (wg niniejszego projektu uksc).		

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			d) bezpieczeństwo łańcucha dostaw, w tym aspekty związane z bezpieczeństwem dotyczące stosunków między każdym podmiotem a jego bezpośrednimi dostawcami lub usługodawcami	Art. 8.1.2) d) bezpieczeństwo i ciągłość łańcucha dostaw produktów ICT, usług ICT i procesów ICT, od których zależy świadczenie usługi z uwzględnieniem związków pomiędzy dostawcą sprzętu lub oprogramowania a podmiotem kluczowym lub podmiotem ważnym,		
			e) bezpieczeństwo w procesie nabywania, rozwoju i utrzymania sieci i systemów informatycznych, w tym postępowanie w przypadku podatności i ich ujawnianie	Art. 8.1.2) b) utrzymanie i bezpieczną eksploatację systemu informacyjnego – punkt ten pasuje również do ciągłości działania – por. Pkt c z kolumny obok. Art. 8.1.2) f) objęcie systemu informacyjnego wykorzystywanego do świadczenia usługi systemem monitorowania w trybie ciągłym, Art. 8.1.3) zbieranie informacji o cyberzagrożeniach i podatnościach na incydenty systemu informacyjnego wykorzystywanego do świadczenia usługi; Art. 8.1.5) stosowanie środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego wykorzystywanego do świadczenia usługi, w tym: a) stosowanie mechanizmów zapewniających poufność, integralność, dostępność i autentyczność danych przetwarzanych w systemie informacyjnym, b) regularne przeprowadzanie aktualizacji oprogramowania, stosownie do zaleceń producenta, z uwzględnieniem analizy wpływu aktualizacji na bezpieczeństwo świadczonych usług oraz poziomu krytyczności poszczególnych aktualizacji, c) ochronę przed nieuprawnioną modyfikacją w systemie informacyjnym,		

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

				d) niezwłoczne podejmowanie działań po dostrzeżeniu podatności lub cyberzagrożeń;		
			f) polityki i procedury służące ocenie skuteczności środków zarządzania ryzykiem w cyberbezpieczeństwie	Art. 8.1.2) g) polityki i procedury oceny skuteczności środków technicznych i organizacyjnych,		
			g) podstawowe praktyki cyberhigieny i szkolenia w zakresie cyberbezpieczeństwa	Art. 8.1.2) h) edukację z zakresu cyberbezpieczeństwa dla personelu podmiotu, w tym podstawowe zasady cyberhigieny,		
			h) polityki i procedury stosowania kryptografii i, w stosownych przypadkach, szyfrowania	Art. 8.1.2) i) polityki i procedury stosowania kryptografii, w tym szyfrowania;		
			i) bezpieczeństwo zasobów ludzkich, polityka kontroli dostępu i zarządzanie aktywami	Art. 8.1.2) c) bezpieczeństwo fizyczne i środowiskowe, uwzględniające kontrolę dostępu, Brakuje w projekcie bezpieczeństwa zasobów ludzkich (jest to częściowo zaadresowane w artkule 8f1 i2, ale nie wyczerpuje tematu (Background checks to również sprawdzenie osób w kontekście powiązań kapitałowych, prania brudnych pieniędzy, list terrorystycznych, oraz przeszłości zatrudnienia, itp.). Ponadto brakuje		

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			j) stosowanie uwierzytelniania wieloskładnikowego lub ciągłego, zabezpieczonych połączeń głosowych, tekstowych i wideo oraz zabezpieczonych systemów łączności wewnątrz podmiotu w sytuacjach nadzwyczajnych Art. 8.1.6) stosowanie bezpiecznych środków komunikacji elektronicznej w ramach krajowego systemu cyberbezpieczeństwa, Art. 8.1.6) stosowanie bezpiecznych środków komunikacji elektronicznej w ramach krajowego systemu cyberbezpieczeństwa, uwzględniających uwierzytelnianie wieloskładnikowe.		
			Brakuje ponadto wskazania norm ISO/IEC 30111:2019 oraz ISO/IEC 29147:2018 w zakresie zarządzania podatnościami i ujawniania podatności, które zostały wskazane w Dyrektywie NIS2 motyw (58). Normy te jasno pokazują sposób realizacji zarządzania podatnościami, co jest kluczowe dla ujednolicenia dobrych praktyk w tym zakresie i zagwarantowania jasności zakresu wymagań w tym zakresie. Podobnie brakuje wskazania odniesień do normy ISO/IEC 17788:2014 wskazanej w Motywie (33) Dyrektywy NIS2 (obecnie jest wspomniana norma zastąpiona przez normę ISO/IEC 22123-1/2:2023) w zakresie stosowanych pojęć z obszaru Chmury Obliczeniowej (przy okazji prac nad uksc należy uspoźnić Komunikat Chmurowy UKNF, również w kontekście rozporządzenia DORA i uspoźnić zalecenia z Ministerstwem Finansów koordynującym wdrożenie DORA).		
318.	Polska Izba Informatyki i Telekomunikacji	Art. 8	Przyjmujemy, że wymóg posiadania „<i>polityki szacowania ryzyka oraz bezpieczeństwa systemu informacyjnego, w tym polityki tematyczne</i>” stanowi przeniesienie art. 21 ust. 2 lit. a) NIS2 wskazującego na „<i>politykę analizy ryzyka i bezpieczeństwa systemów informatycznych</i>”. Wnosimy jednak o wyjaśnienie dodanego wobec dyrektywy sformułowania „<i>w tym polityki tematyczne</i>”. Nie zostało ono zdefiniowane, a dla precyzji przepisów wydaje się to niezbędne.	Wyjaśnienie uwagi	Polityki tematyczne = topic specific policies z ISO 27001. Celem przepisu jest wskazanie, żeby w razie potrzeby podmiot kluczowy/ważne utworzył dedykowaną politykę np. politykę bezpieczeństwa urządzeń mobilnych.
319.	Polska Izba Informatyki i Telekomunikacji	Art. 8	Projektowany przepis zawiera istotne rozszerzenie zakresu badania łańcucha dostaw, wymaganego zgodnie z dyrektywą NIS2 i wprowadza tym samym nadmiarowe obciążenie. Dyrektywa NIS2 wskazuje na „<i>bezpieczeństwo łańcucha dostaw, w tym aspekty związane z bezpieczeństwem dotyczące stosunków między każdym podmiotem a jego bezpośrednimi dostawcami lub usługodawcami</i>” Wnosimy o przyjęcie następującego brzmienia projektu: <i>d) bezpieczeństwo i ciągłość łańcucha dostaw produktów ICT, usług ICT i procesów ICT, od których zależy świadczenie usługi z uwzględnieniem związków pomiędzy bezpośrednim dostawcą sprzętu lub oprogramowania a podmiotem kluczowym lub podmiotem ważnym</i>	Uwaga uwzględniona	Przepis będzie się odnosił do bezpośrednich dostawców.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

320.	Polska Izba Informatyki i Telekomunikacji	Art. 8	Art. 8 pkt 2 lit e – katastrofa W doprecyzowaniu dotychczasowego przepisu dodano „ <i>oraz planów awaryjnych umożliwiających odtworzenie systemu informacyjnego po katastrofie</i> ” Sformułowanie „po katastrofie” nie zostało zdefiniowane. Sugerujemy jego usunięcie lub zdefiniowanie lub wskazanie odpowiedniego odwołania do istniejących definicji, co może być jednak problematyczne. Możliwe jest też jego zastąpienie zwrotem „ <i>po przerwaniu ciągłości jego działania</i> ” lub powiązania konieczności odtworzenia systemu informacyjnego po wystąpieniu incydentu poważnego, krytycznego lub cyberzagrożenia na dużą skalę. Z uwagi na potencjalne kary pieniężne konieczne jest zachowanie maksymalnej precyzji pojęć używanych do opisu wymagań.	Wyjaśnienie uwagi Wprowadzimy definicję katastrofy.
321.	Polska Izba Informatyki i Telekomunikacji	Art. 8	Art. 8 ust. 2 Wnioskujemy o uwzględnienie w tym przepisie wymagań wskazanych w normie ISO/IEC 27001 oraz ISO/IEC 22301. Niektóre podmioty mogą posiadać certyfikaty na zgodność z angielskojęzyczną wersją przywołanych norm - wskazanie wersji polskojęzycznej w przepisie nie powinno dyskwalifikować tych certyfikatów, ponieważ ich treść, a tym samym wymogi pozostają niezmiennie w obu wersjach językowych.	Wyjaśnienie uwagi Zmieniono podejście – minister będzie mapował różne istniejące dokumenty normalizacyjne.
322.	Polska Izba Informatyki i Telekomunikacji	Art. 8	Art. 8 ust. 3 – mapowanie PN Wnioskujemy o jak najszybsze opublikowanie mapowania wymogów PN na obowiązki wynikające z ustawy i przyszłych rozporządzeń. Wydaje się jednocześnie, że do tego typu zadania nie jest konieczne szczególne upoważnienie ustawowe oraz że zadanie to powinno być obowiązkiem ministra ds. informatyzacji a nie możliwością.	Wyjaśnienie uwagi Mapowanie będzie dokonane po zakończeniu procesu legislacyjnego ustawy.
323.	Polska Izba Informatyki i Telekomunikacji	Art. 8	Art. 8 ust. 4 – dostawca Wnosimy o wprowadzenie zmian w pkt 1: <i>1) podatności związane z dostawcą sprzętu lub oprogramowania, o ile zostaną zidentyfikowane w ramach szacowania ryzyka</i> Wnosimy o wprowadzenie zmiany w pkt 3: <i>3) wyniki skoordynowanej oceny bezpieczeństwa przeprowadzonej przez Grupę współpracy, o której mowa w art. 22 ust. 1 dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniającej rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającej dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz. Urz. UE L 333 z 27.12.2022, str. 80), zwanej dalej „dyrektywą 2022/2555”, o ile zostaną wydane.</i> Wydanie skoordynowanych ocen jest fakultatywne. Ponadto definicja dostawcy sprzętu lub oprogramowania obejmuje także importera lub dystrybutora – co obejmuje w konsekwencji bardzo szeroki zakres analiz w przedsiębiorstwie co do podmiotów współpracujących, pod kątem spełniania przez nich wymogów bezpieczeństwa informacji, a w przypadku uznania za HRV także dystrybutora - może to zablokować lub znacząco utrudnić działalność podmiotu kluczowego.	Wyjaśnienie uwagi Jest to zbędne dopowiedzenie.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

324.	Amerykańska Izba Handlowa	Art. 8	Ustalone powyższym artykułem brzmienie art. 8 uksc zawiera regulacje dotyczące systemu zarządzania bezpieczeństwem informacji oraz enumeratywne wyliczenie funkcji, które ma ten system zapewnić. Przepisy ustawy z oczywistych przyczyn zawierają w tym zakresie sformułowania bardzo ogólne. Jednocześnie liczba podmiotów objętych nowymi przepisami i różnorodność sektorów, z których się wywodzą jest znaczna. Prowadzi to do problemu polegającego na nałożeniu na przedsiębiorców obowiązków bez jednoczesnego wskazania, czy kierunek podejmowanych przez nich działań i wprowadzanych do ich systemów zmian jest według organu właściwego słuszny i spełnia oczekiwania, a przede wszystkim czy w ocenie organu jest zgodny z przepisami. Ma to szczególne znaczenie w kontekście ust. 4 omawianego przepisu, w której podmioty objęte ustawą mają uwzględniać podatności danego dostawcy oraz „ogólną jakość produktów ICT (...)”. Stoimy na stanowisku, że przewidziane w ustawie mechanizmy doprecyzowania obowiązków nakładanych na podmioty objęte ustawą oraz ułatwiający im samodzielną ocenę legalności podejmowanych przez nie działań wymagają modyfikacji: a) Art. 67a uksc w brzmieniu ustalonym projektem przewiduje fakultatywną kompetencję Pełnomocnika ds. cyberbezpieczeństwa do wydania stosownych rekomendacji dla podmiotów krajowego systemu cyberbezpieczeństwa mających formułę aktów prawa miękkiego, co zapewnia przedsiębiorcom rozsądny zakres elastyczności. Warta rozważenia byłaby w naszej opinii modyfikacja tego przepisu poprzez wprowadzenie kompetencji obligatoryjnej do wydania stosownych rekomendacji lub wytycznych dla przedsiębiorców ułatwiających stosowanie ustawy; b) Art. 8a wprowadzany projektem ustawy normuje fakultatywną kompetencję Rady Ministrów do ustalenia szczegółowych wymagań dla systemu zarządzania bezpieczeństwem informacji w drodze rozporządzenia. Wyznaczenie Rady Ministrów jako organu właściwego może jednak prowadzić do przewlekłości i nieefektywności procesu zapewnienia zgodności systemów zarządzania bezpieczeństwem informacji. Dlatego stoimy na stanowisku, że – o ile forma wiążących wymagań ma być zachowana – organem wyposażonym w kompetencję do wydawania tego rodzaju rozporządzeń powinien być minister właściwy ds. cyfryzacji.	Uwaga nieuwzględniona Rekomendacje – przyjęta formuła rekomendacji umożliwia wydawanie wielu rekomendacji z różnych dziedzin. Rozporządzenie – zakres przedmiotowy rozporządzeń będzie dotyczyć wielu sektorów, nadzorowanych przez kilku ministrów. Z tego powodu proponuje się, żeby to Rada Ministrów była organem wydającym rozporządzenie.
325.	Audytel	Art. 8	W zakresie obowiązków nakładanych na podmioty kluczowe oraz ważne brak jest wymagań w zakresie przeprowadzania testów bezpieczeństwa. Jest to o tyle niezrozumiałe, że obejmujące sektor finansowy Rozporządzenie DORA, wskazuje precyzyjne wymagania w tym zakresie. W naszej ocenie obecne propozycje nie wskazują dość wyraźnie na obowiązek przeprowadzenia testów bezpieczeństwa, w tym testów penetracyjnych. Z naszej praktyki audytów w zakresie bezpieczeństwa informacji (w tym audytów prowadzonych zgodnie z ustawą KSC oraz rozporządzeniem KRI) wynika, że zdecydowana większość podmiotów nie wykonuje żadnych testów bezpieczeństwa lub wykonuje je w stopniu niewystarczającym do zapewnienia bezpieczeństwa. W związku z powyższym proponujemy w Art. 8. 1 punkt 2 dodanie pod literą j) dodanie następującego zapisu:	Uwaga częściowo uwzględniona Zostanie dodany wymóg testowania systemów informacyjnych, ale bez takiego doszczegółowienia – podmiot powinien sam podjąć decyzję o rodzaju testów.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			j) wykonywania regularnych testów bezpieczeństwa, w tym testów podatności, socjotechnicznych oraz zaawansowanych testów penetracyjnych.	
326.	Audytel	Art. 8	Komentowany przepis wprowadza do Ustawy art. 8. 2. „Wymagania, o których mowa w ust. 1, uznaje się za spełnione, gdy podmiot kluczowy i podmiot ważny zapewnia system zarządzania bezpieczeństwem informacji, z uwzględnieniem wymagań określonych w Polskiej Normie PN EN ISO/IEC 27001 oraz PN EN ISO/IEC 22301. Normy międzynarodowe w tym przytoczone w/w normy podlegają okresowym zmianom lub też w ich miejsce wchodzi normy oznaczone innymi numerami. Każda nowelizacja normy otrzymuje numer z rokiem jej wydania. Przykładowo norma ISO/IEC 27001 została znowelizowana w roku 2023 i posiada numer 27001:2023. Numer po dwukropku oznacza rok wydania normy. Podobna sytuacja występuje z normą ISO/IEC 22301. W związku z tym proponujemy, aby w/w przepis przyjął następującą treść: „Wymagania, o których mowa w ust. 1, uznaje się za spełnione, gdy podmiot kluczowy i podmiot ważny zapewnia system zarządzania bezpieczeństwem informacji, z uwzględnieniem wymagań określonych aktualnych wydaniach międzynarodowych norm ISO/IEC 27001 oraz PN-EN ISO/IEC 22301. W przypadku uchylenia normy należy stosować wymagania normy, która ją zastąpi.	Wyjaśnienie uwagi Pod wpływem różnych uwag koncepcja została zmieniona. Art. 8 ust. 2 zostanie usunięty. W zamian minister właściwy do spraw informatyzacji będzie mógł mapować różne normy/standardy na wymogi ustawowe i rozporządzeń.
327.	Audytel	Art. 8	Komentowany przepis wprowadza do Ustawy art. 8 ust. 4 „4. Wdrażając środki, o których mowa w ust. 1 pkt 2 lit. c, podmiot kluczowy i podmiot ważny uwzględnia: 1) podatności związane z dostawcą sprzętu lub oprogramowania;” 2) ogólną jakość produktów ICT, usług ICT i procesów ICT pochodzących od dostawcy sprzętu lub oprogramowania; Tymczasem ust. 1 pkt 2 lit c, dotyczy: „c) bezpieczeństwo fizyczne i środowiskowe, uwzględniające kontrolę dostępu,” Bezpieczeństwa związanego z dostawcami dotyczy zaś 1 pkt 2 lit c: „d) bezpieczeństwo i ciągłość łańcucha dostaw produktów ICT, usług ICT i procesów ICT, od których zależy świadczenie usługi z uwzględnieniem związków pomiędzy dostawcą sprzętu lub oprogramowania a podmiotem kluczowym lub podmiotem ważnym, ...” Wydajesię, że mamy tutaj do czynienia z oczywistą omyłką, a prawidłowa treść art. 8 ust. 4 powinna brzmieć: „4. Wdrażając środki, o których mowa w ust. 1 pkt 2 lit. d, podmiot kluczowy i podmiot ważny uwzględnia: 1) podatności związane z dostawcą sprzętu lub oprogramowania;” 2) ogólną jakość produktów ICT, usług ICT i procesów ICT pochodzących od dostawcy sprzętu lub oprogramowania;”	Uwaga uwzględniona Przepis zostanie zmieniony – wprowadzone zostanie odwołanie do lit. d.
328.	Fundacja Bezpieczna Cyberprzestrzeń	Art. 8	Art. 1 pkt 12, treść art. 8 ust. 1 „Podmiot kluczowy lub podmiot ważny wdraża system zarządzania bezpieczeństwem informacji w procesach wpływających <u>na świadczenie usług przez ten podmiot</u>,” –	Wyjaśnienie uwagi Naszym zdaniem prowadzenie działalności, np. gospodarczej, polega na

Tabela uwag zgłoszonych w ramach konsultacji publicznych do *projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw* (UC32) cz. I

			NIS2 mówi w art. 21 o prowadzeniu działalności a nie tylko świadczeniu usługi, zakresem powinno więc być prowadzenie działalności a nie tylko świadczenie usługi.	świadczeniu usług. Zresztą sama dyrektywa odnosi się potem do usług np. przy zgłoszeniach incydentu.
329.	Fundacja Bezpieczna Cyberprzestrzeń	Art. 8	Art. 1 pkt 12, treść Art. 8 ust. 1 pkt 2 <i>wdrożenie „odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, uwzględniających najnowszy stan wiedzy, koszty wdrożenia, wielkość podmiotu, prawdopodobieństwo wystąpienia incydentów, narażenie podmiotu na ryzyka,”</i> NIS2 w art. 21 mówi o narażeniu nie tylko podmiotu na ryzyk, ale również ocenie „skutków społecznych i gospodarczych” a więc wszystkich interesariuszy.	Uwaga uwzględniona Przepis zostanie uzupełniony.
330.	Fundacja Bezpieczna Cyberprzestrzeń	Art. 8	Art. 1 pkt 12, treść art. 8 ust. 1 pkt 2 lit. a – normy ISO 27001 i 27002 nie przewidują opracowania polityki szacowania ryzyka. Taki zapis na pewno spowoduje błędy interpretacyjne lub dążenie do opracowania dokumentów nieistniejących w dokumentach normatywnych. Proponuje się rozdzielić lit. a na dwie odrębne, odpowiadające wymaganiom normy ISO 27001 i wytycznym opisanym w ISO27002: „art. 8 ust. 1 pkt 2 a) polityki bezpieczeństwa informacji oraz dostosowanych i komplementarnych polityk tematycznych, w tym - polityki i procedury oceny skuteczności środków technicznych i organizacyjnych, - polityki i procedury stosowania kryptografii, w tym szyfrowania, b) metodyki szacowania ryzyka oraz polityki zarządzania ryzykiem,...” oraz usunąć litery g oraz i, jako wymienione w politykach tematycznych. Alternatywnie można wskazać polityki tematyczne określone w normie ISO27002 (wskazówki do punktu 5.1): a) kontrol; b) physical and environmental security; c) management; d) information technology; e) secure configuration and handling of user endpoints; f) network security; g) information security identification management; h) backup; i) cryptography and key management; j) information confidentiality and handling; k) management of third-party vulnerability; l) secure development. W ten sposób ograniczając treść całego ustępu 1 oraz kompletując listę wymagań dla systemu zarządzania bezpieczeństwem informacji.	Wyjaśnienie uwagi Pod wpływem różnych uwag koncepcja została zmieniona. Art. 8 ust. 2 zostanie usunięty. W zamian minister właściwy do spraw informatyzacji będzie mógł mapować różne normy/standardy na wymogi ustawowe i rozporządzeń.
331.	ISAC-Kolej	Art. 8	„e) „wdrażanie, dokumentowanie i utrzymywanie planów działania umożliwiających ciągłe i niezakłócone świadczenie usługi oraz zapewniających bezpieczeństwo systemów informacyjnych i technologii operacyjnych, oraz planów awaryjnych umożliwiających ich odtworzenie po katastrofie” Atrybuty związane z bezpieczeństwem systemów informacyjnych (poufność, integralność, dostępność i autentyczność) oraz bezpieczeństwem technologii operacyjnych, jeśli zostaną do projektu ustawy prowadzone (odporność na zdarzenia, które nie są częścią oczekiwanego działania systemu lub usługi), zawarte są w określeniach (pojęciach) wskazanych w art. 2, stąd nie ma konieczności odwoływać się do nich szczegółowo w treści pozostałych zapisów ustawy.	Wyjaśnienie uwagi Tak jak wskazywano wyżej system informacyjny obejmuje także systemy OT – przepis nie musi być zmieniany.
332.	ISAC-Kolej	Art. 8	„3) zbieranie informacji o cyberzagrożeniach i podatnościach na incydenty systemu informacyjnego i technologii operacyjnych wykorzystywanych do świadczenia usługi” Zbieranie informacji o cyberzagrożeniach nie powinno dotyczyć tylko systemów informacyjnych, ale także technologii operacyjnych.	Wyjaśnienie uwagi Tak jak wskazywano wyżej system informacyjny obejmuje także systemy OT – przepis nie musi być zmieniany.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

333.	ISAC-Kolej	Art. 8	Do zapisów odwołujących się w art. 8 ust. 1 tylko do systemu informacyjnego wykorzystywanego do świadczenia usługi dodać zapis „... i technologii operacyjnych wykorzystywanych do świadczenia usługi” Monitorowanie systemów w trybie ciągłym, zbieranie informacji o cyberzagrożeniach i podatnościach na incydenty czy stosowanie środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo nie powinno dotyczyć tylko systemów informacyjnych, ale również technologii operacyjnych.	Wyjaśnienie uwagi Tak jak wskazywano wyżej system informacyjny obejmuje także systemy OT – przepis nie musi być zmieniany.
334.	ISAC-Kolej	Art. 8	„a) stosowanie mechanizmów zapewniających bezpieczeństwo danych przetwarzanych w systemie informacyjnym oraz aktywów, procesów i zdarzeń nadzorujących procesy fizyczne w stosowanej technologii operacyjnej” Atrybuty związane z bezpieczeństwem systemów informacyjnych (poufność, integralność, dostępność i autentyczność) oraz bezpieczeństwem technologii operacyjnych, jeśli zostaną do projektu ustawy prowadzone (odporność na zdarzenia, które nie są częścią oczekiwanego działania systemu lub usługi), zawarte są w określeniach (pojęciach) wskazanych w art. 2, stąd nie ma konieczności odwoływać się do nich szczegółowo w treści pozostałych zapisów ustawy. Ponadto stosowanie mechanizmów zapewniających bezpieczeństwo powinno dotyczyć nie tylko systemów informacyjnych, ale również technologii operacyjnych stosowanych u operatorów usług kluczowych i podmiotów ważnych.	Wyjaśnienie uwagi Tak jak wskazywano wyżej system informacyjny obejmuje także systemy OT – przepis nie musi być zmieniany.
335.	ISAC-Kolej	Art. 8	„c) ochronę przed nieuprawnioną modyfikacją w systemie informacyjnym i/lub technologii operacyjnej” Ochronę przed nieuprawnioną modyfikacją powinna dotyczyć nie tylko systemów informacyjnych, ale również technologii operacyjnych stosowanych u operatorów usług kluczowych i podmiotów ważnych. Jest to o tyle istotne, że technologie operacyjne stosowane w kolejnictwie np. systemy sterowania ruchem kolejowym, zgodnie ze standardami i wymaganiami branżowymi zobowiązane są posiadać zaimplementowane poziomy nienaruszalności bezpieczeństwa, które osiąga się poprzez spełnienie wymagań dotyczących ograniczenia uszkodzeń oraz wykluczenia lub ograniczenia ujemnych skutków uszkodzeń.	Wyjaśnienie uwagi Tak jak wskazywano wyżej system informacyjny obejmuje także systemy OT – przepis nie musi być zmieniany.
336.	ISAC-Kolej	Art. 8	„2. Wymagania, o których mowa w ust. 1, uznaje się za spełnione, gdy podmiot kluczowy i podmiot ważny zapewnia: 1) system zarządzania bezpieczeństwem informacji, z uwzględnieniem wymagań określonych w Polskiej Normie PN-EN ISO/IEC 27001, 2) system bezpieczeństwa systemów sterowania i automatyki przemysłowej, z uwzględnieniem wymagań określonych w Polskiej Normie PN-EN IEC 62443 lub normach i standardach branżowych mających zastosowanie w danym sektorze lub podsektorze, 3) system zarządzania ciągłością działania, z uwzględnieniem wymagań określonych w Polskiej Normie PN-EN ISO/IEC 22301. Spełnienie wymagań określonych w art. 8 ust 1 powinno zostać uznane za spełnione, gdy podmiot kluczowy i podmiot ważny spełniają wymagania nie tylko w odniesieniu do systemu zarządzania bezpieczeństwem informacji z uwzględnieniem wymagań określonych w normie ISO27001, ale również	Wyjaśnienie uwagi Tak jak wskazywano wyżej system informacyjny obejmuje także systemy OT – przepis nie musi być zmieniany.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			innych mających zastosowanie zwłaszcza w użytkowanych przez podmioty kluczowe i ważne technologiach operacyjnych. Ponadto system zarządzania ciągłością działania to nie to samo co system zarządzania bezpieczeństwem informacji jak wskazuje zapis art. 8 ust. 2 projektu ustawy.	
337.	ISACA	Art. 8	polityki szacowania ryzyka oraz bezpieczeństwa systemu informacyjnego, w tym polityki tematyczne {jakie?} Wyjaśnienia lub usunięcia wymagają "polityki tematyczne" Pojęcie nie jest nigdzie zdefiniowane	Wyjaśnienie uwagi Polityki tematyczne występują w ISO 27001 – jako topic specific policies. Chodzi o to, aby w razie potrzeby podmiot ustanowił właściwą politykę np. politykę bezpieczeństwa urządzeń mobilnych.
338.	ISACA	Art. 8	Podmiot kluczowy lub podmiot ważny wdraża {SZBI} w procesach wpływających na świadczenie usług przez ten podmiot, zapewniający (...) wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, uwzględniających najnowszy stan wiedzy, koszty wdrożenia, wielkość podmiotu, prawdopodobieństwo wystąpienia incydentów, narażenie podmiotu na ryzyka, w szczególności (...) "Wymaga preredagowania zgodnie z NIS2 - art. 21 ust. 1. ""Podmiot kluczowy lub ważny wprowadza odpowiednie i proporcjonalne środki techniczne, operacyjne i organizacyjne w celu zarządzania ryzykiem dla bezpieczeństwa sieci i systemów informatycznych wykorzystywanych przez te podmioty do prowadzenia działalności lub świadczenia usług oraz w celu zapobiegania wpływowi incydentów na odbiorców ich usług lub na inne usługi bądź minimalizowania takiego wpływu. Przy uwzględnieniu najnowszego stanu wiedzy oraz, w stosownych przypadkach, odpowiednich norm europejskich i międzynarodowych, a także kosztów wdrożenia środki, o których mowa w akapicie pierwszym, zapewniają poziom bezpieczeństwa sieci i systemów informatycznych odpowiedni do istniejącego ryzyka. Oceniając proporcjonalność tych środków, należy uwzględnić stopień narażenia podmiotu na ryzyko, wielkość podmiotu i prawdopodobieństwo wystąpienia incydentów oraz ich dotkliwość, w tym ich skutki społeczne i gospodarcze."" "Zapis nie jest skuteczną transpozycją [NIS2 art. 21 ust. 1] Państwa członkowskie zapewniają, aby podmioty kluczowe i ważne wprowadzały odpowiednie i proporcjonalne środki techniczne, operacyjne i organizacyjne w celu zarządzania ryzykiem dla bezpieczeństwa sieci i systemów informatycznych wykorzystywanych przez te podmioty do prowadzenia działalności lub świadczenia usług oraz w celu zapobiegania wpływowi incydentów na odbiorców ich usług lub na inne usługi bądź minimalizowania takiego wpływu. Przy uwzględnieniu najnowszego stanu wiedzy oraz, w stosownych przypadkach, odpowiednich norm europejskich i międzynarodowych, a także kosztów wdrożenia środki, o których mowa w akapicie pierwszym, zapewniają poziom bezpieczeństwa sieci i systemów informatycznych odpowiedni do istniejącego ryzyka. Oceniając proporcjonalność tych środków, należy uwzględnić stopień	Wyjaśnienie uwagi Przepis odpowiada wymogom art. 21 dyrektywy NIS2. Jest wprowadzony wymóg proporcjonalności, przy wdrażaniu środków technicznych i organizacyjnych uwzględnia się najnowszy stan wiedzy, koszty wdrożenia, wielkość podmiotu, prawdopodobieństwo wystąpienia incydentów, narażenie podmiotu na ryzyka, skutki społeczne i gospodarcze.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do *projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw* (UC32) cz. I

			narażenia podmiotu na ryzyko, wielkość podmiotu i prawdopodobieństwo wystąpienia incydentów oraz ich dotkliwość, w tym ich skutki społeczne i gospodarcze."	
339.	ISACA	Art. 8	stosowanie bezpiecznych środków komunikacji elektronicznej w ramach krajowego systemu cyberbezpieczeństwa, uwzględniających uwierzytelnianie wieloskładnikowe, Wymaga preredagowania - najlepiej bezpośredniego przeniesienia zapisów art. 21 ust.2 NIS2 "Brakuje w projekcie jasnego zapisu, czego dotyczy (że również wewnątrz organizacji!) Zapis nie jest skuteczną transpozycją [NIS2 art. 21 ust. 2 lit. j)] w stosownych przypadkach – stosowanie uwierzytelniania wieloskładnikowego lub ciągłego, zabezpieczonych połączeń głosowych, tekstowych i wideo oraz zabezpieczonych systemów łączności wewnątrz podmiotu w sytuacjach nadzwyczajnych."	Uwaga uwzględniona Przepis zostanie poprawiony.
340.	ISACA	Art. 8	"pkt 1 lit b) utrzymanie i bezpieczną eksploatację systemu informacyjnego pkt 1 lit f) objęcie systemu informacyjnego wykorzystywanego do świadczenia usługi systemem monitorowania w trybie ciągłym {i co z tego wynika?} 3) zbieranie informacji o cyberzagrożeniach i podatnościach na incydenty systemu informacyjnego wykorzystywanego do świadczenia usługi {i co z tego wynika?} 5) stosowanie środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego wykorzystywanego do świadczenia usługi, w tym: stosowanie mechanizmów zapewniających poufność, integralność, dostępność i autentyczność danych przetwarzanych w systemie informacyjnym, regularne przeprowadzanie aktualizacji oprogramowania, stosownie do zaleceń producenta, z uwzględnieniem analizy wpływu aktualizacji na bezpieczeństwo świadczonej usługi oraz poziomu krytyczności poszczególnych aktualizacji, ochronę przed nieuprawnioną modyfikacją w systemie informacyjnym, [] wło [] pod [] mow [] i d [] i [] n po do [] tr [] ż [] iu pod [] t [] oś [] i lub [] yb [] r [] groź []; "Wymaga preredagowania - najlepiej bezpośredniego przeniesienia zapisów art. 21 ust.2 NIS2 "Zapis nie jest skuteczną transpozycją [NIS2 art. 21 ust. 2 lit. e)] bezpieczeństwo w procesie nabywania, rozwoju i utrzymania sieci i systemów informatycznych, w tym po [] t [] pow [] i [] w pr [] y p [] dku pod [] t [] oś [] i i [] h uj [] w [] i [] i [] Zapisy nie uwzględniają całego cyklu życia (vide wyróżnienie powyżej)."	Uwaga częściowo uwzględniona Odnosnie monitorowania – chodzi o to aby zapewnić rozliczalność i odtworzenie tego co się działo w systemie. Zbieranie informacji o cyberzagrożeniach i podatnościach – istotne jest aby podmiot interesował się i najpierw szukał informacji na temat cyberzagrożeń i podatności a potem podejmował adekwatne działania. Kwestie bezpieczeństwa w procesie nabywania, rozwoju i utrzymania sieci i systemów informatycznych zostaną ujęte w przepisie.
341.	ISACA	Art. 8	"pkt 2 lit c) bezpieczeństwo fizyczne i środowiskowe, uwzględniające kontrolę dostępu, "Wymaga preredagowania - najlepiej bezpośredniego przeniesienia zapisów art. 21 ust.2 NIS2 "Brakuje w projekcie bezpieczeństwa zasobów ludzkich (jest to częściowo uwzględnione w art. 8f, ale nie wyczerpuje wymagania ISO/IEC 27001 A.7.1.1 Postępowanie sprawdzające) Ponadto brakuje kluczowego dla bezpieczeństwa obszaru zarządzania aktywami. Zapis nie jest skuteczną transpozycją [NIS2 art. 21 ust. 2 lit. i)] b [] pi [] i [] n [] t [] wo [] o [] bów lud [] ki [] h. polityke ko [] t [] roli do [] t [] epu i [] r [] ad [] i [] i [] ktyw [] mi;	Uwaga uwzględniona Kwestie bezpieczeństwa zasobów ludzkich oraz zarządzania aktywami zostaną uzupełnione.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			W szczególności pomija zagrożenia związane z niewłaściwym wykorzystaniem wykorzystaniem posiadanych uprawnień lub niewłaściwymi (nadmiarowymi) uprawnieniami użytkowników systemu, które zawarte są pojęciowo w obszarze bezpieczeństwa zasobów ludzkich."	
342.	ISACA	Art. 8	"pkt 2 lit. d) bezpieczeństwo i ciągłość łańcucha dostaw produktów ICT, usług ICT i procesów ICT, od których zależy świadczenie usługi z uwzględnieniem związków pomiędzy dostawcą sprzętu lub oprogramowania a podmiotem kluczowym lub podmiotem ważnym pkt 2 lit. e) wdrażanie, dokumentowanie i utrzymywanie planów działania umożliwiających ciągle i niezakłócone świadczenie usługi oraz zapewniających poufność, integralność, dostępność i autentyczność informacji, oraz planów awaryjnych umożliwiających odtworzenie systemu informacyjnego po katastrofie 4) zarządzanie incydentami" Wymaga preredagowania - najlepiej bezpośredniego przeniesienia zapisów art. 21 ust.2 NIS2, aby w pełni odzwierciedlić wymagania NIS2 np. przywracanie normalnego działania tylko po katastrofie, a także wyłączenia systemu i odwołanie go; określ i właściwego zakresu łańcucha dostaw. "Zapis nie jest skuteczną transpozycją [NIS2 art. 21 ust. 2 lit. b) do d)] a) obsługę i wydanie; b) ciągłość działania, np. zarządzanie kopiami zapasowymi i przywracanie normalnego działania po wyłączeniu systemu i odwołanie go, i zarządzanie kryzysowe; c) bezpieczeństwo łańcucha dostaw, w tym aspekty związane z bezpieczeństwem dotyczące stosunków między każdym podmiotem i jego bezpośrednimi dostawcami lub usługodawcami;"	Wyjaśnienie uwagi Naszym zdaniem kwestie te już są ujęte w przepisie. Zarządzanie incydentami obejmuje obsługę incydentów. Wskazano na konieczność wdrożenia planów ciągłości działania. Zakres łańcuchów dostaw obejmuje sprzęt i oprogramowanie.
343.	ISACA	Art. 8	"Nie zdefiniowano nigdzie celu analizy ryzyka {kontekst} – ochrona sieci i systemów informatycznych oraz środowiska fizycznego tych systemów przed incydentami, z uwzględnieniem wszystkich zagrożeń. "Wymaga uzupełnienia zgodnie z NIS2 "Zapis nie jest skuteczną transpozycją [NIS2 art. 21 ust. 2] Środki, o których mowa w ust. 1, bazują na podejściu uwzględniającym wszystkie zagrożenia i mającym na celu ochronę sieci i systemów informatycznych oraz środowiska fizycznego tych systemów przed incydentami, i obejmują co najmniej następujące elementy:	Wyjaśnienie uwagi Uwzględniono już bezpieczeństwo fizyczne i środowiskowe w przepisie.
344.	ISACA	Art. 8	"2. Wymagania, o których mowa w ust. 1, uznaje się za spełnione, gdy podmiot kluczowy i podmiot ważny zapewnia system zarządzania bezpieczeństwem informacji, z uwzględnieniem wymagań określonych w Polskiej Normie PN-EN ISO/IEC 27001 oraz PN-EN ISO/IEC 22301. 3. Minister właściwy do spraw informatyzacji może udostępnić w Biuletynie Informacji Publicznej na swojej stronie podmiotowej mapowanie wymogów Polskich Norm, o których mowa w ust. 2, na obowiązki wynikające z ustawy oraz z przepisów wydanych na podstawie art. 8a." wykreślić "Wprowadzony automatyzm jest szkodliwy, a ponadto zawiera błędy. - Polska Norma „wprowadza normę międzynarodową” (nawet bez tłumaczenia na język polski) – certyfikaty są wydawane często na normę międzynarodową co może prowadzić do zamieszania - Nie jest jasne co oznacza, że podmiot „zapewnia system zarządzania”. W praktyce występuje pojęcie certyfikatu dla systemu zarządzania	Wyjaśnienie uwagi Pod wpływem różnych uwag koncepcja została zmieniona. Art. 8 ust. 2 zostanie usunięty. W zamian minister właściwy do spraw informatyzacji będzie mógł mapować różne normy/standardy na wymogi ustawowe i rozporządzeń.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			- Kto powinien być uprawniony do wydania takiego certyfikatu? Tylko i wyłącznie jednostka akredytowana w tym zakresie. Akredytacja jest potwierdzeniem kompetencji podmiotu (jednostki certyfikującej wyroby, usługi, osoby, systemy), laboratorium (badawczego, wzorcującego, etc.), jednostki inspekcyjnej, do działań w określonym zakresie. Zakres akredytacji jest załącznikiem do certyfikatu akredytacji i precyzuje obszar potwierdzonych kompetencji. W Polsce jedynym organem akredytacyjnym jest Polskie Centrum Akredytacji. Akredytacja w UE jest „transgraniczna”, co oznacza, że jednostka akredytowana do certyfikacji np. systemów zarządzania na zgodność z normą PN-EN ISO/IEC 27001 przez PCA, może na podstawie tej akredytacji działać w każdym państwie członkowskim UE. Polskie Centrum Akredytacji (PCA) prowadzi działalność na podstawie ustawy z dnia 13.04.2016 r. o systemach oceny zgodności i nadzoru rynku (tj.. Dz.U.2022 poz.1854). PCA jest krajową jednostką akredytującą, upoważnioną do akredytacji jednostek oceniających zgodność, posiada status państwowej osoby prawnej i jest nadzorowane przez ministra właściwego do spraw gospodarki. Nie do końca wiadomo jaki powinien być zakres takiego akredytowanego certyfikatu? Pomimo wprowadzenia powyższych warunków, proponowany automatyzm („uznaje się za spełnione”) ma swoje wady. - System certyfikacji nie jest szczelny. - Niestety często „certyfikowane systemy” mają charakter fasadowy („broniony” przed audytorami raz na rok – badanie ma charakter próbki). - Należy usunąć zapis w celu likwidacji „automatyzmu”."	
345.	Polskie Stowarzyszenie Fotowoltaiki	Art. 8 ust. 1-2	[Obowiązek wdrożenia systemu zarządzania bezpieczeństwem informacji] PK i PW będą zobowiązane do wdrożenia systemu zarządzania bezpieczeństwem informacji w procesach wpływających na świadczenie przez nich usług. SZBI powinien obejmować w szczególności: - systemy przetwarzania danych i ryki wytypi i wyd tu or r r d i ryki m; - odpowiedzi i środki t h i i org i yj; - grom d i i form i o yb r g r o z i i h i p o d t o s i h i i y d t y; - r d i i y d t m i; - t o w i i s r o d k o w p o b i g j a y h i o g r i i j a y h w p l y w i y d t o w; - stosowanie bezpiecznych środków komunikacji elektronicznej w ramach krajowego systemu cyberbezpieczeństwa. Wymaganie wdrożenia systemu zarządzania bezpieczeństwem informacji uważa się za spełnione w razie korzystania przez PK lub PW z systemu zarządzania bezpieczeństwem informacji, z uwzględnieniem wymagań określonych w Polskiej Normie PN-EN ISO/IEC 27001 oraz PN-EN ISO/IEC 22301.	Wyjaśnienie uwagi Art. 8 wskazuje na wprowadzenie proporcjonalnych środków technicznych i organizacyjnych w ramach SZBI. Dopuszczalne jest stosowanie innych norm niż ISO 27001. Pod wpływem różnych uwag koncepcja została zmieniona. Art. 8 ust. 2 zostanie usunięty. W zamian minister właściwy do spraw informatyzacji będzie mógł mapować różne normy/standardy na wymogi ustawowe i rozporządzeń.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			Ogólny wpływ regulacji: PK i PW zobowiązane są do wdrożenia systemu zarządzania bezpieczeństwem informacji w procesach wpływających na świadczenie przez nich usług. W zależności od rodzaju podmiotu realizacja tego obowiązku będzie wymagała: - wdrożenia SZBI w odniesieniu do całości świadczonych przez podmiot usług – w przypadku podmiotów i tych iż operatorów usług kluczowych w rozumieniu KSC; - dostosowania obecnego SZBI wdrożonego na podstawie KSC do nowych wymogów oraz objęcia nimi innych procesów niż wyłącznie systemy informacyjne wykorzystywane do świadczenia usługi kluczowej w rozumieniu KSC. Ww. obowiązek ma dotyczyć ponad 38 tys. podmiotów w Polsce. W przypadku wielu przedsiębiorstw, które będą kwalifikowane jako PK lub PW, realizacja wszystkich obowiązków określonych w art. 8 ust 1 KSC wg Projektu może stanowić, istotne wyzwanie oraz utrudnienie w prowadzeniu działalności biznesowej. Zakres wymagań względem systemu zarządzania bezpieczeństwem informacji jest jednakowy niezależnie od faktycznych okoliczności dot. danego podmiotu lub specyfiki prowadzonej przez nich działalności gospodarczej jak również ekspozycji na ryzyko zw. z cyberbezpieczeństwem, które w zależności od sektora jest różne. W efekcie, wdrożenie systemu zarządzania bezpieczeństwem informacji zgodnego z wymogami określonymi w Projekcie może wymagać znacznych nakładów finansowych i organizacyjnych, które nie będą pozostawały bez wpływu na działalność operacyjną przedsiębiorstw. Ponadto, zakres wymagań względem systemu oraz środków technicznych i organizacyjnych jakie PK lub PW powinien podjąć zgodnie z art. 8 ust. 1 KSC wg Projektu wykracza poza zakres określony w Dyrektywie NIS2. Odnosi się to m.in. do obowiązku systematycznego szacowania ryzyka wystąpienia incydentu, (aktywnego) zbierania informacji o cyberzagrożeniach i podatnościach, zapewnienia ciągłego monitoringu systemów. Ponadto, niektóre z wprowadzonych obowiązków są ogólne co może skutkować arbitralną oceną zgodności PK i PW z wymogami w zakresie cyberbezpieczeństwa (m.in. wymóg zapewnienia bezpieczeństwa fizycznego i środowiskowego) Wpływ na sektor energetyczny: Uwagi jw. – brak specyficznego wpływu na sektor energetyczny. [Nadregulacja względem do Dyrektywy NIS2] Zakres wymagań względem systemu zarządzania bezpieczeństwem informacji oraz środków technicznych i organizacyjnych jakie PK lub PW powinien podjąć zgodnie z art. 8 ust. 1 KSC wg Projektu wykracza poza zakres określony w Dyrektywie NIS2 i stanowi nadregulację. Rekomendacja: - uwzględnienie możliwości wykazania zgodności z obowiązkami określonymi w art. 8 ust. 1 KSC wg Projektu poprzez korzystanie z systemu zarządzania bezpieczeństwem informacji zgodnego z innymi, równoważnymi normami i standardowymi umiłowymi kryteriami;	

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			- ograniczenie wymaganych funkcjonalności i środków technicznych i organizacyjnych do tych wymaganych na podstawie Dyrektywy NIS2 w celu zachowania minimalnego charakteru harmonizacji. - wprowadzenie zasady proporcjonalności w wymaganiach względem systemu zarządzana bezpieczeństwem informacji.	
346.	Fundacja Bezpieczna Cyberprzestrzeń	Art. 8	Art. 1 pkt 12, treść art. 8 ust. 2 – wydaje się, że uznanie (w rozumieniu bez dodatkowej weryfikacji) spełniania wymagań określonych w art. 8 ust. 1 jedynie na podstawie „zapewnienia systemu zarządzania bezpieczeństwem informacji, z uwzględnieniem wymagań określonych w Polskiej Normie PN-EN ISO/IEC 27001 oraz PN-EN ISO/IEC 22301” jest zbyt przychylne. W opinii FBC uznanie spełnienia wymagań powinny mieć certyfikowane systemy zarządzania bezpieczeństwem informacji oraz ciągłości działania. Jakkolwiek można mieć uwagi do procesu certyfikacji, tym niemniej certyfikowany system jest poddany weryfikacji przez audytorów zewnętrznych i daje minimalną gwarancję (w przeciwieństwie do deklaracji podmiotu kluczowego) rzetelnej realizacji wymagań. W związku z tym proponuje się nadanie art. 8 ust. 2 następującą treść: „Art. 8 ust. 2. Wymagania, o których mowa w ust. 1, uznaje się za spełnione, gdy podmiot kluczowy i podmiot ważny zapewnia certyfikowany system zarządzania bezpieczeństwem informacji, z uwzględnieniem wymagań określonych w Polskiej Normie PN-EN ISO/IEC 27001 oraz certyfikowany system zarządzania ciągłością działania, z uwzględnieniem wymagań określonych w Polskiej Normie PN-EN ISO/IEC 22301.”. Nie będzie to działanie nadmiarowe w stosunku do podmiotów mniejszych lub mniej dojrzałych w zakresie cyberbezpieczeństwa, gdyż w art. 8a przewidziano wydanie rozporządzenia Rady Ministrów, określającego szczegółowe wymagania w tym zakresie. W takim rozporządzeniu mogą być zawarte wyłączenia z obowiązku certyfikacji systemów zarządzania bezpieczeństwem informacji oraz zarządzania ciągłością działania. Ponadto samo stwierdzenie, że „Wymagania, o których mowa w ust. 1, uznaje się za spełnione..”, jest wątpliwe, ponieważ żadna z wymienionych norm nie odnosi się, lub odnosi się w sposób niewystarczający do wymogów z ustępu pierwszego takich jak „monitorowanie systemu w trybie ciągłym”, „bezpieczeństwo i ciągłość łańcucha dostaw produktów ICT, usług ICT i procesów ICT, od których zależy świadczenie usługi z uwzględnieniem związków pomiędzy dostawcą sprzętu lub oprogramowania a podmiotem kluczowym lub podmiotem ważnym”, „edukację z zakresu cyberbezpieczeństwa dla personelu podmiotu, w tym podstawowe zasady cyberhigieny”, „zbieranie informacji o cyberzagrożeniach i podatnościach na incydenty systemu informacyjnego wykorzystywanego do świadczenia usługi”. Tematy wymienione wyżej, powinny zostać wdrożone w podmiotach kluczowych i podmiotach ważnych w szerszym zakresie niż wymagają tego normy ISO/IEC 27001 i PN-EN ISO 22301 (powołanie się na normę ISO/IEC 22301 w przypadku normy PN-EN ISO 22301 jest błędem). Stwierdzenie, że budowa systemu bezpieczeństwa opartego wyłącznie na tych normach uznawana jest jako spełnienie wymogów ustawowych jest nieprawdziwa i dodatkowo sprzeczna z NIS2.	Wyjaśnienie uwagi Pod wpływem różnych uwag koncepcja została zmieniona. Art. 8 ust. 2 zostanie usunięty. W zamian minister właściwy do spraw informatyzacji będzie mógł mapować różne normy/standardy na wymogi ustawowe i rozporządzeń.
347.	ISAC-Kolej	Art. 8 ust. 4	„1) ryzyka i podatności związane z dostawcą sprzętu lub oprogramowania”	Wyjaśnienie uwagi

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			Bezpieczeństwo fizyczne i środowiskowe, uwzględniające kontrolę dostępu powinno obejmować nie tylko podatności, ale również ryzyka związane z dostawcą sprzętu lub oprogramowania. Jest to o tyle istotne, że w niektórych podmiotach metodyka zarządzania ryzykiem, oprócz prawdopodobieństwa i skutków, uwzględnia również przy wyliczaniu ryzyka elementy związane z podatnościami.	Przed wszystkim w ust. 4 zostanie poprawione odwołanie – obecnie błędnie odwołuje się do bezpieczeństwa fizycznego i środowiskowego a powinno do bezpieczeństwa łańcuchów dostaw.
348.	ISAC-Kolej	Art. 8 ust. 4	„2. ogólną jakość produktów ICT, usług ICT i procesów ICT pochodzących od dostawcy usługi, sprzętu lub oprogramowania”. Przepis w pierwszej części odnosi się do produktów ICT, usług ICT i procesów ICT a w dalsze części tylko do sprzętu lub oprogramowania. Pominięto usługę jaką w zakresie systemów informacyjnych lub technologii operacyjnych może świadczyć ich dostawca.	Wyjaśnienie uwagi Przepis odnosi się do dostawcy sprzętu i oprogramowania a jest nim producent, upoważniony przedstawiciel, importer lub dystrybutor, w rozumieniu odpowiednio art. 2 pkt 3–6 rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 765/2008 z dnia 9 lipca 2008 r. ustanawiającego wymagania w zakresie akredytacji i uchylającego rozporządzenie (EWG) nr 339/93 (Dz. Urz. UE L 218 z 13.08.2008, str. 30, z późn. zm.)), produktu ICT, usługi ICT lub procesu ICT;
349.	Polskie Stowarzyszenie Fotowoltaiki	Art. 8 ust. 4	[Środki w zakresie bezpieczeństwa i ciągłości łańcucha dostaw produktów ICT, usług ICT i procesów ICT] Obowiązek uwzględnienia przez PK i PW podatności związanych z dostawcą sprzętu lub oprogramowania, ogólnej jakości produktów ICT, usług ICT i procesów ICT oraz wyniki skoordynowanej oceny bezpieczeństwa przeprowadzonej przez Grupę współpracy, o której mowa w art. 22 ust. 1 Dyrektywy NIS2 przy zapewnieniu bezpieczeństwa fizycznego i środowiskowego (art. 8 ust. 1 pkt 2 lit c) KSC wg Projektu). Ogólny wpływ regulacji: Wdrożenie środków zapewniających bezpieczeństwa i ciągłości łańcucha dostaw produktów ICT, usług ICT i procesów ICT będzie wiązało się z istotnymi nakładami finansowymi związanym z m.in.: - opracowaniem oraz wdrożeniem kompleksowych systemów zarządzania ryzykiem - zatrudnieniem specjalistów ds.cyberbezpieczeństwa. Wpływ na sektor energetyczny: Niezbędne nakłady finansowe w celu zapewnienia bezpieczeństwa i ciągłości łańcucha dostaw produktów ICT, usług ICT i procesów ICT w sektorze energetyki będą przewyższały inne sektory z	Uwaga częściowo uwzględniona Wprowadzone zostanie odniesienie do bezpośredniego dostawcy.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			uwagi na zwiększoną ekspozycję sektora. 9% ataków cybernetycznych na łańcuchach dostaw w UE wykrytych pomiędzy lipcem 2022 r. a czerwcem 2023 r. dotyczyło sektora energetycznego¹⁵. [Nadregulacja względem Dyrektywy NIS2] Dyrektywa NIS2, przewiduje w art. 21 ust. 3 obowiązek uwzględnienia podatności charakterystycznych dla każdego <i>bezpośredniego</i> dostawcy i usługodawcy, podczas gdy Projekt odnosi się ogólnie do <i>dostawcy sprzętu lub oprogramowania</i>, którym w rozumieniu Projektu jest również producent oraz importer (pośredni dostawca) – nadregulacja względem Dyrektywy NIS2. Ponadto, w projekcie występuje błąd redakcyjny o istotnym znaczeniu dla zakresu obowiązków PK i PW – w świetle Dyrektywy NIS2 odwołanie powinno dotyczyć art. 8 ust. 1 pkt 2 lit. d) KSC wg Projektu. Rekomendacje: Doprecyzowanie art. 8 ust. 4 KSC wg Projektu o wskazanie: - obowiązku uwzględnienia podatności związanych z bezpośrednim dostawcą sprzętu lub oprogramowania; - właściwego odniesienia do art. 8 ust. 1 pkt 2 lit. d) KSC wg Projektu. - rekomendowane określenie z przedstawicielami rynku sektorowych (w tym dla sektora energetyki) uproszczonych i jednolitych procedur i mechanizmów zapewniających bezpieczeństwo i ciągłość łańcucha dostaw produktów ICT, usług ICT i produktów ICT; Na marginesie wskazujemy, że Dyrektywa NIS2 przewiduje w art. 21 ust. 3 obowiązek uwzględnienia podatności charakterystycznych dla każdego bezpośredniego <i>dostawcy i usługodawcy</i> oraz ogólną jakość <i>produktów i praktyk cyberbezpieczeństwa</i> dostawców i usługodawców. Tymczasem, Projekt odnosi się wyłącznie do <i>dostawców sprzętu lub oprogramowania</i> oraz węższej kategorii <i>produktów ICT, usług ICT i produktów ICT</i>;	
350.	Fundacja Bezpieczna Cyberprzestrzeń	Art. 8	Art. 1 pkt 12, treść art. 8 ust. 4 – wydaje się, że podano błędny odnośnik do ust. 1 pkt 2. Wskazano bowiem literę c, która wydaje się nie mieć związku z wymaganiami wskazanymi w ust. 4. Poprawne wydaje się odniesienie do lit. b.	Uwaga uwzględniona
351.	Międzynarodowe Centrum Bezpieczeństwa Chemicznego	Art. 8	2. Wprowadzenie obowiązku posiadania kwalifikacji przez podmioty krytyczne Propozycja zapisu: W rozdziale 3 [OBOWIĄZKI PODMIOTÓW KLUCZOWYCH I WAŻNYCH] dodaje się punkt dotyczący obowiązku posiadania kwalifikacji: „Podmioty wchodzące w skład krajowego systemu cyberbezpieczeństwa, w szczególności te zarządzające infrastrukturą krytyczną, są zobowiązane do zatrudniania osób posiadających kwalifikacje zawodowe w zakresie cyberbezpieczeństwa w przemyśle.” Uzasadnienie: Zapewnienie, że podmioty krytyczne zatrudniają wykwalifikowanych specjalistów, jest kluczowe dla skutecznego zarządzania ryzykiem i bezpieczeństwem. Art. 7 NIS 2 (Krajowa	Uwaga nieuwzględniona Aby prawidłowo wykonywać obowiązki z rozdziału 3 należy posiadać wykwalifikowany personel. Nie ma potrzeby doprecyzowania tego na poziomie ustawy.

¹⁵ ENISA, ENISA Threat Landscape 2023, <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023>.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			strategia cyberbezpieczeństwa), nakłada na państwa członkowskie w para. 1.h) posiadanie planu, zawierającego kluczowe środki do podniesienia ogólnego poziomu wiedzy obywateli o cyberbezpieczeństwie; w para. 1.f): państwa członkowskie podejmują działania: promujące i rozwijające kształcenie i szkolenie w dziedzinie cyberbezpieczeństwa, umiejętności z zakresu cyberbezpieczeństwa, podnoszenia świadomości oraz inicjatyw badawczo-rozwojowych, a także wytyczne dotyczące dobrych praktyk i kontroli w zakresie cyberhigieny, skierowane do obywateli, zainteresowanych stron i podmiotów. , co wymaga odpowiednich kompetencji.	
352.	Międzynarodowego Centrum Bezpieczeństwa Chemicznego	Art. 8	3. Obowiązek zgłaszania incydentów przez wykwalifikowany personel Propozycja zapisu: Proponujemy dodać zapis dotyczący kwalifikacji osób zgłaszających incydenty: „Zgłoszenia incydentów bezpieczeństwa powinny być dokonywane przez osoby posiadające stosowne kwalifikacje w zakresie cyberbezpieczeństwa.” Uzasadnienie: Skuteczność zgłaszania i zarządzania incydentami zależy od kompetencji osób odpowiedzialnych za te działania. Artykuł 12 Dyrektywy NIS 2 wymaga zgłaszania istotnych incydentów, co wymaga odpowiednich umiejętności i wiedzy.	Uwaga nieuwzględniona Aby prawidłowo wykonywać obowiązki z rozdziału 3 należy posiadać wykwalifikowany personel. Nie ma potrzeby doprecyzowania tego na poziomie ustawy.
353.	Międzynarodowego Centrum Bezpieczeństwa Chemicznego	Art. 8	4. Wprowadzenie wymogu regularnych szkoleń i certyfikacji Propozycja zapisu: Proponujemy dodać zapis dotyczący regularnych szkoleń: „Minister właściwy do spraw cyfryzacji we współpracy z odpowiednimi instytucjami certyfikującymi, zapewnia dostępność szkoleń i programów certyfikacyjnych dla kwalifikacji zawodowych w zakresie cyberbezpieczeństwa w przemyśle.” Uzasadnienie: Regularne szkolenia są niezbędne dla utrzymania wysokiego poziomu kompetencji. Art. 18 nakłada obowiązek oceny rozwoju zdolności w zakresie cyberbezpieczeństwa, co podkreśla potrzebę kwalifikacji i kompetencji.	Wyjaśnienie uwagi Minister właściwy do spraw informatyzacji prowadzi już obecnie szkolenia z zakresu cyberbezpieczeństwa.
354.	PGE SA	Art. 8 ust. 1	W podpunktach wskazane są także elementy zapewnienia ciągłości działania. Dlatego rekomendujemy zmianę brzmienia art. 8 ust. 1: „Podmiot kluczowy lub podmiot ważny wdraża system zarządzania bezpieczeństwem informacji i <u>ciągłości działania</u> w procesach wpływających na świadczenie usług przez ten podmiot, zapewniający...”	Uwaga uwzględniona Przepis zostanie uzupełniony.
355.	PGE SA	Art. 8 ust. 1	Zwracamy uwagę, że obecne brzmienie art. 8 ust. 1 ustawy może być interpretowane jako zobowiązanie do wdrożenia systemu zarządzania bezpieczeństwem informacji dla całości działań podmiotu, a nie tylko w zakresie usług wskazanych w załączniku 1 lub załączniku 2.	Wyjaśnienie uwagi Jest to dobra interpretacja – dyrektywa NIS2 wskazuje, że środki zarządzania ryzykiem powinny dotyczyć całego podmiotu, a nie tylko jego wycinka.
356.	PGE SA	Art. 8 ust. 1 pkt 2, lit. f	Prosimy o zmodyfikowanie brzmienia przepisu poprzez usunięcie zwrotu „w trybie ciągłym”. Przepis zobowiązuje podmioty do monitorowania systemu informacyjnego wykorzystywanego do świadczenia usług adekwatnie do ryzyka. Zmiana jest konieczna z uwagi na rozszerzenie zakresu systemu zarządzania bezpieczeństwem informacji wynikającym z ustawy, dotychczas obejmowała tylko usługi kluczowe, obecnie obejmuje także wszystkie usługi świadczone przez podmiot.	Uwaga nieuwzględniona W tym przepisie jest mowa o zapewnianiu rozliczalności i dostarczaniu informacji na temat tego co się dzieje w systemie informacyjnym poprzez np. gromadzenie i analizę logów.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			<i>f) objęcie systemu informacyjnego wykorzystywanego do świadczenia usługi systemem monitorowania w trybie ciągłym</i>	
357.	PTI	Art. 8	Zmienione brzmienie art. 8 w ust. 1 w punkcie 2) podpunkt f) zawiera wymóg objęcia systemu informatycznego wykorzystywanego do świadczenia usługi systemem monitorowania w trybie ciągłym. Proponuje się doprecyzowanie wymogu monitorowania przez dodanie wyrazów „pod kątem zagrożeń cyberbezpieczeństwa”, gdyż praktyka audytowa wykazała, że niektóre podmioty za spełniony wymóg uważają prowadzenie monitorowania wyłącznie pod kątem ich standardowej aktywności (obciążenie procesorów, zajętość pamięci RAM, zajętość pamięci zewnętrznych, ruch sieciowy etc.)	Wyjaśnienie uwagi System nie powinien być tylko monitorowany pod kątem cyberzagrożeń. Kwestia ta zostanie opisana w uzasadnieniu.
358.	PTI	Art. 8	W zmienionym brzmieniu art. 8 w ust. 1 w punkcie 5 podpunkt a) proponuje się wykreślić atrybut pomocniczy „autentyczność” (patrz uwaga nr 1)	Uwaga nieuwzględniona Istotne jest aby podkreślić kwestie tego kto podejmował czynności w systemie informacyjnym.
359.	Morskie Centrum Cyberbezpieczeństwa Akademia Marynarki Wojennej w Gdyni	Art. 8 ust. 1	Monitorowanie systemu w trybie ciągłym Art. 8 ust f wskazuje na potrzebę objęcia systemu informacyjnego wykorzystywanego do świadczenia usługi systemem monitorowania w trybie ciągłym. Należy zdefiniować co ustawodawca rozumie przez monitoring w trybie ciągłym. Na rynku funkcjonują już interpretacje wskazujące, że: • jeśli system będzie gromadził logi to będzie monitorowany w trybie ciągłym; • wystarczające jest weryfikowanie czy system działa/nie działa lub sprawdzanie obciążenia procesora czy ilości wolnego miejsca na dyskach; • oprogramowanie antywirusowe działające na poszczególnych komputerach działa w trybie ciągłym, więc tym samym stale prowadzi monitoring... A dodatkowo usługi „ciągłego monitoringu” bywają zakupowane od jednoosobowych działalności gospodarczych, które nie posiadają partnerów czy współpracowników i nie mają możliwości świadczenia tych usług. Niemniej w umowach zapewniają oni brak jakichkolwiek przerw w usłudze. Powyższe to tylko przykłady pokazujące jak mało świadomi kierownicy będą starać się obejść przepisy, jeśli nie będą one precyzyjnie określone.	Wyjaśnienie uwagi W tym przepisie jest mowa o zapewnianiu rozliczalność i dostarczaniu informacji na temat tego co się dzieje w systemie informacyjnym poprzez np. gromadzenie i analizę logów.
360.	Morskie Centrum Cyberbezpieczeństwa Akademia Marynarki Wojennej w Gdyni	Art. 8	Bezpieczny proces SDLC Wiele w usług kluczowych jest wspierane zespołami programistów. Stąd wydaje się zadane wskazanie w art. 8 że <u>proces zakupu, tworzenia, wdrażania i konfiguracji oprogramowania powinien być zdefiniowany i realizowany w sposób bezpieczny.</u>	Wyjaśnienie uwagi Kwestie te znajdują się w zakresie utrzymania i bezpiecznej eksploatacji systemu informacyjnego.
361.	Morskie Centrum	Art. 8	Producenci oprogramowania	Wyjaśnienie uwagi

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

	Cyberbezpieczeństwa Akademia Marynarki Wojennej w Gdyni		Art. 6 ust 4 wskazuje, że „Wdrażając środki o których mowa w ust. 1 pkt 2 lit. c podmiot kluczowy i podmiot ważny uwzględnia 1) podatności związane z dostawcą sprzętu lub oprogramowania”. Wydaje się, że ustawodawca ma na myśli <u>producentów a nie dostawców oprogramowania</u> . W obecnym brzmieniu sugeruje to, że w większości przypadków nie trzeba będzie się tym punktem przejmować, gdyż dostawca zazwyczaj nie jest producentem i tym samym nie są z nim związane szczególnie istotne podatności. Chyba, że ustawodawca, chce podkreślić kwestie bezpiecznego łańcucha dostaw, wtedy punkt powinien dotyczyć <u>producentów i dostawców</u> .	Pod pojęciem dostawcy sprzętu lub oprogramowania mieszczą się producent, dostawca, importer.
362.	Morskie Centrum Cyberbezpieczeństwa Akademia Marynarki Wojennej w Gdyni	Art. 8	Zbieranie informacji o cyberzagrożeniach Art. 8 wymaga od podmiotów „zbierania informacji o cyberzagrożeniach”. Wydaje się zasadnym by ustawodawca doprecyzował czego oczekuje od podmiotów, gdyż posiadanie arkusza kalkulacyjnego z zestawieniem wybranych cyberzagrożeń spełni wymagania, ale nie będzie generować wartości dodanej ani też wpływać pozytywnie na cyberbezpieczeństwo podmiotu.	Wyjaśnienie uwagi Jest to jeden z etapów. Należy na bieżąco zbierać informacje o podatnościach/cyberzagrożeniach, np. w oparciu o publiczne bazy CVE i w razie potrzeby mitygować podatności wykryte w systemie.
363.	Morskie Centrum Cyberbezpieczeństwa Akademia Marynarki Wojennej w Gdyni	Art. 8	Testy bezpieczeństwa Zabezpieczenia w obszarze cyberbezpieczeństwa charakteryzują się tym, że bardzo szybko degraduje się ich skuteczność. Stąd tak istotne jest regularne testowania bezpieczeństwa: testy penetracyjne, testy podatności, analiza kodu źródłowego, przeglądy uprawnień użytkowników... Obszar testów został całkowicie pominięty przez ustawodawcę w art. 8, mimo że stanowi fundament cyberbezpieczeństwa. Rekomendujemy dodanie wymagań w tym zakresie.	Uwaga uwzględniona Testy systemów informacyjnych zostaną dodane do art. 8 – choć warto zauważyć, że dyrektywa NIS2 wprost o nich nie wspomina.
364.	CybermadeinPoland	Art. 8	Zmienione brzmienie art.8 w ust. 1 w punkcie 2) podpunkt f) zawiera wymóg objęcia systemu informatycznego wykorzystywanego do świadczenia usługi systemem monitorowania w trybie ciągłym. Proponuje się doprecyzowanie wymogu monitorowania przez dodanie wyrazów „pod kątem zagrożeń cyberbezpieczeństwa”, gdyż praktyka audytowa wykazała, że niektóre podmioty za spełniony wymóg uważają prowadzenie monitorowania wyłącznie pod kątem ich standardowej aktywności (obciążenie procesorów, zajętość pamięci RAM, zajętość pamięci zewnętrznych, ruch sieciowy etc.).	Uwaga nieuwzględniona System informacyjny powinien być monitorowany nie tylko pod kątem cyberzagrożeń, ale pod kątem wszelkich zdarzeń w systemie informacyjnym.
365.	CybermadeinPoland	Art. 8	W zmienionym brzmieniu art.8 w ust. 1 w punkcie 5 podpunkt a) proponuje się wykreślić atrybut pomocniczy „autentyczność” (patrz uwaga nr 1)	Uwaga nieuwzględniona Wyodrębnienie tego atrybutu (od 2018 r.) jest związane z podkreśleniem wagi kwestii kto dokonuje czynności w systemie informacyjnym.
366.	CybermadeinPoland	Art. 8	W zmienionym brzmieniu art.8 ust.2 wskazującym na wymagania określone w normach błędnie podano tytuł (organizację) przy których norma jest akredytowana. Dotyczy to normy PN-EN ISO	Wyjaśnienie uwagi Pod wpływem różnych uwag koncepcja została zmieniona. Art. 8 ust. 2 zostanie

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			22301 (norma nie jest akredytowana przy IEC). W obecnym brzmieniu art.10 ust.3 pkt 3) podano prawidłową nazwę normy jako PN-EN ISO 22301.	usunięty. W zamian minister właściwy do spraw informatyzacji będzie mógł mapować różne normy/standardy na wymogi ustawowe i rozporządzeń.
367.	CybermadeinPoland	Art. 8	Retencja danych jest jednym z elementów spójnej polityki cyberbezpieczeństwa. Dobrze zdefiniowana polityka retencji danych kategoryzuje dane, określa zasady dostępu do nich oraz okresy ich przechowania. Niewłaściwe zarządzanie danymi może narazić organizację na częstsze i agresywniejsze ataki cybernetyczne (im więcej danych posiada organizacja, tym atrakcyjniejsza staje się dla hakerów). Wdrożenie odpowiedniej polityki retencji danych jest jednym z technicznych i organizacyjnych środków zwiększających cyberbezpieczeństwo (zmniejsza ryzyko naruszenia bezpieczeństwa danych, zapewnia bezpieczeństwo wrażliwych danych i ich odpowiedzialną likwidację), poprawiających efektywność odzyskiwania danych (oszczędza czas i zasoby, upraszczając identyfikację kluczowych danych i dostęp do nich) oraz obniża koszty przechowania (organizacja zachowuje tylko te dane, które są niezbędne do przetwarzania). W związku z powyższym proponujemy następującą zmianę: Art. 8. 1. 2) - dodanie podpunktu; j) polityki retencji danych;	Wyjaśnienie uwagi Retencja danych musi być przede wszystkim zgodna z RODO. NIS2 nie wskazuje wprost retencji danych dlatego nie chcemy tego tutaj dodawać, aby nie naruszać RODO. Podmiot może opracować politykę tematyczną dotyczącą retencji danych.
368.	Cybermadeinpoland	Art. 8	Odpowiedzialna likwidacja niezdatnych danych stanowi nieodłączny, choć często marginalizowany element spójnej polityki cyberbezpieczeństwa. Usuwanie w sposób trwały i nieodwracalny lub anonimizowanie niepotrzebnych lub wygasłych danych jest jednym ze środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informatycznego oraz przyczynia się do zwiększenia cyberbezpieczeństwa. W związku z powyższym proponujemy następującą zmianę: Art. 8. 1. 5) - dodanie podpunktu: e) usuwanie lub niszczenie w sposób trwały i nieodwracalny lub anonimizowanie danych niezwłocznie po stwierdzeniu, że dane te nie są już niezbędne do celów, w których były zbierane lub gdy minął okres ich przydatności;	Uwaga nieuwzględniona Kwestie te powinien sam ustalić podmiot kluczowy lub podmiot ważny z uwzględnieniem przepisów RODO i innych przepisów ustaw szczególnych.
369.	Cybermadeinpoland	Art. 8	Zgodnie z przesłanką (89) Dyrektywy NIS2 "Podmioty kluczowe i ważne powinny przyjąć szeroki wachlarz podstawowych praktyk dotyczących cyberhigieny, takich jak zasady zerowego zaufania, aktualizacje oprogramowania, konfiguracja urządzeń, segmentacja sieci, zarządzanie tożsamością i dostępem lub świadomość użytkowników, organizować szkolenia dla pracowników oraz szerzyć wiedzę na temat cyberzagrożeń, phishingu lub technik inżynierii społecznej", proponujemy zmianę Art. 8 w ust. 1 pkt 2 lit. h) w brzmieniu "edukację z zakresu cyberbezpieczeństwa dla personelu podmiotu, w tym podstawowe zasady cyberhigieny", "na zapis "edukację z zakresu cyberbezpieczeństwa dla personelu podmiotu, w tym podstawowe zasady phishingu, technik inżynierii społecznej, cyberhigieny".	Wyjaśnienie uwagi Dyrektywa NIS2 szeroko podchodzi do pojęcia cyberhigieny – pojęcie to należy interpretować zgodnie z motywem 89 NIS2.
370.	Cybermadeinpoland	Art. 8	Art. 8 - brak wskazania na parametry jakościowe dla procesu analizy i zarządzania ryzykiem	Wyjaśnienie uwagi Kwestie te będą mogły być doprecyzowane w rozporządzeniu.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

371.	Cybermadeinpol and	Art. 8	Art. 8 pkt. 2d - Dodanie dostawców z krytycznego łańcucha dostaw do łańcucha dostaw, o którego bezpieczeństwo należy zadbać - NIS 2 wskazywał za szeroko cały łańcuch dostaw, wg nas UoKSC za bardzo zawęża tylko to ICT.	Wyjaśnienie uwagi Choć akt o cyberbezpieczeństwie posługuje się pojęciami produktu ICT czy usługi ICT to te definicje obejmują także sprzęt czy oprogramowanie automatyki przemysłowej.
372.	Cybermadeinpol and	Art. 8	Spełnienie wymogów norm PN-EN ISO/IEC 27001 oraz PN-EN ISO/IEC 22301 jest równoznaczne ze spełnieniem wymogów z tego artykułu. Zapewnia to spójność z międzynarodowym systemem norm oraz będzie premiowało te podmioty, które już dbały o cyberbezpieczeństwo, stosując te normy. Natomiast jak najbardziej możliwe jest zapewnienie zgodności z ustawą poprzez wdrożenie systemu zarządzania bezpieczeństwem informacji w oparciu o inne normy czy standardy. Istotne jest to, czy podmiot wdrożył system zarządzania bezpieczeństwem informacji spełniający wymagania z art. 8 ustawy o KSC. Kwestia wyboru normy czy standardu ma drugorzędne znaczenie.”e eJaka norma jest preferowana, jeśli chodzi o wytyczne dot. analizy ryzyka i zarządzania incydemem?eISO27001 – wskazuje na normę ISO27005 w zakresie zarządzania ryzykiem i ISO27035 w zakresie zarządzania incydemem. Obie te normy skupiają się na ryzykach i incydentach związanych z bezpieczeństwem informacji. Czy takie normy będą odpowiednie z pkt. widzenia nowelizacji ustawy o KSC?	Wyjaśnienie uwagi Pod wpływem różnych uwag koncepcja została zmieniona. Art. 8 ust. 2 zostanie usunięty. W zamian minister właściwy do spraw informatyzacji będzie mógł mapować różne normy/standardy na wymogi ustawowe i rozporządzeń. Normy ISO27005 i ISO27035 z pewnością zostaną wzięte pod uwagę przy mapowaniu.
373.	Izba Gospodarcza Wodociągi Polskie	Art. 8	Wdrożenie i stosowanie zapisów zawartych w ustępach znajdujących się w art. 8 - ust. 1,2, i 4 ze względu na zakres konieczności wskazanych wymogów, z uwagi na ograniczone środki finansowe, środki kadrowe, dojrzałość mniejszych podmiotów funkcjonujących w sektorach wody pitnej i ścieków nie jest możliwe we wskazanym w projekcie ustawy czasie. W tekście ustawy powinny znaleźć się zapisy dotyczące zwiększenia czasu na wdrożenie rozwiązań, ale również zmniejszających odpowiedzialność podmiotu w powyższym zakresie.	Uwaga nieuwzględniona termin 6 miesięcy pozostanie z uwagi na wdrożenie dyrektywy NIS2
374.	KGHM Polska Miedź S.A.	Art. 8 ust. 1 pkt. 2 lit. e) (w zw. z art. 67g ust. 10 pkt. 2	W poleceniu zabezpieczającym jest wskazana na możliwość nałożenia obowiązkowego zachowania w postaci „nakazu przeglądu planów ciągłości działania i planów odtworzenia działalności pod kątem ryzyka wystąpienia incydentu krytycznego związanego z daną podatnością;”. Jednocześnie, na liście zadań wskazanych w art. 8 ust. 1 nie wymienia się posiadania planów ciągłości działania ani planów odtworzenia działalności - mowa jest jedynie o planach awaryjnych umożliwiających odtworzenie systemu informacyjnego po katastrofie. Oczywistym jest, że czynności odtworzenia systemu informacyjnego nie wypełnia wymogów planu ciągłości działania ani odtworzenia działalności - dotyczy jedynie systemu informacyjnego, a nie powrotu do działalności biznesowej. Proponuje się alternatywnie: a) zmienić polecenie zabezpieczające tak, aby zawierało przegląd planów awaryjnych odtworzenia systemu informacyjnego, lub b) uzupełnić art. 8 o zadania obejmujące także opracowanie i utrzymanie planów ciągłości działania i planów odtworzenia działalności. Możliwość nałożenia obowiązku dokonywania przeglądu planów bez uprzedniego wymagania ich	Uwaga uwzględniona Przepisy zostaną uspoólnione. Obydwa przepisy będą się odnosić do planów ciągłości działania, planów awaryjnych i planów odtworzenia działalności po katastrofie.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			procedury stanowi niespójność, która wymaga odpowiedniej korekty legislacyjnej. Rekomenduje się ponowną weryfikację zadań i obowiązków wynikających z art. 8 i nast. nowelizowanej ustawy. Celem powinno być zapewnienie kompletności w zakresie oczekiwanych obowiązków, które mogą być nałożone na mocy działań prowadzonych w ramach czynności audytowych, kontrolnych i nadzorczych.	
375.	PIPC	Art. 8 ust. 1 pkt. 2 lit. e) (w zw. z art. 67g ust. 10 pkt. 2 ustawy zmieniającej)	W poleceniu zabezpieczającym jest wskazana na możliwość nałożenia obowiązkowego zachowania w postaci „nakazu przeglądu planów ciągłości działania i planów odtworzenia działalności pod kątem ryzyka wystąpienia incydentu krytycznego związanego z daną podatnością;” Jednocześnie, na liście zadań wskazanych w art. 8 ust. 1 nie wymienia się posiadania planów ciągłości działania ani planów odtworzenia działalności - mowa jest jedynie o planach awaryjnych umożliwiających odtworzenie systemu informacyjnego po katastrofie. Oczywistym jest, że czynności odtworzenia systemu informacyjnego nie wypełnia wymogów planu ciągłości działania ani odtworzenia działalności - dotyczy jedynie systemu informacyjnego, a nie powrotu do działalności biznesowej. Proponuje się alternatywnie: a) zmienić polecenie zabezpieczające tak, aby zawierało przegląd planów awaryjnych odtworzenia systemu informacyjnego lub b) uzupełnić art. 8 o zadania obejmujące także opracowanie i utrzymanie planów ciągłości działania i planów odtworzenia działalności. Możliwość nałożenia obowiązku dokonywania przeglądu planów bez uprzedniego wymagania ich prowadzenia stanowi niespójność, która wymaga odpowiedniej korekty legislacyjnej. Rekomendujemy ponowną weryfikację zadań i obowiązków wynikających z art. 8 i nast. nowelizowanej ustawy. Celem powinno być zapewnienie kompletności w zakresie oczekiwanych obowiązków, które mogą być nałożone na mocy działań prowadzonych w ramach czynności audytowych, kontrolnych i nadzorczych.	Uwaga uwzględniona Przepisy zostaną uspołnione.
376.	Związek Pracodawców Polska Miedź	Art. 8 ust. 1 pkt. 2 lit. e) (w zw. z art. 67g ust. 10 pkt. 2)	W poleceniu zabezpieczającym jest wskazana na możliwość nałożenia obowiązkowego zachowania w postaci „nakazu przeglądu planów ciągłości działania i planów odtworzenia działalności pod kątem ryzyka wystąpienia incydentu krytycznego związanego z daną podatnością;” Jednocześnie, na liście zadań wskazanych w art. 8 ust. 1 nie wymienia się posiadania planów ciągłości działania ani planów odtworzenia działalności - mowa jest jedynie o planach awaryjnych umożliwiających odtworzenie systemu informacyjnego po katastrofie. Oczywistym jest, że czynności odtworzenia systemu informacyjnego nie wypełnia wymogów planu ciągłości działania ani odtworzenia działalności - dotyczy jedynie systemu informacyjnego, a nie powrotu do działalności biznesowej. Proponuje się alternatywnie: c) zmienić polecenie zabezpieczające tak, aby zawierało przegląd planów awaryjnych odtworzenia systemu informacyjnego, lub d) uzupełnić art. 8 o zadania obejmujące także opracowanie i utrzymanie planów ciągłości działania i planów odtworzenia działalności.	Uwaga uwzględniona Przepisy zostaną uspołnione.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			Możliwość nałożenia obowiązku dokonywania przeglądu planów bez uprzedniego wymagania ich prowadzenia stanowi niespójność, która wymaga odpowiedniej korekty legislacyjnej. Rekomenduje się ponowną weryfikację zadań i obowiązków wynikających z art. 8 i nast. nowelizowanej ustawy. Celem powinno być zapewnienie kompletności w zakresie oczekiwanych obowiązków, które mogą być nałożone na mocy działań prowadzonych w ramach czynności audytowych, kontrolnych i nadzorczych.	
377.	PWPW	Art. 8	Uwaga do art. 1 pkt 12 projektu ustawy (art. 8 ust. 3 ustawy zmienianej). Uwaga do art. 1 pkt 13 projektu ustawy (art. 8a ustawy zmienianej). Ppkt 1) PWPW S.A. proponuje nadanie przepisowi art. 8 ust. 3 zawartemu w art. 1 pkt 12 projektu, następującego brzmienia: „3. Minister właściwy do spraw informatyzacji udostępnia w Biuletynie Informacji Publicznej na swojej stronie podmiotowej mapowanie wymogów Polskich Norm, o których mowa w ust. 2, na obowiązki wynikające z ustawy oraz z przepisów wydanych na podstawie art. 8a.”. Uzasadnienie: Projekt ustawy przewiduje, że minister właściwy do spraw informatyzacji (dalej: Minister) może udostępnić w BIP mapowanie wymogów Polskich Norm. W ocenie PWPW S.A., wynikająca stąd fakultatywność udostępnienia mapowania może wpłynąć negatywnie na prawidłowe wdrażanie wymogów wynikających z ustawy. W przypadku pozostania przy fakultatywności, mapowanie mogłoby nie zostać udostępnione lub mogłoby zostać udostępnione, ale dopiero w dalszej przyszłości, już po tym, jak znacząca część podmiotów zrealizuje stosowne wymogi wdrażając system zarządzania bezpieczeństwem informacji zgodnie z własną interpretacją norm. Takie rozwiązanie, powoduje z jednej strony działanie w warunkach ryzyka niepewności prawnej, co do ewentualnej publikacji takiego mapowania, a z drugiej strony, powstanie ryzyka kosztów dla przedsiębiorców, w wyniku podjęcia działań mających na celu dostosowanie wdrożonego już systemu do opublikowanego mapowania. oW ocenie PWPW S.A., obligatoryjność mapowania i jego udostępniania w BIP przez Ministra, przyczyni się do standaryzacji rozwiązań, do pewności prawnej podmiotów zobowiązanych, w zakresie obowiązków związanych z systemem zarządzania bezpieczeństwem informacji i obniży koszty, eliminując konieczność ewentualnego dostosowania się do opublikowanego dokumentu – który zgodnie z obecną propozycją może, ale nie musi być publikowany. Ppkt 2) W przypadku uwzględnienia powyższej uwagi, PWPW S.A. wnosi o analogiczną zmianę w przepisie art. 8a zawartym w art. 1 pkt 13 projektu, czyli odstąpienie od fakultatywności, na rzecz obligatoryjności określenia przez Radę Ministrów szczegółowych wymagań dla systemu zarządzania bezpieczeństwem informacji dla danych rodzajów działalności tj. przyjęcie następujące brzmienia przepisu art. 8a: „Art. 8a. Rada Ministrów określa, w drodze rozporządzenia, odrębnie dla danego rodzaju działalności wykonywanej przez podmioty kluczowe lub podmioty ważne szczegółowe wymagania dla systemu	Uwaga nieuwzględniona Mapowanie standardów nie jest czynnością wiążącą dla podmiotów oraz nie może nakładać dodatkowych obowiązków względem przepisu. Pozostawiono fakultatywność mapowania, aby zapewnić ministrowi elastyczność. Z uwagi na wielość sektorów pozostawiono fakultatywne rozporządzenie. Każdy sektor należy potraktować odrębnie i odrębnie wskazywać wymogi dla niego. Może się też zdarzyć, że dla konkretnego sektora nie ma sensu precyzować wymagań SZBI. Stąd pozostawiono fakultatywne upoważnienie ustawowe.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			zarządzania bezpieczeństwem informacji, o którym mowa w art. 8 ust. 1, biorąc pod uwagę rekomendacje międzynarodowe o charakterze specjalistycznym, w tym rekomendacje Agencji Unii Europejskiej do spraw Cyberbezpieczeństwa, zwanej dalej „ENISA”, skalę działalności wykonywanej przez te podmioty oraz potrzebę podejmowania przez te podmioty działań zapewniających cyberbezpieczeństwo.”.	
378.	Osoba fizyczna	Art. 8	Ust. 1 Wprowadzenie - Zastosowano zapis „Podmiot (...) wdraża system zarządzania bezpieczeństwem informacji w procesach wpływających na świadczenia usług przez ten podmiot (...)”. W ujęciu zarządzania procesowego wyróżnia się procesy zarządzania, wspomagające i podstawowe/główne, które to bezpośrednio realizują podstawową działalność – usługi. Zapis wskazujący na „procesy wpływające na świadczenie usług” można odnieść albo do wszystkich procesów w podmiocie, albo do procesów zarządzania i wspierających, które nie realizują usługi, a wpływają na jej realizację. Zaproponowany nowy zapis nie uwzględnia systemu informacyjnego, który jest podstawowym bytem w systemie cyberbezpieczeństwa, co jest fundamentalnym odstępieniem do regulacji bazowej – dyrektywy NIS 2, dotyczącej bezpieczeństwa sieci i systemów informatycznych, a nie usług, ani procesów wpływających na usługi. Rezygnacja ze wskazania systemu informacyjnego jako zakresu wdrożenia SZBI powoduje zupełną zmianę kontekstu i znaczenia dalszych zapisów art. 8, które w znacznej części odnoszą się bezpośrednio do systemu informacyjnego, ale też do usługi. Proponuję: 1) przywrócić pierwotny zapis adresujący wymaganie do systemu informacyjnego albo, 2) w przypadku intencji wdrożenia SZBI w szerszym zakresie, wskazanie na „wdrożenie SZBI w świadczonej usłudze, w tym w procesach realizacji usługi i w systemie informacyjnym, od którego zależne jest świadczenie usługi”. W zależności od wybranej opcji, należy odpowiednio dostosować zapisy art. 8 i stosowanie pozostałych artykułów.	Wyjaśnienie uwagi Przepis zostanie zmieniony w ten sposób, że wprowadzone zostanie odniesienie do systemów informacyjnych używanych w procesie świadczenia usługi.
379.	Osoba fizyczna	Art. 8	Ust. 1 – Proponuję w wyszczególnionym zakresie zapewnianym przez SZBI wprowadzić dodatkowe treści uszczegóławiające i wypuklające kontekst cyberbezpieczeństwa i systemu informacyjnego, np. (wprowadzone kursywą): 1) szacowanie ryzyka w zakresie cyberbezpieczeństwa (ryzyka cyberbezpieczeństwa), 2a) polityki szacowania ryzyka w zakresie cyberbezpieczeństwa oraz polityki bezpieczeństwa syst. inf. i polityki cyberbezpieczeństwa [zgodnie z definicjami uKSC2 bezpieczeństwo syst. inform. i cyberbezpieczeństwo to różne, niepokrywające się zakresy pojęciowe], 2e) ... i niezakłócone świadczenie usługi zależne od systemu informacyjnego (...), 2e) proponuję zamienić „planów awaryjnych umożliwiających odtworzenie...” na zapis „planów ciągłości działania oraz planów przywrócenia działalności i odtworzenia systemu informacyjnego” [oczywiście w przypadku nieuwzględnienia propozycji pkt. 3.3], 3) ... podatnościach na cyberzagrożenia...,	Wyjaśnienie uwagi Zdaniem Ministerstwa Cyfryzacji nie ma potrzeby wprowadzania tych zmian.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			5a) stosowanie mechanizmów ... przetwarzanych w systemie informacyjnym i związanych z nimi usług oferowanych przez te systemy [zgodnie z aktualną definicją „bezpieczeństwa systemów informacyjnych”],	
380.	Stowarzyszenie Absolwentów Studiów Cyberbezpieczeństwa MBA	Art. 8	Ryzyko zatrzymania procesów biznesowych w przypadku wdrożenia wymaganych działań w systemach automatyki przemysłowej W projekcie ustawy, ustawodawca wymusza działania w zakresie regularnych aktualizacji systemów oraz wykrywania podatności. W przypadku automatyki przemysłowej wiele działających komponentów (np. sterowniki PLC) nie posiadają aktualizacji producenta lub ich aktualizacja jest możliwa np. 2 razy do roku. Spowodowane jest to, że obsługują one procesy technologicznego przemysłu ciężkiego, które mogą zostać przerwane/zakłócone poprzez aktualizację ich oprogramowania lub skanowanie portów komunikacyjnych przez narzędzia (np. nmap, Nessus etc.). Dodatkowo w zakresie badania podatności, uruchomienie skanowania podatności, w przypadku protokołu MODBUS, który jest protokołem wykorzystywanym w świecie OT i nie wymaga on uwierzytelnienia, pozwala na uruchomienie takiego badania. Badanie to może zostać przez urządzenie zinterpretowane jako wydanie polecenia technologicznego. Może to doprowadzić do niezaplanowanego uruchomienia procesu technologicznego powodując zagrożenia dla zdrowia i życia osób, np. uruchomienie wypalarki laserowej w otoczeniu pracowników, podniesienie pracownika przez metalowe ramię robota lub może powodować wielomilionowe konsekwencje finansowe związane z zatrzymaniem pracy kotła w hucie czy elektrowni. ując zagrożeniaW związku z tak poważnymi ryzykami, należy zastosować w ustawie, zakres dotyczący automatyki przemysłowej. Do zakresu należy wskazać wytyczne przewidziane normą ISA/IEC 62443, oraz uwzględnienie sytuacji w której niemożliwe jest uzyskanie wsparcia technicznego dla danego urządzenia ze względu na zerwanie łańcucha dostaw lub niedostępność usługi wsparcia na runku.	Wyjaśnienie uwagi Podzielamy zdanie Stowarzyszenia jednakże wskazujemy, że już obecne brzmienie przepisu uwzględnia tę okoliczność, bowiem przed aktualizacją ma być przeprowadzona analiza wpływu aktualizacji na bezpieczeństwo świadczonej usługi.
381.	ISSA Polska	Art. 8	Ryzyko zatrzymania procesów biznesowych w przypadku wdrożenia wymaganych działań w systemach automatyki przemysłowej. W projekcie ustawy, ustawodawca wymusza działania w zakresie regularnych aktualizacji systemów oraz wykrywania podatności. W przypadku automatyki przemysłowej wiele działających komponentów (np. sterowniki PLC) nie posiadają aktualizacji producenta lub ich aktualizacja jest możliwa np. 2 razy do roku. Spowodowane jest to, że obsługują one procesy technologicznego przemysłu ciężkiego, które mogą zostać przerwane/zakłócone poprzez aktualizację ich oprogramowania lub skanowanie portów komunikacyjnych przez narzędzia (np. nmap, Nessus, Qualys, etc.). Dodatkowo w zakresie badania podatności, uruchomienie skanowania podatności, w przypadku protokołu MODBUS, który jest protokołem wykorzystywanym w świecie OT i nie wymaga on uwierzytelnienia, pozwala na uruchomienie takiego badania. Badanie to może zostać przez urządzenie zinterpretowane jako wydanie polecenia technologicznego. Może to doprowadzić do niezaplanowanego uruchomienia procesu technologicznego powodując zagrożenia dla zdrowia i życia osób, np. uruchomienie wypalarki laserowej w otoczeniu pracowników, podniesienie pracownika przez metalowe ramię robota lub może powodować wielomilionowe konsekwencje finansowe związane z zatrzymaniem	Wyjaśnienie uwagi Podzielamy zdanie Stowarzyszenia jednakże wskazujemy, że już obecne brzmienie przepisu uwzględnia tę okoliczność, bowiem przed aktualizacją ma być przeprowadzona analiza wpływu aktualizacji na bezpieczeństwo świadczonej usługi.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			pracy kotła w hucie czy elektrowni. W związku z tak poważnymi ryzykami, należy zastosować w ustawie, zakres dotyczący automatyki przemysłowej. Do zakresu należy wskazać wytyczne przewidziane normą ISA/IEC 62443.	
382.	TAURON Polska Energia S.A	Art. 8 ust 1.	Art. 8. 1. Podmiot kluczowy lub podmiot ważny wdraża system zarządzania bezpieczeństwem informacji w procesach wpływających na świadczenie usług przez ten podmiot, zapewniający: (...) Jednym najistotniejszych działań przy budowaniu bezpieczeństwa jest ustalenie ról i odpowiedzialności w zakresie cyberbezpieczeństwa systemów informacyjnych. Proponowane brzmienie: uwzględniające powyższe : Dodanie jako 1): <i>„ustanowienie ról oraz odpowiedzialności za cyberbezpieczeństwo systemów informacyjnych wspierających świadczenie usług kluczowych”</i>	Wyjaśnienie uwagi Te kwestie są do ustalenia przez podmiot w ramach polityki bezpieczeństwa.
383.	TAURON Polska Energia S.A	Art. 8 ust.1 pkt 2 i 2c	2) wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, uwzględniających najnowszy stan wiedzy, koszty wdrożenia, wielkość podmiotu, prawdopodobieństwo wystąpienia incydentów, narażenie podmiotu na ryzyka, w szczególności (...): 2 c) bezpieczeństwo fizyczne i środowiskowe, uwzględniające kontrole dostępu Tak skonstruowany zapis nie precyzuje w jakim zakresie należy stosować właściwe środki techniczne i organizacyjne zapewniające skuteczność i efektywność bezpieczeństwa fizycznego. Należy uwzględnić, że w wielu przypadkach dla podmiotów kluczowych i podmiotów ważnych, bezpieczeństwo fizyczne będzie regulowane na podstawie przepisów ustawy o ochronie osób i mienia (dla obiektów podlegających obowiązkowej ochronie), natomiast dla pozostałych szczegółowe wymagania nie są sprecyzowane. Również uchylenie art. 14, a tym samym wymagań wynikających z rozporządzenia określającego warunki organizacyjne i techniczne dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo eliminuje chociażby konieczność stosowania dedykowanych Polskich Norm w zakresie systemów zabezpieczenia technicznego, w tym systemów kontroli dostępu. Określenie „(...) uwzględniające kontrolę dostępu” nie precyzuje formy tej kontroli, zakresu, a także obszarów/ miejsc, w których nadzór nad dostępem powinien być realizowany. Proponujemy zatem następujący zapis: <i>„ c) bezpieczeństwo fizyczne i środowiskowe, uwzględniające wymagania Polskich Norm dla elektronicznych urządzeń i systemów alarmowych (systemu kontroli dostępu, systemu sygnalizacji włamania i napadu, systemu dozoru wizyjnego) oraz urządzeń i środków zabezpieczenia mechanicznego, w szczególności:</i> - <i>PN-EN 60839-11-2 Systemy alarmowe i elektroniczne systemy zabezpieczeń – Część 11-2: Elektroniczne systemy kontroli dostępu – Wytyczne stosowania,</i> - <i>PKN-CLC/TS 50131-7 Systemy alarmowe – Systemy sygnalizacji włamania i napadu – Część 7: Wytyczne stosowania,</i>	Uwaga nieuwzględniona Dyrektywa NIS2 szczegółowo nie precyzuje środków dotyczących bezpieczeństwa fizycznego. Wskazuje jedynie na konieczność wdrożenia proporcjonalnych środków adekwatnych do ryzyka.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			<i>PN-EN 62676-4 Systemy dozorowe CCTV stosowane w zabezpieczeniach – Część 4: Wytyczne stosowania.”</i>	
384.	ZBP	Art. 8 ust. 1 pkt 2 lit. h	h) edukację z zakresu cyberbezpieczeństwa dla personelu podmiotu, w tym podstawowe zasady cyberhigieny, Uwaga ogólna W treści projektu brak jest definicji „cyberhigieny”.	Wyjaśnienie uwagi Cyberhigiena zostanie opisana w uzasadnieniu.
385.	Osoba fizyczna	Art. 8	Ust. 2 – proponuję rozszerzyć wykaz norm uwzględnianych w SZBI o normy PN-EN/ISO 27002, 20000-1, 20000-2, 27005, wskazane w rozporządzeniu o Krajowych Ramach interoperacyjności... do Ustawy o informatyzacji podmiotów realizujących zadania publiczne jako podstawa do operacyjnego zarządzania systemami teleinformatycznymi i ich bezpieczeństwem.	Wyjaśnienie uwagi Pod wpływem różnych uwag koncepcja została zmieniona. Art. 8 ust. 2 zostanie usunięty. W zamian minister właściwy do spraw informatyzacji będzie mógł mapować różne normy/standardy na wymogi ustawowe i rozporządzeń.
386.	ZPP	Art. 8	Propozycja art. 8 zawiera przepis dotyczący systemu zarządzania bezpieczeństwem informacji oraz dokładne określenie funkcji, które ten system ma spełniać. Ze względu na oczywiste przyczyny, przepisy ustawy są sformułowane ogólnie, a jednocześnie obejmują dużą liczbę podmiotów z różnych sektorów. Problem polega na narzuceniu konkretnych wymogów przedsiębiorcom bez jednoznacznego wskazania, czy ich działania i wprowadzane zmiany są zgodne z oczekiwaniami i przepisami właściwych organów. Ma to szczególne znaczenie w kontekście ust. 4 omawianego przepisu, który wymaga od podmiotów uwzględnienia podatności danego dostawcy oraz „ogólnej jakości produktów ICT (...)”. Ustawa proponuje dwa rozwiązania • Przede wszystkim, art. 67a przewiduje możliwość wydania przez Pełnomocnika ds. cyberbezpieczeństwa stosownych rekomendacji dla podmiotów krajowego systemu cyberbezpieczeństwa. Jest to formuła prawa miękkiego, jednak warto rozważyć, czy przepis nie powinien nakładać obowiązku działania Pełnomocnika ds. cyberbezpieczeństwa, który uzupełniałby przepisy konkretnymi rekomendacjami i przewodnikami dla przedsiębiorców. • Art. 8a wskazuje na możliwość działania Rady Ministrów w drodze rozporządzenia. Choć takie działanie miałoby charakter wiążący dla przedsiębiorców, wyznaczenie Rady Ministrów jako organu właściwego może okazać się nieefektywne. Jeżeli forma rozporządzenia jest konieczna, naszym zdaniem lepszym rozwiązaniem byłoby powierzenie tej funkcji Ministrowi.	Uwaga wyjaśniona Pozostawiamy uprawnienie do wydania rozporządzenia Radzie Ministrów, z uwagi na to że dotyczy to zakresu działań wielu ministrów.
387.	Związek Cyfrowa Polska	Art. 8	Art. 8 projektu zawiera przepis dotyczący systemu zarządzania bezpieczeństwem informacji oraz enumeratywne wyliczenie funkcji, które ma ten system zapewnić. Przepisy ustawy z oczywistych przyczyn zawierają sformułowania ogólne, a jednocześnie liczba podmiotów objętych nowymi przepisami i różnorodność sektorów, z których się wywodzą jest znaczna. Pojawia się tutaj problem polegający na skierowaniu konkretnych wymogów do przedsiębiorców bez jednoczesnego wskazania na to, czy kierunek, wg którego podejmują oni działania i wprowadzają do swoich systemów zmiany – jest wg organu właściwego słuszny i wypełnia oczekiwania, a przede wszystkim jest zgodny z przepisami. Ma to szczególne znaczenie w kontekście ust. 4 omawianego przepisu, w której podmioty	Wyjaśnienie uwagi Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa będzie mógł wydawać wiele rekomendacji, stąd właściwsza wydaje fakultatywna forma wydawania rekomendacji.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			objęte ustawą mają uwzględniać podatności danego dostawcy oraz „ogólną jakość produktów ICT (...)”. W ustawie jest to rozwiązane na dwa sposoby: przede wszystkim art. 67a przewiduje fakultatywne działanie Pełnomocnika ds. cyberbezpieczeństwa w postaci wydania stosownych rekomendacji dla podmiotów krajowego systemu cyberbezpieczeństwa – jest to formuła aktów prawa miękkiego – stosunkowo elastyczna dla przedsiębiorców. Warto byłoby zastanowić się, czy przepis nie powinien zmierzać w kierunku obligatoryjnego działania Pełnomocnika ds. cyberbezpieczeństwa, który uzupełnia przepisy stosownymi rekomendacjami/przewodnikami dla przedsiębiorców.	
388.	Apator	Art. 8 ust. 2	art. 8 ust. 2 Projektu proponujemy, aby otrzymał brzmienie: <i>Wymagania, o których mowa w ust. 1, uznaje się za spełnione, gdy podmiot kluczowy i podmiot ważny zapewnia system zarządzania bezpieczeństwem informacji, z uwzględnieniem wymagań określonych w Polskiej Normie PN-EN ISO/IEC 27001 oraz PN-EN ISO/IEC 22301, oraz w zakresie art. 8 ust. 1 pkt. d współpracuje z kontrahentami świadczącymi usługi bezpośrednio związane z bezpieczeństwem informacji, którzy spełniają wymagania określone w Polskiej Normie PN-EN ISO/IEC 27001 lub innych normach równoważnych i gwarantujących porównywalną ochronę tych informacji.</i> Uzasadnienie proponowanej zmiany: W projekcie nie określono wprost, jakimi kryteriami przy doborze podmiotów współpracujących z podmiotami kluczowymi oraz podmiotami ważnymi w zakresie zapewnienia bezpieczeństwa informacji powinny się kierować podmioty kluczowe lub podmioty ważne. W naszej opinii odwołanie się do norm, stanowi obiektywny i sprawdzalny kryterium należytego zarządzania systemem bezpieczeństwa informacji przez podmioty kluczowe lub podmioty ważne.	Wyjaśnienie uwagi Pod wpływem różnych uwag koncepcja została zmieniona. Art. 8 ust. 2 zostanie usunięty. W zamian minister właściwy do spraw informatyzacji będzie mógł mapować różne normy/standardy na wymogi ustawowe i rozporządzeń. Odnosnie doprecyzowania co do kontrahentów to zdaniem MC może to być nadmierne. Te kwestie podmiot kluczowy/podmiot ważny powinien zawrzeć np. w umowach a takimi podmiotami.
389.	SGS Polska	Art. 8 ust. 2	W związku z pojawieniem się projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32), pragniemy w ramach konsultacji zwrócić uwagę na bardzo ważną kwestię poruszoną w Art. 8 ustęp 1 i 2 proponowanej ustawy: „Art. 8. 1. Podmiot kluczowy lub podmiot ważny wdraża system zarządzania bezpieczeństwem informacji w procesach wpływających na świadczenie usług przez ten podmiot, zapewniający: ...” i dalej w Art. 8 ustęp 2: „Art. 8.2. Wymagania, o których mowa w ust. 1, uznaje się za spełnione, gdy podmiot kluczowy i podmiot ważny zapewnia system zarządzania bezpieczeństwem informacji, z uwzględnieniem wymagań określonych w Polskiej Normie PN-EN ISO/IEC 27001 oraz PN-EN ISO/IEC 22301.” dotyczącą spełnienia warunków wymagań w przypadku zastosowania systemu zarządzania bezpieczeństwem informacji z uwzględnieniem wymagań określonych w Polskiej Normie PN-EN ISO/IEC 27001 oraz PN-EN ISO/IEC 22301. Obecnie wiele podmiotów posiada wdrożony system zarządzania bezpieczeństwem informacji w oparciu o inne wydania norm, a więc ISO/IEC 27001 oraz ISO/IEC 22301. Nasuwa się więc pytanie, czy takie równoważne systemy będą także uznawane w kontekście spełnienia wymagań ustawy KSC.	Wyjaśnienie uwagi Pod wpływem różnych uwag koncepcja została zmieniona. Art. 8 ust. 2 zostanie usunięty. W zamian minister właściwy do spraw informatyzacji będzie mógł mapować różne normy/standardy na wymogi ustawowe i rozporządzeń.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			Niejednokrotnie podmioty należące do grupy firm, zobowiązane są do wdrażania rozwiązań na poziomie korporacyjnym, w zdecydowanej większości z siedzibami głównymi poza Polską, w związku z tym nie mogą samodzielnie podejmować decyzji o wyborze konkretnego wydania normy, w oparciu o którą będą wdrażały system zarządzania bezpieczeństwem informacji. Wydawałoby się zasadne uwzględnienie także takich wdrożeń, aby podmioty te nie były dyskryminowane. Dodatkowo ocena systemów zarządzania bezpieczeństwem informacji dokonywana jest głównie przez jednostki certyfikujące posiadające akredytacje jednostek akredytowanych będących sygnatariuszami porozumienia jednostek akredytujących European Co-operation for Accreditation , w związku z tym poziom implementacji systemu zarządzania bezpieczeństwem informacji jest potwierdzany przez niezależne jednostki. Proponujemy dokonanie zmian w zapisie Art. 8. 2: „Art. 8.2. Wymagania, o których mowa w ust. 1, uznaje się za spełnione, gdy podmiot kluczowy i podmiot ważny zapewnia system zarządzania bezpieczeństwem informacji, z uwzględnieniem wymagań określonych w Normach ISO/IEC 27001 oraz ISO/IEC 22301.” lub dodanie: „Art. 8.2. Wymagania, o których mowa w ust. 1, uznaje się za spełnione, gdy podmiot kluczowy i podmiot ważny zapewnia system zarządzania bezpieczeństwem informacji, z uwzględnieniem wymagań określonych w Polskiej Normie PN-EN ISO/IEC 27001 oraz PN-EN ISO/IEC 22301 (lub normach im równoważnych)” Podobne zapisy zostały już zastosowane np. w Art. 10. 2.	
390.	Stowarzyszenie Absolwentów Studiów Cyberbezpieczeństwa MBA	Art. 8 ust. 2	Rozszerzenie projektowanego przepisu art. 8 pkt. 2 ustawy KSC Projektowany przepis art. 8 ust. 2 ustawy KSC obecnie brzmi: “Wymagania, o których mowa w ust. 1, uznaje się za spełnione, gdy podmiot kluczowy i podmiot ważny zapewnia system zarządzania bezpieczeństwem informacji, z uwzględnieniem wymagań określonych w Polskiej Normie PN-EN ISO/IEC 27001 oraz PN-EN ISO/IEC 22301”. Należy przepis rozszerzyć wskazując w szczególności zastosowanie norm branżowych i dobrych praktyk oraz np. IEC 62443 lub zastosowanie 27019, czy też dobrych praktyk z Podręczników RCB i innych wytycznych, które będą dorocznie publikowane przez Ministra właściwego dla branży lub sektora, których najlepszym przykładem są Narodowe Standardy Cyberbezpieczeństwa. Kolejną rekomendacją jest rozłączne traktowanie norm ISO/IEC 27001 oraz PN-EN ISO/IEC 22301 ze względu na ich niepokrywający się zakres tematyczny.	Wyjaśnienie uwagi Pod wpływem różnych uwag koncepcja została zmieniona. Art. 8 ust. 2 zostanie usunięty. W zamian minister właściwy do spraw informatyzacji będzie mógł mapować różne normy/standardy na wymogi ustawowe i rozporządzeń.
391.	ISSA Polska	Art. 8 ust. 2	Zapis “Wymagania, o których mowa w ust. 1, uznaje się za spełnione, gdy podmiot kluczowy i podmiot ważny zapewnia system zarządzania bezpieczeństwem informacji, z uwzględnieniem wymagań określonych w Polskiej Normie PN-EN ISO/IEC 27001 oraz PN-EN ISO/IEC 22301”. Należy zapis rozszerzyć wskazując w szczególności zastosowanie norm branżowych i dobrych praktyk, np. IEC 62443 lub zastosowanie 27019, czy też dobrych praktyk z Podręczników RCB, czy innych wytycznych, które będą publikowane przez Ministra właściwego dla branży, których	Wyjaśnienie uwagi Pod wpływem różnych uwag koncepcja została zmieniona. Art. 8 ust. 2 zostanie usunięty. W zamian minister właściwy do spraw informatyzacji będzie mógł

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			najlepszym przykładem są Narodowe Standardy Cyberbezpieczeństwa. Kolejną rekomendacją jest rozłączne traktowanie norm ISO ISO/IEC 27001 oraz PN-EN ISO/IEC 22301 ze względu na ich niepokrywający się zakres tematyczny.	mapować różne normy/standardy na wymogi ustawowe i rozporządzeń.
392.	PGE S.A.	Art. 8 ust. 2 ustawy	W art. 8 ust. 2 należy zamienić spójnik „i” na „lub”: 2. Wymagania, o których mowa w ust. 1, uznaje się za spełnione, gdy podmiot kluczowy ~~i~~ lub podmiot ważny zapewnia system zarządzania bezpieczeństwem informacji, z uwzględnieniem wymagań określonych w Polskiej Normie PN-EN ISO/IEC 27001 oraz PN-EN ISO/IEC 22301.	Wyjaśnienie uwagi Pod wpływem różnych uwag koncepcja została zmieniona. Art. 8 ust. 2 zostanie usunięty. W zamian minister właściwy do spraw informatyzacji będzie mógł mapować różne normy/standardy na wymogi ustawowe i rozporządzeń.
393.	Polska Izba Gospodarki Odpadami	Art. 8 ust. 2	1)Art. 1 ust. 12) w zakresie zmiany Art. 8 ust. 2. KSC – wnioskujemy o wskazanie także normy dotyczącej chmury;	Wyjaśnienie uwagi Pod wpływem różnych uwag koncepcja została zmieniona. Art. 8 ust. 2 zostanie usunięty. W zamian minister właściwy do spraw informatyzacji będzie mógł mapować różne normy/standardy na wymogi ustawowe i rozporządzeń.
394.	PTI	Art. 8 ust. 2	Pkt 12, ust. 2: „2. Wymagania, o których mowa w ust. 1, uznaje się za spełnione, gdy podmiot kluczowy i podmiot ważny zapewnia system zarządzania bezpieczeństwem informacji, z uwzględnieniem wymagań określonych w Polskiej Normie PN-EN ISO/IEC 27001 oraz PN-EN ISO 22301.” Przepis jest nieprecyzyjny. Czy ma być to deklaracja? Potwierdzeniem spełnienia wymagań jest certyfikat zgodności dla poprawnie zdefiniowanego zakresu systemu zarządzania bezpieczeństwem informacji, czyli w odniesieniu do KSC, usług świadczonych przez podmiot kluczowy lub podmiot ważny, z wymaganiami norm. Sugeruje się następującą zmianę: „2. Wymagania, o których mowa w ust. 1, uznaje się za spełnione, gdy podmiot kluczowy i podmiot ważny zapewnia system zarządzania bezpieczeństwem informacji, zgodny z wymaganiami ~~z uwzględnieniem wymagań~~ określonymi w Polskiej Normie PN-EN ISO/IEC 27001 oraz PN-EN ISO 22301, co potwierdzają odpowiednie certyfikaty wydane przez akredytowane jednostki certyfikujące lub deklaracja własna podmiotu.”	Wyjaśnienie uwagi Pod wpływem różnych uwag koncepcja została zmieniona. Art. 8 ust. 2 zostanie usunięty. W zamian minister właściwy do spraw informatyzacji będzie mógł mapować różne normy/standardy na wymogi ustawowe i rozporządzeń.
395.	PTI	Art. 8 ust. 2	W zmienionym brzmieniu art. 8 ust. 2 wskazującym na wymagania określone w normach błędnie podano tytuł (organizację) przy których norma jest akredytowana. Dotyczy to normy PN-EN ISO 22301 (norma nie jest akredytowana przy IEC). W obecnym brzmieniu art.10 ust. 3 pkt 3) podano prawidłową nazwę normy jako PN-EN ISO 22301	Wyjaśnienie uwagi Pod wpływem różnych uwag koncepcja została zmieniona. Art. 8 ust. 2 zostanie usunięty. W zamian minister właściwy do spraw informatyzacji będzie mógł mapować różne normy/standardy na wymogi ustawowe i rozporządzeń.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

396.	ZBP	Art. 8 ust. 3	Minister właściwy do spraw informatyzacji może udostępnić w Biuletynie Informacji Publicznej na swojej stronie podmiotowej mapowanie wymogów Polskich Norm, o których mowa w ust. 2, na obowiązki wynikające z ustawy oraz z przepisów wydanych na podstawie art. 8a. Uwaga ogólna Zwracamy uwagę, że mapowanie ułatwiłoby implementację wymagań do już istniejących systemów lub zbudowanie SZBI. Prosimy o rozważenie możliwości wprowadzenia obowiązku udostępnienia takich wymogów.	Wyjaśnienie uwagi Pod wpływem różnych uwag koncepcja została zmieniona. Art. 8 ust. 2 zostanie usunięty. W zamian minister właściwy do spraw informatyzacji będzie mógł mapować różne normy/standardy na wymogi ustawowe i rozporządzeń.
397.	PGE SA	Art. 1 pkt 12, art. 8 ust. 4	Odwołanie w art. 8 ust. 4 powinno być do lit. „d”, tj.: <i>„Wdrażając środki o których mowa w ust. 1 pkt 2 lit. e d podmiot kluczowy i podmiot ważny uwzględnia”</i>	Uwaga uwzględniona Przepis zostanie zmieniony.
398.	Stowarzyszenie Bezpieczeństwo Informacji w Telekomunikacji	Art. 8 ust. 2	W projekcie uKSC zdarzają się odesłania do norm np. Art. 8 ust. 2 zawiera odwołanie do Polskiej Normie PN-EN ISO/IEC 27001 oraz PN-EN ISO/IEC 22301. Wskazane jest aby ustawa zobowiązywała ministra właściwego do spraw cyfryzacji zamieścić na swojej stronie internetowej takie Normy lub istotne ich opracowania. Ponadto np. norma PN-EN ISO/IEC 22301 nie jest dostępna w języku polskim.	Wyjaśnienie uwagi Pod wpływem różnych uwag koncepcja została zmieniona. Art. 8 ust. 2 zostanie usunięty. W zamian minister właściwy do spraw informatyzacji będzie mógł mapować różne normy/standardy na wymogi ustawowe i rozporządzeń. Polskie Normy są chronione prawem autorskim stąd nie jest możliwa ich publikacja na stronie.
399.	TAURON Polska Energia S.A	Art. 8 ust 2	Wymagania, o których mowa w ust. 1, uznaje się za spełnione, gdy podmiot kluczowy i podmiot ważny zapewnia system zarządzania bezpieczeństwem informacji, z uwzględnieniem wymagań określonych w Polskiej Normie PN-EN ISO/IEC 27001 oraz PN-EN ISO/IEC 22301. Określenie „z uwzględnieniem” jest nieprecyzyjne i wprowadza element dowolności w odnoszeniu się do wymagań norm. Normy precyzyjnie określają co jest obowiązkowe, co nie w ich wymaganiach i nie pozostawiają pola do interpretacji i swobodnego wyboru. Stosowanie norm ma sens tylko wtedy kiedy dąży się do zgodności z nimi. Zatem brzmienie zapisu regulacji powinno przywoływać jednoznacznie konieczności zgodności z przedmiotowymi normami. Proponowane brzmienie uwzględniające powyższe: <i>„Wymagania, o których mowa w ust. 1, uznaje się za spełnione, gdy podmiot kluczowy i podmiot ważny zapewnia system zarządzania bezpieczeństwem informacji oraz zarządzania ciągłością działania zgodny z wymaganiami określonymi w Polskiej Normie PN-EN ISO/IEC 27001 oraz PN-EN ISO/IEC 22301.”</i>	Wyjaśnienie uwagi Pod wpływem różnych uwag koncepcja została zmieniona. Art. 8 ust. 2 zostanie usunięty. W zamian minister właściwy do spraw informatyzacji będzie mógł mapować różne normy/standardy na wymogi ustawowe i rozporządzeń.
400.	Stowarzyszenie Bezpieczeństwo Informacji w Telekomunikacji	Art. 8 ust. 3	Art. 8 ust. 3 nadać brzmienie: „Minister właściwy do spraw informatyzacji udostępnia w Biuletynie Informacji Publicznej na swojej stronie podmiotowej mapowanie wymogów Polskich Norm, o których mowa w ust. 2, na obowiązki wynikające z ustawy oraz z przepisów wydanych na podstawie art. 8a.” Ponadto zdefiniować co oznacza pojęcie „mapowanie wymogów Polskich Norm” albo użyć w tym miejscu innego określenia szczegółowo opisującego to przedsięwzięcie.	Wyjaśnienie uwagi Na ten moment zasadne jest wskazanie fakultatywnej kompetencji Ministra. Pojęcie mapowania zostanie zastąpione innym sformułowaniem.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

401.	Morskie Centrum Cyberbezpieczeństwa Akademia Marynarki Wojennej w Gdyni	Art. 8 ust. 4	Art. 6 ust 4 wskazuje na konieczność uwzględniania podczas wdrażania środków ogólnej „jakości produktów ICT, usług ICT i procesów ICT pochodzących od dostawcy sprzętu lub oprogramowania”. Należy do niniejszego punktu dodać również <u>jakość usług zarządzanych w zakresie cyberbezpieczeństwa</u> . Projekt ustawy kilkakrotnie wspomina o tej możliwości, jednak może to zacząć stanowić bardzo duży problem dla podmiotów kluczowych i ważnych, gdyż jakość usług oferowanych przez znaczną część podmiotów jest fatalna. Podmioty te bazując na niewiedzy kadry zarządzającej oferują usługi, które nie są w stanie wygenerować żadnej wartości dodanej. To z kolei będzie można traktować jako marnotrawienie środków publicznych, czego warto zawczasu uniknąć.	Wyjaśnienie uwagi Zawierając umowę z dostawcą usług zarządzanych podmiot kluczowy lub podmiot ważny powinien ująć w niej wymagania jakościowe co do świadczonej usługi wskazując, że jest to wymagane zgodnie z art. 8 KSC.
402.	Osoba fizyczna	Art. 8	Ust. 4 – Wskazano odwołanie do ust. 1 pkt 2 lit. c – prawdopodobnie błędnie, gdyż zakres merytoryczny ustępu 4 w żaden sposób nie odnosi się do bezpieczeństwa fizycznego i środowiskowego, szczególnie że też po wprowadzeniu odniesienia do procesów nie wiadomo, czego bezpieczeństwo fizyczne ma być zapewnione. Proponuję odwołanie do ust. 1.	Uwaga częściowo uwzględniona Zostanie wprowadzone odwołanie do właściwej litery.
403.	KIKE	Art. 8	- poprawienie art. 8 ust. 1 pkt 2 lit. f uKSC w zakresie nieobejmowania podmiotów ważnych obowiązkiem objęcia systemu informacyjnego (chyba informatycznego) wykorzystywanego do świadczenia usługi systemem monitorowania w trybie „ciągłym”. Izba zwraca uwagę, że taki obowiązek nie wynika z przepisów NIS2 oraz jest nieproporcjonalny, zwłaszcza dla podmiotów MŚP. Jego wykonanie wiązałoby się z nieuzasadnionymi kosztami w zakresie zakupu nowych systemów oraz zatrudnienia nowych pracowników. Dotychczas przedsiębiorcy telekomunikacyjni nie mieli obowiązku monitorowania ciągłego swoich systemów i nie ma racjonalnych przesłanek wprowadzenia zmiany tego stanu. Zwracam przy tym na uwagę 12 godzinny termin zgłaszania incydentów poważnych z art. 11 ust. 1a uKSC od ich wykrycia, co wskazuje, że wystarczający będzie system monitorowania raz dziennie.	Wyjaśnienie uwagi Chodzi tutaj o to, aby zapewnić rozliczalność w systemie informacyjnym i analizy zdarzeń, które się wydarzyły. Nie zawsze będzie to oznaczało konieczność zatrudnienia dodatkowych pracowników. Przedsiębiorcy telekomunikacyjni już mają ten obowiązek – wynika on z § 2 pkt 11 rozporządzenie Ministra Cyfryzacji w sprawie minimalnych środków technicznych i organizacyjnych oraz metod, jakie przedsiębiorcy telekomunikacyjni są obowiązani stosować w celu zapewnienia bezpieczeństwa lub integralności sieci lub usług.
404.	KIKE	Art. 8	- zmianę art. 8 ust. 1 pkt 6 uKSC w zakresie stosowania bezpiecznych środków komunikacji elektronicznej w ramach krajowego systemu cyberbezpieczeństwa, uwzględniających uwierzytelnianie wieloskładnikowe. Izba zwraca uwagę, że jest to obowiązek niewynikający z dyrektywy NIS2, generujący duże koszty oraz nieproporcjonalny wobec MŚP. Co więcej, kwestia uwierzytelniania komunikacji poczty elektronicznej była już przedmiotem regulacji w ustawie z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej, gdzie wprowadzono dodatkowe obowiązki na dostawców poczty elektronicznej. Uwierzytelnianie wieloskładnikowe ma być stosowane przy obsłudze podmiotów publicznych a nie w ramach działań podmiotów ważnych czy	Wyjaśnienie uwagi Wymogi dotyczące uwierzytelniania wieloskładnikowego wynikają wprost z art. 21 ust. 2 lit. j dyrektywy NIS 2.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			kluczowych. W opinii Izby dotychczasowe regulacje w tym zakresie są wystarczające, zwłaszcza w stosunku do MŚP.	
405.	KIKE	Art. 8	- zmianę art. 8 ust. 1 pkt 2 lit. d uKSC w zakresie usunięcia obowiązku dla MŚP (lub podmiotów ważnych) obowiązków związanych z procesami ICT. Podmioty ważne jako MŚP nie będą posiadały wiedzy o procesach ICT i nie należy obciążać ich obowiązkami w tym zakresie.	Wyjaśnienie uwagi Generalnie chodzi tutaj o zapewnienie bezpieczeństwa łańcuchów dostaw. Przepis upoważnia podmioty kluczowe i ważne (w tym na pewno średnio przedsiębiorstwa) do np. wprowadzania wymogów z zakresu cyberbezpieczeństwa w umowach z dostawcami procesów.
406.	Konfederacja Lewiatan	Art. 8	Jednostka redakcyjna: art. 8 ust. 1 pkt 2 projektu KSC Jednostka redakcyjna NIS2: 21 ust. 1 Uwaga: Artykuł 21 ust. 1 Dyrektywy NIS2 zobowiązuje państwa członkowskie do zapewnienia, że podmioty kluczowe i ważne wdrażają odpowiednie i proporcjonalne środki techniczne, operacyjne oraz organizacyjne. Wykorzystując najnowszą wiedzę oraz normy europejskie i międzynarodowe, podmioty mają zapewnić poziom bezpieczeństwa adekwatny do istniejącego ryzyka. Istotnym elementem jest tutaj uwzględnienie kosztów wdrożenia tych środków przy ocenie ich proporcjonalności, biorąc pod uwagę wielkość podmiotu oraz prawdopodobieństwo wystąpienia incydentów. Artykuł 8 ust. 1 pkt 2 projektu ustawy, który ma na celu implementację tych wymagań, nie zawiera odniesienia do kosztów wdrożenia jako kryterium oceny proporcjonalności środków. Stanowi to znaczącą różnicę w stosunku do dyrektywy, która podkreśla potrzebę uwzględniania tych kosztów w ocenie proporcjonalności środków zarządzania ryzykiem. Ominięcie rozważań dotyczących kosztów może prowadzić do sytuacji, w której podmioty są zobowiązane do realizacji potencjalnie kosztownych inicjatyw bez względu na ich ekonomiczną wykonalność. Może to nałożyć nadmierne obciążenie finansowe na przedsiębiorstwa, zwłaszcza mniejsze, które mogą nie posiadać zasobów pozwalających spełnić takie rygorystyczne standardy bez kompromisów w innych obszarach działalności.	Wyjaśnienie uwagi W art. 8 w ust. 1 w pkt 2 wprost wskazano, że uwzględnia się koszty wdrożenia środków technicznych i organizacyjnych.
407.	Konfederacja Lewiatan	Art. 8	Jednostka redakcyjna: Art. 8 pkt 2 lit a Przyjmujemy, że wymóg posiadania „ <i>polityki szacowania ryzyka oraz bezpieczeństwa systemu informacyjnego, w tym polityki tematyczne</i> ” stanowi przeniesienie art. 21 ust. 2 lit. a) NIS2 wskazującego na „ <i>politykę analizy ryzyka i bezpieczeństwa systemów informatycznych</i> ;”. Wnosimy jednak o wyjaśnienie dodanego wobec dyrektywy sformułowania „ <i>w tym polityki tematyczne</i> ”. Nie zostało ono zdefiniowane, a dla precyzji przepisów wydaje się to niezbędne.	Wyjaśnienie uwagi Chodziło o <i>topic specific policies</i> które są obecne w normie ISO 27001. Innymi słowy podmiot będzie mógł jeśli będzie to zasadne wprowadzić tematyczną politykę, np. politykę bezpieczeństwa urządzeń mobilnych.
408.	Konfederacja Lewiatan	Art. 8	Jednostka redakcyjna: Art. 8 pkt 2 lit. d	Uwaga uwzględniona Przepis zostanie zmieniony.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			Projektowany przepis zawiera istotne rozszerzenie zakresu badania łańcucha dostaw, wymaganego zgodnie z dyrektywą NIS2 i wprowadza tym samym nadmiarowe obciążenie. Dyrektywa NIS2 wskazuje na „bezpieczeństwo łańcucha dostaw, w tym aspekty związane z bezpieczeństwem dotyczące stosunków między każdym podmiotem a jego <u>bezpośrednimi</u> dostawcami lub usługodawcami” Wnosimy o przyjęcie następującego brzmienia projektu: <i>d) bezpieczeństwo i ciągłość łańcucha dostaw produktów ICT, usług ICT i procesów ICT, od których zależy świadczenie usługi z uwzględnieniem związków pomiędzy <u>bezpośrednim</u> dostawcą sprzętu lub oprogramowania a podmiotem kluczowym lub podmiotem ważnym</i>	
409.	Konfederacja Lewiatan	Art. 8	Jednostka redakcyjna: Art. 8 pkt 2 lit e W doprecyzowaniu dotychczasowego przepisu dodano „ <i>oraz planów awaryjnych umożliwiających odtworzenie systemu informacyjnego po katastrofie</i> ”. Sformułowanie „po katastrofie” nie zostało zdefiniowane. Sugerujemy jego usunięcie lub zdefiniowanie, co może być jednak problematyczne. Możliwe jest też jego zastąpienie zwrotem „po przerwaniu ciągłości jego działania”. Z uwagi na potencjalne kary pieniężne konieczne jest zachowanie maksymalnej precyzji pojęć używanych do opisu wymagań.	Uwaga uwzględniona Zostanie wprowadzona definicja katastrofy do projektu.
410.	Konfederacja Lewiatan	Art. 8	Jednostka redakcyjna: Art. 8 ust. 3 Wnoskujemy o jak najszybsze opublikowanie mapowania wymogów PN na obowiązki wynikające z ustawy i przyszłych rozporządzeń. Wydaje się jednocześnie, że do tego typu zadania nie jest konieczne szczególne upoważnienie ustawowe.	Wyjaśnienie uwagi Pod wpływem różnych uwag koncepcja została zmieniona. Art. 8 ust. 2 zostanie usunięty. W zamian minister właściwy do spraw informatyzacji będzie mógł mapować różne normy/standardy na wymogi ustawowe i rozporządzeń.
411.	Konfederacja Lewiatan	Art. 8	Jednostka redakcyjna: Art. 8 ust. 4 Wnosimy o wprowadzenie zmian w pkt 1: <i>1) podatności związane z dostawcą sprzętu lub oprogramowania, o ile zostaną zidentyfikowane w ramach szacowania ryzyka</i> Wnosimy o wprowadzenie zmiany w pkt 3: <i>3) wyniki skoordynowanej oceny bezpieczeństwa przeprowadzonej przez Grupę współpracy, o której mowa w art. 22 ust. 1 dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniającej rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającą dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz. Urz. UE L 333 z 27.12.2022, str. 80), zwanej dalej „dyrektywą 2022/2555”, o ile zostaną wydane.</i> Wydanie skoordynowanych ocen jest fakultatywne.	Wyjaśnienie uwagi Dodanie tych wyrażen jest nadmiarowe. Natomiast jeśli z powszechnie dostępnych baz CVE jest wiadome o istnieniu podatności to należy je zmiotygować.
412.	Amerykańska Izba Handlowa w Polsce	Art. 8a	Dyrektywa NIS2 przewiduje (art. 25 ust. 1 dyrektywy), że państwa członkowskie mogą wymagać od podmiotów kluczowych i ważnych używania określonych produktów ICT, usług ICT i procesów ICT, opracowanych przez podmiot kluczowy lub ważny, albo pozyskanych od stron trzecich, które są certyfikowane w ramach europejskich schematów certyfikacji cyberbezpieczeństwa przyjętych	Wyjaśnienie uwagi Pierwszy z europejskich programów certyfikacji zacznie obowiązywać od lutego 2025 r. W związku z tym

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			zgodnie z artykułem 49 rozporządzenia (UE) 2019/881. Projekt implementacji nie zobowiązuje podmiotów kluczowych lub ważnych do korzystania z konkretnych produktów ICT. Pojawia się w nim z kolei upoważnienie dla rządu w zakresie wydawania rozporządzeń określających konkretne wymagania dla systemów zarządzania informacją dla różnych rodzajów działalności prowadzonych przez podmioty ważne lub kluczowe. k	wskazanych w uwadze certyfikatów nie ma w obiegu. Dlatego, wprowadzenie takiego obowiązku na obecnym etapie byłoby nieracjonalne.
413.	Apator	Art. 8a	Projektu proponujemy, aby otrzymał brzmienie: <i>Rada Ministrów określi, w drodze rozporządzenia, odrębnie dla danego rodzaju działalności wykonywanej przez podmioty kluczowe lub podmioty ważne szczegółowe wymagania dla systemu zarządzania bezpieczeństwem informacji, o którym mowa w art. 8 ust. 1, biorąc pod uwagę rekomendacje międzynarodowe o charakterze specjalistycznym, w tym rekomendacje Agencji Unii Europejskiej do spraw Cyberbezpieczeństwa, zwanej dalej „ENISA”, skalę działalności wykonywanej przez te podmioty oraz potrzebę podejmowania przez te podmioty działań zapewniających cyberbezpieczeństwo.</i> Uzasadnienie proponowanej zmiany: W naszej opinii niezbędne jest wydanie rozporządzenia wprowadzającego regulacje sektorowe, z uwagi na specyfikę poszczególnych obszarów działalności i duże zróżnicowanie obszarów zagrożonych. Szczegółowe uregulowanie wymagań skierowanych do poszczególnych grup podmiotów mogłoby w istotny sposób ułatwić stosowanie przepisów ustawy, w tym należyte wywiązywanie się z nałożonych ustawą obowiązków. Z tych względów Rada Ministrów powinna mieć nie tylko możliwość, ale wprost obowiązek wydania takiego rozporządzenia. W przygotowaniu takiego rozporządzenia mogłyby w ramach procesu uzgodnień, konsultacji publicznych, opiniowania uczestniczyć podmioty kluczowe i ważne, w tym dostawcy usług, które mają znaczenie z punktu widzenia zarządzania bezpieczeństwem informacji.	Uwaga nieuwzględniona Naszym zdaniem rozporządzenie to nie jest niezbędne do realizacji obowiązków ustawowych. Decyzja o wydaniu rozporządzenia dla danego rodzaju działalności powinna być poprzedzona analizą zasadności jego wydania. Dla niektórych sektorów wystarczające będzie, jeżeli pozostawi się ogólne wymagania ustawowe, a dla niektórych zasadne będzie doszczegółowienie wymagań.
414.	ISAC-Kolej	Art. 8a	„8a. Rada Ministrów może określić, w drodze rozporządzenia, odrębnie dla danego rodzaju działalności wykonywanej przez podmioty kluczowe lub podmioty ważne szczegółowe wymagania dla systemu zarządzania bezpieczeństwem informacji, o którym mowa w art. 8 ust. 1, biorąc pod uwagę rekomendacje międzynarodowe o charakterze specjalistycznym, w tym rekomendacje Agencji Unii Europejskiej do spraw Cyberbezpieczeństwa, zwanej dalej „ENISA”, rekomendacje sektorowych i podsektorowych Agencji Unii Europejskiej, standardy Polskich i Europejskich Organizacji Normalizacyjnych, skalę działalności wykonywanej przez te podmioty oraz potrzebę podejmowania przez te podmioty działań zapewniających cyberbezpieczeństwo. W zapisie tym, biorąc pod uwagę specyfikę działania niektórych podmiotów działających w poszczególnych sektorach lub podsektorach zwłaszcza ściśle regulowanych na poziomie krajowym lub Unii Europejskiej należy uwzględnić rekomendacje sektorowych i podsektorowych Agencji Unii Europejskiej oraz standardy Polskich i Europejskich Organizacji Normalizacyjnych. Jest to o tyle istotne, że niektóre rekomendacje Agencji Unii Europejskiej (np. Europejskiej Agencji Kolejowej – ERA) mogą pośrednio lub bezpośrednio oddziaływać na bezpieczeństwo systemów informacyjnych oraz technologii operacyjnych stosowanych w podsektorze transportu kolejowego.	Wyjaśnienie uwagi Wytyczne uwzględniają także rekomendacje międzynarodowe o charakterze specjalistycznym, w tym także organizacji o których mowa w uwadze.
415.	ISACA	Art. 8a	Art. 8a. Rada Ministrów może określić, w drodze rozporządzenia, odrębnie dla danego rodzaju działalności wykonywanej przez podmioty kluczowe lub podmioty ważne szczegółowe wymagania	Wyjaśnienie uwagi

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			dla systemu zarządzania bezpieczeństwem informacji, o którym mowa w art. 8 ust. 1, biorąc pod uwagę rekomendacje międzynarodowe o charakterze specjalistycznym, w tym rekomendacje Agencji Unii Europejskiej do spraw Cyberbezpieczeństwa, zwanej dalej „ENISA”, skalę działalności wykonywanej przez te podmioty oraz potrzebę podejmowania przez te podmioty działań zapewniających cyberbezpieczeństwo. Proponujemy doprecyzowania, jakiego typu szczegółowe wymagania mogą być określone w tym trybie. "Art. 8a pozwala Radzie Ministrów określać szczegółowe wymagania dla systemu zarządzania bezpieczeństwem informacji, uwzględniając rekomendacje międzynarodowe, skalę działalności podmiotów oraz potrzebę zapewnienia cyberbezpieczeństwa. Wytyczne te wydają się jednak zbyt ogólne i nieprecyzyjne. Należy zweryfikować, czy brak konkretnych wskazówek co do zakresu i treści rozporządzenia nie prowadzi do nadmiernej swobody regulacyjnej Rady Ministrów, co może skutkować znaczną ingerencją w prawa podmiotów. Wytyczne mogłyby być bardziej szczegółowe, aby lepiej spełniać wymogi konstytucyjne dotyczące upoważnień ustawowych, zapewniając większą transparentność i możliwość kontroli sądowej."	Szczegółowe wymagania SZBI określone w rozporządzeniu nie mogą wykraczać poza wymogi określone w art. 8.
416.	Związek Cyfrowa Polska	Art. 8a	W art. 8a wskazano fakultatywną możliwość działania Rady Ministrów w drodze rozporządzenia – o ile to działanie będzie miało charakter wiążący dla przedsiębiorcy, to wyznaczenie Rady Ministrów jako organu właściwego może okazać się nieefektywne dla całego procesu zapewnienia zgodności systemów zarządzania bezpieczeństwem informacji.	Wyjaśnienie uwagi Wprowadzono upoważnienie dla Rady Ministrów, ponieważ zakres dotyczy podmiotów kluczowych i podmiotów ważnych które będą nadzorowane przez wielu ministrów, stąd też wydaje się jednak wskazane, żeby to Rada Ministrów wydała rozporządzenie.
417.	KGHM Polska Miedź S.A.	Art. 8a	Ważne jest, aby w momencie wydania rozporządzeń na podstawie art. 8a wprowadzić adekwatny okres vacatio legis (rekomendujemy nie krótszy niż 6 miesiące), w zakresie dostosowania i wdrożenia w podmiocie zobowiązanym odpowiednich wymagań dla systemu zarządzania informacjami. Adekwatnie do treści uwagi	Wyjaśnienie uwagi Zgodnie z art. 2 Konstytucji i wynikającą z niej zasadą odpowiedniego vacatio legis prawodawca musi zapewnić adekwatny okres dostosowawczy dla adresatów norm prawnych.
418.	PIPC	Art. 8a	Ważne jest, aby w momencie wydania rozporządzeń na podstawie art. 8a wprowadzić adekwatny okres vacatio legis (rekomendujemy nie krótszy niż 6 miesiące), w zakresie dostosowania i wdrożenia w podmiocie zobowiązanym odpowiednich wymagań dla systemu zarządzania informacjami. Adekwatnie do treści uwagi	Wyjaśnienie uwagi Ta kwestia będzie uregulowana w wydawanych rozporządzeniach.
419.	Związek Pracodawców Polska Miedź	Art. 8a	Ważne jest, aby w momencie wydania rozporządzeń na podstawie art. 8a wprowadzić adekwatny okres vacatio legis (rekomendujemy nie krótszy niż 6 miesiące), w zakresie dostosowania i wdrożenia w podmiocie zobowiązanym odpowiednich wymagań dla systemu zarządzania informacjami. Adekwatnie do treści uwagi	Wyjaśnienie uwagi Ta kwestia będzie uregulowana w wydawanych rozporządzeniach.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

420.	Polskie Stowarzyszenie Fotowoltaiki	Art. 8a	Dodatkowe wymagania systemu zarządzania bezpieczeństwem informacji] Obowiązek uwzględnienia dodatkowych wymagań dla systemu zarządzania bezpieczeństwem informacji przyjętych w drodze rozporządzenia Rady Ministrów dla danego rodzaju działalności Ogólny wpływ regulacji: Konieczność spełnienia dodatkowych wymagań dla systemu zarządzania bezpieczeństwem informacji nieokreślonych w ustawie. Brak możliwości oceny rzeczywistego wpływu regulacji. Wpływ na sektor energetyczny: Jak zostało to już wyżej wskazane, sektor energii odgrywa kluczową rolę punktu widzenia planowania strategicznego oraz bezpieczeństwa państwa, w związku z czym jest również jednym z najbardziej uregulowanych sektorów – nie tylko w Polsce, ale w całej Unii Europejskiej. Wprowadzenie dodatkowych obowiązków nałożonych na podmioty z sektora energetycznego uznawane za PK lub PW może prowadzić do powstania złożonego systemu regulacyjnego w zakresie cyberbezpieczeństwa i rozbieżności w zakresie wymogów regulacyjnych względem innych państw UE, co jest jednoznacznie sprzeczne z celem Dyrektywy NIS2. Widzimy zatem potencjalne ryzyko, że nowe obowiązki nakładane na PK lub PW w drodze rozporządzenia zostaną uchwalone bez zachowania spójności z pozostałymi aktami prawnymi regulującymi działalność sektora energetycznego. W konsekwencji, wprowadzanie nowych obowiązków na PK lub PW powinno zostać przeprowadzone z uwzględnieniem specyfiki sektora energetycznego w Polsce. Nadregulacja względem Dyrektywy NIS2] Dyrektywa NIS2 nie przewiduje kompetencji organów krajowych do określania dalej idących wymagań dla systemu zarządzania bezpieczeństwem informacji. Przeciwnie, w celu zachowania spójności na poziomie europejskim, Dyrektywa NIS2 w art. 22 in fine przewiduje kompetencje Komisji Europejskiej do określania wymogów sektorowych. Proponowany przepis może zatem stanowić nadregulację względem Dyrektywy NIS2 a ponadto skutkować, w razie skorzystania z kompetencji przez Radę Ministrów oraz Komisję Europejskiej, nałożeniem podwójnych reżimów w zakresie dodatkowych wymagań dla systemu zarządzania bezpieczeństwem informacji. Co więcej, odmienności krajowych regulacji względem wymogów w innych krajach UE mogą mieć istotnie negatywny wpływ na międzynarodową działalność podmiotów sektora energetycznego. Rekomendacja: - wycofanie przepisu w celu pozostawienia Komisji Europejskiej kompetencji do określania jednolitych dodatkowych wymagań na poziomie unijnym; - niezależnie, w zależności od sektora i podsektora, wymogi odnośnie do systemów zarządzania bezpieczeństwem informacji mogą być odmienne w celu uwzględnienia specyfiki danej branży. W związku z tym wskazane jest, aby dodatkowe wymagania dla systemu zarządzania bezpieczeństwem informacji były:	Wyjaśnienie uwagi Szczegółowe wymagania dot. SZBI, które będą określone w rozporządzeniu nie mogą wychodzić poza zakres SZBI określony w art. 8. Nie są to więc dodatkowe wymagania, tylko doszczegółowienie.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			• opracowywane z uwzględnieniem sektora i podsektora w którym działa PK lub PW, do którego dodatkowe wymogi mają mieć zastosowanie oraz; • opracowane w porozumieniu z przedstawicielami sektora oraz podmiotów posiadających w danym sektorze wiedzę specjalistyczną	
421.	Konfederacja Lewiatan	Art. 8a	Odnotowujemy, że w związku z brakiem publikacji projektów rozporządzeń nie jest możliwe odniesienie do ewentualnego dalszego uszczegółowienia wymagań. Tym samym nie jest możliwe dokonanie oceny przyszłych wymagań. W szczególności jednak dalsze uszczegółowienia wymagań w drodze rozporządzenia nie powinny uniemożliwiać stosowania projektowanego art. 8 ust. 2, który wskazuje, że „Wymagania, o których mowa w ust. 1, uznaje się za spełnione, gdy podmiot kluczowy i podmiot ważny zapewnia system zarządzania bezpieczeństwem informacji, z uwzględnieniem wymagań określonych w Polskiej Normie PN-EN ISO/IEC 27001 oraz PN-EN ISO/IEC 22301”. Apelujemy, aby projekty rozporządzeń zostały opublikowane jak najszybciej. Podkreślamy jednocześnie, że przyjęte podejście musi uwzględniać sytuację podmiotów, które będą kwalifikowały się jako kluczowe lub ważne w ramach kilku rodzajów działalności. W upoważnieniu przewiduje się natomiast możliwość wydania różnych rozporządzeń np. wobec działalności telekomunikacyjnej, chmury obliczeniowej lub centrów danych, które często będą łączone w ramach jednego podmiotu. Ewentualne zróżnicowanie wymagań szczegółowych może poważnie utrudniać wdrożenie. W naszej ocenie należy przede wszystkim unikać zróżnicowania wymagań w ramach poszczególnych sektorów. Poza powyższym, zauważamy również, że zgodnie z samą dyrektywą NIS2: <i>Do 17 października 2024 r. Komisja przyjmuje akty wykonawcze określające wymogi techniczne i metodykę dotyczącą środków, o których mowa w ust. 2, w odniesieniu do dostawców usług DNS, rejestrów nazw TLD, dostawców usług chmurowych, dostawców usług ośrodka przetwarzania danych, dostawców sieci dostarczania treści, dostawców usług zarządzanych, dostawców usług zarządzanych w zakresie bezpieczeństwa, dostawców internetowych platform handlowych, wyszukiwarek internetowych oraz platform sieci społecznościowych i dostawców usług zaufania. Komisja może przyjąć akty wykonawcze określające wymogi techniczne i metodykę, a w razie potrzeby również wymogi sektorowe dotyczące środków, o których mowa w ust. 2, w odniesieniu do podmiotów kluczowych i ważnych innych niż te, o których mowa w akapicie pierwszym niniejszego ustępu.</i> Powyższe oznacza, że na obecnym etapie nie jest możliwe odniesienie się do szczegółowych wymagań, a sam projekt ustawy nie dostarcza informacji istotnie wykraczających poza same ogólne sformułowania dyrektywy NIS2. W praktyce ogranicza to możliwość rozpoczęcia przygotowań zorientowanych na osiągnięcie oczekiwanych regulacyjnie efektów.	Wyjaśnienie uwagi Rozporządzenia są fakultatywne i w tej chwili nie przewidujemy ich wydania. Jeśli będą wydane to muszą zawierać odpowiednie vacatio legis oraz muszą być zgodne z prawem unijnym także z aktami wykonawczymi KE.
422.	Związek Telewizji Kablowych Izba Gospodarcza	Art. 8a	Zupełnie niezrozumiałe jest dla czegoż to woła projektodawcy Rada Ministrów, która jedynie może określić w drodze rozporządzenia odrębnie dla każdego rodzaju działalności wykonywanej przez podmioty kluczowe lub podmioty ważne szczegółowe wymagania dla systemu zarządzania bezpieczeństwem informacji miałyby brać pod uwagę rekomendacje międzynarodowe o charakterze specjalistycznym, w tym rekomendacje Agencji Unii Europejskiej do spraw Cyberbezpieczeństwa,	Wyjaśnienie uwagi Jest to element wytycznych. Agencja ENISA tworzy bardzo dobre materiały, wspomagając przez to państwa

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			zwanej dalej ENISA, w sytuacji gdy tego rodzaju rekomendacje nie stanowią ani źródła prawa unijnego, gdyż nie zostały wymienione w art. 288 zd. 1 Traktatu o funkcjonowaniu Unii Europejskiej, ani też nie stanowią przepisów prawa powszechnie obowiązującego w ujęciu art. 87 Konstytucji RP. Nie wiadomo skąd u Ministra Cyfryzacji nieprzeparte dążenie do nakładania na Radę Ministrów obowiązku uwzględniania dodatkowych wymogów opartych na aktach nie stanowiących źródła prawa ani krajowego, ani też wspólnotowego. Proponujemy zatem wprowadzenie zmiany art. 1 pkt. 13 projektu ustawy zmieniającej ustawę o KSC zasadzającą w wykreśleniu z dodawanego art. 8 a ustawy o KSC słów w brzmieniu „<i>rekomendacje międzynarodowe o charakterze specjalistycznym, w tym rekomendacje Agencji Unii Europejskiej do spraw Cyberbezpieczeństwa, zwanej dalej „ENISA”</i>” oraz następującego po tej treści przecinka.	członkowskie w tworzeniu przepisów prawa.
423.	Polska Izba Informatyki i Telekomunikacji	Art. 8a	Odnotowujemy, że w związku z brakiem publikacji projektów rozporządzeń nie jest możliwe odniesienie do ewentualnego dalszego uszczegółowienia wymagań. Tym samym nie jest możliwe dokonanie oceny przyszłych wymagań. W szczególności jednak dalsze uszczegółowienia wymagań w drodze rozporządzenia nie powinny uniemożliwiać stosowania projektowanego art. 8 ust. 2, który wskazuje, że „Wymagania, o których mowa w ust. 1, uznaje się za spełnione, gdy podmiot kluczowy i podmiot ważny zapewnia system zarządzania bezpieczeństwem informacji, z uwzględnieniem wymagań określonych w Polskiej Normie PN-EN ISO/IEC 27001 oraz PN-EN ISO/IEC 22301”. Apelujemy, aby projekty rozporządzeń zostały opublikowane jak najszybciej. Podkreślamy jednocześnie, że przyjęte podejście musi uwzględniać sytuację podmiotów, które będą kwalifikowały się jako kluczowe lub ważne w ramach kilku rodzajów działalności. W upoważnieniu przewiduje się natomiast możliwość wydania różnych rozporządzeń np. wobec działalności telekomunikacyjnej, chmury obliczeniowej lub centrów danych, które często będą łączone w ramach jednego podmiotu. Ewentualne zróżnicowanie wymagań szczegółowych może poważnie utrudniać wdrożenie. W naszej ocenie należy przede wszystkim unikać zróżnicowania wymagań w ramach poszczególnych sektorów. Poza powyższym, zauważamy również, że zgodnie z samą dyrektywą NIS2: Do 17 października 2024 r. Komisja przyjmuje akty wykonawcze określające wymogi techniczne i metodykę dotyczącą środków, o których mowa w ust. 2, w odniesieniu do dostawców usług DNS, rejestrów nazw TLD, dostawców usług chmurowych, dostawców usług ośrodka przetwarzania danych, dostawców sieci dostarczania treści, dostawców usług zarządzanych, dostawców usług zarządzanych w zakresie bezpieczeństwa, dostawców internetowych platform handlowych, wyszukiwarek internetowych oraz platform sieci społecznościowych i dostawców usług zaufania. Komisja może przyjąć akty wykonawcze określające wymogi techniczne i metodykę, a w razie potrzeby również wymogi sektorowe dotyczące środków, o których mowa w ust. 2, w odniesieniu do podmiotów kluczowych i ważnych innych niż te, o których mowa w akapicie pierwszym niniejszego ustępu. Powyższe oznacza, że na obecnym etapie nie jest możliwe odniesienie się do szczegółowych wymagań, a sam projekt ustawy nie dostarcza informacji istotnie wykraczających poza same ogólne	Wyjaśnienie uwagi W tej chwili nie jest planowane wydanie rozporządzeń na podstawie art. 8a. Ew. wydane rozporządzenia muszą być zgodne z aktami KE.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			sformułowania dyrektywy NIS2. W praktyce ogranicza to możliwość rozpoczęcia przygotowań zorientowanych na osiągnięcie oczekiwanych regulacyjnie efektów.	
424.	Osoba fizyczna	Art. 8h	Ust. 1 pkt 2) – proponuję modyfikacje treści na: zwiększa poziom cyberbezpieczeństwa i bezpieczeństwa systemu informacyjnego, ... [zgodnie z definicjami uKSC2 bezpieczeństwo systemów informacyjnych i cyberbezpieczeństwo to różne, niepokrywające się zakresy pojęciowe].	Uwaga nieuwzględniona Dyrektywa NIS2 odnosi się tutaj do pojęcia cyberbezpieczeństwa Art. 29 ust. 1 lit. b (b) enhances the level of cybersecurity
425.	KIKE	Art. 8 i 10	zmianę lub uzupełnienie art. 8 ust. 2 i art. 10 ust. 3 pkt 1 i 3 uKSC w zakresie stosowanych norm. W opinii Izby należy albo usunąć wskazanie tych norm (przynajmniej w zakresie podmiotów ważnych lub w ogóle MŚP) lub też dodać, że jest możliwe stosowanie norm równoważnych do wymienionych w przepisie.	Wyjaśnienie uwagi Pod wpływem różnych uwag koncepcja została zmieniona. Art. 8 ust. 2 zostanie usunięty. W zamian minister właściwy do spraw informatyzacji będzie mógł mapować różne normy/standardy na wymogi ustawowe i rozporządzeń.
426.	Polskie Stowarzyszenie Fotowoltaiki	Art. 8b	Obowiązek zastosowania zasad dotyczących aspektów cyberbezpieczeństwa w transgranicznych przepływach energii elektrycznej przyjętych na podstawie Pr. Energ. przez podmioty kluczowe z podsektora energii elektrycznej realizujących zadania określone w art. 9 ust. 3 i 4 Pr. Energ. Wpływ na sektor energetyczny: Zwracamy uwagę, że jak zostało to wskazane w samej Dyrektywie NIS2 (motyw 4), wymogi nałożone przez jedno państwo członkowskie, które różnią się od wymogów nałożonych przez inne państwo członkowskie lub nawet są z nimi sprzeczne, mogą w istotny sposób wpływać na transgraniczną działalność poszczególnych podmiotów, oferujących towary transgranicznie. Należy mieć na uwadze, iż odmienne regulacje w zakresie cyberbezpieczeństwa pomiędzy poszczególnymi krajami członkowskimi mogą nie tylko opóźniać, ale i utrudniać proces transgranicznych przepływów energii elektrycznej. W tym kontekście, zaproponowane w Projekcie nadregulacje mogą wywrzeć negatywny wpływ na poziom cyberbezpieczeństwa innych państw członkowskich – wszelkie rozbieżności w implementacji Dyrektywy NIS2 mogą powodować fragmentację rynku wewnętrznego, oddziałując na transgraniczne świadczenie usług oraz poziom cyberbezpieczeństwa ze względu na stosowanie różnych środków przez poszczególne państwa członkowskie. Ponadto, odmienne regulacje mogą w konsekwencji prowadzić do większej podatności na cyberzagrożenia przez niektóre państwa członkowskie. [Stosunek do Dyrektywy NIS2] Celem Dyrektywy NIS2 jest wyeliminowanie rozbieżności w zakresie regulacji dotyczących cyberbezpieczeństwa we wszystkich krajach członkowskich, w szczególności przez określenie przepisów minimalnych dotyczących funkcjonowania skoordynowanych ram regulacyjnych, ustanowienie mechanizmów skutecznej współpracy między odpowiedzialnymi organami w poszczególnych państwach członkowskich, zaktualizowanie wykazu sektorów i działań podlegających obowiązkowi w zakresie cyberbezpieczeństwa oraz wprowadzenie skutecznych	Uwaga uwzględniona Przepisy dotyczące stosowania Rozporządzenia delegowanego Komisji (UE) 2024/1366 z dnia 11 marca 2024 r. uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/943 poprzez ustanowienie kodeksu sieci dotyczącego zasad sektorowych w zakresie aspektów cyberbezpieczeństwa w transgranicznych przepływach energii elektrycznej zostaną uwzględnione w przepisach.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			środków naprawczych i środków egzekwowania, które są kluczowe dla skutecznego egzekwowania tych obowiązków. Rekomendacje: W tym kontekście, implementacja Dyrektywy NIS2 powinna zostać przeprowadzona z uwzględnieniem zasady proporcjonalności oraz minimalnej harmonizacji.	
427.	Konfederacja Lewiatan	Art. 8b	Projektowany przepis wprowadza obowiązek podmiotów objętych tzw. rozporządzeniem systemowym do stosowania zasad <i>dotyczących aspektów cyberbezpieczeństwa w transgranicznych przepływach energii elektrycznej, w tym zasad dotyczących wspólnych wymogów minimalnych, planowania, monitorowania, sprawozdawczości i zarządzania kryzysowego odpowiednio</i> . Zauważamy, że rozporządzenie obejmuje także spółki obrotu, których dotyczy rzdz. 3 pt. <i>Sposób prowadzenia obrotu energią elektryczną</i> . Przepisy te nie dotyczą kwestii cyberbezpieczeństwa w transgranicznych przepływach. Wydaje się, że stosowanie tych wymagań do spółek obrotu jest nieadekwatne i powinno zostać wyraźnie wyłączone.	Wyjaśnienie uwagi Przepisy dotyczące stosowania Rozporządzenia delegowanego Komisji (UE) 2024/1366 z dnia 11 marca 2024 r. uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/943 poprzez ustanowienie kodeksu sieci dotyczącego zasad sektorowych w zakresie aspektów cyberbezpieczeństwa w transgranicznych przepływach energii elektrycznej zostaną uwzględnione w przepisach.
428.	Polska Izba Informatyki i Telekomunikacji	Art. 8b	Projektowany przepis wprowadza obowiązek podmiotów objętych tzw. rozporządzeniem systemowym do stosowania zasad <i>dotyczących aspektów cyberbezpieczeństwa w transgranicznych przepływach energii elektrycznej, w tym zasad dotyczących wspólnych wymogów minimalnych, planowania, monitorowania, sprawozdawczości i zarządzania kryzysowego odpowiednio</i> . Zauważamy, że rozporządzenie obejmuje także spółki obrotu, których dotyczy rozdz. 3 pt. <i>Sposób prowadzenia obrotu energią elektryczną</i> . Przepisy te nie dotyczą kwestii cyberbezpieczeństwa w transgranicznych przepływach. Wydaje się, że stosowanie tych wymagań do spółek obrotu jest nieadekwatne i powinno zostać wyraźnie wyłączone.	Wyjaśnienie uwagi Zrezygnowano z tego przepisu.
429.	CyberMadeinPoland	Art. 8c	W dodanym artykule 8c pkt 3 należy doprecyzować odpowiedzialność kierownika podmiotu kluczowego także w przypadku gdy wszystkie obowiązki wynikające ze zmienionej ustawy zostały powierzone innej osobie za jej zgodą (wersja w projekcie wskazuje jedynie na przekazanie „niektórych obowiązków”)	Uwaga uwzględniona
430.	ISAC-Kolej	Art. 8c	„2. W przypadku, gdy kierownikiem podmiotu kluczowego lub podmiotu ważnego jest organ wieloosobowy i nie została wskazana w sposób formalny osoba odpowiedzialna, odpowiedzialność ponoszą wszyscy członkowie tego organu Wskazanie kierownika podmiotu kluczowego lub podmiotu ważnego powinno nastąpić w sposób formalny w trybie przewidzianym w danym podmiocie (uchwała, zarządzanie, decyzja).	Wyjaśnienie uwagi Kwestia ta wychodzi poza zakres ustawy, stosują się tutaj ogólne przepisy ustrojowe dla danego rodzaju podmiotu np. Kodeks spółek handlowych.
431.	ISAC-Kolej	Art. 8c	„3. Kierownik podmiotu kluczowego lub podmiotu ważnego ponosi odpowiedzialność także wtedy, gdy niektóre z obowiązków zostały powierzone innej osobie w sposób formalny i udokumentowany za jej zgodą”	Wyjaśnienie uwagi Kwestia ta wychodzi poza zakres ustawy, stosują się tutaj ogólne przepisy np. Kodeksu pracy czy kodeksu cywilnego,

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			Obowiązki kierownika podmiotu kluczowego lub podmiotu ważnego powinny zostać powierzone ewentualnie innej osobie, ale w sposób formalny przyjęty w danym pomioście (uchwała, zarządzenie, decyzja).	ew. kodeksu spółek handlowych albo inne przepisy właściwe dla danego rodzaju podmiotu.
432.	PTI	Art. 8c	W dodanym artykule 8c pkt 3 należy doprecyzować odpowiedzialność kierownika podmiotu kluczowego, także w przypadku, gdy wszystkie obowiązki wynikające ze zmienionej ustawy zostały powierzone innej osobie za jej zgodą (wersja w projekcie wskazuje jedynie na przekazanie „niektórych obowiązków”)	Uwaga uwzględniona
433.	PGE SA	Art. 8c ust. 2 i ust. 3 ustawy	Postanowienia art. 8c ust. 2 i ust. 3 są mało precyzyjne i można je interpretować jako wykluczające się. Jeżeli dobrze odczytujemy intencję punktów, to powinny być zmienione przez precyzyjne wskazanie, iż w ust. 2 chodzi o osobę wskazaną - członka Zarządu, a w ust. 3 osobę nie będącą członkiem Zarządu.	Wyjaśnienie uwagi Jest to dobra interpretacja, ale jednak nie uważamy zmiany przepisów za koniecznej.
434.	ZPP	Art. 8c do 8e i art. 73a	ODPOWIEDZIALNOŚĆ ZARZĄDZAJĄCYCH Zgodnie z dyrektywą NIS2, państwa członkowskie muszą zapewnić, że zarządy kluczowych i ważnych podmiotów zatwierdzają i nadzorują wdrażanie środków zarządzania ryzykiem cyberbezpieczeństwa, zgodnie z artykułem 21. Odpowiedzialność za naruszenia tego artykułu może spoczywać na tych organach. Polski projekt implementacji określa obowiązki zarządów oraz zasady dotyczące kar finansowych (artykuł 8c do 8e i artykuł 73a). Kara może być nałożona, jeśli zarząd nie spełni swoich obowiązków lub jeśli podmiot nie wypełni swoich obowiązków wynikających z implementacji NIS2. Kara nie może przekroczyć 600% wynagrodzenia ukaranej osoby. Te przepisy różnią się od zasad określonych w dyrektywie, ponieważ nie uwzględniają zdolności finansowej osoby karanej. Ponadto, artykuł 53 ust. 1 projektu daje władzom szersze uprawnienia egzekucyjne, w tym możliwość zawieszenia lub cofnięcia licencji, usunięcia z rejestru działalności, czasowego zakazu pełnienia funkcji przez zarząd oraz nakazu przeprowadzania audytów bezpieczeństwa. Rozszerzenie tych uprawnień może prowadzić do nadmiernej ingerencji w działalność podmiotów, co może destabilizować ich funkcjonowanie. Zalecamy ponowną analizę przepisów w celu znalezienia bardziej zrównoważonego rozwiązania, które zapewni bezpieczeństwo, minimalizując jednocześnie ryzyko nadmiernych obciążeń i zakłóceń.	Wyjaśnienie uwagi W projekcie jest wprost napisane, że ustalając wymiar kary bierze się pod uwagę możliwości finansowe kierownika podmiotu.
435.	Polskie Stowarzyszenie Fotowoltaiki	Art. 8c	- Kierownik lub członkowie organu kierowniczego podmiotu kluczowego lub podmiotu ważnego ponoszą odpowiedzialność za wykonywanie obowiązków w zakresie cyberbezpieczeństwa przez PK lub PW, o których mowa w art. 7, art. 8, art. 8d, art. 8e, art. 8f ust. 2, art. 8h, art. 9–11 i art. 15 KSC wg Projektu. - Projekt przewiduje odpowiedzialność każdego z członków organu, o ile nie została wskazana osoba odpowiedzialna. - Projekt przewiduje odpowiedzialność kierownika podmiotu kluczowego lub podmiotu ważnego w razie powierzenia obowiązków innej osobie. Ogólny wpływ regulacji: Zakres odpowiedzialności za wykonywanie obowiązków, o których mowa w przepisie:	Uwaga nieuwzględniona Naszym zdaniem przepis art. 8c odpowiada dyrektywie. Celem jest wskazanie zakresu odpowiedzialności kierowników podmiotów kluczowych/ważnych, aby zaczęli doceniać kwestię cyberbezpieczeństwa.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			- obejmuje czynności, co do których PK lub PW nie jest zobowiązany – m.in. uczestnictwo w wymianie informacji dotyczących cyberbezpieczeństwa zgodnie z art. 8h ust. 1 KSC wg Projektu; - wykracza istotnie poza zakres podstaw nałożenia kary pieniężnej na kierownika PK lub PW zgodnie z art. 73a KSC wg Projektu. Wpływ na sektor energetyczny: jw. – brak specyficznego wpływu na sektor energetyczny [Nadregulacja względem Dyrektywy NIS2] Dyrektywa NIS2 zobowiązuje do zapewnienia, aby osoby fizyczne odpowiedzialne za PK i PW mogły być pociągnięte do odpowiedzialności za niewywiązanie się z obowiązku zapewnienia przestrzegania niniejszej dyrektywy. Dyrektywa NIS2 nie wskazuje jednak odrębnego katalogu obowiązków wobec tych osób niezależnych od obowiązków PK lub PW (z wyłączeniem zapewnienia, że odbywają one regularne szkolenia z zakresu cyberbezpieczeństwa – vide art. 20 ust. 2 Dyrektywy NIS2) Rekomendacja: Dostosowanie zakresu odpowiedzialności kierownika lub członków organu kierowniczego PK lub PW do zakresu obowiązków PK lub PW i określenie tej odpowiedzialności w sposób minimalny, wymagany Dyrektywą NIS2. Zob. dodatkowe uwagi do Art. 8d – 8f KSC wg Projektu.	
436.	Morskie Centrum Cyberbezpieczeństwa Akademia Marynarki Wojennej w Gdyni	Art. 8d	W art. 8d wskazane jest 5 ogólnych odpowiedzialności kierowników podmiotów kluczowych lub ważnych. Wydaje się zasadne z punktu widzenia późniejszego rozliczania słuszności podejmowanych przez nich decyzji dodanie punktów dotyczących: • <u>zatrudniania kompetentnych pracowników;</u> • <u>wdrażania rekomendacji płynących z audytów.</u> Pragniemy również zwrócić uwagę, że nie każdy kierownik będzie posiadać wiedzę w tym zakresie. Należy też tym samym podkreślić w ustawie, że w tym zakresie kierownik powinien być <u>wspierany przez Radę Nadzorczą</u>, jeśli tylko taka funkcjonuje. Jednocześnie proponujemy wskazanie w ustawie <u>sankcji nakładanych imiennie na członków zarządu</u>, którzy swoimi decyzjami działali <u>wbrew wnioskowi płynącemu z samodzielnie przeprowadzanych w organizacji analiz ryzyka</u>.	Wyjaśnienie uwagi Aby realizować zadania z zakresu cyberbezpieczeństwa należy zatrudnić kompetentne osoby. Rekomendacje z audytu nie mają charakteru władczego. Nie jest rolą Rady Nadzorczej wspieranie kierownika podmiotu.
437.	ISAC-Kolej	Art. 8d	„1) „podejmuje decyzje w zakresie przygotowania, wdrażania, stosowania i przeglądu systemu zarządzania bezpieczeństwem informacji, systemu bezpieczeństwa systemów sterowania i automatyki przemysłowej oraz systemu zarządzania ciągłością działania w podmiocie” System zarządzania bezpieczeństwem informacji nie jest jedynym systemem zarządzania odnoszącym się do wszystkich zadań realizowanych przez podmiot kluczowy lub podmiot ważny. Oprócz systemu zarządzania bezpieczeństwem informacji ustawa wskazuje również system zarządzania ciągłości działania, a opcjonalnie również podmiot w zakresie stosowanych technologii operacyjnych zobowiązany będzie wdrożyć i stosować system bezpieczeństwa systemów sterowania i	Uwaga nieuwzględniona Jak już wskazywano wyżej, definicja systemu informacyjnego obejmuje systemy OT, więc nie ma potrzeby zmiany przepisów.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			automatyki przemysłowej (wynikający z normy ISO62443 lub norm branżowych mających zastosowanie w pomiotach danego sektora lub podsektora)	
438.	TAURON Polska Energia S.A	Art. 8d pkt 1	1) podejmuje decyzje w zakresie przygotowania, wdrażania, stosowania i przeglądu systemu zarządzania bezpieczeństwem informacji w podmiocie; Zgodnie z przywołanymi w regulacji normami dotyczącymi systemów zarządzania, kierownictwo ma również określone istotne obowiązki wynikające z norm. Wydaje się, że brzmienie tego zapisu powinno być poszerzone o odniesienie się do tych obowiązków. Proponowane brzmienie uwzględniające powyższe: „ 1) podejmuje decyzje w zakresie przygotowania, wdrażania, stosowania systemu zarządzania bezpieczeństwem informacji oraz systemu zarządzania ciągłością działania; 2) realizuje obowiązki wynikające ze stosowania systemów zarządzania wymienionych, w tym realizuje przeglądy systemów zarządzania wymienionych w 1).”	Wyjaśnienie uwagi Kwestie te mieszczą się w art. 8d pkt 1.
439.	ISACA	Art. 8d	"Kierownik (...) zapewnia, że personel podmiotu jest świadomy obowiązków z zakresu cyberbezpieczeństwa i zna przepisy prawa oraz wewnętrzne regulacje podmiotu w tym zakresie; " Wykreślić "i zna przepisy prawa" Wymaganie jest nadmiarowe w stosunku do całego personelu	Uwaga uwzględniona Przepis zostanie zmieniony.
440.	ISACA	Art. 8d	"W szczególności nigdzie nie jest wskazane jednoznacznie, że organ zarządzający (tu kierownik podmiotu) ma zatwierdzać środki zarządzania ryzykiem oraz nadzorować ich wdrażanie. Zapis proponowanego art. 8d pkt 1 w brzmieniu „podejmuje decyzje w zakresie przygotowania, wdrażania, stosowania i przeglądu systemu zarządzania bezpieczeństwem informacji w podmiocie” nie zapewnia osobistego wykonywania czynności wymaganych w NIS2. Zatwierdzanie „środków postępowania z ryzykiem” nie jest równoznaczne z planowaniem „środków finansowych na realizację obowiązków z zakresu cyberbezpieczeństwa” (art. 8d pkt 2 projektu). Zapewnienie zgodności (art. 8d pkt 5) nie jest równoznaczne z nadzorowaniem wdrażania, ze szczególnym uwzględnieniem skuteczności, o której mowa w art. 8 ust. 1 pkt 2 lit. g." zapis art. 8d wymaga dogłębnego przerehabrowania zgodnie z NIS2 "Transpozycja nie wyczerpuje regulacji zawartej w Dyrektywie [NIS2 art. 20 ust. 1] Państwa członkowskie zapewniają, aby organy zarządzające podmiotów kluczowych i ważnych zatwierdzały środki zarządzania ryzykiem w cyberbezpieczeństwie przyjęte przez te podmioty w celu zapewnienia zgodności z art. 21, nadzorowały ich wdrażanie i mogły być pociągnięte do odpowiedzialności za naruszanie przez te podmioty tego artykułu. Stosowanie niniejszego ustępu nie narusza przepisów krajowych dotyczących zasad odpowiedzialności instytucji publicznych oraz odpowiedzialności urzędników publicznych oraz urzędników wybranych lub mianowanych.	Uwaga częściowo uwzględniona Art. 8d pkt 1 zostanie uzupełniony o kwestie nadzorcze. Celowo wskazano konieczność adekwatnego planowania środków finansowych, aby wzmocnić pozycję osób odpowiedzialnych za cyberbezpieczeństwo w podmiotach.
441.	Osoba fizyczna	Art. 8d	Osobami zobowiązanymi do corocznego uczestnictwa w szkoleniach z zakresu cyberzagrożeń powinny być oprócz kierownictwa podmiotu kluczowego również osoby upoważnione przez kierownictwo do realizacji obowiązków wynikających z bycia podmiotem kluczowym.	Wyjaśnienie uwagi

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			<u>Uzasadnienie:</u> Takie osoby będą wykonywały wszystkie czynności związane z wykonywaniem obowiązków podmiotu kluczowego i raportowały do kierownictwa podmiotu kluczowego a także kontaktowały się z CESIRT sektorowym więc powinny również podlegać takiemu obowiązkowi.	W tym zakresie dyrektywa przewiduje tylko zachęcanie do szkoleń. Kwestie są już objęte art. 8.
442.	Konfederacja Lewiatan	Art. 8d	Projektowany przepis wymaga, aby kierownik zapewniał „<i>że personel podmiotu jest świadomy obowiązków z zakresu cyberbezpieczeństwa i zna przepisy prawa oraz wewnętrzne regulacje podmiotu w tym zakresie</i>”. W naszej ocenie przepis ten jest zdecydowanie nadmiarowy i zupełnie pomija specyfikę działania firm, a w szczególności dużych organizacji. Taka redakcja przepisu może być adekwatna jedynie w przypadku podmiotów o ścisłej specjalizacji, gdzie faktyczna wiedza prawna (sic!) jest wymagana dla prawidłowej realizacji obowiązków. Szeroko rozumianym personelem pracowników są też osoby zupełnie niezwiązane z systemami informatycznymi i usługami kluczowymi lub krytycznymi. Wymaganie od nich posiadania specjalistycznej wiedzy prawnej w obszarze cyberbezpieczeństwa jest skrajnie nieuzasadnione. Przyjmujemy oczywiście, że ogólna wiedza o cyberbezpieczeństwie jest istotna z uwagi na różne wektory ataków, ale musi ona być dostosowywana do konkretnych potrzeb na różnych stanowiskach pracy. W motywie 89 NIS2, wskazano: „<i>szkolenia dla pracowników oraz szerzyć wiedzę na temat cyberzagrożeń, phishingu lub technik inżynierii społecznej</i>”. W art. 20 ust. 2 wskazano natomiast, aby państwa członkowskie „<i>zachęcały podmioty kluczowe i ważne do oferowania podobnych (jak kierownikom) szkoleń ich pracownikom</i>”. Z tych względów proponujemy poniższe brzmienie: 4) <u>zapewnia, że personel podmiotu ma dostęp do szkoleń dotyczących cyberzagrożeń, phishingu lub technik inżynierii społecznej, jest świadomy</u> obowiązków z zakresu cyberbezpieczeństwa, ~~i zna~~ przepisów prawa oraz wewnętrznych regulacji podmiotu w tym zakresie;	Uwaga uwzględniona Usunięty zostanie wymóg wiedzy o przepisach prawa z zakresu cyberbezpieczeństwa.
443.	Polska Izba i Informatyki i Telekomunikacji	Art. 8d	Projektowany przepis wymaga, aby kierownik zapewniał „<i>że personel podmiotu jest świadomy obowiązków z zakresu cyberbezpieczeństwa i zna przepisy prawa oraz wewnętrzne regulacje podmiotu w tym zakresie</i>”. W naszej ocenie przepis ten jest zdecydowanie nadmiarowy i zupełnie pomija specyfikę działania firm, a w szczególności dużych organizacji. Taka redakcja przepisu może być adekwatna jedynie w przypadku podmiotów o ścisłej specjalizacji, gdzie faktyczna wiedza prawna (sic!) jest wymagana dla prawidłowej realizacji obowiązków. Szeroko rozumianym personelem pracowników są też osoby zupełnie niezwiązane z systemami informatycznymi i usługami kluczowymi lub krytycznymi. Wymaganie od nich posiadania specjalistycznej wiedzy prawnej w obszarze cyberbezpieczeństwa jest skrajnie nieuzasadnione. Przyjmujemy oczywiście, że ogólna wiedza o cyberbezpieczeństwie jest istotna z uwagi na różne wektory ataków, ale musi ona być dostosowywana do konkretnych potrzeb na różnych stanowiskach pracy. W motywie 89 NIS2, wskazano: „<i>szkolenia dla pracowników oraz szerzyć wiedzę na temat cyberzagrożeń, phishingu lub technik inżynierii społecznej</i>”. W art. 20 ust. 2 wskazano natomiast, aby	Uwaga nieuwzględniona Kwestie szkoleń i edukacji z zakresu cyberbezpieczeństwa są już ujęte w art. 8.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			państwa członkowskie „zachęcały podmioty kluczowe i ważne do oferowania podobnych (jak kierownikom) szkoleń ich pracownikom.”. Z tych względów proponujemy poniższe brzmienie: 4) <i>zapewnia, że personel podmiotu ma dostęp do szkoleń dotyczących cyberzagrożeń, phishingu lub technik inżynierii społecznej, jest świadomy obowiązków z zakresu cyberbezpieczeństwa, i zna przepisy prawa oraz wewnętrznych regulacji podmiotu w tym zakresie;</i>	
444.	Polskie Stowarzyszenie Fotowoltaiki	Art. 8d-8f	Projekt przewiduje nałożenie na kierownika PK lub PW poniższych obowiązków i wymogów: - podejmowanie decyzji w zakresie systemu zarządzania bezpieczeństwem informacji; - zabezpieczenie środków finansowych na realizację obowiązków związanych z cyberbezpieczeństwem; - zarządzanie zadaniami z zakresu cyberbezpieczeństwa; - zapewnienie świadomości personelu z zakresu cyberbezpieczeństwa i obowiązków; - zapewnienie zgodności działania z przepisami prawa i wewnętrznymi regulacjami; - udokumentowany udział w szkoleniu z zakresu wykonywania obowiązków dot. cyberbezpieczeństwa co najmniej raz w roku; - brak uprzedniego skazania za przestępstwa przeciwko ochronie informacji (weryfikacja niekaralności przez PK/PW). Ogólny wpływ regulacji: Obowiązki wskazane w przepisach Projektu odnoszą się bezpośrednio do kierownika PK lub PW i są niezależne od obowiązków PK i PW w zakresie cyberbezpieczeństwa. W rezultacie skutkuje to koniecznością zapewnienia przez PK i PW zgodności z wymogami na dwóch płaszczyznach. Wpływ na sektor energetyczny: jw. – brak specyficznego wpływu na sektor energetyczny [Nadregulacja względem Dyrektywy NIS2] Dyrektywa NIS2 nie nakłada na kierowników PK i PW dodatkowych wymogów niezależnych od obowiązków samych PK i PW (z wyłączeniem zapewnienia, że odbywają oni regularne szkolenia z zakresu cyberbezpieczeństwa – vide art. 20 ust. 2 Dyrektywy NIS2), a jedynie zobowiązuje do zapewnienia możliwości pociągnięcia tych osób do odpowiedzialności w razie naruszenia wymogów przez PK lub PW. Co istotne, określone w art. 8d i 8e KSC wg Projektu wymogi wobec kierownika pośrednio realizują ogólne wymogi mające zastosowanie względem PK i PW. Tym samym, realizacja zadań, do których na gruncie Projektu zobowiązany jest kierownik PK i PW i tak musiałaby być zapewniona przez sam PK lub PW poprzez wewnętrzne regulacje. Stosunek prawny na podstawie którego kierownik PK i PW jest zaangażowany w organizacji może być różnorodny. W zależności od rodzaju stosunku prawnego, możliwość pociągnięcia kierownika do odpowiedzialności istnieje na podstawie kontraktowej (jak również prawa pracy), co realizować będzie wymogi określone w Dyrektywie NIS2 (art. 20 ust. 1 Dyrektywy).	Wyjaśnienie uwagi Przypisanie odpowiedzialności za realizację zadań w obszarze cyberbezpieczeństwa przez kierowników ma na celu zwiększenie świadomości kadry kierowniczej na ten obszar. Odpowiedzialność kierowników wynika także z dyrektywy NIS2. Wymogi wskazane w projekcie wskazują na podstawie kwestie związane z zarządzaniem cyberbezpieczeństwem w podmiocie.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			Jednocześnie, nałożenie dodatkowych obowiązków kierownika PK lub PW wraz określeniem odrębnej podstawy nałożenia kary pieniężnej z tytułu ich naruszenia (art. 73a) może skutkować stosowaniem wobec niego równoległych reżimów odpowiedzialności – np. odpowiedzialność karna członka zarządu na zasadach ogólnych kodeksu karnego oraz na podstawie KSC. Rekomendacja Ograniczenie w możliwie szerokim zakresie obowiązków kierownika PK i PW w Projekcie w celu zachowania minimalnego charakteru implementacji Dyrektywy NIS2.	
445.	ISAC-Kolej	Art. 8e	„8e. Kierownik podmiotu kluczowego lub podmiotu ważnego raz w roku kalendarzowym przechodzi wewnętrzne szkolenie z zakresu wykonywania obowiązków, o których mowa w art. 7, art. 8, art. 8d, art. 8e, art. 8f ust. 2, art. 8h, art. 9–11 i art. 15. Udział w szkoleniu jest udokumentowany. Ustawa powinna precyzyjnie określić czy kierownik podmiotu kluczowego lub podmiotu ważnego ma być szkolony wewnętrznie w ramach szkoleń organizowanych w danym podmiocie czy powinien przejść szkolenie poza organizacją np. organizowane przez organ właściwy. Założyć należy, że ma to być szkolenie wewnętrzne, stąd propozycja doprecyzowania zapisu	Wyjaśnienie uwagi Nie jest to konieczne, skoro dopuszczamy szkolenie wewnętrzne. Nikt nie powinien zabronić korzystania ze szkoleń zewnętrznych.
446.	ISACA	Art. 8e	Kierownik podmiotu kluczowego lub podmiotu ważnego raz w roku kalendarzowym przechodzi szkolenie z zakresu wykonywania obowiązków, o których mowa w art. 7, art. 8, art. 8d, art. 8e, art. 8f ust. 2, art. 8h, art. 9–11 i art. 15. Udział w szkoleniu jest udokumentowany. "Wymaga dogłębnego przerehabilitowania w celu osiągnięcia zgodności z NIS2 - art. 20 ust. 2 Kto zapewni odpowiednią jakość szkoleń (najtańsze)? Należałoby co najmniej opracować SYLABUS oraz jakąkolwiek weryfikację umiejętności osób prowadzących! Jaki powinien być zakres szkoleń dla organów zarządzających? Szkolenie ma dostarczyć wiedzę, a nie się odbyć – jaki powinien być mechanizm weryfikacji tej wiedzy (ignorantia juris nocet vs. Impossibilium nulla obligatio est)" "Zapis nie jest skuteczną transpozycją [NIS2 art. 20 ust. 2] Państwa członkowskie zapewniają, aby członkowie organu zarządzającego podmiotów kluczowych i ważnych mieli obowiązek odbywać regularne szkolenia w celu zdobycia wystarczającej wiedzy i umiejętności pozwalających im rozpoznać ryzyko i ocenić praktyki zarządzania ryzykiem w cyberbezpieczeństwie oraz ich wpływ na usługi świadczone przez dany podmiot, a także zachęcają podmioty kluczowe i ważne do oferowania podobnych szkoleń ich pracownikom.."	Wyjaśnienie uwagi Organ właściwy do spraw cyberbezpieczeństwa będzie mógł w drodze czynności nadzorczych zweryfikować czy szkolenie się odbyło. Zakres szkolenia powinien obejmować stosowanie i wdrażanie SZBI w podmiocie.
447.	KIKE	Art. 8e	zmianę art. 8e uKSC w zakresie zniesienia obowiązku dla kierowników podmiotów ważnych do odbywania corocznych szkoleń. Obowiązek ten nie uwzględnia faktu, że podmioty mikro i małe na czas takich szkoleń będą miały problemy z wykonywaną przez siebie działalnością gospodarczą (braki kadrowe). Z tego względu ich udział w szkoleniach powinien mieć charakter dobrowolny,	Uwaga nieuwzględniona Obowiązek szkoleń kierowników podmiotów kluczowych i ważnych wynika z art. 20 ust. 2 dyrektywy NIS2 2. Państwa członkowskie zapewniają, aby członkowie organu zarządzającego podmiotów kluczowych i ważnych mieli obowiązek odbywać regularne szkolenia w celu zdobycia wystarczającej wiedzy i

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

				umiejętności pozwalających im rozpoznać ryzyko i ocenić praktyki zarządzania ryzykiem w cyberbezpieczeństwie oraz ich wpływ na usługi świadczone przez dany podmiot, a także zachęcają podmioty kluczowe i ważne do oferowania podobnych szkoleń ich pracownikom.
448.	Cybermadeinpol and	Art. 8e	Doprecyzowanie zakresu szkoleń oraz minimalnych kwalifikacji podmiotów przeprowadzających szkolenie w Art 8e.	Wyjaśnienie uwagi Zakres szkolenia powinien obejmować stosowanie i wdrażanie SZBI w podmiocie.
449.	ZBP	Art. 8e	Kierownik podmiotu kluczowego lub podmiotu ważnego raz w roku kalendarzowym przechodzi szkolenie z zakresu wykonywania obowiązków, o których mowa w art. 7, art. 8, art. 8d, art. 8e, art. 8f ust. 2, art. 8h, art. 9–11 i art. 15. Udział w szkoleniu jest udokumentowany Uwaga ogólna Prosimy o doprecyzowanie – czy tego rodzaju szkolenie powinno być przeprowadzane przez podmiot zewnętrzny.	Wyjaśnienie uwagi Przepis nie przewiduje, aby szkolenie było przeprowadzane przez podmiot zewnętrzny.
450.	Fundacja Bezpieczna Cyberprzestrzeń	Art. 8f	art. 1 pkt 13, treść art. 8f ust. 1 – jeśli intencją ustawodawcy jest by każda osoba realizująca obowiązki wskazane w art. 8 i art. 11 była objęta weryfikacją lepszym byłoby zastosowanie liczby mnogiej w tym przepisie, co wykluczy to selektywną weryfikację po stronie podmiotów kluczowych i ważnych. Wydaje się również zasadne, by określić związek danej osoby z realizacją ww. zadań, co pozwoli ograniczyć liczbę osób podlegających weryfikacji (zmniejszenie obciążeń administracyjnych podmiotów kluczowych i ważnych) oraz skoncentruje się na osobach, które rzeczywiście wykonują wskazane obowiązki. W związku z tym proponuje się nadać art. 8f ust. 1 następujące brzmienie: „1. Osoby bezpośrednio realizujące zadania, o których mowa w art. 8 i art. 11, nie mogą być skazane prawomocnym wyrokiem sądu za przestępstwa przeciwko ochronie informacji.”n	Wyjaśnienie uwagi W języku prawnym używa się liczby pojedynczej. Może zaistnieć problem z interpretacją kim jest osoba bezpośrednio realizująca zadania – a kim jest osoba która realizuje zadania niebezpośrednio? Wydaje się, że kwestię tę można ustalić pracodawca w zakresie obowiązków osoby czy w innych stosunkach zatrudnienia w umowie.
451.	ISAC-Kolej	Art. 8f	„2. Weryfikacji niekaralności osób realizujących zadania, o których mowa w art. 8 i art. 11, dokonuje podmiot kluczowy i podmiot ważny co najmniej raz w roku”. W przepisie tym powinna zostać precyzyjnie określona częstotliwość takiej weryfikacji np. raz w roku, raz na dwa lata, itd. Jeśli weryfikacja niekaralności będzie scedowana na podmiot kluczowy lub pomiot ważny, to czy przepis ten będzie we wniosku do Krajowego Rejestru Karnego podstawą do składania wniosku o sprawdzenie karalności i w ten sposób podmiot kluczowy lub podmiot ważny będzie zwolniony z opłaty z tytułu tej weryfikacji (np. jak ma to miejsce w przypadku sprawdzania niekaralności w KRK przez Pełnomocnika ds. ochrony informacji niejawnych). Ponadto warto rozważyć, czy obowiązek ten nie powinien być scedowany na organ właściwy	Wyjaśnienie uwagi Przepis zostanie doprecyzowany w związku z uwagami UODO. Przede wszystkim to osoba realizująca zadania będzie musiała przedstawić zaświadczenie o niekaralności na początku oraz poinformować o zmianach w tym zakresie. Dodatkowo podmiot będzie uprawniony do żądania w uzasadnionych przypadkach o

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

				przedstawienie zaświadczenia o niekaralności.
452.	ISAC-Kolej	Art. 8f	„3. Wymaganie, o którym mowa w ust. 1 uznaje się za spełnione, jeśli osoba realizująca zadania, o których mowa w art. 8 i art. 11 posiada aktualne i ważne poświadczenie bezpieczeństwa w zakresie dostępu do informacji niejawnych o klauzuli „poufne” lub wyższej”. Należy rozważyć, czy weryfikacja karalności jest konieczna w przypadku, gdy osoby realizujące zadania, o których mowa w art. 8 i art. 11 posiadają aktualne i ważne poświadczenia bezpieczeństwa w zakresie dostępu do informacji niejawnych o klauzuli „poufne” lub wyższej”.	Uwaga uwzględniona Przepis zostanie dodany zgodnie z propozycją.
453.	KGHM Polska Miedź S.A.	Art. 8f	Wymogi dla osób realizujących zadania art. 8 i 11 powinny być bardziej precyzyjne w zw. z bardzo szerokim obszarem działań i uprawnień w zakresie dostępu do informacji, szczególnie w art. 8h w zakresie zdefiniowanych zakresów przekazywanych informacji, w tym w zakresie wymiany informacji w procesie zarządzania i obsługi incydentów. Art. 8f 1. Osoba realizująca zadania, o których mowa w art. 8 i art. 11, osoba musi być zdolna do spełnienia wymogów dla zapewnienia ochrony informacji. 2. Weryfikacji, czy osoba realizująca zadania, o których mowa w art. 8 i art. 11 jest zdolna do spełnienia wymogów dla zapewnienia ochrony informacji, dokonuje podmiot kluczowy i podmiot ważny przez weryfikację niekaralności - brak skazania prawomocnym wyrokiem sądu za przestępstwa przeciwko ochronie informacji. W uzasadnionych przypadkach podmiot kluczowy i podmiot ważny realizują weryfikację zdolności osoby do spełnienia wymogów dla zapewnienia ochrony informacji przez uzyskanie poświadczenia bezpieczeństwa. Osoby wykonujące zadania określone m. in. w art. 8 i 11 projektowanej ustawy będą miały faktyczny dostęp do kluczowych informacji. Rekomenduje się doprecyzowanie poprzez jednoznaczne wskazanie katalogu przestępstw, które wykluczają możliwość rekrutowania i trwania stosunku pracy (danie możliwości zweryfikowania w trakcie prowadzonego postępowania rekrutacyjnego, jak również w trakcie obowiązywania umowy przesłanki skazania za określone przestępstwo nastąpi). Nie tylko skazanie za przestępstwa przeciwko ochronie informacji mogą rzutować na należytą opinię i prawidłowe wykonywanie powierzonych obowiązków. Pod rozważyć należy wziąć okoliczność, czy i w jakim zakresie osoby wykonujące zadania określone w art. 8 i 11 projektowanej ustawy w pewnym zakresie nie powinny być kwalifikowane jako posiadające dostęp do informacji niejawnej (kwestia wskazania, że tak kwalifikować należy dostęp audytora do takiej informacji – zob. art. 15 ust. 4 projektowanej ustawy). W związku z tym, powinna istnieć podstawa prawna dla przeprowadzania postępowań sprawdzających w trybie ustawy z dnia 5 sierpnia 2010 r. o ochronie informminformacji niejawnych, t.j. Dz. U. z 2024 r. poz. 632 (dalej: ustawa o ochronie informacji niejawnych).mmOgraniczenie zakresu weryfikacji spełnienia wymogów dla zapewnienia ochrony informacji jedynie do potwierdzenia niekaralności za przestępstwa przeciwko ochronie informacji jest zbyt wąskie, i w konsekwencji ograniczy możliwości przekazywania	Uwaga częściowo uwzględniona Po pierwsze przepis umożliwi sprawdzenie niekaralności przed nawiązaniem współpracy, jak i w trakcie. Wprowadzenie wymogu uzyskania poświadczenia bezpieczeństwa nie jest zasadne. Z pewnością przyczyni się to do zwiększenia bezpieczeństwa podmiotu, ale uzyskanie dla pracownika poświadczenia do poziomu poufne wymaga wcześniejszego zatrudnienia przez podmiot Pełnomocnika do spraw ochrony informacji niejawnych. Zatrudnienie takiej osoby może być utrudnione przez wiele podmiotów, zwłaszcza tych mniejszych.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			informacji stanowiący tajemnice prawnie chronione, co szczególnie obniży skuteczność reagowania na incydenty.mZ powyższych względów proponuje się rozszerzenie regulacji, tak aby dać możliwość zwiększenia zakresu weryfikacji o uzyskanie poświadczenia bezpieczeństwa (ustawa o ochronie informacji niejawnych) i w ten sposób umożliwić operacyjne „odblokowanie” działań dla obszarów szczególnie chronionych i obronnych państwa.	
454.	PIPC	Art. 8f ust. 1 - 2	Wymogi dla osób realizujących zadania art. 8 i 11 powinny być bardziej precyzyjne w zw. z bardzo szerokim obszarem działań i uprawnień w zakresie dostępu do informacji, szczególnie w art. 8h w zakresie zdefiniowanych zakresów przekazywanych informacji, w tym w zakresie wymiany informacji w procesie zarządzania i obsługi incydentów. Art. 8f 1. Osoba realizująca zadania, o których mowa w art. 8 i art. 11, osoba musi być zdolna do spełnienia wymogów dla zapewnienia ochrony informacji. 2. Weryfikacji, czy osoba realizująca zadania, o których mowa w art. 8 i art. 11 jest zdolna do spełnienia wymogów dla zapewnienia ochrony informacji, dokonuje podmiot kluczowy i podmiot ważny przez weryfikację niekaralności - brak skazania prawomocnym wyrokiem sądu za przestępstwa przeciwko ochronie informacji. W uzasadnionych przypadkach podmiot kluczowy i podmiot ważny realizują weryfikację zdolności osoby do spełnienia wymogów dla zapewnienia ochrony informacji przez uzyskanie poświadczenia bezpieczeństwa. Osoby wykonujące zadania określone m. in. w art. 8 i 11 projektowanej ustawy będą miały faktyczny dostęp do kluczowych informacji. Rekomendujemy doprecyzowanie poprzez jednoznaczne wskazanie katalogu przestępstw, które wykluczają możliwość rekrutowania i trwania stosunku pracy (danie możliwości zweryfikowania w trakcie prowadzonego postępowania rekrutacyjnego, jak również w trakcie obowiązywania umowy przesłanki skazania za określone przestępstwo nastąpi). Nie tylko skazanie za przestępstwa przeciwko ochronie informacji mogą rzutować na należytą opinię i prawidłowe wykonywanie powierzonych obowiązków. Pod rozważę należy wziąć okoliczność, czy i w jakim zakresie osoby wykonujące zadania określone w art. 8 i 11 projektowanej ustawy w pewnym zakresie nie powinny być kwalifikowane jako posiadające dostęp do informacji niejawnej (kwestia wskazania, że tak kwalifikować należy dostęp audytora do takiej informacji – zob. art. 15 ust. 4 projektowanej ustawy). W związku z tym, powinna istnieć podstawa prawna dla przeprowadzania postępowań sprawdzających w trybie ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, t.j. Dz. U. z 2024 r. poz. 632 (dalej: ustawa o ochronie informacji niejawnych). Ograniczenie zakresu weryfikacji spełnienia wymogów dla zapewnienia ochrony informacji jedynie do potwierdzenia niekaralności za przestępstwa przeciwko ochronie informacji jest zbyt wąskie i w konsekwencji ograniczy możliwości przekazywania informacji stanowiący tajemnice prawnie chronione, co szczególnie obniży skuteczność reagowania na incydenty.	Uwaga częściowo uwzględniona Po pierwsze przepis umożliwi sprawdzenie niekaralności przed nawiązaniem współpracy, jak i w trakcie. Wprowadzenie wymogu uzyskania poświadczenia bezpieczeństwa nie jest zasadne. Z pewnością przyczyni się to do zwiększenia bezpieczeństwa podmiotu, ale uzyskanie dla pracownika poświadczenia do poziomu poufne wymaga wcześniejszego zatrudnienia przez podmiot Pełnomocnika do spraw ochrony informacji niejawnych. Zatrudnienie takiej osoby może być utrudnione przez wiele podmiotów, zwłaszcza tych mniejszych.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			Z powyższych względów proponujemy rozszerzenie regulacji, tak aby dać możliwość zwiększenia zakresu weryfikacji o uzyskanie poświadczenia bezpieczeństwa (ustawa o ochronie informacji niejawnych) i w ten sposób umożliwić operacyjne „odblokowanie” działań dla obszarów szczególnie chronionych i obronnych państwa.	
455.	Związek Pracodawców Polska Miedź	Art. 8f ust. 1 - 2	Wymogi dla osób realizujących zadania art. 8 i 11 powinny być bardziej precyzyjne w zw. z bardzo szerokim obszarem działań i uprawnień w zakresie dostępu do informacji, szczególnie w art. 8h w zakresie zdefiniowanych zakresów przekazywanych informacji, w tym w zakresie wymiany informacji w procesie zarządzania i obsługi incydentów. Art. 8f 1. Osoba realizująca zadania, o których mowa w art. 8 i art. 11, osoba musi być zdolna do spełnienia wymogów dla zapewnienia ochrony informacji. 2. Weryfikacji, czy osoba realizująca zadania, o których mowa w art. 8 i art. 11 jest zdolna do spełnienia wymogów dla zapewnienia ochrony informacji, dokonuje podmiot kluczowy i podmiot ważny przez weryfikację niekaralności - brak skazania prawomocnym wyrokiem sądu za przestępstwa przeciwko ochronie informacji. W uzasadnionych przypadkach podmiot kluczowy i podmiot ważny realizują weryfikację zdolności osoby do spełnienia wymogów dla zapewnienia ochrony informacji przez uzyskanie poświadczenia bezpieczeństwa. Osoby wykonujące zadania określone m. in. w art. 8 i 11 projektowanej ustawy będą miały faktyczny dostęp do kluczowych informacji. Rekomenduje się doprecyzowanie poprzez jednoznaczne wskazanie katalogu przestępstw, które wykluczają możliwość zrekrutowania i trwania stosunku pracy (danie możliwości zweryfikowania w trakcie prowadzonego postępowania rekrutacyjnego, jak również w trakcie obowiązywania umowy przesłanki skazania za określone przestępstwo nastąpi). Nie tylko skazanie za przestępstwa przeciwko ochronie informacji mogą rzutować na należytą opinię i prawidłowe wykonywanie powierzonych obowiązków. Pod rozważę należy wziąć okoliczność, czy i w jakim zakresie osoby wykonujące zadania określone w art. 8 i 11 projektowanej ustawy w pewnym zakresie nie powinny być kwalifikowane jako posiadające dostęp do informacji niejawnej (kwestia wskazania, że tak kwalifikować należy dostęp audytora do takiej informacji – zob. art. 15 ust. 4 projektowanej ustawy). W związku z tym, powinna istnieć podstawa prawna dla przeprowadzania postępowań sprawdzających w trybie ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, t.j. Dz. U. z 2024 r. poz. 632 (dalej: ustawa o ochronie informacji niejawnych).m Ograniczenie zakresu weryfikacji spełnienia wymogów dla zapewnienia ochrony informacji jedynie do potwierdzenia niekaralności za przestępstwa przeciwko ochronie informacji jest zbyt wąskie, i w konsekwencji ograniczy możliwości przekazywania informacji stanowiący tajemnice prawnie chronione, co szczególnie obniży skuteczność reagowania na incydenty. Z powyższych względów proponuje się rozszerzenie regulacji, tak aby dać możliwość zwiększenia zakresu weryfikacji o uzyskanie poświadczenia bezpieczeństwa (ustawa o ochronie informacji	Uwaga częściowo uwzględniona Po pierwsze przepis umożliwi sprawdzenie niekaralności przed nawiązaniem współpracy, jak i w trakcie. Wprowadzenie wymogu uzyskania poświadczenia bezpieczeństwa nie jest zasadne. Z pewnością przyczyni się to do zwiększenia bezpieczeństwa podmiotu, ale uzyskanie dla pracownika poświadczenia do poziomu poufne wymaga wcześniejszego zatrudnienia przez podmiot Pełnomocnika do spraw ochrony informacji niejawnych. Zatrudnienie takiej osoby może być utrudnione przez wiele podmiotów, zwłaszcza tych mniejszych.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			niejawnych) i w ten sposób umożliwić operacyjne „odblokowanie” działań dla obszarów szczególnie chronionych i obronnych państwa.	
456.	ZBP	Art. 8f ust. 2	Weryfikacji niekaralności osób realizujących zadania, o których mowa w art. 8 i art. 11, dokonuje podmiot kluczowy i podmiot ważny Weryfikacji niekaralności osób realizujących zadania, o których mowa w art. 8 i art. 11, dokonuje podmiot kluczowy i podmiot ważny w oparciu o rejestry publiczne. Prosimy o doprecyzowanie jaki powinien być sposób weryfikacji niekaralności – czy powinno być to oświadczenie o niekaralności czy zaświadczenie o osobie z KRK. Jakie powinien być zakres sprawdzenia - pełne sprawdzenie (rejestr skazanych i rejestr toczących się spraw) czy zwykłe (rejestr skazanych za przestępstwa umyślne). Dodatkowo, powstaje wątpliwość, czy weryfikacja powinna następować tylko przy zatrudnieniu, czy w trakcie trwania zatrudnienia (cyklicznie).	Uwaga częściowo uwzględniona Po pierwsze przepis umożliwi sprawdzenie niekaralności przed nawiązaniem współpracy, jak i w trakcie. Po drugie wprowadzimy model przedstawienia zaświadczeń o niekaralności.
457.	Konfederacja Lewiatan	Art. 8f	Poważne niejasności budzi wymóg potwierdzania niekaralności wszystkich osób wykonujących zadania, o których mowa w art. 8 i 11. W pierwszej kolejności zauważamy, że wymóg ten nie wynika z dyrektywy NIS2 i jest wobec niej nadmiarowy. Zauważamy, że z uwagi na bardzo rozległy zakres zadań realizowanych na podstawie art. 8 i 11 zadania te będą wykonywane w niektórych organizacjach przez znaczną liczbę osób, a wobec części z nich wymaganie „zaświadczenia”, tj. zapewne zaświadczenia z Krajowego Rejestru Karnego będzie nieproporcjonalne. Postulujemy wprowadzenie wymagania zgodnego z normą ISO 27001, do której odnosi się uzasadnienie projektu. Przewiduje ona środek kontrolny wskazujący, że <i>Przed dołączeniem do organizacji i na bieżąco należy przeprowadzać badanie przeszłości wszystkich kandydatów na pracowników, z uwzględnieniem obowiązujących przepisów prawa, regulacji i zasad etycznych, a także proporcjonalnie do wymagań działalności, klasyfikacji informacji, do których pracownik ma mieć dostęp, oraz postrzeganego ryzyka.</i> W szczególności wymagania dot. potwierdzenia niekaralności powinny zostać ograniczone do zakresu kluczowego personelu definiowanego przez pracodawcę.	Wyjaśnienie uwagi Naszym zdaniem kwestia ta mieści się w ramach wspomnianego środka kontrolnego.
458.	Polska Izba Informatyki i Telekomunikacji	Art. 8f	Poważne niejasności budzi wymóg potwierdzania niekaralności wszystkich osób wykonujących zadania, o których mowa w art. 8 i 11. W pierwszej kolejności zauważamy, że wymóg ten nie wynika z dyrektywy NIS2 i jest wobec niej nadmiarowy. Zauważamy, że z uwagi na bardzo rozległy zakres zadań realizowanych na podstawie art. 8 i 11 zadania te będą wykonywane w niektórych organizacjach przez znaczną liczbę osób, a wobec części z nich wymaganie „zaświadczenia”, tj. zapewne zaświadczenia z Krajowego Rejestru Karnego będzie nieproporcjonalne. Postulujemy wprowadzenie wymagania zgodnego z normą ISO 27001, do której odnosi się uzasadnienie projektu. Przewiduje ona środek kontrolny wskazujący, że <i>„Przed dołączeniem do organizacji i na bieżąco należy przeprowadzać badanie przeszłości wszystkich kandydatów na pracowników, z uwzględnieniem obowiązujących przepisów prawa, regulacji i zasad etycznych, a</i>	Uwaga nieuwzględniona Naszym zdaniem konieczna jest weryfikacja niekaralności pracowników albo innych osób zatrudnionych przy realizacji zadań z zakresu cyberbezpieczeństwa.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			<i>także proporcjonalnie do wymagań działalności, klasyfikacji informacji, do których pracownik ma mieć dostęp, oraz postrzeganego ryzyka”.</i> W szczególności wymagania dotyczące potwierdzenia niekaralności powinny zostać ograniczone do zakresu kluczowego personelu definiowanego przez pracodawcę.	
459.	Amerykańska Izba Handlowa	Art. 8g	Wprowadzany powyższym artykułem art. 8g uksc kreuje w pkt 2 obowiązek ujawniania na stronie internetowej przez dostawcę usług zarządzanych w zakresie cyberbezpieczeństwa dodatkowych informacji. Należą do nich „zasady współpracy i wymiany informacji” oraz „polityka komunikacyjna”. Terminy te nie są dla przedsiębiorców z branży jasne, a co za tym idzie wskazane byłoby ich zdefiniowanie lub zrozumiałe dookreślenie w tekście ustawy. Uznajemy szczególną rolę, jaką dostawcę usług zarządzanych odgrywają w ekosystemie cyberbezpieczeństwa, co uzasadnia ich zwiększone obowiązki w zakresie przejrzystości. Stoimy jednak na stanowisku, że jasna i jednoznaczna terminologia jest niezbędna aby zapewnić skuteczne wdrożenie przepisów dyrektywy NIS 2.e	Wyjaśnienie uwagi W tym przepisie chodzi o informacje wymagane przez RFC 2350 w pkt 3.4.2. Jest to powszechnie przyjęty standard w zakresie publikowania podstawowych informacji o CSIRT. https://datatracker.ietf.org/doc/html/rfc2350#section-3.4.2 W tym miejscu powinien się znaleźć krótki opis z jakimi podmiotami współpracuje CSIRT i w jakim celu to robi.
460.	Amerykańska Izba Handlowa	Art. 8g	Wprowadzany powyższym artykułem art. 8g uksc nakłada w pkt 4 lit. c na dostawców usług zarządzanych w zakresie cyberbezpieczeństwa nowy obowiązek w postaci publikacji "danych o wykorzystywanych kluczach publicznych i sposobach szyfrowania komunikacji". Biorąc pod uwagę wrażliwość tych informacji, stoimy na stanowisku, że obowiązkowe ujawnienie ich, może w sposób niezamierzony negatywnie wpłynąć na poziom cyberbezpieczeństwa. Proponujemy ponowną ocenę tego wymogu w celu dostosowania go do najlepszych praktyk, które chronią poufność i integralność metod szyfrowania.k	Wyjaśnienie uwagi W tym przepisie chodzi o informacje wymagane przez RFC 2350 w pkt 3.4.3. Jest to powszechnie przyjęty standard w zakresie publikowania podstawowych informacji o CSIRT. https://datatracker.ietf.org/doc/html/rfc2350#section-3.4.3 W tym miejscu powinna znaleźć się informacja o publicznym kluczu PGP i sposobie przekazywaniu informacji.
461.	Cybermadeinpol and	Art. 8g	Art. 8g. P. 2) b) oraz c) - dodanie definicji “zasad współpracy i wymiany informacji” oraz “polityki komunikacji” wraz z wytycznymi co do treści.	Wyjaśnienie uwagi W tym przepisie chodzi o informacje wymagane przez RFC 2350 w pkt 3.4.2. Jest to powszechnie przyjęty standard w zakresie publikowania podstawowych informacji o CSIRT. https://datatracker.ietf.org/doc/html/rfc2350#section-3.4.2 W tym miejscu powinien się znaleźć krótki opis z jakimi podmiotami

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

				współpracuje CSIRT i w jakim celu to robi.
462.	Cybermadeinpol and	Art. 8g	Art. 8g. P. 4) c) cel zapisu o ‘wykorzystywanych kluczach’ jest niejasny, proponujemy zmianę brzmienia na “dane o sposobach szyfrowania komunikacji z dostawcą”.	Wyjaśnienie uwagi W tym przepisie chodzi o informacje wymagane przez RFC 2350 w pkt 3.4.3. Jest to powszechnie przyjęty standard w zakresie publikowania podstawowych informacji o CSIRT. https://datatracker.ietf.org/doc/html/rfc2350#section-3.4.3 W tym miejscu powinna znaleźć się informacja o publicznym kluczu PGP i sposobie przekazywaniu informacji.
463.	Morskie Centrum Cyberbezpieczeństwa Akademia Marynarki Wojennej w Gdyni	Art. 8g	Jednocześnie w art. 8g proponujemy zobowiązać dostawców usług zarządzanych w zakresie cyberbezpieczeństwa by <u>opracowali propozycję mierników podkreślających jakość oferowanych przez nich usług.</u>	Uwaga nieuwzględniona Taki przepis musiałby dotyczyć wszystkich podmiotów kluczowych i ważnych, bowiem wszystkie te podmioty świadczą istotne usługi dla społeczeństwa. Mogłoby to być nadmierne obciążenie.
464.	Polskie Stowarzyszenie Fotowoltaiki	Art. 8g	[Obowiązki informacyjne dostawców usług zarządzanych w zakresie cyberbezpieczeństwa] Art. 8g zobowiązuje dostawców usług zarządzanych w zakresie cyberbezpieczeństwa do publikacji na swojej stronie internetowej określonych informacji o prowadzonej działalności. Ogólny wpływ regulacji: Obowiązek publikacji i utrzymywania na swojej stronie internetowej dodatkowych informacji o podmiocie kwalifikowanym jako dostawca usług zarządzanych w zakresie cyberbezpieczeństwa. Wpływ na sektor energetyczny: jw. – brak specyficznego wpływu na sektor energetyczny Nadregulacja względem Dyrektywy NIS2] Obowiązek nie wynika z Dyrektywy NIS2. Zgodnie z uzasadnieniem Projektu wprowadzenie obowiązku wynika z nieformalnej praktyki stosowanej przez różne jednostki reagowania na incydenty cyberbezpieczeństwa ¹⁶ . Rekomendacja: Wycofanie proponowanego przepisu art. 8g z Projektu.	Uwaga nieuwzględniona Przepis nie stanowi utrudnienia dla przedsiębiorców a wręcz ułatwi kontakt z dostawcami usług zarządzanych w zakresie cyberbezpieczeństwa.

¹⁶ <https://datatracker.ietf.org/doc/html/rfc2350#section-3.3>

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

465.	Fundacja Open Allies	Art. 8h	Treść art. 8h ust. 1 nowelizowanej UKSC wskazuje, że <i>podmioty kluczowe i podmioty ważne wymieniają między sobą informacje dotyczące cyberbezpieczeństwa</i>, bez wskazania, że wymiana odbywa się na zasadach dobrowolności. W związku z treścią ust. 2 można wnioskować, że wymiana jest dobrowolna, co jednak wynika wprost z ust. 1, którego brzmienie może sugerować wymianę obowiązkową. Z kolei art. 29 ust. 1 dyrektywy NIS2 wprost wskazuje na dobrowolną wymianę danych. Zwracamy się o doprecyzowanie art. 8h ust. 1 przez wskazanie, że wymiana danych jest dobrowolna.	Uwaga uwzględniona Wskazane zostanie, że wymiana jest dobrowolna.
466.	ISAC-Kolej	Art. 8h	„1. „Podmioty kluczowe i podmioty w ramach utworzonego dla danego sektora i podsektora ISAC-a wymieniają między sobą informacje dotyczące cyberbezpieczeństwa, w tym informacje o cyberzagrożeniach, potencjalnych zdarzeniach dla cyberbezpieczeństwa, podatnościach, technikach i procedurach, oznakach naruszenia integralności systemu, wrogich taktykach, a także informacje o grupach przestępczych, ostrzeżenia dotyczące cyberbezpieczeństwa i zalecenia dotyczące konfiguracji narzędzi bezpieczeństwa mających wykrywać cyberataki”. Zapisy, o których mowa w art. 8h ust. 1 – 6 sankcjonują tak naprawdę zasady działania struktury ISAC powołanych w danym sektorze lub podsektorze.	Uwaga nieuwzględniona Ta uwaga sugeruje, że ISAC jest podmiotem prawa, a w praktyce nim nie jest, ma charakter luźnego porozumienia. Poza tym uwaga sugeruje, że może być tylko jeden ISAC w sektorze/podsektorze, co nie wydaje się słuszne.
467.	ISAC-Kolej	Art. 8h	„3) „odbywa się tylko w ramach utworzonego dla danego sektora i podsektora ISAC-a” Wymiana informacji, ostrzeżeń i zaleceń, o których mowa w art. 8h ust. 1 powinna być dopuszczalna, jeśli odbywa się w ramach utworzonego dla danego sektora i podsektora ISAC-a.	Uwaga nieuwzględniona Ta uwaga sugeruje, że ISAC jest podmiotem prawa, a w praktyce nim nie jest, ma charakter luźnego porozumienia. Poza tym uwaga sugeruje, że może być tylko jeden ISAC w sektorze/podsektorze, co nie wydaje się słuszne.
468.	ISAC-Kolej	Art. 8h	„3. Wymiana informacji, ostrzeżeń i zaleceń, o których mowa w ust. 1, odbywa się przy wykorzystaniu systemu teleinformatycznego, o którym mowa w art. 46 ust. 1, systemów teleinformatycznych zapewnianych przez organy właściwe do spraw cyberbezpieczeństwa lub w drodze porozumień na utworzenie ISAC-a sektorowego lub podsektorowego”, o których mowa w ust. 5”. Przepis powinien dokładnie precyzować, że porozumienie dotyczy utworzenia ISAC-a sektorowego lub podsektorowego.	Uwaga nieuwzględniona Chcemy zapewnić większą elastyczność. Nie każdy podmiot może chcieć dołączyć do ISACa sektorowego.
469.	ISAC-Kolej	Art. 8h	„5. Podmioty kluczowe, podmioty ważne, CSIRT sektorowy lub inne podmioty mogą zawierać porozumienia w sprawie utworzenia ISAC-a sektorowego i podsektorowego, o których mowa w ust. 1, określając sposób wymiany informacji i zachowania informacji w poufności pomiędzy stronami porozumienia”. Przepis powinien dokładnie precyzować, że porozumienie dotyczy utworzenia ISAC-a sektorowego lub podsektorowego	Uwaga nieuwzględniona Naszym zdaniem ta możliwość już wynika z proponowanego przepisu.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

470.	Polskie Stowarzyszenie Fotowoltaiki	Art. 8h	[Wymiana informacji, ostrzeżeń i zaleceń dotyczących cyberbezpieczeństwa] - Obowiązek stosowania systemu teleinformatycznego, o którym mowa w art. 46 ust. 1 KSC wg Projektu (tzw. system S46), w celu wymiany informacji o cyberzagrożeniach - Obowiązek oznaczenia zakresu odbiorców przekazywanych informacji. Ogólny wpływ regulacji: Obowiązek PK i PW stosowania określonego systemu teleinformatycznego w razie wymiany informacji o cyberzagrożeniach. Przepis nie wskazuje w sposób wyraźny, że uczestnictwo w wymianie informacji wskazanych powyżej jest dobrowolne. Co więcej, niewykonanie obowiązków określonych w art. 8h ust 1 KSC wg Projektu ma stanowić podstawę odpowiedzialności kierownika PK lub PW na podstawie art. 73a ust. 1 pkt 6 KSC wg Projektu. Wpływ na sektor energetyczny: jw. – brak specyficznego wpływu na sektor energetyczny [Nadregulacja względem Dyrektywy NIS2] Nałożenie obowiązku uczestnictwa w wymianie informacji dotyczących cyberbezpieczeństwa stanowi nadregulację względem wymogów wynikających z Dyrektywy NIS2 (vide. art. 30 dot. dobrowolnego zgłaszania ważnych informacji). Rekomendacja: Doprecyzowanie przepisu poprzez jednoznaczne wskazanie dobrowolności uczestnictwa w wymianie informacji dotyczących cyberbezpieczeństwa oraz odpowiednie dostosowanie przepisów dot. odpowiedzialności PK i PW lub kierownika tych podmiotów.	Uwaga uwzględniona Wskazane zostanie, że wymiana informacji jest dobrowolna.
471.	Konfederacja Lewiatan	Art. 8h	W naszej ocenie w ust. 1 należy wprowadzić fakultatywność wymiany informacji, w miejsce aktualnego bezwzględnie obowiązku. Początek ust. 1 powinien więc brzmieć: „<i>Podmioty kluczowe i podmioty ważne <u>mogą wymieniać</u> ~~wymieniają~~ między sobą informacje dotyczące cyberbezpieczeństwa (...)</i>”.	Uwaga uwzględniona Wskazane zostanie, że wymiana jest dobrowolna.
472.	Polska Izba Informatyki i Telekomunikacji	Art. 8h	W naszej ocenie w ust. 1 należy wprowadzić fakultatywność wymiany informacji, w miejsce aktualnego bezwzględnie obowiązku. Początek ust. 1 powinien więc brzmieć: „<i>Podmioty kluczowe i podmioty ważne <u>mogą wymieniać</u> ~~wymieniają~~ między sobą informacje dotyczące cyberbezpieczeństwa (...)</i>”. W obecnym brzmieniu projektu zmian w ksc wymiana informacji de facto jest obowiązkiem, podczas gdy zgodnie z art. 29 NIS2 wymiana ta ma się odbywać na zasadzie dobrowolności, tym bardziej, że jest to obowiązek penalizowany. Obowiązkiem powinna być objęta tylko wymiana informacji z CSIRT, jak w NIS 2.	Uwaga uwzględniona Zostanie wprowadzona fakultatywność wymiany informacji.
473.	Fundacji Rozwoju Obrotu	Art. 8i	2) Przede wszystkim nie są precyzyjnie określone relacje pomiędzy Dyrektywą NIS 2 a DORA. W szczególności chodzi o podmioty, które są objęte obiema regulacjami. Wprawdzie z jednej strony,	Wyjaśnienie uwagi

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

	Bezgotówkowe		zgodnie z art. 8i Projektu wyłącza się stosowanie wobec podmiotów podlegających DORA postanowień rozdziału 3, ponieważ odpowiednie obowiązki należy wdrażać na podstawie DORA, które jest stosowane bezpośrednio. Z drugiej jednak strony, w uzasadnieniu wyjaśnia się, że: „Dyrektywa NIS 2 odeszła od wdrażania środków zapewniających bezpieczeństwo systemów informacyjnych tylko w zakresie świadczonych usług kluczowych. Podmiot ma dbać o bezpieczeństwo wszystkich swoich systemów wykorzystywanych do prowadzenia swojej działalności”. W związku z tym nie jest jasne w jaki przykładowo sposób, podmiot kluczowy NIS 2 (który miałby wdrożyć obowiązki we wszystkich swoich systemach), ma wdrażać obowiązki z NIS 2 w swoich systemach służących także do działalności objętej DORA, czyli teoretycznie wyłączonej. W związku z powyższym wskazujemy na konieczność wydłużenia okresu konsultacji o dodatkowe 30 dni, aby strona rządowa oraz podmioty objęte nowelizacją miały możliwość dokładnego zbadania i podjęcia działań prowadzących do uniknięcia kolizji aktów prawnych.	Przepis zostanie zmieniony zgodnie z uwagami KNF.
474.	Krzysztof Rożko i Wspólnicy Kancelaria Prawna sp. k.	Art. 8i	UWAGA ZGŁOSZONA W RAMACH ZGŁOSZENIA LOBBINGOWEGO Zwracamy uwagę, że w projekcie nowelizacji uKSC, w art. 1 pkt 13 (w proj art. 8i uKSC), przewidziano wyłączenie od stosowania przepisów rozdziału 3. uKSC w zakresie w jakim podmioty kluczowe i ważne z sektora bankowość i infrastruktura rynków finansowych mają obowiązek stosować Rozporządzenie 2022/2554. Tymczasem w projekcie art. 16a uKSC proponowanym na podstawie projektu ustawy wdrażającej DORA, przewidziana jest analogiczna regulacja, w której jednak wprost wskazano konkretne przepisy uKSC, które nie znajdą zastosowania do podmiotów ważnych lub kluczowych w rozumieniu Dyrektywy NIS 2. Wobec powyższego postulujemy odpowiednie skoordynowanie treści projektowanych przepisów w celu uniknięcia nałożenia się zakresu regulacji. W przypadku pozostawienia metody regulacji, określonej w projekcie ustawy wdrażającej DORA, która zakłada wprost wymienienie przepisów, do których stosowania nie są zobowiązane podmioty, do których stosuje się przepisy rozporządzenia DORA, co jest metodą zapewniającą większą jasność odnośnie zakresu obowiązków spoczywających na takich podmiotach, należałoby zrewidować przepisy, z których stosowania są zwolnione podmioty kluczowe lub podmioty ważne, z sektora „Bankowość i infrastruktura rynków finansowych”. Przykładowo błędnym wydaje się wyłącznie ze stosowania przez takie podmioty art. 11a uKSC, którego wprowadzenie zostało zaproponowane na gruncie projektu ustawy wdrażającej DORA.	Wyjaśnienie uwagi Przepis zostanie zmieniony zgodnie z uwagami KNF.
475.	Polskie Stowarzyszenie Fotowoltaiki	Art. 8i	Wyłączenie stosowania wymogów Rozdziału 3 przez PK i PW z sektora bankowość i infrastruktura rynków finansowych w zakresie w jakim zobowiązane są do stosowania Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (Rozporządzenie DORA). Ogólny wpływ regulacji: <i>Dotyczy wyłącznie PK i PW z sektora bankowość i infrastruktura rynków finansowych.</i> Wpływ na sektor energetyczny:	Uwaga przyjęta do wiadomości

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			<i>Nie dotyczy podmiotów sektora energetyk</i>	
476.	Stowarzyszenie Absolwentów Studiów Cyberbezpieczeństwa MBA	Art. 8i	Brak zwolnienia sektora bankowego i rynków finansowych z obowiązków wynikających z ustawy KSC wbrew dyrektywie NIS2 Projekt ustawy o krajowym systemie cyberbezpieczeństwa wprowadza zasadniczą różnicę w stosunku do dyrektywy NIS2, która zwalnia sektor bankowy i rynki finansowe z obowiązków dyrektywy. W projekcie ustawy KSC, sektor ten jest zobowiązany do przestrzegania ustawy KSC w zakresie, w jakim nie stosuje on rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2554. Tymczasem, zgodnie z art. 2 ust. 2 dyrektywy NIS2, podmioty te są całkowicie wyłączone z obowiązków wynikających z dyrektywy. To rozwiązanie wydaje się być nie tylko sprzeczne z duchem dyrektywy NIS2, ale także wprowadza dodatkowe, potencjalnie zbędne obciążenia dla sektora bankowego i rynków finansowych. Sektory te są już wysoko regulowane i objęte ścisłymi przepisami dotyczącymi cyberbezpieczeństwa, co czyni obowiązki wynikające z ustawy KSC w najlepszym przypadku redundantnymi, a w najgorszym — generującymi dodatkowe, niepotrzebne koszty administracyjne i operacyjne. Takie podejście nie tylko nie przyczynia się do rzeczywistego wzrostu poziomu cyberbezpieczeństwa, ale może również prowadzić do nadmiernego skomplikowania procesów regulacyjnych w sektorze. Proponujemy ujednolicenie oraz zsynchronizowanie przygotowania ustaw wdrażających dyrektywę NIS2, rozporządzenie DORA i dyrektywę CER.	Wyjaśnienie uwagi Będziemy dążyć do uspoźnienia projektów.
477.	Związek Banków Polskich	Art. 8i	Art. 8i. Podmioty kluczowe i podmioty ważne z sektora bankowości i infrastruktura rynków finansowych nie stosują przepisów niniejszego rozdziału w zakresie w jakim mają obowiązek stosować rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (Dz. Urz. UE L 333 z 27.12.2022, str. 1).”; Art. 8i. Podmioty kluczowe i podmioty ważne z sektora bankowości i infrastruktura rynków finansowych nie stosują przepisów niniejszego rozdziału, rozdziałów 11, 12a i 14 oraz art. 46 ust. 4 w zakresie w jakim mają obowiązek stosować rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (Dz. Urz. UE L 333 z 27.12.2022, str. 1).”; Należy zwrócić uwagę, że dyrektywa NIS 2 wskazuje co prawda bankowość jako jeden z sektorów kluczowych oraz instytucje kredytowe (w tym banki - zgodnie z definicją w art. 4 pkt 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 575/2013) jako podmioty kluczowe, niemniej, zgodnie z art. 4 dyrektywy NIS 2, do podmiotów sektora bankowego nie stosuje się „odpowiednich przepisów [...] dyrektywy, w tym przepisów dotyczących nadzoru i egzekwowania przepisów określonych w rozdziale VII” o ile, stosowne obowiązki wynikają z „sektorowych aktów prawnych Unii”. Za tego rodzaju akt należy uznać rozporządzenie 2022/2554 (tzw. rozporządzenie DORA).	Wyjaśnienie uwagi Przepis zostanie zmieniony zgodnie z uwagami KNF.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			Zgodnie z projektem ustawy o zmianie niektórych ustaw w związku z zapewnieniem operacyjnej odporności cyfrowej sektora finansowego (nr z wykazu prac RM: UC11), to Komisja Nadzoru Finansowego, stanie się właściwym organem w rozumieniu art. 46 rozporządzenia 2022/2554 – tj. organem nadzoru posiadającym wobec uczestników sektora bankowego uprawnienia nadzorcze – w tym m.in. uprawnienia do przeprowadzania stosownych inspekcji oraz nakładania kar. Takie rozwiązanie pozostaje zgodne z jednym z celów rozporządzenia 2022/2554 – tj. uregulowania w sposób odrębny obowiązków oraz zasad nadzoru dotyczących sektora finansowego w obszarze cyberbezpieczeństwa i odporności cyfrowej. Brak jest zatem uzasadnienia do nakładania na przedstawicieli sektora bankowego dodatkowych obowiązków związanych m.in z obowiązkiem uczestniczenia w systemie teleinformatycznym o którym mowa w art. 46 ustawy. Tego rodzaju obowiązek nie został przewidziany w treści Dyrektywy NIS 2 oraz brak jest argumentów pozwalających przyjąć, że obowiązek uczestniczenia w systemie nie jest objęty wyłączeniem o którym mowa w art. 4 dyrektywy NIS 2. Ponadto uczestniczenie w przedmiotowym systemie będzie wymagało poniesienia przez sektor bankowy kosztów nieproporcjonalnych do osiągniętych korzyści. Z uwagi na stosowne uregulowania wynikające z rozporządzenia DORA oraz ze względu na uregulowania przewidziane w ww. projekcie ustawy, brak jest możliwości sprawowania wobec sektora finansowego nadzoru na podstawie ustawy o krajowym systemie cyberbezpieczeństwa. Stosowne uprawnienia KNF w tym zakresie zostaną wprowadzone do ustawy z dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym. Umożliwienie sprawowania bezpośredniego nadzoru nad podmiotami sektora bankowego na podstawie ustawy o krajowym systemie cyberbezpieczeństwa będzie prowadziło do dualizmu uprawnień w tym zakresie oraz szeregu możliwych trudności interpretacyjnych i praktycznych.	
478.	Konfederacja Lewiatan	Art. 8i	Uwaga: Projekt ustawy o krajowym systemie cyberbezpieczeństwa wprowadza zasadniczą różnicę w stosunku do dyrektywy NIS2, która zwalnia sektor bankowy i rynki finansowe z obowiązków dyrektywy. W projekcie ustawy KSC, sektor ten jest zobowiązany do przestrzegania ustawy KSC w zakresie, w jakim nie stosuje on rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2554. Tymczasem, zgodnie z art. 2 ust. 10 dyrektywy NIS2, podmioty te są całkowicie wyłączone z obowiązków wynikających z dyrektywy na podstawie zwolnienia. Zgodnie z tym przepisem: <i>Niniejsza dyrektywa nie ma zastosowania do podmiotów, które państwa członkowskie zwolniły z zakresu stosowania rozporządzenia (UE) 2022/2554 zgodnie z art. 2 ust. 4 tego rozporządzenia.</i> To rozwiązanie wydaje się być nie tylko sprzeczne z duchem dyrektywy NIS2, ale także wprowadza dodatkowe, potencjalnie zbędne obciążenia dla sektora bankowego i rynków finansowych. Sektory te są już wysoko regulowane i objęte ścisłymi przepisami dotyczącymi cyberbezpieczeństwa, co czyni obowiązki wynikające z ustawy KSC w najlepszym przypadku redundantnymi, a w najgorszym — generującymi dodatkowe, niepotrzebne koszty administracyjne i operacyjne. Takie podejście nie tylko nie przyczynia się do rzeczywistego wzrostu poziomu cyberbezpieczeństwa, ale może również prowadzić do nadmiernego skomplikowania procesów regulacyjnych w sektorze.	Wyjaśnienie uwagi Przepis zostanie zmieniony zgodnie z uwagami KNF.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

479.	Issa Polska	Art. 8i	Brak zwolnienia sektora bankowego i rynków finansowych z obowiązków wynikających z ustawy KSC wbrew dyrektywie NIS2 Projekt ustawy o krajowym systemie cyberbezpieczeństwa wprowadza zasadniczą różnicę w stosunku do dyrektywy NIS2, która zwalnia sektor bankowy i rynki finansowe z obowiązków dyrektywy. W projekcie ustawy KSC, sektor ten jest zobowiązany do przestrzegania ustawy KSC w zakresie, w jakim nie stosuje on rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2554. Tymczasem, zgodnie z art. 2 ust. 2 dyrektywy NIS2, podmioty te są całkowicie wyłączone z obowiązków wynikających z dyrektywy. To rozwiązanie wydaje się być nie tylko sprzeczne z duchem dyrektywy NIS2, ale także wprowadza dodatkowe, potencjalnie zbędne obciążenia dla sektora bankowego i rynków finansowych. Sektory te są już wysoko regulowane i objęte ścisłymi przepisami dotyczącymi cyberbezpieczeństwa, co czyni obowiązki wynikające z ustawy KSC w najlepszym przypadku redundantnymi, a w najgorszym — generującymi dodatkowe, niepotrzebne koszty administracyjne i operacyjne. Takie podejście nie tylko nie przyczynia się do rzeczywistego wzrostu poziomu cyberbezpieczeństwa, ale może również prowadzić do nadmiernego skomplikowania procesów regulacyjnych w sektorze. Proponujemy ujednolicenie oraz zsynchronizowanie przygotowania ustaw wdrażających dyrektywę NIS2, rozporządzenie DORA i dyrektywę CER.	Wyjaśnienie uwagi Przepis zostanie zmieniony zgodnie z uwagami KNF.
480.	Związek Pracodawców Technologii Cyfrowych Lewiatan	Art. 8i	Uwzględnienie European Health Data Spaces (art. 8i) Podobnie jak wymieniona w tym artykule DORA dla sektora finansowego należy uwzględnić European Health Data Spaces dla sektora ochrony zdrowia.	Uwaga nieuwzględniona Przepisy te nie są jeszcze przyjęte i nie możemy ich uwzględnić w projekcie.
481.	Cybermadeinpol and	Art. 9	Doprecyzowanie wymagań względem zakresu materiałów w art. 9 p. 2) - nie sposób edukować o każdym możliwym ryzyku.	Wyjaśnienie uwagi To prawda, natomiast chodzi o podstawowe informacje dotyczące cyberbezpieczeństwa, o typowych cyberzagrożeniach, z którymi mierzą się użytkownicy usług.
482.	Konfederacja Lewiatan	Art. 9	Projektowany przepis wskazuje na rozpoczęcie korzystania z S46 w 2 tygodnie od wpisu do rejestru. Projektowany art. 46 ust. 4 określa, że rozpoczęcie korzystania następuje po wpisie, bez wskazania na termin 2 tygodni. Z kolei z art. 15 ustawy nowelizującej wynika, że <i>minister właściwy do spraw informatyzacji ogłasza komunikat określający harmonogram rozpoczęcia korzystania z S46</i>. Co więcej komunikat ten może być <i>zmieniany jeżeli z powodów technicznych lub organizacyjnych niemożliwe jest dokonanie wpisów i rozpoczęcie korzystania z S46</i>. Poza tym, wątpliwości budzi wskazanie, że podmiot korzysta z s46 w pełnym zakresie funkcji określonych w art. 46 ust. 1. Wśród nich znajdują się takie, które wydają się wykraczać poza jego	Uwaga uwzględniona Przepisy zostały uszójnione - podmiot kluczowy i podmiot ważny rozpoczyna realizację obowiązków z zakresu cyberbezpieczeństwa oraz podłącza się do systemu S46 w terminie 6 miesięcy od spełnienia przesłanek uznania za podmiot kluczowy lub podmiot ważny.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			możliwości, jak np.: <i>generowanie i przekazywanie rekomendacji dotyczących działań podnoszących poziom cyberbezpieczeństwa czy szacowanie ryzyka na poziomie krajowym</i>. Nowe funkcjonalności S46 wynikające z pkt 6 i 7, mają być jednocześnie uruchomione dopiero w okresie do roku od wejścia w życie ustawy, co wynika z art. 16. Z uwagi na potencjalną karę pieniężną związaną z korzystaniem z S46 kwestia ta wymaga jednoznacznego wyjaśnienia w przepisach ustawy. Wnosimy również o przedstawienie założeń funkcjonowania nowego S46 w ramach spotkania warsztatowego.	
483.	Akademia Górniczo-Hutnicza	Art. 9	Ustawa powinna dopuszczać także jednostki organizacyjne jako punkty kontaktowe. Wyznaczenie dwóch osób zapewnia minimalne zapewnienie dostępności punktu kontaktowego, jednakże ogranicza możliwości podmiotu kluczowego lub ważnego do kształtowania swojej struktury organizacyjnej. Właściwym również będzie zezwolenie tutaj na wyznaczenie punktu kontaktowego w postaci jednostki organizacyjnej podmiotu kluczowego lub ważnego. Taka jednostka (np. wewnętrzny dział SOC, który na przykład działa w trybie 24/7), może zapewnić większą responsywność i lepszą komunikatywność niż dwie osoby fizyczne o ograniczonym czasie pracy.	Wyjaśnienie uwagi Nic nie stoi na przeszkodzie, aby osobą kontaktową był pracownik danej jednostki organizacyjnej – wewnętrznego działu SOC.
484.	Polska Izba Informatyki i Telekomunikacji	Art. 9	Projekt ustawy przewiduje zmianę w art. 9 ust. 1 pkt 1) ustawy o krajowym systemie cyberbezpieczeństwa, tak, aby obowiązkiem podmiotów kluczowych i ważnych było wyznaczanie dwóch osób odpowiedzialnych za utrzymywanie kontaktów z innymi podmiotami kluczowymi i ważnymi. W naszej ocenie wymóg wskazywania konkretnych dwóch osób nie jest optymalnym rozwiązaniem i powinien zostać zastąpiony wymogiem określenia i wskazania sposobu i kanału kontaktu, który może być wykorzystywany do kontaktowania się z podmiotem w sprawach związanych z wykonywaniem ustawy i cyberbezpieczeństwem. Czyli zamiast wymogu wyznaczania dwóch osób wymóg wyznaczenia adresu e-mail i numeru telefonu, które będą służyły do kontaktu. Biorąc pod uwagę, że podmiotów kluczowych i ważnych w nowym systemie cyberbezpieczeństwa będą tysiące nie ma najmniejszych szans na ustanowienie relacji personalnych pomiędzy tymi podmiotami, relacji, które uzasadniałyby konieczność określenia konkretnych osób jako kontaktowych. A jednocześnie wskazywanie punktów kontaktowych z imienia i nazwiska, wobec dużej rotacji na rynku pracy, będzie skutkowało zarówno po stronie administracji jak i po stronie podmiotów kluczowych i ważnych wymogiem ciągłej aktualizacji danych osób kontaktowych. Lepszym rozwiązaniem byłaby możliwość wskazania adresu e-mail i numeru telefonu do kontaktu (albo innych powszechnie wykorzystywanych kanałów komunikacji), przy zapewnieniu, że adres ten i numer telefonu będą obsługiwane przez osobę albo zespół osób, których zadaniem w danym czasie jest obsługiwanie spraw związanych z cyberbezpieczeństwem.	Uwaga nieuwzględniona W sytuacjach kryzysowych niezbędne jest skontaktowanie się z konkretnymi osobami.
485.	Polska Izba Informatyki i Telekomunikacji	Art. 9	Projektowany przepis wskazuje na rozpoczęcie korzystania z S46 w 2 tygodnie od wpisu do rejestru. Projektowany art. 46 ust. 4 określa, że rozpoczęcie korzystania następuje po wpisie, bez wskazania na termin 2 tygodni. Z kolei z art. 15 ustawy nowelizującej wynika, że <i>minister właściwy do spraw informatyzacji ogłasza komunikat określający harmonogram rozpoczęcia korzystania z S46</i>. Co więcej komunikat ten może być <i>zmieniany, jeżeli z powodów technicznych lub organizacyjnych niemożliwe jest dokonanie wpisów i rozpoczęcie korzystania z S46</i>.	Uwaga uwzględniona Terminy zostaną przeanalizowane.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			Poza tym wątpliwości budzi wskazanie, że podmiot korzysta z s46 w pełnym zakresie funkcji określonych w art. 46 ust. 1. Wśród nich znajdują się takie, które wydają się wykraczać poza jego możliwości, jak np. <i>generowanie i przekazywanie rekomendacji dotyczących działań podnoszących poziom cyberbezpieczeństwa czy szacowanie ryzyka na poziomie krajowym</i>. Nowe funkcjonalności S46 wynikające z pkt 6 i 7 mają być jednocześnie uruchomione dopiero w okresie do roku od wejścia w życie ustawy, co wynika z art. 16. Z uwagi na potencjalną karę pieniężną związaną z korzystaniem z S46 kwestia ta wymaga jednoznacznego wyjaśnienia w przepisach ustawy. Wnosimy również o przedstawienie założeń funkcjonowania nowego S46 w ramach spotkania warsztatowego.	
486.	Polskie Stowarzyszenie Fotowoltaiki	Art. 9-10	Dodatkowe obowiązki PK i PW - wyznaczenie dwóch osób kontaktowych w sprawach dot. cyberbezpieczeństwa; - zapewnienie użytkownikom dostępu do wiedzy w zakresie cyberzagrożeń (w szczególności na stronie internetowej); - stosowanie systemu S46 w terminie 14 dni od wpisu do Wykazu; - opracowanie, stosowanie i aktualizacja dokumentacji (normatywnej oraz operacyjnej) dot. bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usług (w formie papierowej lub elektronicznej). Dokumentacja normatywna dotycząca systemu zarządzania bezpieczeństwem informacji oraz zarządzania ciągłością działania usługi powinna być stworzona zgodnie z wymaganiami Polskich Norm PN-EN ISO odpowiednio 27001 i 22301 (lub norm im równoważnych); - zapewnienie nadzoru nad dokumentacją dot. bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usług oraz przechowywanie jej przez 2 lata od dnia jej wycofania z użytkowania lub zakończenia świadczenia usługi, liczony od 1 stycznia następnego roku; - obowiązek protokolowania zniszczenia wycofanej z użytkowania dokumentacji Ogólny wpływ regulacji: Realizacja obowiązków określonych w art. 9-10 KSC wg Projektu, w szczególności w zakresie wyznaczania określonej liczby osób kontaktowych, zapewniania dostępu do wiedzy oraz szczegółowe wymogi w odniesieniu do dokumentacji dot. bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usług wymaga poniesienia przez podmioty zobowiązane istotnych nakładów organizacyjnych oraz finansowych jak również zapewnienia odpowiednich zasobów ludzkich. Wpływ na sektor energetyczny: jw. – brak specyficznego wpływu na sektor energetyczny [Nadregulacja względem Dyrektywy NIS2] Obowiązki wynikające z Dyrektywy NIS2 nie obejmują w ogóle bądź nie precyzują tak szczegółowo obowiązków jakie mają zostać nałożone na PK i PW na podstawie Projektu. W rezultacie, stanowią one daleko idącą nadregulację względem Dyrektywy NIS2.	Wyjaśnienie uwagi Dla celów nadzorczych oraz audytowych niezbędne jest aby podstawowe działania w obszarze cyberbezpieczeństwa były dokumentowane. Przy czym dokumentacja może być prowadzona w postaci elektronicznej.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			Jednocześnie, nałożenie na podmioty zobowiązane tak szczegółowych obowiązków ustawowych w zakresie m.in. przechowywania oraz niszczenia dokumentacji dot. bezpieczeństwa systemów informacyjnych nie znajdują uzasadnienia w świetle wymogów Dyrektywy NIS2. Rekomendacja Ograniczenie obowiązków PK i PW, w szczególności w odniesieniu do przechowywania dokumentacji po jej wycofaniu oraz niszczenia.	
487.	Polska Izba Informatyki i Telekomunikacji	Art. 10	W art. 10 ust. 4 wskazano, że dokumentacja może być prowadzona elektronicznie ALBO papierowo. Wydaje się, że właściwym byłoby użycie alternatywy łącznej, tj. LUB. Dodatkowe zastrzeżenia budzą: • Art. 10 ust. 3 pkt 5 - co gdy zostaną wydane rekomendacje z art. 8a? Co ma zrobić podmiot kluczowy z posiadaną dokumentacją? • Art. 10 ust. 5 pkt 2 - integralność to właśnie ochrona przed jakąkolwiek modyfikacją Ponadto za nieuzasadniony i uciążliwy, a zatem zbędny, należy uznać wymóg protokolarnego niszczenia dokumentacji bezpieczeństwa systemu informacyjnego. Projektowany art. 10 ust. 7 ustawy stanowi, że zniszczenie wycofanej z użytkowania dokumentacji potwierdza się protokołem brakowania zawierającym w szczególności: datę protokołu, oznaczenie niszczonej dokumentacji, dane osoby zatwierdzającej protokół. Protokoły brakowania dokumentacji mają być przechowywane w sposób trwały. W przypadku dużych organizacji, korzystających z licznych systemów informacyjnych, spełnienie tego wymogu – nawet przy spełnieniu wszystkich innych wymogów związanych z nadzorem nad tymi dokumentami – będzie zadaniem uciążliwym, czasochłonnym, a zatem kosztownym. Dokumentacja taka może być bowiem przechowywana w kilku różnych egzemplarzach, w różnych zasobach, co oznacza, że wymóg protokolarnego niszczenia dokumentów pośrednio oznacza wymóg ciągłego inwentaryzowania wszystkich egzemplarzy i kopii tych dokumentów. Z drugiej strony, jeśli dokumentacja jest odpowiednio chroniona, to nie jest konieczne jej niszczenie, a tym bardziej nieszczelnie protokolarne. I nie sposób pominąć wymogu bezterminowego (czyli po wsze czasy) przechowywania protokołów. Prosimy o usunięcie w całości ust. 7 z art. 10 ustawy. Zwracamy również uwagę na potrzebę weryfikacji prawidłowości zapisów w ust. 6 w art. 10 ustawy (w brzmieniu nadawanym projektowaną ustawą), który to przepis wyznacza termin (i określa sposób liczenia tego terminu) przechowywania dokumentacji systemu informacyjnego wykorzystywanego do świadczenia usługi, która została wycofana. Przepis ten stanowi, że momentem początkowym, od którego należy liczyć dwuletni termin jest 1 stycznia roku następującego po roku, w którym wygasa okres jej przechowywania. Nie wiadomo jak rozumieć ten przepis, bo literalnie rzecz ujmując przepis wymaga, aby początek terminu przechowywania dokumentacji liczyć od momentu wygaśnięcia okresu przechowywania.	Uwaga częściowo uwzględniona Dokumentacja będzie prowadzona w postaci elektronicznej lub papierowej. Wprowadzenie przepisu o protokołowaniu zniszczenia dokumentacji jest konieczne aby wykazać, że ta dokumentacja w ogóle istniała.
488.	Audyty	Art. 10	Komentowany przepis wprowadza do Ustawy art. 10 ust. 2. pkt 3 „3. Dokumentację normatywną stanowią:	Uwaga nieuwzględniona w związku z rezygnacją z odwołania się do norm

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			1)dokumentacja dotycząca systemu zarządzania bezpieczeństwem informacji wytworzona zgodnie z wymaganiami Polskiej Normy PN-EN ISO/IEC 27001 lub normy jej równoważnej;" oraz „3)dokumentacja systemu zarządzania ciągłością działania usługi wytworzona zgodnie z wymaganiami Polskiej Normy PN-EN ISO 22301 lub normy jej równoważnej;" Proponujemy podobnie jak w poz. 1 zastosować analogiczne zmiany, czyli komentowany przepis przyjąłby następujące brzmienie. „3. Dokumentację normatywną stanowią: 1)dokumentacja dotycząca systemu zarządzania bezpieczeństwem informacji wytworzona zgodnie z wymaganiami aktualnego wydania międzynarodowej normy ISO/IEC 27001. W przypadku uchylenia normy należy stosować wymagania normy, która ją zastąpi.” oraz „3)dokumentacja systemu zarządzania ciągłością działania usługi wytworzona zgodnie z wymaganiami aktualnego wydania międzynarodowej normy ISO/IEC 22301. W przypadku uchylenia normy należy stosować wymagania normy, która ją zastąpi;"	
489.	Cybermadeinpol and	Art. 10	Art. 10 p. 3. 1) - doprecyzowanie czy zgodność dokumentacji z normami musi być potwierdzona przez jednostkę akredytującą.	Wyjaśnienie uwagi Zrezygnowano z odniesienia do norm technicznych.
490.	Cybermadeinpol and	Art. 10	Art. 10 7. - zmiana brzmienia na: 7. Trwałe i nieodwracalne zniszczenie wycofanej z użytkowania dokumentacji potwierdza się protokołem brakowania zawierającym w szczególności: datę protokołu, oznaczenie niszczonej dokumentacji, metody i parametrów niszczenia, dane osoby zatwierdzającej protokół. Protokoły brakowania dokumentacji są przechowywane w sposób trwały.	Uwaga częściowo uwzględniona Zostanie przepis uzupełniony o sposób niszczenia dokumentacji.
491.	Cybermadeinpol and	Art. 10	Definicja trwałego przechowywania art. 10 p. 7 oraz dodanie wyjątku dla rejestrów, które obowiązują retencja (np. logi).	Uwaga nieuwzględniona Uwaga jest zbyt ogólna i niejasna aby ją uwzględnić.
492.	Fundacja Bezpieczna Cyberprzestrzeń	Art. 10	art. 1 pkt 14, treść art. 10 ust. 1 – ust. 4 (uwagę należy czytać w powiązaniu z uwagami w pkt 9 i 10) – wymagania normatywne ISO27001 (ISO27002) oraz ISO 22301 uwzględniają wszystkie aspekty prowadzonej działalności, w tym jej charakter i specyfikę oraz wszelkie uwarunkowania (określone w normie jako kontekst organizacji). Ponadto bezpieczeństwo fizyczne stanowi ważną część systemu zarządzania bezpieczeństwem informacji i stanowi jedną z domen bezpieczeństwa wskazanych w nowych wersjach norm 27001 i 27002. W opinii FBC, biorąc pod uwagę wcześniejsze uwagi nie ma potrzeby ponownie wskazywać konkretnej dokumentacji, jako elementów systemu zarządzania bezpieczeństwem informacji (jeśli celem jest zachowanie spójności systemu zarządzania bezpieczeństwem informacji). Oznacza to w praktyce, że rzetelnie wdrożony system zarządzania bezpieczeństwem informacji oraz system zarządzania ciągłością działania wypełnią treść art. 10 ust. 1 do ust. 4. W związku z powyższym proponuje się ograniczenie treści przepisów art. 10 do ust. 5, ust. 6 i ust. 7.	Wyjaśnienie uwagi W przepisie usunięte zostaną odniesienia do norm technicznych.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

493.	ISAC-Kolej	Art. 10	„2. Do dokumentacji, o której mowa w ust. 1, zalicza się:” W ustępie tym powinno się odwołać do dokumentacji dotyczącej bezpieczeństwa systemu informacyjnego lub technologii operacyjnej wykorzystywanej do świadczenia usługi wskazanej w ust. 1	Uwaga nieuwzględniona Jak wyżej wskazano definicja systemu informacyjnego obejmuje systemy OT, więc nie ma potrzeby zmiany przepisu.
494.	ISAC-Kolej	Art. 10	„2) dokumentacja ochrony infrastruktury, z wykorzystaniem której świadczona jest usługa, obejmująca: a) charakterystykę usługi oraz infrastruktury, w której świadczona jest usługa, b) ocenę aktualnego stanu ochrony infrastruktury, c) szacowanie ryzyka dla obiektów infrastruktury, d) plan postępowania z ryzykiem, e) opis zabezpieczeń technicznych obiektów infrastruktury, f) zasady organizacji i wykonywania ochrony fizycznej infrastruktury, g) dane o specjalistycznej uzbrojonej formacji ochronnej, o której mowa w art. 2 pkt 7 ustawy z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz. U. z 2021 r. poz. 1995.), chroniącej infrastrukturę – jeżeli występuje” W przepisie tym należy zachować chronologię podejmowanych działań związanych z zarządzaniem bezpieczeństwem infrastruktury, co powinno być odzwierciedlone w dokumentacji. Ocena aktualnego stanu ochrony infrastruktury to coś innego niż plan postępowania z ryzykiem, który stanowi element opisujący podejmowane działania w stosunku do ryzyk nieakceptowanych lub nietolerowanych określonych w procesie zarządzania ryzykiem.	Uwaga uwzględniona Przepis zostanie zmieniony – w pkt 2 porządek liter zostanie zmieniony.
495.	ISAC-Kolej	Art. 10	„4) „dokumentacja systemu bezpieczeństwa systemów sterowania i automatyki przemysłowej wytworzona zgodnie z wymaganiami Polskiej Normy PN-EN IEC 62443 lub normach i standardach branżowych mających zastosowanie w danym sektorze lub podsektorze;” Dokumentację normatywną powinna stanowić również dokumentacja dotycząca technologii operacyjnych użytkowanych przez podmioty kluczowe i ważne, bez względu na to czy jest to dokumentacja wynikająca z normy ISO62443 czy z innych norm branżowych i standardów obowiązujących w danym sektorze lub podsektorze.	Uwaga nieuwzględniona W związku z rezygnacją ze wskazywania norm w przepisie.
496.	ISSA Polska	Art. 10	Zakres dokumentacji ochrony infrastruktury W art. 10 ust. 3 pkt. 2 ustawy o KSC znalazły się postanowienia nakładające obowiązki dotyczące posiadania dokumentacji ochrony infrastruktury. Treść tych zapisów jest oparta na regulacjach zawartych w ustawie o zarządzaniu kryzysowym (dla podmiotów infrastruktury krytycznej). W związku z tym nie ma sensu powtarzania zapisów dla tych podmiotów kluczowych i ważnych, które są podmiotami infrastruktury krytycznej. Dla podmiotów niekrytycznych zakres dokumentacji powinien być określony adekwatnie do skali i specyfiki prowadzonej działalności, na podstawie ustawy o ochronie osób i mienia, która reguluje omawianą materię. Ze względu na istotność usług dla życia społecznego, w każdej dokumentacji dotyczącej ochrony, bez względu na charakter infrastruktury, powinny być uwzględnione kwestie zagrożeń atakami terrorystycznymi. Rodzaje dokumentacji wymaganej zgodnie z art. 10 ust. 3 (w poszczególnych punktach) są określone w sposób, który może	Wyjaśnienie uwagi Art. 10 ust. 3 nie wymaga tworzenia odrębnych dokumentów, wskazuje jedynie na ich zakres.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			prorowadzić do powstawania dokumentów o zachodzącej na siebie treści, dublując liczbę dokumentów bez potrzeby. Wskazane jest więc przejrzenie sposobu sformułowania zapisów w tym punkcie w celu zoptymalizowania organizacji systemu zarządzania bezpieczeństwem (ograniczenie formalizmów, które nie przełożą się odpowiednio na efekty w zakresie cyberbezpieczeństwa). Np. dokumentacja SZBI zawiera w sobie elementy ciągłości działania.	
497.	ISACA	Art. 10	Dokumentację operacyjną stanowią zapisy poświadczające wykonywanie czynności wymaganych przez postanowienia zawarte w dokumentacji normatywnej, w tym automatycznie generowane zapisy w dziennikach systemów teleinformatycznych. Zastąpić zapisem normy ISO/IEC 27001 "udokumentowane informacje, określone przez organizację jako niezbędne dla skuteczności systemu zarządzania bezpieczeństwem informacji". Należy zwrócić uwagę, że zakres udokumentowanych informacji w systemie zarządzania bezpieczeństwem informacji może być różny dla różnych organizacji, (...) "Zgodnie z normą [PN-EN ISO/IEC 27001 7.5.1] System zarządzania bezpieczeństwem informacji w organizacji powinien zawierać: - udokumentowane informacje wymagane przez niniejszą Normę Międzynarodową; oraz - udokumentowane informacje, określone przez organizację jako niezbędne dla skuteczności systemu zarządzania bezpieczeństwem informacji. Celem jest skuteczność, a nie posiadanie dokumentacji, w szczególności ""wykonywania"" jakiś bliżej nieokreślonych czynności, które nie wiadomo czemu mają służyć."	Wyjaśnienie uwagi Zgadamy się, że celem środków jest skuteczność. Natomiast bardzo ważna jest rozliczalność czynności podejmowanych w systemie informacyjnym. Kwestie te są także niezbędne do prawidłowego przeprowadzenia audytu oraz do czynności nadzorczych.
498.	ISACA	Art. 10	"3. Dokumentację normatywną stanowią: 1) dokumentacja dotycząca systemu zarządzania bezpieczeństwem informacji wytworzona zgodnie z wymaganiami Polskiej Normy PN-EN ISO/IEC 27001 lub normy jej równoważnej; 2) dokumentacja ochrony infrastruktury, z wykorzystaniem której świadczona jest usługa, obejmująca: a) charakterystykę usługi oraz infrastruktury, w której świadczona jest usługa, b) szacowanie ryzyka dla obiektów infrastruktury, c) ocenę aktualnego stanu ochrony infrastruktury (plan postępowania z ryzykiem), d) opis zabezpieczeń technicznych obiektów infrastruktury, e) zasady organizacji i wykonywania ochrony fizycznej infrastruktury, f) dane o specjalistycznej uzbrojonej formacji ochronnej, o której mowa w art. 2 pkt 7 ustawy z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz. U. z 2021 r. poz. 1995.), chroniącej infrastrukturę – jeżeli występuje; 3) dokumentacja systemu zarządzania ciągłością działania usługi wytworzona zgodnie z wymaganiami Polskiej Normy PN-EN ISO 22301 lub normy jej równoważnej; 4) dokumentacja techniczna systemu informacyjnego wykorzystywanego do świadczenia usługi; 5) dokumentacja wynikająca ze specyfiki świadczonej usługi w danym sektorze lub podsektorze. " "zastąpienie ustępu następującą treścią:	Wyjaśnienie uwagi Zrezygnowano z odniesienia się do konkretnej normy technicznej w przepisie. Pod pojęciem infrastruktury należy rozumieć urządzenia i usługi umożliwiające świadczenie usługi przez dany podmiot. Dokumentowanie i ocena stosowanych rozwiązań kryptograficznych oraz szacowanie ryzyka dla łańcucha dostaw mieści się w ramach dokumentacji SZBI.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

		3. Dokumentację normatywną stanowią: 1) uzasadnienie wyboru odpowiedniej normy lub norm w kontekście ocenianego ryzyka oraz specyfiki prowadzonej działalności, wraz z kompletnym mapowaniem wymagań wybranej normy lub norm na obowiązki wynikające z art. 8 ust. 1 ustawy, jeżeli podmiot nie korzysta z mapowania, o którym mowa w art. 8 ust. 3; 2) dokumentacja dotycząca systemów zarządzania bezpieczeństwem informacji oraz zarządzania ciągłością działania, wytworzona zgodnie z wymaganiami wybranej normy lub norm, pod warunkiem opracowania kompletnego mapowania wymagań wybranej normy lub standardu na obowiązki wynikające z art. 8 ust. 1 ustawy, jeżeli podmiot nie korzysta z mapowania, o którym mowa w art. 8 ust. 3; punktu nie stosuje się, jeżeli podmiot nie wdraża systemu zarządzania bezpieczeństwem informacji zgodnie z wymaganiami Polskiej Normy lub międzynarodowej normy; 3) dokumentacja ochrony infrastruktury, z wykorzystaniem której świadczona jest usługa, obejmująca: a) charakterystykę usługi oraz infrastruktury, w tym obiektów, urządzeń, systemów, sieci, z wykorzystaniem których świadczona jest usługa, b) szacowanie ryzyka dla elementów infrastruktury oraz łańcucha dostaw, c) ocenę aktualnego stanu ochrony infrastruktury (plan postępowania z ryzykiem), d) opis zabezpieczeń technicznych elementów infrastruktury, e) zasady organizacji i wykonywania ochrony fizycznej infrastruktury, "f) dane o specjalistycznej uzbrojonej formacji ochronnej, o której mowa w art. 2 pkt 7 ustawy z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz.U. z 2021 r. poz. 1995), chroniącej infrastrukturę – jeżeli występuje, g) opis stosowanych rozwiązań kryptograficznych lub ich braku, oraz ocena ryzyka z tym związana, w tym ocena wystarczalności zastosowanych rozwiązań kryptograficznych. 4) dokumentacja techniczna systemu informacyjnego wykorzystywanego do świadczenia usługi oraz działalności wykonywanej przez podmiot, od której uzależnione jest świadczenie usługi; 5) dokumentacja wynikająca ze specyfiki świadczonej usługi w danym sektorze lub podsektorze. 6) W przypadku, gdy podmiot kluczowy lub podmiot ważny wdraża wymagania art. 8 ust. 1 ustawy, bez posługiwania się normą lub standardem, o których mowa w Art 8. ust 2, dokumentacja powinna obejmować szczegółowy opis sposobu spełnienia poszczególnych obowiązków wynikających z art. 8 ust. 1 ustawy." "1. Poprzednie brzmienie ustawy ograniczało się do konkretnych Polskich Norm, co mogło nie odpowiadać specyficznym potrzebom i kontekstowi działalności różnych podmiotów. Nowe brzmienie uwzględnia możliwość stosowania innych uznanych międzynarodowych norm lub standardów, co zwiększa elastyczność i pozwala na lepsze dostosowanie systemu zarządzania do specyfiki działalności podmiotu. 2. Wprowadzenie możliwości wdrażania wymagań art. 8 ust. 1 ustawy wprost, bez posługiwania się normą lub standardem, pozwala podmiotom na bezpośrednie spełnienie przepisów ustawy. W takim	

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			przypadku dokumentacja musi obejmować szczegółowy opis sposobu spełnienia poszczególnych obowiązków, co zapewnia przejrzystość i kompletność wdrożenia. Poprzednie brzmienie ust. 3 niezależnie od decyzji podmiotu co do wdrożenia lub niewdrożenia norm ISO/IEC 27001 oraz ISO 22301, przez konieczność posiadania dokumentacji określonej tymi normami de facto i tak zmuszało do wdrożenia tych norm - co powodowało pozorność art. 8 ust. 2 (możliwość oparcia się o normy a nie konieczność ich implementacji). 3. Rozszerzenie dokumentacji technicznej systemu informacyjnego o działalność wykonywaną przez podmiot, od której uzależnione jest świadczenie usługi, zapewnia, że wszystkie aspekty techniczne i operacyjne są odpowiednio udokumentowane, co zwiększa przejrzystość i efektywność zarządzania bezpieczeństwem informacji. 4. Rozszerzenie wymagań pkt. 3 jest podyktowane: - Koniecznością zdefiniowania, co ustawodawca ma na myśli pod pojęciem infrastruktury. W poprzednim brzmieniu nie było dookreślone, co dokładnie obejmuje infrastruktura. Nowe brzmienie precyzuje, że infrastruktura obejmuje urządzenia, systemy, sieci i instytucje, co pozwala na dokładniejsze zrozumienie zakresu ochrony. - Uwzględnieniem w szacowaniu ryzyka łańcucha dostaw. Podmioty mogą mieć skomplikowane łańcuchy dostaw, od których uzależnione jest świadczenie usługi. Szacowanie ryzyka dla łańcucha dostaw zapewnia, że wszystkie kluczowe zależności są brane pod uwagę i odpowiednio zarządzane. - Uwzględnieniem oceny stosowanych rozwiązań kryptograficznych lub uzasadnieniem ich braku oraz oceną związanych z tym ryzyk. Dokumentowanie i ocena stosowanych rozwiązań kryptograficznych zapewnia, że aspekty związane z bezpieczeństwem informacji są odpowiednio zarządzane. Ocena wystarczalności tych rozwiązań dokumentuje adekwatność stosowanych środków do poziomu ryzyka, co jest kluczowe dla zapewnienia bezpieczeństwa informacji."	
499.	ISACA	Art. 10	4. Dokumentacja, o której mowa w ust. 1, może być prowadzona w postaci papierowej albo w postaci elektronicznej. Zmiana spójnika na "lub" Wprowadzenie zmiany spójnika z "albo" na "lub" w ustępie 4 ustawy, dotyczącej możliwości prowadzenia dokumentacji w postaci papierowej albo elektronicznej, umożliwi podmiotom prowadzenie dokumentacji w sposób mieszany – zarówno papierowy, jak i elektroniczny. Obecne brzmienie ogranicza podmioty do wyboru jednej formy, co nie zawsze jest praktyczne ani efektywne.	Uwaga uwzględniona Zostanie umożliwione prowadzenie dokumentacji w postaci papierowej lub elektronicznej.
500.	ISACA	Art. 10	"Zniszczenie wycofanej z użytkowania dokumentacji potwierdza się protokołem brakowania zawierającym w szczególności: datę protokołu, oznaczenie niszczonej dokumentacji, dane osoby zatwierdzającej protokół. Protokoły brakowania dokumentacji są przechowywane w sposób trwały. "usunąć Wymaganie jest dalece nadmiarowe. Zgodnie z zasadami SZBI organizacja powinna określić sposób postępowania z informacjami w całym cyklu życia.	Uwaga nieuwzględniona Kwestia brakowania dokumentacji powinna zostać uregulowana. Poza tym dla celów kontroli/audytu – skoro przepis ustawy przewidywał istnienie dokumentacji, a tej dokumentacji nie ma, ponieważ została zastąpiona, to byłoby dobrze, żeby pozostał jakiś ślad, że ta dokumentacja w okresie, który jest

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

				kontrolowany, istniała i że została zniszczona przez konkretną osobę konkretnego dnia.
501.	ISACA	Art. 10	Brak informacji dotyczących postępowania z dokumentami spoza organizacji. Należy uzupełnić zapis i rozważyć przebudowanie całego art. 10 zgodnie z ISO/IEC 27001 7. Zagadnienie nie jest uregulowane, a jest istotne	Uwaga nieuwzględniona
502.	Osoba fizyczna	Art. 10	Ust. 1 – Zastosowano zapis odwołujący się do dokumentacji bezpieczeństwa systemu informacyjnego, podczas gdy jednocześnie wprowadzono nowy zapis art. 8 ust. 1 zobowiązujący do wdrożenia SZBI w procesach. Proponuję przyjąć jednorodne podejście przedmiotowe i konsekwentną realizację [ref. Propozycja pkt. 3.3]. Tego typu niespójność przewija się w całym dokumencie, co wymaga korekty.	Wyjaśnienie uwagi Przepis będzie odnosił się do dokumentacji bezpieczeństwa systemu informacyjnego wykorzystywanego w procesie świadczenia usługi.
503.	Osoba fizyczna	Art. 10	Ust. 3 – Wskazano zakres dokumentacji normatywnej bezpieczeństwa systemu informacyjnego, proponuję, nawiązując do propozycji pkt. 4.2 (ref. Art. 8 ust. 2) rozszerzyć zakres tej dokumentacji poprzez dodanie kolejnych pkt: „3a) dokumentacja systemu zarządzania usługami IT wytworzona zgodnie z wymaganiami Polskiej Normy PN-EN/ISO 20000-1 lub jej równoważnej, 3b) dokumentacja zarządzania ryzykiem bezpieczeństwa informacji (ryzykiem cyberbezpieczeństwa) wytworzona zgodnie z wymaganiami Polskiej Normy PN-EN/ISO 27005 lub jej równoważnej”.	Uwaga wyjaśniona Zrezygnowano z odniesienia się do norm technicznych w tym przepisie.
504.	Polska Izba Gospodarki Odpadami	Art. 10	Art. 1 ust 14) w zakresie zmiany Art. 10 ust. 3. pkt 1) KSC - Wyżej mowa jest, że gdy spełni się ISO27001 to spełniony jest warunek. Warto wskazać normę równoważną pytanie jaka norma? Czy mogą to być Narodowe Standardy Cyberbezpieczeństwa? Czy autor chciał pozostawić możliwość stosowania np. zaleceń amerykańskich NIST czy polskich NSC, które jednak nie są normami?	Uwaga uwzględniona Narodowe Standardy Cyberbezpieczeństwa nie są normą w rozumieniu ustawy o normalizacji. Odniesienie do norm zostanie usunięte.
505.	Polska Izba Gospodarki Odpadami	Art. 10	Art. 1 ust 14) w zakresie zmiany Art. 10 ust. 3. pkt 3) KSC – uwaga j.w.	Uwaga uwzględniona Narodowe Standardy Cyberbezpieczeństwa nie są normą w rozumieniu ustawy o normalizacji. Odniesienie do norm zostanie usunięte.
506.	Rada Bezpieczeństwa Biznesowego Grupy MiSOT	Art. 10	2. Jak wskazano na wstępie, sprzeciwiamy się obowiązkowi tworzenia dokumentacji zgodnie z normami ISO 27001 i ISO 22301. KSC powinna poprzestać na obowiązku zarządzania ryzykiem i tworzenia dokumentacji w sposób proporcjonalny do ryzyka związanego z działalnością danego przedsiębiorcy. Proponujemy również zmianę art. 10 ust. 1 KSC: „Podmiot kluczowy i podmiot ważny opracowuje, stosuje i aktualizuje dokumentację dotyczącą Zintegrowanego Systemu Zarządzania Bezpieczeństwem i Ciągłości Działania systemu informacyjnego wykorzystywanego do świadczenia usługi”. Uzasadnienie: W pierwszej kolejności pragniemy zwrócić uwagę, że normy ISO zmieniają się częściej niż ustawy. Odesłanie wprost do konkretnych norm ISO (jak w art. 10 ust. 3 KSC) doprowadza to do ryzyka	Uwaga uwzględniona Odniesienia do konkretnych norm w art. 10 zostaną usunięte.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			nagłego (a zatem i niebezpiecznego) przeprowadzania rewolucji w prowadzonych dokumentacjach po każdej zmianie normy ISO, aby wypełnić obowiązki wynikające z przepisów prawa. Przepis art. 10 ust. 3 pkt 2 lit. F i pkt 3, odwołując się do norm ISO, nie wskazuje, jakie wymogi dokumentacja systemu informacyjnego powinna spełniać. Zamiast tego zawiera blankietowe odesłanie do dokumentów wypracowywanych przez prywatne organizacje. Zmusza ten przepis każdy podmiot kluczowy i ważny do zakupu normy, a następnie każdej jej aktualizacji, nawet jeśli nie zamierza się certyfikować. Są to dokumenty objęte licencją i nie ma dostępnych “darmowych” norm aktualnych, aby zobaczyć jaka jest ich zawartość. Świetnym przykładem jest obecna wersja normy IEC/ISO 27001, gdzie aktualizacja całkowicie odbiega od normy obowiązującej jeszcze dwa lata temu. Co więcej konstrukcja wskazanych zapisów w tych artykułach będzie budziła niejasności, gdyż w żadnej z tych norm nie ma spisu treści dokumentacji wymaganej przy prowadzeniu systemu. Trzeba prześledzić całą normę aby wychwycić elementy, które muszą być “udokumentowane” aby pokazać nam się obraz spisu treści niezbędnej dokumentacji systemowej. Będzie to za każdym razem wymagało opinii specjalistów z tego zakresu. A przecież dla potrzeb bezpieczeństwa kraju można wpisać te dane wprost do ustawy, na których ustawodawcy konkretnie zależy. W załączeniu przesyłam szkoleniową wersję poprzedniej normy (niestety nie dysponuję szkoleniową wersją obecnej, a jak pisałem, są to dokumenty licencjonowane). Proszę spróbować określić dokumentację systemową ISO27001 na podstawie normy bez wsparcia certyfikowanego Audytora wiodącego albo wewnętrznego. Ile będzie interpretacji zawartości takiej dokumentacji i jak Państwo będziecie później podchodzili na kontrolach do sprawdzenia prawidłowości wykonania tych zapisów ustawowych. Proponujemy, aby wprowadzić zapisy wymaganej dokumentacji systemowej. W związku z powołaniem się na dwie normy (normę ciągłości działania oraz normę bezpieczeństwa) proponujemy w art. 10 ust. 1 KSC zastosować wymóg wprowadzenia “Zintegrowanego Systemu Zarządzania Bezpieczeństwem i Ciągłością działania”. Każda ze wskazanych norm posiada swój zakres dokumentacji systemowej. Pozostawienie takiego zapisu ustawowego skutkuje podwojeniem dokumentacji w rozumieniu literalnym, kiedy tak naprawdę normy dopuszczają integrację systemów zarządzania, a tym samym wyznaczenia części wspólnej dla obu systemów bez konieczności dokumentowania ich osobno. Dzięki takiemu zapisowi wskazujemy przejrzystą drogę stosowania systemu Zarządzania bez pozostawiania pola do interpretacji w zakresie intencji ustawodawcy.	
507.	Konfederacja Lewiatan	Art. 10	W art. 10 ust. 4 wskazano, że dokumentacja może być prowadzona elektronicznie ALBO papierowo. Wydaje się, że właściwym byłoby użycie alternatywy łącznej, tj. LUB.	Uwaga uwzględniona Zostanie wskazane możliwości prowadzenia dokumentacji w postaci elektronicznej lub papierowej.
508.	Konfederacja Lewiatan	Art. 10	Uwaga: Zgodnie z art. 10 ust. 3 pkt 1 i 3 projektu ustawy podmioty kluczowe i ważne zobowiązane są do stosowania dokumentacji dotyczącej systemu zarządzania: a) bezpieczeństwem informacji wytworzonej zgodnie z wymaganiami Polskiej Normy PN-EN ISO/IEC 27001 lub normy jej równoważnej;	Uwaga uwzględniona Odniesienia do norm zostaną usunięte.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			b) ciągłością działania usługi wytworzonej zgodnie z wymaganiami Polskiej Normy PN-EN ISO 22301 lub normy jej równoważnej. Jednakże, zgodnie z art. 25 dyrektywy NIS2 normy techniczne nie powinny być stosowane obligatoryjnie. Państwa członkowskie powinny zachęcać do ich stosowania, ale nie wymagać tego. Co więcej, normy techniczne ulegają szybkiej dezaktualizacji, co oznacza, że każda zmiana norm w tym zakresie będzie wymagała przejścia przez cały proces legislacyjny w ramach nowelizacji ustawy. Takich dylematów nie posiada ustawodawca unijny, który odwołuje się do najnowszego stanu wiedzy i odpowiednich norm europejskich (por. art. 21 dyrektywy NIS2, motyw 79).	
509.	ZBP	Art. 10 ust. 1.	Podmiot kluczowy i podmiot ważny opracowuje, stosuje i aktualizuje dokumentację dotyczącą bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi Uwaga ogólna Czy SZBI zgodnie z zaproponowanym brzmieniem, musi być certyfikowany w zakresie zgodności przez niezależną jednostkę?	Wyjaśnienie uwagi Nie ma takiego wymogu w projekcie.
510.	TAURON Polska Energia S.A	Art. 10 ust 3 pkt 1 i 3	Dokumentację normatywną stanowią: 1) dokumentacja dotycząca systemu zarządzania bezpieczeństwem informacji wytworzona zgodnie z wymaganiami Polskiej Normy PN-EN ISO/IEC 27001 lub normy jej równoważnej (...) 3) dokumentacja systemu zarządzania ciągłością działania usługi wytworzona zgodnie z wymaganiami Polskiej Normy PN-EN ISO 22301 lub normy jej równoważnej; W nawiązaniu do propozycji zmian dotyczących art. 8 ust 2) (patrz pkt 4) w celu zachowania spójności i jednolitości proponujemy wykreślenie ze wskazanych przepisów: „lub normy jej równoważnej”.	Uwaga nieuwzględniona w związku z usunięciem odniesienia do norm.
511.	Związek Pracodawców Technologii Cyfrowych Lewiatan	Art. 10	Uwzględnienie różnych modeli przetwarzania (art.10) Obecne zapisy pasują wyłącznie do opisu infrastruktury własnej. Istnieją co najmniej dwa możliwe rozwiązania dla opisu innych modeli przetwarzania. • Opis wymagań dla poszczególnych modeli przetwarzania (outsourcing, hosting, kolokacja, chmura obliczeniowa, przetwarzanie w infrastrukturze innego podmiotu np. w grupie itd. itp. w tym modele, których jeszcze nie znamy) • Zapis, że w przypadku przetwarzania poza infrastrukturą własną przetwarzanie może być wykonane tylko w infrastrukturze podmiotu, który także jest podmiotem kluczowym/ważnym Brak takich zapisów będzie skutkowało tworzeniem wielu bardzo rozbudowanych i często niezbyt sensownych wariantów zapytań do podmiotów, u których może być wykonywane przetwarzanie. Rekomendujemy zatem drugie, proste rozwiązanie. Propozycja: <i>Art. 10. Ust. 8. W przypadku systemu informacyjnego wykorzystywanego do świadczenia usługi i wykorzystującego produkty ICT, procesy ICT lub usługi ICT podmiotów trzecich wymagane jest aby były one podmiotami kluczowymi lub podmiotami ważnymi.</i>	Wyjaśnienie uwagi Dostawca usług chmurowych jest co do zasady podmiotem kluczowym/podmiotem ważnym – chyba że nie spełnia kryteriów wielkościowych. W razie potrzeby organ właściwy do spraw cyberbezpieczeństwa będzie mógł w drodze decyzji uznać dostawcę nie spełniającego progów wielkościowych za podmiot kluczowy.
512.	ISSA Polska	Art. 11	Kryteria kwalifikacji incydentu jako poważnego niespójne z NIS2	Wyjaśnienie uwagi

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			Kryteria dotyczące progów uznania incydentu za poważny w oparciu o zakres informacji wymienionych w art. 11 ust. 4 były dotychczas przekładane na przepisy rozporządzenia bez odniesienia realnej możliwości dokonania oceny poszczególnych zdarzeń w oparciu o możliwe do uzyskania informacje dotyczące zdarzenia (w szczególności określenie skali zdarzenia przez liczbę dotkniętych nim osób czy zasięg geograficzny, zwłaszcza jeżeli były definiowane przez liczbę mieszkańców gospodarstw domowych przyłączonych do sieci lub fakt uszkodzenia osób w wyniku zdarzenia). Katalog wymieniony w tym przepisie nie jest przeniesiony z NIS2, nie pokrywa aktualnej definicji podmiotu poważnego, a pozostawienie kategorii kryteriów kwalifikacji incydentu jako poważnego w dotychczasowym brzmieniu będzie stanowiło problem legislacyjny przy tworzeniu treści późniejszego aktu wykonawczego. Zgodnie z dyrektywą NIS2 (art. 11 ust. 5 tego aktu), CSIRT powinny promować ujednolicenie klasyfikacji w zakresie procedur zarządzania incydentami. Na gruncie przepisów projektowanego aktu znalazły się zapisy dotyczące określenia progów uznania za incydent poważny w formie rozporządzenia. Nie jest to złe rozwiązanie. Biorąc jednak pod uwagę, że dotychczas określone progi narażały trudności w ich zastosowaniu w codziennym stosowaniu podmiotom krajowego systemu cyberbezpieczeństwa, proces określania takich progów powinien odbyć się w oparciu o dane zgromadzone już przez CSIRT na podstawie dokonywanych zgłoszeń. Pozostaje w tym miejscu pytanie, czy przepisy nie powinny zostawić większej elastyczności, do doprecyzowania progów przez CSIRT	Informacje jakie mają być przekazywane we wczesnym ostrzeżeniu czy zgłoszeniu incydentu wynikają z NIS2 oraz z obecnie obowiązującej ustawy. Nie są to więc nowe informacje, ani nie oznaczają ich niezgodności z NIS2. Rozporządzenie określające progi uznania incydentu za incydent poważny zostanie dostosowane do projektowej ustawy. Jego wydanie możliwe będzie dopiero po uchwaleniu projektowanej ustawy.
513.	ISSA Polska	Art. 11	Sformalizowane raportowanie incydentów Zgodnie z projektowanymi przepisami, podmioty kluczowe i ważne mają zgłaszać najpierw wczesne ostrzeżenie, potem incydent poważny, a na koniec przedłożyć sprawozdanie końcowe z obsługi incydentu poważnego. Obecnie w Polsce rynek cierpi na braki w zakresie specjalistów ds. cyberbezpieczeństwa. Osoby realizujące prace na takich stanowiskach, są obciążone bardzo dużym zakresem zadań w zakresie dokumentowania działań (wynikających z wymogów SZBI czy ciągłości działania). Wprowadzenie obowiązku sporządzania sprawozdań dodatkowo ograniczy ich czas na zajęcie się praktycznymi działaniami związanymi z ochroną zasobów. Dodatkowo nie każde zdarzenie, które będzie musiało być zakwalifikowane jako incydent poważny tylko z tego powodu, że potencjalnie może wywołać skutki właściwe dla takiego incydentu, będzie z racjonalnego punktu widzenia wymagało szczegółowej analizy. Część cyberzagrożeń cechuje duża skala występowania (np. phishingi, ataki DDoS), ale przy odpowiednio wdrożonym SZBI, mała szansa wywołania realnego skutku. Wskazane przepisy wymuszają nie tylko raportowanie takich pojedynczych zdarzeń, ale również sporządzanie sprawozdań z ich obsługi. Zwłaszcza, że wykonywanie obowiązków określonych w tych przepisach jest powiązane z treścią projektowanej zmiany do art. 73 ust. 1 pkt. 8 i 11 – czyli zagrożone karą dla podmiotu, a także art. 73a ust. 1 pkt. 9 – czyli zagrożone karą dla kierownika podmiotu. Wskazane jest rozważenie wprowadzenia sprawozdawczości w systemie w oparciu o predefiniowaną formatkę, zbudowaną w	Uwaga nieuwzględniona Zgłaszanie incydentów oraz przygotowanie stosownych sprawozdań wynika z dyrektywy NIS2. Nie jest możliwe wprowadzenie odrębnych rozwiązań, ponieważ byłoby to niezgodne z tą dyrektywą.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			oparciu o realną ocenę zakresu informacji potrzebnych CSIRT do realizacji ustawowych zadań z zaangażowaniem personelu podmiotów kluczowych i ważnych odpowiednio do rzeczywistych wymogów bezpieczeństwa. Zwłaszcza, że dyrektywa NIS2 w art. 23 ust. 4 lit. d) precyzuje zakres takiego sprawozdania.	
514.	ISSA Polska	Art. 11	Kwalifikacja znamion przestępstwa we wczesnym ostrzeżeniu Zgodnie z projektowanym przepisem art. 12 ust. 1 pkt. 5 ustawy o KSC wczesne ostrzeżenie musi zawierać informację czy incydent poważny wyczerpuje znamiona przestępstwa. Osoby dokonujące zgłoszeń do systemów na ogół są inżynierami bezpieczeństwa. Kwalifikacja znamion przestępstwa nie tylko stanowi domenę prawną. Kwalifikacja w ciągu 24h czy zdarzenie wyczerpuje znamiona przestępstwa w praktyce może być niemożliwa do realizacji. Zwłaszcza biorąc pod uwagę, że organy ścigania po otrzymaniu zgłoszenia takiego zdarzenia, prowadząc czynności dochodzeniowo-śledcze dochodzą często do wniosku, że mimo wstępnej kwalifikacji zgłaszającego, zdarzenie znamion przestępstwa nie wyczerpuje. Przepisy mają określony cel – w tym przypadku jest nim ustalenie czy zdarzenie będzie zgłoszone organom ścigania. I tak stylistycznie powinien zostać sformułowany wskazany przepis – nie w kwestii wypełnienia znamion przestępstwa, tylko informacji, czy incydent został zgłoszony organom ścigania. Zmienia to diametralnie podejście do zakresu przekazywanych informacji przez osoby wypełniające zgłoszenie. Pozwoli również na udzielenie informacji, co do których możliwa jest ocena ich prawdziwości i zapewnienie realnej odpowiedzialności za jej treść. W NIS2 (art. 23 ust. 4 lit. a)) jest mowa o zawarciu we wczesnym ostrzeżeniu informacji o przypuszczeniu wywołania incydentu poważnego działaniem bezprawnym lub działaniem w złym zamiarze. Jeżeli zapisy powołanego powyżej przepisu projektu mają implementować ten właśnie zakres, to powinny literalnie odnosić się do nomenklatury NIS2 (czym innym jest spełnienie znamion przestępstwa, a czym innym ocena bezprawności działania lub złego zamiaru, które można ocenić biorąc pod uwagę sprawcę (atakującego) i skutki zdarzenia na poziomie technicznym).	Uwaga uwzględniona Przepis art. 12 ust. 1 pkt 5 został przeredagowany i otrzymał brzmienie: „5) wskazanie czy incydent poważny został wywołany działaniem bezprawnym lub działaniem w złej wierze, jeżeli możliwe jest dokonanie takiej oceny;”.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

515.	Polskie Stowarzyszenie Fotowoltaiki	Art. 11-12b	Obowiązki PK i PW w zakresie: - obsługi incydentów; - zapewnienia organom właściwym dostępu do informacji; - klasyfikacji incydentu jako poważny na podstawie progów określonych w rozporządzeniu Rady Ministrów; - zgłaszania wczesnych ostrzeżeń o incydencie poważnym (w ciągu max. 24h; przez system S46); - zgłaszania incydentów poważnych (w ciągu max. 72; przez system S46); - przekazywania sprawozdań okresowych oraz końcowych z obsługi incydentów (w ciągu miesiąca od wykrycia lub miesiąca od zakończenia obsługi, jeśli trwa dłużej; przez system S46); - współdziałania w obsłudze incydentu poważnego i krytycznego właściwym CSIRT MON, CSIRT NASK lub CSIRT GOV; - usuwania na wezwanie organu właściwego podatności, które doprowadziły lub mogłyby doprowadzić do incydentu poważnego lub krytycznego i notyfikacja usunięcia organowi właściwemu; - informowania użytkowników o możliwych środkach zapobiegawczych w razie zaistnienia znaczącego cyberzagrożenia, lub samym znaczącym cyberzagrożeniu; - informowania użytkowników o incydencie poważnym, jeżeli ma on niekorzystny wpływ na świadczenie usług; - aktualizacji informacji o incydentach w toku obsługi incydentu; - uwzględniania w ostrzeżeniach lub zgłoszeniach informacji stanowiących tajemnicę przedsiębiorstwa z oznaczeniem ich poufnego charakteru Ogólny wpływ regulacji: Przepisy określają obowiązki PK i PW związane z obsługą oraz zgłaszaniem incydentu do właściwego CSIRT sektorowego, jak również zakres przekazywanych w ramach incydentu informacji do właściwego CSIRT sektorowego. Zapewnienie realizacji ww. wymogów może wymagać wdrożenia lub dostosowania obecnie przyjętych procedur i polityk dotyczących obsługi incydentów jak również wyznaczenia specjalistycznego personelu. Wpływ na sektor energetyczny: Uwagi jw. – brak specyficznego wpływu na sektor energetyczny Nadregulacja względem Dyrektywy NIS2] Przepisy art. 11-12b KSC wg Projektu stanowią co do zasady bezpośrednią implementację postanowień Dyrektywy NIS2. Niemniej jednak analizowane przepisy wykraczają w nieznacznym zakresie poza zakres przedmiotowy Dyrektywy NIS2 i stanowią względem niej nadregulację: - przepisy lub motywy Dyrektywy NIS2 nie przewidują dalej idących regulacji w zakresie kwalifikacji przez PK i PW incydentu jako poważny, a jedynie wskazują na istotne w tym zakresie czynniki (zakres skutków dla funkcjonowania usługi, czas trwania incydentu lub liczba dotkniętych	Wyjaśnienie uwagi Zawarte w projekcie obowiązki związane z e zgłaszaniem incydentów wynikają zarówno z dyrektywy NIS2 (terminy zgłoszenia, informacje zgłaszane w ramach wczesnego ostrzeżenia) jaki z obowiązującej ustawy o krajowym systemie cyberbezpieczeństwa (zgłoszenie incydentu). Informacje o przyczynie zaistnienia incydentu poważnego czy o podjętych działaniach zapobiegawczych i naprawczych są informacjami niezbędnymi do obsługi incydentu. Projektowana procedura zgłaszania incydentów oparta jest na obowiązującej procedurze dzięki temu możliwe będzie zapewnienie skutecznej obsługi incydentów.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			nim odbiorców usług – vide Motyw 101 Dyrektywy NIS2). Kryteria określenia progów istotności incydentów zgodnie z art. 11 ust. 4 wykraczają poza ww. katalog; - zakres informacji jakie PK i PW jest zobowiązany do przekazania wraz ze zgłoszeniem incyduentu wykracza poza zakres określony w art. 23 ust. 4(b) Dyrektywy NIS2 i obejmuje m.in. przyczynę zaistnienia incyduentu poważnego; informacje o podjętych działaniach zapobiegawczych; informacje o podjętych działaniach naprawczych. Informacje te powinny zgodnie z Dyrektywą NIS2 być uwzględnione w sprawozdaniach, w szczególności sprawozdaniu końcowym. Wskazanie wszystkich informacji określonych w art. 12 ust. 3 KSC wg Projektu w terminie tam określonym może nie być realnie możliwe. Rekomendacja: - ograniczenie zakresu informacji przekazywanych w ramach zgłoszenia poważnego incyduentu do informacji określonych w Dyrektywie NIS2.	
516.	Amerykańska Izba Handlowa w Polsce	art. 11	Przedsiębiorcy komunikacji elektronicznej są zobowiązani do zgłaszania wczesnego ostrzeżenia o poważnym incydencie bez zbędnej zwłoki, nie później niż 12 godzin od jego wykrycia (art. 1 pkt 15 lit. b projektu ustawy). Stoimy na stanowisku, żeby lepszym rozwiązaniem byłoby utrzymanie terminu 24 godzin na zgłaszanie incydentów wynikającego z art. 23 ust. 4 dyrektywy NIS 2. Biorąc pod uwagę normalne warunki pracy przedsiębiorców, termin 12 godzin należy uznać za ekstremalnie krótki i niezwykle trudny do praktycznego zachowania. Stoimy na stanowisku, że obowiązki w zakresie zgłaszania incydentów powinny być jasne, koncentrować się na incydentach, które są naprawdę istotne, zapewniać wystarczająco dużo czasu na dostarczenie cennych informacji i zachęcać podmioty do priorytetowego traktowania wprowadzania skutecznych środków zaradczych w zakresie naruszeń cyberbezpieczeństwa.	Uwaga uwzględniona Wszystkie podmioty kluczowe i ważne będą zgłaszać wczesne ostrzeżenie nie później niż w ciągu 24 godzin od momentu jego wykrycia incyduentu poważnego.
517.	Amerykańska Izba Handlowa	Art. 11	Art. 11 ust. 1 uksc w brzmieniu ustalonym projektem przewiduje, że incydenty zgłaszane są zasadniczo do odpowiednich CSIRT sektorowych. Stoimy na stanowisku, że – zwłaszcza w kontekście licznych nowych wymogów sprawozdawczych – korzystniejsze byłoby utworzenie jednego punktu zgłaszania incydentów na poziomie krajowym, zamiast oddzielnych "sektorowych" punktów zgłaszania. Ważne jest, aby uniknąć fragmentacji, potencjalnego wielokrotnego raportowania tego samego incyduentu raportowania i generowania nadmiernych obciążeń administracyjnych zarówno dla branży, jak i organów publicznych.	Wyjaśnienie uwagi Tym jednym punktem zgłaszania incydentów jest system S46.
518.	Fundacja Bezpieczna Cyberprzestrzeń	Art. 11	art. 1 pkt 15 lit. d, treść art. 11 ust. 2a (uwagę należy czytać w powiązaniu z uwagą w pkt. 5) – proponuje się następującą treść ust. 2a: „2a. W przypadku zaistnienia cyberzagrożenia mogącego wpłynąć na bezpieczeństwo systemów informacyjnych podmiotów kluczowych i podmiotów ważnych, podmioty te informują swoich użytkowników, na których takie cyberzagrożenie może mieć wpływ o możliwych środkach zapobiegawczych, które użytkownicy ci mogą podjąć w celu minimalizacji wystąpienia tego cyberzagrożenia.”. Wydaje się, że oczekiwaniem ustawodawcy jest ostrzeżenie użytkowników usług kluczowych i ważnych o potencjalnych zagrożeniach, które mogą mieć wpływ na dostęp do usług kluczowych i ważnych (co wydaje się uzasadnione) i wprowadzenie przez tych użytkowników działań zapobiegawczych.	Wyjaśnienie uwagi Przepis został przeredagowany określenie: „informuje swoich użytkowników” zostało zastąpione określeniem „informuje użytkowników swoich usług”. Ponadto, należy zauważyć, że dyrektywa NIS2 nie używa pojęcia usług kluczowych oraz pojęcia usług ważnych,

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

				dlatego też nie można wskazywać tych usług w projektowanej ustawie.
519.	KIKE	Art. 11	- zmianę art. 11 ust. 1 pkt 1 uKSC w zakresie współpracy podmiotów ważnych z sektorowym CSIRT. Zdaniem Izby, podmioty ważne jako MŚP powinny być zobowiązane do współpracy tylko z jednym konkretnym sektorowym CSIRT (który powinien przekazywać informację do innych CSIRT). Ponadto przekazywanie tych informacji powinno odbywać się na zasadzie dobrowolności a nie obowiązku ustawowego. Izba ponownie wskazuje tu zasadę legislacyjną z art. 67 pkt 2 Prawa przedsiębiorców.	Wyjaśnienie uwagi Po pierwsze incydent będzie zgłaszany w jedno miejsce – za pomocą systemu S46, który z kolei przekaze informację o zgłoszeniu incydentu do właściwego zespołu CSIRT. Przekazywanie zgłoszeń o incydentach poważnych, w tym także wczesnego ostrzeżenia, wynika wprost z dyrektywy NIS2 i dotyczy także podmiotów ważnych.
520.	KIKE	Art. 11	- zmianę art. 11 ust. 1a uKSC w zakresie terminu zgłoszenia wczesnego ostrzeżenia poważnego incydentu z 12 godzin na obecnie obowiązujące 24 godziny (przynajmniej dla podmiotów MŚP lub podmiotów ważnych. Zdaniem Izby brak jest przesłanek do skrócenia tego terminu.	Uwaga uwzględniona Wszystkie podmioty kluczowe i ważne będą zgłaszać wczesne ostrzeżenie nie później niż w ciągu 24 godzin od momentu jego wykrycia incydentu poważnego.
521.	Fundacja Open Allies	Art. 11	Art. 11 ust. 1 pkt 2 nowelizowanej UKSC wyraźnie wykracza poza zobowiązania wynikające z art. 30 ust. 1 dyrektywy NIS2. Zgodnie z dyrektywą NIS2, podmioty ważne i kluczowe mogą informować właściwy CSIRT o incydentach innych niż poważne na zasadach dobrowolności. Tymczasem zgodnie z Projektem, CSIRTy będą miały stały dostęp do informacji o wszystkich rejestrowanych incydentach u podmiotów ważnych i podmiotów kluczowych. Zwracamy się o wykreślenie art. 11 ust. 1 pkt 2 jako niezgodnego z dyrektywą NIS2.	Uwaga nieuwzględniona Zespoły CSIRT mają prawo do klasyfikowania każdego incydentu jako incydentu krytycznego oraz prawo do zmiany klasyfikacji incydentu. Z tego powodu, na ich żądanie podmiot powinien zapewnić im dostęp do rejestru incydentów.
522.	Fundacja Open Allies	Art. 11	[ART. 11 UST. 1A ZGŁOSZENIE WCZESNEGO OSTRZEŻENIA O INCYDENCIE POWAŻNYM PRZEZ PRZEDSIĘBIORCĘ KOMUNIKACJI ELEKTRONICZNEJ] Wnosimy o nienakładanie na przedsiębiorców komunikacji elektronicznej, w tym przedsiębiorców telekomunikacyjnych, obowiązków istotnie trudniejszych niż na inne podmioty systemu cyberbezpieczeństwa. Brak jest uzasadnienia skracania terminu zgłoszenia wczesnego ostrzeżenia o incydencie poważnym dla jednej, arbitralnie wybranej branży. Termin zgłoszenia ostrzeżenia w 24 godziny jest bardzo krótkim terminem i w praktyce oznacza obowiązek utrzymania stałego zespołu monitorującego cyberbezpieczeństwo. Skracanie go do 12 godzin geometrycznie zwiększa koszty funkcjonowania systemu cyberbezpieczeństwa.	Uwaga uwzględniona Wszystkie podmioty kluczowe i ważne będą zgłaszać wczesne ostrzeżenie nie później niż w ciągu 24 godzin od momentu jego wykrycia incydentu poważnego.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			Wnosimy o równe traktowanie wszystkich podmiotów w ramach kategorii podmiotów ważnych i podmiotów kluczowych oraz ustalenie jednego terminu na zgłoszenie wczesnego ostrzeżenia o incydencie poważnym.	
523.	CyberMadeinPoland	Art. 11	Art. 11 p. 2a. - dodanie terminu realizacji takich czynności, np. 48 godzin.	Wyjaśnienie uwagi Zdaniem Ministerstwa Cyfryzacji nie jest to dobry pomysł, z uwagi na to, że trudno wskazać dokładny moment zidentyfikowania znacznego cyberzagrożenia.
524.	Stowarzyszenie Bezpieczeństwo Informacji w Telekomunikacji	Art. 11	Art. 11 ust. 1a i 1b. rekomenduje się usunięcie ust. 1a i 1b w art. 11. Szczególnie przepis art. 1a nakłada na przedsiębiorcę komunikacji elektronicznej obowiązek utrzymywania w ciągłym dyżurze osób odpowiedzialnych zarówno za nadzór techniczny (administratorów systemów informatycznych) jak i osoby odpowiedzialne za prawidłową ocenę incydentów. Na ogół będą to co najmniej dwie osoby w ciągłej pracy całodobowej co stanowi to co najmniej dziewięć osób o wysokich kwalifikacjach. Przyjmuje się, że na jedno stanowisko w pracy ciągłej należy zatrudnić 4,5 osoby. Dla wielu mikro lub małych przedsiębiorców komunikacji elektronicznej będzie to wydatek wykraczający ich możliwości.	Uwaga częściowo uwzględniona W zakresie 1a – Uwaga uwzględniona: wszystkie podmioty kluczowe i ważne będą zgłaszać wczesne ostrzeżenie nie później niż w ciągu 24 godzin od momentu jego wykrycia incydentu poważnego. W zakresie 1b – Skrócenie terminu na zgłoszenie incydentu poważnego przez dostawcę usługi zaufania wynika z art. 23 ust. 4 ostatnie zdanie dyrektywy NIS2.
525.	ZPP	Art. 11	Polski projekt implementacji NIS2 rozszerza zasady zgłaszania incydentów. Elektroniczni operatorzy muszą zgłaszać poważne incydenty w ciągu 12 godzin od ich wykrycia (art. 11 ust. 1a). Projekt definiuje poważny incydent jako taki, który powoduje szkodę materialną lub niematerialną, wpływając na inne podmioty (art. 2 pkt 7). W przeciwieństwie do dyrektywy NIS2, nie odnosi się do "znaczej" szkody ani możliwości wpływu incydentu na osoby. Poważne zagrożenie cybernetyczne to takie, które może poważnie wpłynąć na bezpieczeństwo systemów informatycznych, powodując szkodę (art. 2 pkt 20). Dodatkowo przepisy różnicują termin na zgłoszenie wczesnego ostrzeżenia o incydencie poważnym – dla podmiotów ważnych i kluczowych 24 godziny zgodnie z przepisami NIS2, a dla przedsiębiorcy komunikacji elektronicznej – 12 godzin od momentu jego wykrycia. Sugerujemy, żeby zgodnie z przepisami dyrektywy NIS2, ustawodawca trzymał się terminu 24 godziny na zgłaszanie takich incydentów. Termin 12 godzin jest zbyt krótki, przy uwzględnieniu warunków pracy przedsiębiorcy.	Uwaga uwzględniona Wszystkie podmioty kluczowe i ważne będą zgłaszać wczesne ostrzeżenie nie później niż w ciągu 24 godzin od momentu jego wykrycia incydentu poważnego.
526.	Związek Cyfrowa Polska	Art. 11	W zakresie zasad dotyczących zgłaszania znaczących incydentów, opiniowany projekt implementacji wykracza poza dyrektywę NIS2 w zakresie: Przedsiębiorcy komunikacji elektronicznej są zobowiązani do zgłaszania wczesnego ostrzeżenia o poważnym incydencie bez zbędnej zwłoki, nie później niż 12 godzin od jego wykrycia (art. 11 ust. 1a projektu polskiej ustawy implementującej).	Uwaga uwzględniona Wszystkie podmioty kluczowe i ważne będą zgłaszać wczesne ostrzeżenie nie później niż w ciągu 24 godzin od momentu jego wykrycia incydentu poważnego.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

527.	Związek Cyfrowa Polska	Art. 11	Przepisy różnicują termin na zgłoszenie wczesnego ostrzeżenia o incydencie poważnym – dla podmiotów ważnych i kluczowych 24 godziny zgodnie z przepisami NIS2, a dla przedsiębiorcy komunikacji elektronicznej – 12 godzin od momentu jego wykrycia. Sugerujemy, żeby zgodnie z przepisami dyrektywy NIS2, ustawodawca trzymał się terminu 24 godziny na zgłaszanie takich incydentów. Termin 12 godzin jest ekstremalnie krótki, przy uwzględnieniu warunków pracy przedsiębiorcy.	Uwaga uwzględniona Wszystkie podmioty kluczowe i ważne będą zgłaszać wczesne ostrzeżenie nie później niż w ciągu 24 godzin od momentu jego wykrycia incydentu poważnego.
528.	Konfederacja Lewiatan	Art. 11	Zalecamy utworzenie jednego punktu przyjmowania zgłoszeń incydentów na poziomie krajowym, zwłaszcza w kontekście nowych wymogów dotyczących zgłaszania incydentów w ramach CRA, zamiast oddzielnych „sektorowych” punktów przyjmowania zgłoszeń. Ważne jest, aby uniknąć fragmentacji, podwójnego raportowania i niepotrzebnego obciążenia zarówno dla branży, jak i organów publicznych.	Wyjaśnienie uwagi Zgłoszenia będą się odbywały za pomocą jednego punktu - systemu S46.
529.	Konfederacja Lewiatan	Art. 11	Projekt ustawy przewiduje, że przedsiębiorcy komunikacji elektronicznej mają być zobowiązani do zgłaszania wczesnych ostrzeżeń o incydencie poważnym niezwłocznie, nie później niż w ciągu 12 godzin od momentu jego wykrycia, do właściwego CSIRT sektorowego, stanowiąc w ten sposób nieuzasadniony wyjątek od terminu wynoszącego 24 godziny, który mają na zgłoszenie pozostałe podmioty kluczowe i ważne. Wnioskujemy o wykreślenie art. 11 ust. 1a jako nadmiernego zaostrzenia reżimu raportowania wobec jedynej wybranej grupy, tj. przedsiębiorców telekomunikacyjnych. Zgodnie z NIS2 prawie wszystkie podmioty mają identyczny termin zgłoszenia wczesnego ostrzeżenia, tj. 24 godziny, a jedyny wyjątek przewidziano dla dostawców usług zaufania, którzy w 24 godziny zgłaszają incydent poważny, a nie wczesne ostrzeżenie. Jednocześnie w NIS2 dla żadnej z kategorii nie wprowadzono terminu 12-godzinnego. Zauważamy również, że na gruncie aktualnie obowiązujących przepisów PT nie został określony sztywny termin dokonywania zgłoszeń, a ustalona praktyka współpracy z UKE wskazuje, że obowiązek niezwłocznego zgłoszenia naruszenia uznaje się za spełniony, jeśli zgłoszenie nastąpi w okresie 4-5 dni roboczych. Raportowanie w terminie 12-godzinnym jest obowiązkiem nieproporcjonalnym. Skoro na poziomie UE nie uznano za zasadne zaostrzanie tych wymagań, tym bardziej nie jest uzasadnione jego dokonywanie na poziomie krajowym. Ponadto, zróżnicowanie terminów będzie problematyczne w przypadku operatorów, którzy klasyfikują się także wg innych kategorii usług kluczowych lub ważnych. Oznaczałoby to trudności w ustaleniu właściwego terminu raportowania, tj. czy w związku z tym, że operator jako podmiot kluczowy jako przedsiębiorca telekomunikacyjny, ale też np. jako operator punktu wymiany ruchu powinien raportować w ciągu 12 czy 24 godzin. Także z tego względu, właściwym rozwiązaniem jest wprowadzenie jednolitych wymagań na poziomie 24 godzin.	Uwaga uwzględniona Wszystkie podmioty kluczowe i ważne będą zgłaszać wczesne ostrzeżenie nie później niż w ciągu 24 godzin od momentu jego wykrycia incydentu poważnego.
530.	Konfederacja Lewiatan	Art. 11	Wnioskujemy o pilne przedstawienie projektu rozporządzenia dot. progów incydentów. Bez jego tekstu nie jest możliwe odniesienie się do potencjalnej uciążliwości wdrożenia obowiązków, ich kosztu oraz czasu niezbędnego na dostosowanie.	Uwaga uwzględniona Rozporządzenie dot. progów incydentów zostanie przedstawione na następnym etapie procesu legislacyjnego.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			Sygnalizujemy, że na etapie prac nad poprzednimi projektami nowelizacji zgłaszaliśmy liczne uwagi dot. uszczegółowienia progów raportowania w ówczesnym projekcie rozporządzenia. Skutkowałyby one ogromnym zwiększeniem liczby incydentów, których większość – w naszej ocenie – nie byłaby faktycznie incydentami zasługującymi na klasyfikację jako incydenty poważne. Liczymy, że uwagi te zostaną uwzględnione w toku prac nad nowym projektem rozporządzenia. Ponadto zgłaszamy wątpliwości co do obligatoryjnego charakteru upoważnienia w związku z art. 23 ust. 11 NIS2, który wskazuje, że: <i>Do dnia 17 października 2024 r. Komisja, w odniesieniu do dostawców usług DNS, rejestrów nazw TLD, dostawców usług chmurowych, dostawców usług ośrodka przetwarzania danych, dostawców sieci dostarczania treści, dostawców usług zarządzanych, dostawców usług zarządzanych w zakresie bezpieczeństwa, jak również dostawców internetowych platform handlowych, wyszukiwarek internetowych i platform usług sieci społecznościowych, przyjmuje akty wykonawcze doprecyzowujące przypadki, w których incydent uznaje się za poważny zgodnie z ust. 3. Komisja może przyjąć takie akty wykonawcze w odniesieniu do innych podmiotów kluczowych i ważnych.</i> W przypadku wydania w tym samym zakresie przepisów krajowych może wystąpić kolizja norm.	
531.	TAURON Polska Energia S.A	Art.11 ust. 2a i 2b	„2a. W przypadku zaistnienia znaczącego cyberzagrożenia podmiot kluczowy i podmiot ważny informuje swoich użytkowników, na których takie cyberzagrożenie może mieć wpływ, (...). Podmiot kluczowy i podmiot ważny informuje tych użytkowników (...) 2b. Podmiot kluczowy i podmiot ważny informuje swoich użytkowników o incydencie poważnym, (...) W zakresie określenia obowiązków dotyczących informowania przez podmioty kluczowe i ważne swoich użytkowników, biorąc pod uwagę brak definicji legalnej jak również wątpliwości przy stosowaniu interpretacji celowościowej, należy rozważyć zmianę zapisów poprzez doprecyzowanie czy chodzi o użytkowników (usług świadczonych przez podmioty kluczowe i ważne) czy są chodzi o stricte zidentyfikowanych użytkowników usług czy też potencjalnych. Ma to znaczenie w szczególności w zakresie prawidłowego procesu informowania o cyberzagrożeniach jak również incydentach bezpieczeństwa mających lub mogących mieć wpływ na użytkowników.	Wyjaśnienie uwagi Chodzi tutaj o użytkowników usług świadczonych przez podmioty kluczowe i ważne. Przepis został przeredagowany określenie: „informuje swoich użytkowników” zostało zastąpione określeniem „informuje użytkowników swoich usług”.
532.	ZBP	Art. 11 ust. 2a i 2b	2a. W przypadku zaistnienia znaczącego cyberzagrożenia podmiot kluczowy i podmiot ważny informuje swoich użytkowników, na których takie cyberzagrożenie może mieć wpływ, o możliwych środkach zapobiegawczych, które użytkownicy ci mogą podjąć. Podmiot kluczowy i podmiot ważny informuje tych użytkowników o samym znaczącym cyberzagrożeniu, jeżeli nie spowoduje to zwiększenia poziomu ryzyka dla bezpieczeństwa systemów informacyjnych. 2b. Podmiot kluczowy i podmiot ważny informuje swoich użytkowników o incydencie poważnym, jeżeli ma on niekorzystny wpływ na świadczenie usług.” Uwaga ogólna Czy obowiązek informacyjny należy spełnić w jakimś konkretnym terminie? Jaka powinna być forma takich informacji (komunikat na stronie, powiadomienia wysyłane do każdego klienta, itp)? Czy	Wyjaśnienie uwagi Formę komunikacji należy dostosować do rodzaju i liczby użytkowników danej usługi. Jeżeli jest to zasadne może być to komunikat na stronie. Ocena należy do podmiotu. Wskazujemy, że warto posłużyć się tutaj poradnikiem przygotowanym przez ENISA. https://www.enisa.europa.eu/publications/cyber-threats-outreach-in-telecom

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			ocena wpływu na świadczenie usług leży po stronie podmiotu, czy będą zdefiniowane jakieś ustawowe kryteria oceny?	
533.	Polska Izba Informatyki i Telekomunikacji	Art. 11	Słowo „użytkownicy” może wprowadzać w błąd. Dlatego też, aby poprawić przejrzystość i zharmonizowane podejście w całej UE, sugerujemy użycie sformułowań określonych w dyrektywie NIS 2 (UE) 2022/2555 https://eur-lex.europa.eu/eli/dir/2022/2555 Dyrektywa NIS2, Artykuł 23 - Obowiązki w zakresie zgłaszania incydentów” „W stosownych przypadkach dane podmioty bez zbędnej zwłoki powiadamiają odbiorców swoich usług o poważnych incydentach, które mogą mieć niekorzystny wpływ na świadczenie tych usług.” Jeśli chodzi o zgłaszanie incydentów, jeżeli znaczący incydent obejmuje całą UE, prawo powinno zapewniać, że taki znaczący incydent powinien być zgłaszany do jednego zespołu CSIRT: zespołu CSIRT państwa członkowskiego, w którym znajduje się siedziba ważnego podmiotu, lub unijnego zespołu CSIRT.	Uwaga nieuwzględniona Odbiorca danej usługi jest jej użytkownikiem. Zgodnie z dyrektywą NIS2 przedsiębiorca telekomunikacyjny podlega właściwości państwa członkowskiego, w której przedsiębiorca świadczy usługi. I jeżeli w tym państwie będzie miał miejsce incydent poważny związany z danym przedsiębiorcą telekomunikacyjnym to powinien on być zgłoszony do CSIRT w danym państwie.
534.	Polska Izba Informatyki i Telekomunikacji	Art. 11	Wnioskujemy o wykreślenie art. 11 ust. 1a jako nadmiernego zaostrzenia reżimu raportowania wobec jedynej wybranej grupy, tj. przedsiębiorców telekomunikacyjnych. Zgodnie z NIS2 prawie wszystkie podmioty mają identyczny termin zgłoszenia wczesnego ostrzeżenia, tj. 24 godziny, a jedyny wyjątek przewidziano dla dostawców usług zaufania, którzy w 24 godziny zgłaszają incydent poważny, a nie wczesne ostrzeżenie. Jednocześnie w NIS2 dla żadnej z kategorii nie wprowadzono terminu 12-godzinnego. Zauważamy również, że na gruncie aktualnie obowiązujących przepisów PT nie został określony sztywny termin dokonywania zgłoszeń, a ustalona praktyka współpracy z UKE wskazuje, że obowiązek niezwłocznego zgłoszenia naruszenia uznaje się za spełniony, jeśli zgłoszenie nastąpi w okresie 4-5 dni roboczych. Raportowanie w terminie 12-godzinnym jest obowiązkiem nieproporcjonalnym. Skoro na poziomie UE nie uznano za zasadne zaostrzanie tych wymagań, tym bardziej nie jest uzasadnione jego dokonywanie na poziomie krajowym. Ponadto, zróżnicowanie terminów będzie problematyczne w przypadku operatorów, którzy klasyfikują się także wg innych kategorii usług kluczowych lub ważnych. Oznaczałoby to trudności w ustaleniu właściwego terminu raportowania, tj. czy w związku z tym, że operator jako podmiot kluczowy jako przedsiębiorca telekomunikacyjny, ale też np. jako operator punktu wymiany ruchu powinien raportować w ciągu 12 czy 24 godzin. Także z tego względu, właściwym rozwiązaniem jest wprowadzenie jednolitych wymagań na poziomie 24 godzin.	Uwaga uwzględniona Zostanie przywrócony termin 24 godzin na zgłoszenie incydentu.
535.	Polska Izba Informatyki i Telekomunikacji	Art. 11	Art. 11 ust. 4 – progi incydentu poważnego Wnioskujemy o pilne przedstawienie projektu rozporządzenia dot. progów incydentów. Bez jego tekstu nie jest możliwe odniesienie się do potencjalnej uciążliwości wdrożenia obowiązków, ich kosztu oraz czasu niezbędnego na dostosowanie.	Uwaga nieuwzględniona Nie wykluczamy wcześniejszego przedstawienia projektu rozporządzenia do prekonsultacji. Jednakże na tym etapie

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			Sygnalizujemy, że na etapie prac nad poprzednimi projektami nowelizacji zgłaszaliśmy liczne uwagi dot. uszczegółowienia progów raportowania w ówczesnym projekcie rozporządzenia. Skutkowałyby one ogromnym zwiększeniem liczby incydentów, których większość – w naszej ocenie – nie byłaby faktycznie incydentami zasługującymi na klasyfikację jako incydenty poważne. Liczymy, że uwagi te zostaną uwzględnione w toku prac nad nowym projektem rozporządzenia. Ponadto zgłaszamy wątpliwości co do obligatoryjnego charakteru upoważnienia w związku z art. 23 ust. 11 NIS2, który wskazuje, że: <i>Do dnia 17 października 2024 r. Komisja, w odniesieniu do dostawców usług DNS, rejestrów nazw TLD, dostawców usług chmurowych, dostawców usług ośrodka przetwarzania danych, dostawców sieci dostarczania treści, dostawców usług zarządzanych, dostawców usług zarządzanych w zakresie bezpieczeństwa, jak również dostawców internetowych platform handlowych, wyszukiwarek internetowych i platform usług sieci społecznościowych, przyjmuje akty wykonawcze doprecyzowujące przypadki, w których incydent uznaje się za poważny zgodnie z ust. 3. Komisja może przyjąć takie akty wykonawcze w odniesieniu do innych podmiotów kluczowych i ważnych.</i> W przypadku wydania w tym samym zakresie przepisów krajowych może wystąpić kolizja norm.	istotne jest opracowanie jak najlepszy rozwiązań w projektowanej ustawie. Obecnie obowiązujące rozporządzenie nie utraci mocy z dniem wejścia w życie projektowej ustawy. Ponadto za późniejszym opracowaniem projektu rozporządzenia przemawia uspołnienie jego treści z aktami wykonawczymi, które zostaną wydane przez Komisję.
536.	Amerykańska Izba Handlowa	Art. 12	Wprowadzany powyższym artykułem art. 12 ust. 3. uksc przewiduje bardzo szczegółowy katalog informacji, które mają być zawarte w zgłoszeniu incydentu. Stoimy na stanowisku, że ustalanie tego katalogu na poziomie ustawowym jest niewskazane, ponieważ wzory formularzy i katalog informacji, które mają być udostępniane, ma zostać ujednolicony w całej UE w nadchodzącym akcie wykonawczym dotyczącym zgłaszania incydentów. Ujednolicenie wzorów formularzy raportowania w całej UE pomaga zapewnić kompatybilność raportów, ułatwiając w ten sposób transgraniczną wymianę i analizę informacji. Pomaga to również firmom działającym w dwóch lub więcej krajach UE uniknąć niejasności prawnych i nadmiernych nakładów na wdrożenie różnych systemów sprawozdawczości.	Wyjaśnienie uwagi Podstawowy zakres danych i informacji, które jest zbierane przez państwo musi zostać ustalony na poziomie ustawy.
537.	Amerykańska Izba Handlowa	Art. 12	We wprowadzanych powyższym artykułem art. 12, ust. 6-8 uksc określone zostały warunki, na jakich podmioty kluczowe i ważne są zobowiązane do ujawniania informacji prawnie uprzywilejowanych lub tajemnic handlowych, w szczególności, gdy jest to konieczne do wspierania działań CSIRT w obsłudze istotnych incydentów cyberbezpieczeństwa. Chociaż przepisy te mają na celu ułatwienie reagowania na incydenty, istnieje obawa o możliwość ich niewłaściwego wykorzystania. Sugerujemy, aby uprawnienia te były jasno określone i ściśle kontrolowane w celu skutecznej ochrony wrażliwych informacji korporacyjnych. Parametry takich ujawnień powinny być wyraźnie określone, z rygorystycznymi zabezpieczeniami zapobiegającymi nadużyciom.	Wyjaśnienie uwagi CSIRT są zobowiązane do zachowania tych informacji w tajemnicy zgodnie z ustawą. Poza tym, abstrahując od kwestii prawnych, gdyby zespoły CSIRT zaczęły ujawniać te informacje to straciłyby swoją wiarygodność.
538.	Fundacja Bezpieczna Cyberprzestrzeń	Art. 11	art. 1 pkt 15 lit. d, treść art. 11 ust. 1 pkt 4 – zgodnie z art. 12 ust. 1 pkt 4 we wczesnym ostrzeżeniu o incydencie poważnym trzeba wskazać moment wystąpienia i wykrycia incydentu poważnego oraz czas jego trwania, a na zgłoszenie wczesnego ostrzeżenia są 24 godziny. Natomiast sam incydent poważny trzeba zgłosić w ciągu 72 godzin. W jaki sposób podmiot kluczowy lub podmiot ważny będzie wiedział, że ma do czynienia z incydemtem poważnym ostrzegając o nim przed samym zgłoszeniem? Wydaje	Uwaga nieuwzględniona Zdaniem projektodawcy należy się tutaj posłużyć terminologią z NIS2, która mówi o wczesnym ostrzeżeniu

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			się, że adekwatne byłoby nazwanie wczesnego ostrzeżenia o incydencie poważnym, zgłoszeniem podejrzenia incyduentu poważnego. Wtedy podmiot zgłaszający miałby 48 godzin na potwierdzenie podejrzeń i zgłoszenie faktycznego incyduentu poważnego. Zatem proponuje się nadać punktowi 4 art. 11 ust 1 następującą treść: „zgłasza podejrzenie wykrycia incyduentu poważnego niezwłocznie, nie później niż w ciągu 24 godzin od momentu jego wykrycia, do właściwego CSIRT sektorowego;”. W przypadku akceptacji uwagi zamiana wyrazów wczesne ostrzeżenia na zgłoszenie podejrzenia powinna nastąpić odpowiednio. np. w art. 12 ust. 1 i ust. 2.	
539.	Związek Telewizji Kablowych Izba Gospodarcza	Art. 11	Art. 11 ust. 1 pkt. 2 ustawy o KSC Wprowadzenie zmiany art. 11 ust. 1 pkt. 2 ustawy o KSC zasadzające się w dodaniu po słowie „właściwym” słów „CSIRT sektorowemu”, po której to treści zostają wymienione trzy CSIRT-MON, NASK i GOV budzi wątpliwości natury językowej zasadzające się w tym, czy poza właściwym CSIRT sektorowym będzie dodatkowo podmiot kluczowy obciążał obowiązek zapewnienia dostępu do informacji o rejestrowanych incydentach także CSIRT MON, CSIRT NASK i CSIRT GOV, czy też obowiązek ten winien zostać wyeliminowany. Przy pierwszej bowiem opcji wskazane by było w art. 11 ust. 1 pkt. 2 ustawy o KSC po dodawanej treści postawienie przecinka, z kolei przy wyborze drugiej opcji należałoby skreślić treść w brzmieniu „CSIRT MON, CSIRT NASK lub CSIRT GOV”, co skutkowałoby zmianą w obu przypadkach regulacji art. 1 pkt. 15 lit. a tiret 2 projektu ustawy zmieniającej ustawę o KSC.	Wyjaśnienie uwagi Dostęp do rejestru incydentów powinny mieć zarówno CSIRT sektorowy jak i CSIRT krajowy. CSIRT krajowe mają prawo do zmiany klasyfikacji incydentów. CSIRT sektorowe wspierają podmioty kluczowe i ważne w obsłudze incydentów. Stąd muszą mieć dostęp do rejestru incydentów.
540.	Fundacja Bezpieczna Cyberprzestrzeń	Art. 12	Art. 1 pkt 16, treść art. 12 ust. 1 – podanie danych wskazanych w art. 12 ust. 1 pkt 4 w opinii FBC nie będzie możliwe, ze względu na wczesny charakter zdarzenia. Ponadto zakres informacji wymaganych przy zgłoszeniu podejrzenia incyduentu poważnego (patrz uwaga nr 14) w żaden sposób nie wskazuje na alarmujący charakter zgłoszenia. W związku z powyższym proponuje się, żeby zgłoszenie podejrzenia incyduentu poważnego zawierało co najmniej następujące informacje: (1) których systemów, urządzeń lub usług dotyczą nie (2) ożądane zdarzenia,pczas zaobserwowania zdarzeń objętych podejrzeniem wystąpienia incyduentu poważnego, (3) objawy (co zostało zaobserwowane, zgłoszone), (4) podjęte działania analityczne, zapobiegawcze, naprawcze (na chwilę zgłoszenia podejrzenia incyduentu poważnego), (5) planowane działania (analityczne, zapobiegawcze, naprawcze), (6) dane kontaktowe osoby uczestniczącej w obsłudze incyduentu.	Wyjaśnienie uwagi Wczesne ostrzeżenie ma na celu przekazanie jedynie informacji o wystąpieniu incyduentu. Dodatkowe informacje o incydencie zostaną przekazane w zgłoszeniu incyduentu oraz podczas obsługi incyduentu. Projektowana procedura zgłaszania incydentów oparta jest na już funkcjonującej procedurze.
541.	Fundacja Open Allies	Art. 12	Zgodnie z art. 12 ust. 2 nowelizowanej UKSC, po wczesnym ostrzeżeniu zawierającym wniosek o „wskazanie wytycznych dotyczących możliwych do wdrożenia środków ograniczających skutki incyduentu poważnego lub o wsparcie techniczne przy obsłudze incyduentu”, CSIRT sektorowy może udzielić odpowiedzi w terminie aż 24 godzin. Tak długi termin może powodować rozszerzenie incyduentu na kolejne elementy infrastruktury podmiotu objętego zdarzeniem lub nawet objęcie nowych podmiotów.	Uwaga nieuwzględniona Z uwagi na liczbę podmiotów podlegających ustawie CSIRT muszą mieć odpowiedni czas na reakcję. Ponadto należy zauważyć, że ten termin wynika z dyrektywy NIS2.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			Zwracamy się o skrócenie tego terminu. CSIRT sektorowy powinien udzielać wsparcia w terminie nie dłuższym niż 12 godzin.	
542.	Fundacja Bezpieczna Cyberprzestrzeń	Art. 12	Art. 1 pkt 16, treść art. 12 ust. 3 pkt 1 lit. e – proponuje się dodać na początku wyraz „prawdopodobną”. W ciągu 72 godzin mogą nie być dostępne znane (art. 12 ust. 5) i pewne informacje dotyczące przyczyn wystąpienia incydentu.	Wyjaśnienie uwagi Zgłaszający incydent na każdym etapie ma przekazywać informacje, które posiada. Nie musi podawać informacji
543.	Fundacja Bezpieczna Cyberprzestrzeń	Art. 12	Art. 1 pkt 16, treść art. 12 ust. 3 pkt 2 – proponuje się dodać wyraz „prawdopodobnych”, przed wyrazem przyczyn.	Uwaga nieuwzględniona Zaproponowany katalog informacji jakie ma zawierać zgłoszenie incydentu jest identyczny z informacjami jakie obecnie przekazywane są na podstawie art. 12 obowiązujące KSC. Jest to wykorzystanie już przyjętych procedur, co w dużym stopniu wpłynie na skuteczną obsługę incydentu. Ponadto chodzi o przekazanie informacji znanych w dniu wystąpienia incydentu, natomiast na kolejnym etapie obsługi incydentu dane te będą uzupełniane.
544.	ISAC-Kolej	Art. 12	Co jeśli przekazane informacje klasyfikowane są jako informacje niejawne w rozumieniu przepisów ustawy o ochronie informacji niejawnych np. posiadają klauzulę „zastrzeżone”, których nieuprawnione ujawnienie, zgodnie z ustawą, może mieć szkodliwy wpływ na wykonywanie przez organy władzy publicznej lub inne jednostki organizacyjne zadań w zakresie obrony narodowej, polityki zagranicznej, bezpieczeństwa publicznego, przestrzegania praw i wolności obywateli, wymiaru sprawiedliwości albo interesów ekonomicznych Rzeczypospolitej Polskiej.	Wyjaśnienie uwagi Informacje niejawne należy przekazywać w sposób zgodny z ustawą o ochronie informacji niejawnych.
545.	Stowarzyszenie Absolwentów Studiów Cyberbezpieczeństwa MBA	Art. 12	Kwalifikacja znamion przestępstwa we wczesnym ostrzeżeniu Zgodnie z projektowanym przepisem art. 12 ust. 1 pkt. 5 ustawy o KSC wczesne ostrzeżenie musi zawierać informację czy incydent poważny wyczerpuje znamiona przestępstwa. Osoby dokonujące zgłoszeń do systemów na ogół są inżynierami bezpieczeństwa. Kwalifikacja znamion przestępstwa stanowi nie tylko domenę prawną. Kwalifikacja w ciągu 24h czy zdarzenie wyczerpuje znamiona przestępstwa w praktyce może być niemożliwa do realizacji. Zwłaszcza biorąc pod uwagę, że organy ścigania po otrzymaniu zgłoszenia takiego zdarzenia, prowadząc czynności dochodzeniowo-śledcze dochodzą często do wniosku, że mimo wstępnej kwalifikacji zgłaszającego, zdarzenie znamion przestępstwa nie wyczerpuje. Przepisy mają określony cel – w tym przypadku jest nim ustalenie czy zdarzenie będzie zgłoszone organom ścigania. Tak właśnie powinien zostać sformułowany wskazany przepis – nie w kwestii wypełnienia znamion przestępstwa, tylko informacji, czy incydent został zgłoszony organom ścigania. Zmienia to diametralnie podejście do zakresu przekazywanych informacji przez osoby wypełniające zgłoszenie.	Uwaga uwzględniona Przepis został przeredagowany i otrzymał brzmienie: „5) wskazanie czy incydent poważny został wywołany działaniem bezprawnym lub działaniem w złej wierze”. Należy zauważyć, że obowiązek przekazania takiej informacji wynika z dyrektywy NIS2 (art. 23 ust. 4 lit. a).

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			Pozwoli również na udzielenie informacji, co do których możliwa jest ocena ich prawdziwości i zapewnienie realnej odpowiedzialności za jej treść. W NIS2 (art. 23 ust. 4 lit. a)) jest mowa o zawarciu we wczesnym ostrzeżeniu informacji o przypuszczeniu wywołania incydentu poważnego działaniem bezprawnym lub działaniem w złym zamiarze. Jeżeli zapisy powołanego powyżej przepisu projektu mają implementować ten właśnie zakres, to powinny literalnie odnosić się do nomenklatury NIS2 (czym innym jest spełnienie znamion przestępstwa, a czym innym ocena bezprawności działania lub złego zamiaru, które można ocenić biorąc pod uwagę sprawcę (atakującego) i skutki zdarzenia na poziomie technicznym).	
546.	Konfederacja Lewiatan	Art. 12	W art. 12 ust. 1 pkt 5 wskazano, że należy przekazać: „ <i>wskazanie czy incydent poważny wyczerpuje znamiona przestępstwa</i> ”. Wymóg ten wymaga przeformułowania zgodnie z brzmieniem NIS2. Dyrektywa wskazuje w tym zakresie następująco: „ <i>w którym w stosownych przypadkach wskazuje się, czy poważny incydent został przypuszczalnie wywołany działaniem bezprawnym lub działaniem w złym zamiarze</i> ”. Podmioty kluczowe lub ważne, a w szczególności podmioty prywatne, nie posiadają żadnych uprawnień do dokonywania klasyfikacji czynów jako przestępstw. Takie podmioty mogą natomiast informować o swoich przypuszczeniach lub podejrzeniach co do ew. nieuprawnionego naruszenia ich dóbr, w tym poprzez ew. dokonanie czynności o charakterze przestępstwa. Klasyfikacji zdarzeń jako przestępstw powinny zaś dokonywać uprawnione do tego służby państwowe.	Uwaga uwzględniona Przepis został przeredagowany i otrzymał brzmienie: „5) wskazanie czy incydent poważny został wywołany działaniem bezprawnym lub działaniem w złej wierze”. Należy zauważyć, że obowiązek przekazania takiej informacji wynika z dyrektywy NIS2 (art. 23 ust. 4 lit. a).
547.	Konfederacja Lewiatan	Art. 12	Art. 12 ust. 3 projektu ustawy zawiera bardzo szczegółowy zestaw parametrów, które należy udostępnić w ramach zgłoszenia incydentu. Zalecamy unikanie takich specyfikacji, ponieważ szablony i rodzaje informacji, które mają być udostępniane, zostaną ujednolicone w całej UE w nadchodzącym akcie wykonawczym dotyczącym zgłaszania incydentów. Ujednolicenie szablonów zgłoszeń w całej UE pomaga w zapewnieniu kompatybilności zgłoszeń, ułatwiając tym samym transgraniczną wymianę i analizę informacji. Pomaga to również firmom, które działają w dwóch lub więcej krajach UE, uniknąć zamieszania prawnego i niepotrzebnych inwestycji zasobów w celu radzenia sobie z różnymi systemami sprawozdawczości.	Wyjaśnienie uwagi Zaproponowany katalog informacji jakie ma zawierać zgłoszenie incydentu jest identyczny z informacjami jakie obecnie przekazywane są na podstawie art. 12 obowiązujące KSC. Jest to wykorzystanie już przyjętych procedur, co w dużym stopniu wpłynie na skuteczną obsługę incydentu. Należy zauważyć, że wydanie aktu wykonawczego rodzaju informacji i procedury zgłaszania incydentu ma charakter fakultatywny. Jeżeli więc taki akt zostanie wydany, to przepisy ustawy zostaną z nim uspołnione.
548.	Konfederacja Lewiatan	Art. 12	Sygnalizujemy, że powtórzona została ta sama norma w dwóch przepisach dot. zgłoszenia incydentu. <i>f) przyczynę zaistnienia incydentu poważnego i sposób jego przebiegu oraz skutki jego oddziaływania na systemy informacyjne lub świadczone usługi</i> <i>2) opis przyczyn tego incydentu, sposób jego przebiegu oraz prawdopodobne skutki oddziaływania na systemy informacyjne</i>	Uwaga uwzględniona Usunięto lit. f.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

549.	Polska Izba Informatyki i Telekomunikacji	Art. 12	Art. 12 ust. 1 pkt 5 – wczesne ostrzeżenie W art. 12 ust. 1 pkt 5 wskazano, że należy przekazać: „wskazanie czy incydent poważny wyczerpuje znamiona przestępstwa”. Wymóg ten wymaga przeformułowania zgodnie z brzmieniem NIS2. Dyrektywa wskazuje w tym zakresie następująco: „w którym w stosownych przypadkach wskazuje się, czy poważny incydent został przypuszczalnie wywołany działaniem bezprawnym lub działaniem w złym zamiarze”. Podmioty kluczowe lub ważne, a w szczególności podmioty prywatne, nie posiadają żadnych uprawnień do dokonywania klasyfikacji czynów jako przestępstw. Takie podmioty mogą natomiast informować o swoich przypuszczeniach lub podejrzeniach co do ew. nieuprawnionego naruszenia ich dóbr, w tym poprzez ew. dokonanie czynności o charakterze przestępstwa. Klasyfikacji zdarzeń jako przestępstw powinny zaś dokonywać uprawnione do tego służby państwowe.	Uwaga uwzględniona Przepis zostanie stosowanie preredagowany.
550.	Polska Izba Informatyki i Telekomunikacji	Art. 12	Art. 12 ust. 3 pkt 1 lit. f w zw. z ust. 2 Sygnalizujemy, że powtórzona została ta sama norma w dwóch przepisach dot. zgłoszenia incyduentu. <i>f) przyczynę zaistnienia incyduentu poważnego i sposób jego przebiegu oraz skutki jego oddziaływania na systemy informacyjne lub świadczone usługi</i> <i>2) opis przyczyn tego incyduentu, sposób jego przebiegu oraz prawdopodobne skutki oddziaływania na systemy informacyjne</i>	Uwaga uwzględniona Przepis zostanie zmieniony przez usunięcie lit. e z pkt 1 w ust. 3.
551.	Konfederacja Lewiatan	Art. 12a i 12b	Jednostka redakcyjna: art. 12a i art. 12b Jednostka redakcyjna NIS2: 23 ust. 4 lit d) Uwaga: Art. 12a projektu KSC wymaga, aby sprawozdanie końcowe dotyczące incyduentu poważnego zawierało: – szczegółowy opis incyduentu, w tym spowodowane zakłócenia i szkody; – rodzaj zagrożenia lub przyczynę, która prawdopodobnie była źródłem incyduentu; – zastosowane i wdrażane środki ograniczające ryzyko; – w odpowiednich przypadkach transgraniczne skutki incyduentu. Art. 12b ust. 1 i 2 projektu KSC określają obowiązek składania sprawozdań okresowych i końcowych w przypadku, gdy obsługa incyduentu poważnego nie zakończyła się w terminie składania sprawozdania końcowego. Obowiązek przedstawienia szczegółowego opisu incyduentu może wymagać ujawnienia informacji, które są kluczowe dla funkcjonowania przedsiębiorstwa, w tym danych dotyczących jego infrastruktury technicznej, procedur bezpieczeństwa oraz potencjalnych słabych punktów systemu. Takie informacje mogą stanowić tajemnicę przedsiębiorstwa zgodnie z definicją zawartą w art. 11 ust. 4 ustawy o zwalczaniu nieuczciwej konkurencji, która chroni informacje techniczne, technologiczne oraz organizacyjne przedsiębiorstwa, jeżeli nie są one powszechnie znane i mają wartość gospodarczą. Ujawnienie rodzaju zagrożenia lub przyczyny incyduentu może odsłonić wrażliwe informacje dotyczące mechanizmów zabezpieczeń stosowanych przez przedsiębiorstwo oraz potencjalnych luk, które mogły zostać wykorzystane przez atakujących. Tego typu informacje,	Wyjaśnienie uwagi Art. 40 ust. 3 ustawy o krajowym systemie cyberbezpieczeństwa nakazuje CSIRT zachowanie w tajemnicy informacji, w tym informacji stanowiących tajemnice prawnie chronione, uzyskanych w związku z realizacją zadań. Tajemnice przedsiębiorstwa są więc zabezpieczone.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			jeśli staną się publiczne, mogą zostać wykorzystane przez konkurencję lub osoby trzecie w sposób szkodliwy dla przedsiębiorstwa. Wymóg raportowania zastosowanych środków ograniczających ryzyko narusza zasadę ochrony tajemnicy przedsiębiorstwa, gdyż może prowadzić do ujawnienia szczegółowych informacji na temat strategii zabezpieczeń, technologii oraz procesów wewnętrznych przedsiębiorstwa. Takie dane mogą być strategicznie istotne i ich ujawnienie może osłabić konkurencyjność firmy oraz zwiększyć ryzyko przyszłych ataków. Art. 51 ust. 2 Konstytucji RP stanowi, że "władze publiczne nie mogą uzyskiwać, gromadzić ani udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym". Ochrona tajemnicy przedsiębiorstwa jest fundamentalnym elementem wolności gospodarczej i praw własności. Przepisy Art. 12a i Art. 12b nie uwzględniają jednak mechanizmów zabezpieczających przed nieuprawnionym dostępem do informacji, które mogą stanowić tajemnicę przedsiębiorstwa.	
552.	ZBP	Art. 13	Art. 13. 1. Podmiot kluczowy i podmiot ważny może przekazywać do właściwego CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT sektorowego informacje: 1) o innych incydentach; 2) o cyberzagrożeniach; 3) dotyczące szacowania ryzyka; 4) o podatnościach; 5) o potencjalnych zdarzeniach dla cyberbezpieczeństwa; 6) o wykorzystywanych technologiach. Art. 13. 1. Podmiot kluczowy i podmiot ważny może przekazywać do właściwego CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT sektorowego lub centrum wymiany i analiz informacji, informacje: 1) o innych incydentach; 2) o cyberzagrożeniach; 3) dotyczące szacowania ryzyka; 4) o podatnościach; 5) o potencjalnych zdarzeniach dla cyberbezpieczeństwa; 6) o wykorzystywanych technologiach. Umożliwienie podmiotom kluczowym i podmiotom ważnym przekazywanie do centrum wymiany i analiz informacji wskazanych informacji pozwoliłoby na wzmocnienie zdolności sektora bankowego do skutecznego przeciwdziałania podatnościom i incydentom. Pozyskiwanie tego rodzaju informacji pozwoliłoby jednocześnie na przeciwdziałanie stratom finansowym klientów sektora oraz zagrożeniom stabilności rynkowej.	Uwaga nieuwzględniona Kwestia ta jest zaadresowana w art. 8h – tam jest uregulowana kwestia dot. przekazywania informacji do porozumień typu ISAC.
553.	Związek Pracodawców Technologii Cyfrowych Lewiatan	Art. 13	Przekazywanie tajemnic prawnie strzeżonych (art. 13 pkt 3) Wydaje się, że prosty zapis w art. 13 pkt 3. jest jednak niewystarczający. Byłby wystarczający jeśli system S46 spełniał wymagania związane ze wszelkimi rodzajami tajemnic prawnie strzeżonych. Proponujemy następujący zapis:	Wyjaśnienie uwagi Informacje niejawne należy przekazywać w sposób zgodny z ustawą o ochronie informacji niejawnych.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. I

			3. Wszelkie informacje prawnie strzeżone przekazywane przez podmiot kluczowy i podmiot ważny są przekazywane zgodnie z obowiązującymi przepisami.	
554.	CyberMadeinPo land	Art. 14	Uchylenie art.14 zmienianej ustawy tworzy niepewność co do obowiązku utworzenia własnych struktur odpowiedzialnych za cyberbezpieczeństwo lub możliwości powierzenia tych zadań podmiotowi zewnętrznemu. Szczególne znaczenie może to mieć dla podmiotów publicznych których działania nie mogą opierać się na zasadzie „co nie jest zakazane jest dozwolone”	Uwaga uwzględniona Przepis art. 14 ust. 1 zostanie przywrócony.
555.	Fundacja Bezpieczna Cyberprzestrzeń	Art. 14	Art. 1 pkt 19 – uchylenie art. 14 obecnie obowiązującej ustawy bez wskazania alternatywy dla obowiązku powołania wewnętrznych struktur odpowiedzialnych za bezpieczeństwo lub skorzystania z usług dostawców usług zarządzanych w zakresie cyberbezpieczeństwa należy uznać za błąd. Brak takiego wymogu spowoduje, że takie struktury nie powstaną lub będą miały charakter wirtualny (łączenie kompetencji wielu osób z różnych działów, co jak pokazuje praktyka jest nieefektywne z punktu widzenia zapewnienia cyberbezpieczeństwa. Obecnie proponowane przepisy wskazują tym samym jedynie na obowiązek wdrożenia systemu zarządzania bezpieczeństwem informacji, co należy uznać za niewystarczające. Tylko najdojrzalsze organizacje wdrożą taki system z uwzględnieniem wymogów dotyczących personelu i jego kompetencjach, koncentrując się na zdolnościach do zarządzania bezpieczeństwem informacji, a nie jedynie na spełnieniu wymagań w zakresie dokumentacji. Proponuje się przywrócić art. 14 obecnej ustawy lub podjąć działania zmierzające do zmiany tego artykułu, zgodnie z oczekiwaniami ustawodawcy.	Uwaga uwzględniona Przepis art. 14 ust. 1 zostanie przywrócony.
556.	Osoba fizyczna	Art. 14	Dzień dobry, projekt nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa zakłada uchylenie art. 14 ustawy w jej obecnym brzmieniu. Z uzasadnienia projektu wynika, że regulacja ta jest zbędna ze względu na wymagania wobec podmiotów świadczących usługi z zakresu cyberbezpieczeństwa, wynikające z innych przepisów nowelizacji. Uchylenie tego artykułu zwalnia jednak operatorów również z powołania wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo. Czy taki jest cel, czy też powołanie tych struktur wynika z innych przepisów nowelizacji? Uprzejmie proszę o odpowiedź.	Uwaga uwzględniona Przepis art. 14 ust. 1 zostanie przywrócony.
557.	Polskie Towarzystwo Informatyczne	Art. 14	Uchylenie art. 14 zmienianej ustawy tworzy niepewność co do obowiązku utworzenia własnych struktur odpowiedzialnych za cyberbezpieczeństwo, lub możliwości powierzenia tych zadań podmiotowi zewnętrznemu. Szczególne znaczenie może to mieć dla podmiotów publicznych których działania nie mogą opierać się na zasadzie „co nie jest zakazane jest dozwolone”	Uwaga uwzględniona Przepis art. 14 ust. 1 zostanie przywrócony.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

Lp.	Zgłaszający uwagę	Jedn. red.	Treść uwagi	Stanowisko Ministra Cyfryzacji
1.	Osoba fizyczna	Art. 15	Sprawozdanie z przeprowadzonego audytu (bardzo krótki czas). <i>w art. 15:</i> <i>a) ust. 1 otrzymuje brzmienie:</i> <i>b) po ust. 1 dodaje się ust. 1a i 1b w brzmieniu:</i> <i>„1a. Podmiot kluczowy lub podmiot ważny przedstawia w postaci elektronicznej sprawozdanie z przeprowadzonego audytu, o którym mowa w ust. 1, organowi właściwemu, w terminie trzech dni roboczych od dnia jego otrzymania przez podmiot kluczowy lub podmiot ważny.</i> Uzasadnienie: Przekazanie raportu w ciągu 3 dni jest możliwy, natomiast przekazanie jego w takim terminie może być zbyt krótkie aby Zarządy mogły się z nimi zapoznać. Rekomendowałbym 7 dni.	Wyjaśnienie uwagi W zakresie terminu na przekazanie sprawozdania z audytu podkreślić należy, że chodzi o przekazanie kopii sprawozdania. Jest to zatem termin odpowiedni.
2.	Polskie Stowarzyszenie Fotowoltaiki	Art. 15	Art. 15 PK oraz PW są zobowiązane do przeprowadzania co najmniej raz na 2 lata audytu bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi: - obowiązek przedstawienia organowi właściwemu sprawozdania z audytu w postaci elektronicznej w terminie 3 dni od dnia jego otrzymania oraz innym organom na wniosek; obowiązek przeprowadzenia pierwszego audytu w terminie 12 miesięcy od uznania za PK lub PW Brak istotnego wpływu względem aktualnie obowiązujących przepisów KSC. W zakresie terminu na przekazanie sprawozdania z audytu organowi właściwemu zastosowanie znajdują poniższe uwagi dot. wpływu na sektor energetyczny. Wpływ na sektor energetyczny: w odniesieniu do dużych organizacji, jakimi jest wiele spółek sektora energetycznego, termin w wymiarze 3 dni na przekazanie sprawozdania z audytu od dnia jego otrzymania jest istotnie zbyt krótki. Termin ten nie uwzględnia również czasu na zapoznanie się z wynikami audytu wewnątrz w ramach audytowanej organizacji. [Nadregulacja względem Dyrektywy NIS2] Na podstawie Dyrektywy NIS2 organ właściwy może objąć PK lub PW ukierunkowanym audytem, niemniej nie przewiduje obowiązku przeprowadzania przez PW lub PK regularnych audytów. Obowiązek przekazywania wyników audytów prowadzonych samodzielnie przez podmioty nie wynika również z Dyrektywy NIS2. Mimo funkcjonowania obowiązku regularnego przeprowadzania audytu przez operatora usługi kluczowej na gruncie obecnie obowiązujących przepisów KSC, rekomendujemy postulowanie ograniczenia obowiązku przeprowadzania regularnego audytu przez PK i PW. Rekomendacja: - wycofanie z Projektu i z KSC bezwzględnego obowiązku przeprowadzania regularnych audytów bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi - wydłużenie terminu na przekazanie wyników audytów systemu informacyjnego wykorzystywanego do świadczenia usługi, co najmniej do 30 dni; - zmiana konstrukcji przepisów w taki sposób, aby wyniki audytów bezpieczeństwa systemu bezpieczeństwa informacji przekazywane były wyłącznie na żądanie właściwego organu	Wyjaśnienie uwagi Wskazać należy, że regularne audyty funkcjonują już na podstawie obecnych przepisów ustawy o krajowym systemie cyberbezpieczeństwa i pełnią istotną rolę w zapewnianiu wysokiego poziomu bezpieczeństwa. W zakresie terminu na przekazanie sprawozdania z audytu podkreślić należy, że chodzi o przekazanie kopii sprawozdania. Jest to zatem termin odpowiedni. Wyniki audytu powinny być przekazywane niezależnie od żądania właściwego organu z uwagi na to, że audyt ten dotyczy podmiotów kluczowych nad którymi sprawowany jest również nadzór prewencyjny.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

		Uwagi uzupełniające PK oraz PW są zobowiązane do przeprowadzania co najmniej raz na 2 lata audytu bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi: - obowiązek przedstawienia organowi właściwemu sprawozdania z audytu w postaci elektronicznej w terminie 3 dni od dnia jego otrzymania oraz innym organom na wniosek; - obowiązek przeprowadzenia pierwszego audytu w terminie 12 miesięcy od uznania za PK lub PW. Ogólny wpływ regulacji: Brak istotnego wpływu względem aktualnie obowiązujących przepisów KSC. W zakresie terminu na przekazanie sprawozdania z audytu organowi właściwemu zastosowanie znajdują poniższe uwagi dot. wpływu na sektor energetyczny. Wpływ na sektor energetyczny: W odniesieniu do dużych organizacji, jakimi jest wiele spółek sektora energetycznego, termin w wymiarze 3 dni na przekazanie sprawozdania z audytu od dnia jego otrzymania jest istotnie zbyt krótki. Termin ten nie uwzględnia również czasu na zapoznanie się z wynikami audytu wewnętrznie w ramach audytowanej organizacji. Nadregulacja względem Dyrektywy NIS2] Na podstawie Dyrektywy NIS2 organ właściwy może objąć PK lub PW ukierunkowanym audytem, niemniej nie przewiduje obowiązku przeprowadzania przez PW lub PK regularnych audytów. Obowiązek przekazywania wyników audytów prowadzonych samodzielnie przez podmioty nie wynika również z Dyrektywy NIS2. Mimo funkcjonowania obowiązku regularnego przeprowadzania audytu przez operatora usługi kluczowej na gruncie obecnie obowiązujących przepisów KSC, rekomendujemy postulowanie ograniczenia obowiązku przeprowadzania regularnego audytu przez PK i PW. Rekomendacja: - wycofanie z Projektu i z KSC bezwzględnego obowiązku przeprowadzania regularnych audytów bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi - wydłużenie terminu na przekazanie wyników audytów systemu informacyjnego wykorzystywanego do świadczenia usługi, co najmniej do 30 dni;	

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

			- zmiana konstrukcji przepisów w taki sposób, aby wyniki audytów bezpieczeństwa systemu bezpieczeństwa informacji przekazywane były wyłącznie na żądanie właściwego organu.	
3.	Cybermadeinpol and	Art. 15	Art. 15 p. 1 – doprecyzowanie o zakresie audytu, tj. przynajmniej czy audyt każdorazowo ma obejmować pełen zakres zgodności.	Wyjaśnienie uwagi Audyt każdorazowo powinien obejmować pełen zakres zgodności. Jednak w sytuacji w której będzie to audyt doraźny, zlecony przez organ właściwy do spraw cyberbezpieczeństwa w ramach sprawowanego nadzoru, organ ten będzie mógł wskazać zakres audytu. Tym samym wykluczy to obowiązek przeprowadzenia audytu bezpieczeństwa wszystkich systemów informacyjnych.
4.	IAB Polska	Art. 15	Audyty bezpieczeństwa systemu informatycznego. [art. 1 ust. 20 lit. a) i b) projektu nowelizacji / art. 15 ust. 1 i 1a nowelizowanego UKSC] W projekcie nowelizacji nakłada się na podmioty kluczowe i podmioty ważne obowiązek regularnego przeprowadzania audytu bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi, a następnie przedstawienia właściwemu organowi sprawozdania z takiego audytu w terminie trzech dni roboczych od dnia jego otrzymania przez podmiot kluczowy lub podmiot ważny. W tym miejscu warto przypomnieć sygnalizowane już wcześniej wątpliwości dotyczące posługiwania się w projekcie nowelizacji pojęciem „świadczonej usługi” i „systemu informacyjnego wykorzystywanego do świadczenia usługi”. Nie jest bowiem jasne, jakiego systemu miałyby dotyczyć przeprowadzane audyty. Co więcej, projekt nowelizacji nie wprowadza żadnych ustandaryzowanych wymagań dla sprawozdań z audytu, a także wyznacza bardzo krótki czas na przedstawienia właściwemu organowi takiego sprawozdania. Mając to na uwadze, IAB Polska postuluje, aby obowiązek przeprowadzania audytu bezpieczeństwa nie dotyczył „systemu informacyjnego wykorzystywanego do świadczenia usługi”, a raczej „systemu zarządzania bezpieczeństwem informacji”. Alternatywnie, w razie nieuwzględnienia powyższego postulatu, IAB Polska wskazuje na potrzebę konkretyzacji systemów informacyjnych, których miałyby dotyczyć obowiązki audytowe. IAB Polska postuluje również wprowadzenie ustandaryzowanych wymagań dla sprawozdań z audytu, a także wydłużenie czasu na przedstawienia właściwemu organowi takiego sprawozdania do 14 dni.	Uwaga nieuwzględniona Ustawa wyraźnie wskazuje, że audytowi podlega system informacyjny wykorzystywany w procesie świadczenia usługi. Usługa ta ma być relewantna z punktu widzenia ustawy. Audyt przeprowadzany jest w pełnym zakresie co 3 lata i tylko w sytuacji zlecenia audytu doraźnego przez organ właściwy do spraw cyberbezpieczeństwa jego zakres może być zawężony. Dodatkowo należy wskazać, że w terminie 3 dni przedstawiana jest wyłącznie kopia sprawozdania z audytu. Wprowadzenie ustandaryzowanych wymagań dla sprawozdań z audytu zostanie przeanalizowane na dalszym etapie.
5.	Rada Bezpieczeństwa Biznesowego Grupy MiSOT	Art. 15	„Art. 15. 2. Audyt może być przeprowadzony przez: 2) co najmniej dwóch audytorów dla podmiotu kluczowego i co najmniej jednego audytora dla podmiotów ważnych, posiadających.” Uzasadnienie: Biorąc pod uwagę wielkość mikro podmiotów telekomunikacyjnych, które zostaną podmiotami ważnymi, postulujemy, aby dla podmiotów ważnych pozostawić wymóg jednego audytora co znacznie obniży koszty przeprowadzanych audytów. Audytor na rynku wycenia własną pracę za	Wyjaśnienie uwagi Obowiązkowe regularne audyty dla podmiotów ważnych zostały usunięte z projektu. Pozostały audyty ad hoc nakładane w drodze decyzji administracyjnej. Stąd uwaga jest bezprzedmiotowa.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

			dwa dni audytowe (minimalny czas przeprowadzenia Audytu ISO27001) jako kwotę do 3 tys zł za dzień. Do tego należy dołożyć koszty sporządzenia raportu. Norma ISO19011 dopuszcza przeprowadzanie Audytu w mikro przedsiębiorstwach przez jednego Audytora. Podwojenie kosztów Audytu dla mikroprzedsiębiorcy jest dla niego znacznie większym obciążeniem w sensie kosztu niż dla podmiotów średnich. Co więcej nie ma takiego uzasadnienia w normach. Dlatego postulujemy aby dla podmiotów ważnych wprowadzono wymóg przeprowadzania Audytów przez 1 Audytora.	
6.	Konfederacja Lewiatan	Art. 15	Nieprawidłowa forma wpisu operatorów usług kluczowych do wykazu podmiotów kluczowych i ważnych. Jednostka redakcyjna: art. 15 ust. 2 projektu KSC Jednostka redakcyjna NIS2: 3 ust. 2 Uwaga: Zgodnie z art. 15 ust. 2 projektu KSC, organ właściwy do spraw cyberbezpieczeństwa wpisuje z urzędu do wykazu podmiotów kluczowych i podmiotów ważnych operatorów usług kluczowych wpisanych przed dniem wejścia w życie niniejszej ustawy do wykazu operatorów usług kluczowych. Niemniej jest to czynność o charakterze materialnym, tj. umieszczenie w wykazie podmiotów ważnych i kluczowych ma charakter materialny, kształtujący prawa i obowiązki operatorów usług kluczowych. Treść tego przepisu pozwala uznać, że wpis stanowi czynność materialno-techniczną, która należy do czynności faktycznych administracji, służących bezpośredniej i praktycznej realizacji konkretnych zadań administracji. Niemniej fakt wpisania do wykazu powinien być realizowany w formie decyzji administracyjnej, ponieważ wpływa na prawa i obowiązki jej adresata. Wpisanie operatora usług kluczowych do wykazu podmiotów kluczowych i ważnych determinuje jego obowiązki i uprawnienia wynikające z ustawy, co jednoznacznie wskazuje na konieczność wydania decyzji administracyjnej, aby zapewnić przejrzystość, pewność prawa i możliwość odwołania się od takiej decyzji. Obecna forma przepisu jest zbyt uproszczona i nie uwzględnia konieczności formalnego uregulowania wpływu na prawa i obowiązki operatorów usług kluczowych.	Wyjaśnienie uwagi Wobec operatorów usług kluczowych zostały już wydane decyzje administracyjne na podstawie których wykonują oni obowiązki z obecnie obowiązującej ustawy o krajowym systemie cyberbezpieczeństwie. Nowelizacja zakłada rozszerzenie systemu co wiąże się z dodaniem do niego podmiotów, a nie oznacza usunięcia z niego już uwzględnionych podmiotów. Należy również podkreślić, że każdy z tych podmiotów będzie spełniać przesłanki uznania za podmiot kluczowy.
7.	Konfederacja Lewiatan	Art. 15	W Dyrektywie NIS2 wymóg regularnych audytów bezpieczeństwa nie ma zastosowania do podmiotów ważnych Jednostka redakcyjna: art. 15 ust.1 projektu KSC Jednostka redakcyjna NIS2: art. 32 ust. 2 lit. b) Uwaga: Art. 32 ust. 4 lit. b) Dyrektywy NIS2 wprowadza obowiązek objęcia podmiotów kluczowych regularnymi, ukierunkowanymi audytami bezpieczeństwa, które prowadzone są przez niezależną instytucję lub właściwy organ. Audyty te opierają się na oszacowaniach ryzyka przeprowadzonych przez właściwy organ lub badany podmiot, bądź na innych dostępnych informacjach dotyczących ryzyka. Propozycja implementacji tego przepisu w polskim ustawodawstwie rozszerza ten obowiązek na podmioty ważne, co stanowi rozszerzenie w stosunku do wymagań Dyrektywy. Ponadto zgodnie z proponowanymi przepisami, audyt jest obligatoryjny dla wszystkich tych podmiotów, co dwa lata, bez względu na wcześniejsze oszacowanie ryzyka.	Uwaga uwzględniona Przepis został zmieniony pozostawiając obowiązek regularnych audytów tylko w stosunku do podmiotów kluczowych – podmioty ważne nie będą do niego zobowiązane.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

			Oznacza to, że polskie przepisy implementują przepisy NIS2 w sposób nadmierny w tym zakresie. Jest to również istotne dla jednostek samorządu terytorialnego, gdyż nowe przepisy obejmą także te podmioty obowiązku audytami – sam OSR wymienia prawie 28 000 podmiotów jako podmioty z sektora administracji publicznej.	
8.	IAB Polska	Art. 15	1) W art. 15 wskazuje, że audyt może być przeprowadzany m.in. przez dwóch audytorów z 3 letnią praktyką. Pragniemy zauważyć, że audyt bezpieczeństwa systemów w – przykładowo - powiatowym urzędzie pracy czy rodzinnej spółce handlowej zdecydowanie różni się od audytu w potężnym przedsiębiorstwie energetycznym. Rekomendujemy doprecyzowanie wymagań z zakresie doświadczenia zawodowego audytorów. 2) 2a. Audyt nie może być przeprowadzony przez osobę realizującą w podmiocie audytowanym zadania, o których mowa w art. 8 i art. 11, lub która realizowała te zadania w podmiocie audytowanym przez rok przed rozpoczęciem audytu. Mamy wrażenie, że ustawodawca ma na myśli „w przeciągu roku”. 3) Zdecydowanie jednocześnie podkreślamy, że zasady prowadzenia kontroli zdecydowanie różnią się od zasad prowadzenia audytów. Art. 15 ust 3 pkt 4 oraz 5 obowiązkowo powinny być usunięte!	Uwaga: 1) nieuwzględniona Doświadczenie audytorów powinno być tożsame dla wszystkich podmiotów zobowiązanych do jego przeprowadzenia. Nie jest zasadne wprowadzanie różnic pomiędzy podmiotami w ich obowiązkach jeśli podmioty te należą do tej samej kategorii tzn. są podmiotami kluczowymi. 2) uwzględniona Zmieniono brzmienie zgodnie z propozycją 3) nieuwzględniona Uwaga nie zasługuje na uwzględnienie ze względu na to, że pomimo działania na podstawie ustawy o kontroli w administracji rządowej lub ustawy o Najwyższej Izbie Kontroli konieczne jest spełnienie wymogów z ust. 3 tj. posiadanie odpowiednio długiego doświadczenia w wykonywaniu audytów.
9.	Polska Izba Przemysłu Chemicznego	Art. 15	art. 1 pkt 20 ustawy zmieniającej, w zakresie art. 15 ust. 1b - Rekomendujemy doprecyzowanie sformułowania, zgodnie z którym nakazanie zlecenia audytu następuje jedynie w sytuacji, gdy podmiot kluczowy lub podmiot ważny nie daje należytej gwarancji wykonania audytu w terminie określonym w ustępie 1. Alternatywnie proponujemy jednoznaczne wskazanie katalogu przesłanek uzasadniających nakazanie takiego dodatkowego działania. Doprecyzowanie miałooby na celu wykluczenie interpretacji, zgodnie z którą organ właściwy ds. cyberbezpieczeństwa może nakazać przeprowadzenie innych dodatkowych audytów we wskazanym okresie referencyjnym.	Uwaga nieuwzględniona Zlecenie audytów dodatkowych to uprawnienie nadzorcze wynikające z art. 53 ust. 2 pkt 2.
10.	Konfederacja Lewiatan	Art. 15	W Dyrektywie NIS2 wymóg regularnych audytów bezpieczeństwa nie ma zastosowania do podmiotów ważnych Jednostka redakcyjna: art. 15 ust.1 projektu KSC Jednostka redakcyjna NIS2: art. 32 ust. 2 lit. b) Uwaga: Art. 32 ust. 4 lit. b) Dyrektywy NIS2 wprowadza obowiązek objęcia podmiotów kluczowych regularnymi, ukierunkowanymi audytami bezpieczeństwa, które prowadzone są przez niezależną instytucję lub właściwy organ. Audyty te opierają się na oszacowaniach ryzyka przeprowadzonych przez właściwy organ lub badany podmiot, bądź na innych dostępnych	Uwaga uwzględniona Przepis został przeredagowany w ten sposób, aby swoim zakresem obejmować wyłącznie podmioty kluczowe. Podmioty ważne objęte zostały wyłącznie audytem zleconym w ramach nadzoru sprawowanego następczo.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

			informacjach dotyczących ryzyka. Propozycja implementacji tego przepisu w polskim ustawodawstwie rozszerza ten obowiązek na podmioty ważne, co stanowi rozszerzenie w stosunku do wymagań Dyrektywy. Ponadto zgodnie z proponowanymi przepisami, audyt jest obligatoryjny dla wszystkich tych podmiotów, co dwa lata, bez względu na wcześniejsze oszacowanie ryzyka. Oznacza to, że polskie przepisy implementują przepisy NIS2 w sposób nadmierny w tym zakresie. Jest to również istotne dla jednostek samorządu terytorialnego, gdyż nowe przepisy obejmą także te podmioty obowiązkowymi audytami – sam OSR wymienia prawie 28 000 podmiotów jako podmioty z sektora administracji publicznej.	
11.	Centrum Wymiany i Analiz Informacji podsektora transportu kolejowego „ISAC-Kolej”	Art. 15	w art. 15 ust. 1a i 1b wprowadzić zmianę zapisu na: „1a. Podmiot kluczowy lub podmiot ważny przedstawia w postaci elektronicznej raport z przeprowadzonego audytu, o którym mowa w ust. 1, organowi właściwemu, w terminie trzech dni roboczych od dnia jego otrzymania przez podmiot kluczowy lub podmiot ważny. 1b. Organ właściwy do spraw cyberbezpieczeństwa może nakazać, w drodze decyzji, przeprowadzenie audytu, o którym mowa w ust. 1, wraz z określeniem terminu przekazania raportu z przeprowadzonego audytu”. Audyty kończą się raportem, a nie sprawozdaniem. Stanowią o tym m.in. normy i standardy branżowe w zakresie prowadzenia i realizacji audytów. Przykładowo norma ISO 19011 Wytyczne dotyczące auditowania systemów zarządzania w pkt 6.5 określa „Przygotowanie i rozpowszechnianie raportu z auditu”	Uwaga uwzględniona
12.	Centrum Wymiany i Analiz Informacji podsektora transportu kolejowego „ISAC-Kolej”	Art. 15	w art. 15 ust. 7 wprowadzić zmianę zapisu na: „Podmiot kluczowy lub podmiot ważny przekazuje kopię raportu z przeprowadzonego audytu na wniosek:” Audyty kończą się raportem, a nie sprawozdaniem. Stanowią o tym m.in. normy i standardy branżowe w zakresie prowadzenia i realizacji audytów. Przykładowo norma ISO 19011 Wytyczne dotyczące auditowania systemów zarządzania w pkt 6.5 określa „Przygotowanie i rozpowszechnianie raportu z auditu”	Uwaga uwzględniona
13.	Polska Izba Komunikacji Elektronicznej (PIKE)	Art. 15	Jako przykłady nadregulacji możemy wskazać: • zrównanie kwestii związanych z kontrolą i audytami bezpieczeństwa dla podmiotów kluczowych i ważnych,	Wyjaśnienie uwagi Przepis został zmieniony w ten sposób, że regularne audyty nie będą dotyczyły podmiotów ważnych, a wyłącznie kluczowe.
14.	Grupa MiSOT	Art. 15	Wbrew dyrektywie NIS2 zdecydowana większość obowiązków została nałożona na podmioty ważne oraz podmioty kluczowe w niemal takim samym zakresie. Jako szczególnie jaskrawy przykład należy wskazać art. 15 ust. 1 KSC, zgodnie z którym nie tylko podmioty kluczowe, lecz również podmioty ważne mają obowiązek przeprowadzać cykliczny audyt bezpieczeństwa systemu informacyjnego „wykorzystywanego do świadczenia usługi”.	Uwaga wyjaśniona Przepis został zmieniony w ten sposób, że regularne audyty nie będą dotyczyły podmiotów ważnych, a wyłącznie kluczowe.
15.	Grupa MiSOT	Art. 15	„Art. 15. 2. Audyt może być przeprowadzony przez: 2) co najmniej dwóch audytorów dla podmiotu kluczowego i co najmniej jednego audytora dla podmiotów ważnych, posiadających:”	Uwaga nieuwzględniona Przepis został przeredagowany w ten sposób, że obowiązek regularnych audytów

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

			Biorąc pod uwagę wielkość mikro podmiotów telekomunikacyjnych, które zostaną podmiotami ważnymi, postulujemy, aby dla podmiotów ważnych pozostawić wymóg jednego audytora co znacznie obniży koszty przeprowadzanych audytów. Audytor na rynku wycenia własną pracę za dwa dni audytowe (minimalny czas przeprowadzenia Audytu ISO27001) jako kwotę do 3 tys zł za dzień. Do tego należy dołożyć koszty sporządzenia raportu. Norma ISO19011 dopuszcza przeprowadzanie Audytu w mikro przedsiębiorstwach przez jednego Audytora. Podwojenie kosztów Audytu dla mikroprzedsiębiorcy jest dla niego znacznie większym obciążeniem w sensie kosztu niż dla podmiotów średnich. Co więcej nie ma takiego uzasadnienia w normach. Dlatego postulujemy aby dla podmiotów ważnych wprowadzono wymóg przeprowadzania Audytów przez 1 Audytora.	dotyczył będzie wyłącznie podmiotów kluczowych. Podmioty ważne objęte zostaną wyłącznie obowiązkiem audytów ad hoc, zleconych w ramach sprawowania nadzoru następczego. W takiej sytuacji obciążenia finansowe podmiotów ważnych będą znacznie niższe niż przy obowiązku przeprowadzania regularnych audytów. Jednocześnie należy zagwarantować, że audyty zlecone w ramach nadzoru będą przeprowadzone rzetelnie i na tożsamym poziomie, odpowiadającym poziomowi audytów prowadzonych w podmiotach kluczowych. Z tego względu projektodawca stoi na stanowisku, że należy pozostawić tożsamą liczbę audytorów, niezależnie od podmiotu.
16.	Fundacja Open Allies	Art. 15	Zwracamy się o zmniejszenie częstotliwości audytów bezpieczeństwa systemu informacyjnego. Zgodnie z art. 15 ust. 1 nowelizowanej UKSC, audyt powinien być przeprowadzany co 2 lata. Zwracamy uwagę, że przeprowadzenie audytu zajmuje określony okres czasu. Zbyt duża częstotliwość audytów może doprowadzić do sytuacji, w której podmiot będzie albo przeprowadzał audyt albo wdrażał wytyczne ustalone w ramach audytu. Wnosimy o ustalenie częstotliwości obowiązkowego audytu nie częściej niż co 3 lata.	Uwaga uwzględniona
17.	Morskie Centrum Cyberbezpieczeństwa Akademia Marynarki Wojennej w Gdyni	Art. 15	1) W art. 15 wskazuje, że audyt może być przeprowadzany m.in. przez dwóch audytorów z 3 letnią praktyką. Pragniemy zauważyć, że audyt bezpieczeństwa systemów w – przykładowo - powiatowym urzędzie pracy czy rodzinnej spółce handlowej zdecydowanie różni się od audytu w potężnym przedsiębiorstwie energetycznym. Rekomendujemy doprecyzowanie wymagań z zakresie doświadczenia zawodowego audytorów. 2) 2a. Audyt nie może być przeprowadzony przez osobę realizującą w podmiocie audytowanym zadania, o których mowa w art. 8 i art. 11, lub która realizowała te zadania w podmiocie audytowanym <u>przez rok</u> przed rozpoczęciem audytu. Mamy wrażenie, że ustawodawca ma na myśli „w <u>przeciągu roku</u> ” 3) Zdecydowanie jednocześnie podkreślamy, że zasady prowadzenia kontroli zdecydowanie różnią się od zasad prowadzenia audytów. <u>Art. 15 ust 3 pkt 4 oraz 5 obowiązkowo powinny być usunięte!</u>	Uwaga: 1) nieuwzględniona Doświadczenie audytorów powinno być tożsame dla wszystkich podmiotów zobowiązanych do jego przeprowadzenia. Nie jest zasadne wprowadzanie różnic pomiędzy podmiotami w ich obowiązkach jeśli podmioty te należą do tej samej kategorii tzn. są podmiotami kluczowymi; 2) uwzględniona Zmieniono brzmienie zgodnie z propozycją; 3) nieuwzględniona Uwaga nie zasługuje na uwzględnienie z uwagi na to, że pomimo działania na podstawie ustawy o kontroli w administracji

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

				rządowej lub ustawy o Najwyższej Izbie Kontroli konieczne jest spełnienie wymogów z ust. 3 tj. posiadania odpowiednio długiego doświadczenia w wykonywaniu audytów.
18.	Osoba fizyczna	Art. 15	Sprawozdanie z przeprowadzonego audytu (bardzo krótki czas). w art. 15: a) ust. 1 otrzymuje brzmienie: b) po ust. 1 dodaje się ust. 1a i 1b w brzmieniu: „1a. Podmiot kluczowy lub podmiot ważny przedstawia w postaci elektronicznej sprawozdanie z przeprowadzonego audytu, o którym mowa w ust. 1, organowi właściwemu, w terminie trzech dni roboczych od dnia jego otrzymania przez podmiot kluczowy lub podmiot ważny. Uzasadnienie: Przekazanie raportu w ciągu 3 dni jest możliwy, natomiast przekazanie jego w takim terminie może być zbyt krótkie aby Zarządy mogły się z nimi zapoznać. Rekomendowałbym 7 dni.	Uwaga nieuwzględniona Obowiązek przekazania sprawozdania w postaci elektronicznej w terminie 3 dni roboczych odnosi się do kopii sprawozdania, a nie oryginału. Oryginał w dalszym ciągu pozostaje w podmiocie. Jednocześnie takie sprawozdanie jest już zatwierdzone (podpisane przez audytora). Oznacza to, że nabrało ono moc urzędową i wnioski pochodzące z tego sprawozdania powinny być realizowane. Tym samym zakreslenie 3 dniowego terminu na przekazanie takiego sprawozdania jest w ocenie projektodawcy terminem wystarczającym, gdyż czynność ta sprowadza się do czynności technicznej.
19.	Polskie Towarzystwo Informatyczne	Art. 15	W proponowanym brzmieniu art. 15 pkt a) ust.1zmienianej ustawy nakłada się obowiązek przeprowadzania regularnego audytu (co 2 lata) zarówno na podmioty kluczowe jak i podmioty ważne, co wykracza poza wytyczne dyrektywy NIS 2 która nakłada obowiązek wykonywania takich (regularnych) audytów jedynie na podmioty kluczowe. Zważywszy na oszacowaną obecnie liczbę podmiotów kluczowych i ważnych (ok. 38 tys.) wykonanie tego obowiązku przez oba typy wskazanych podmiotów jest wątpliwe. Proponuje się sformułowanie: <i>Podmiot kluczowy ma obowiązek zapewnić przeprowadzenie, na własny koszt, co najmniej raz na 2 lata, audytu bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi, zwanego dalej „audytem”</i> .	Uwaga uwzględniona
20.	Polskie Towarzystwo Informatyczne	Art. 15	W art. 15 ust. 2 pkt 2 podpunkt b) i c) zmienianej ustawy pozostawiono możliwość wykonywania audytów przez osoby nie posiadające certyfikatów uprawniających do wykonywania audytów. Dotychczasowa praktyka dowiodła, że często osoby te nie potrafią należycie ocenić bezpieczeństwa ocenianego podmiotu. Jako minimalny wymóg proponuje się w miejsce podpunktów b) i c) wstawić punkt b) <i>co najmniej trzyletnią praktykę w zakresie audytu bezpieczeństwa uzyskaną po otrzymaniu certyfikatu audytora wewnętrznego w zakresie normy PN-EN ISO/IEC 27001</i> .	Uwaga nieuwzględniona Uwzględnienie uwagi i obniżenie rangi audytora z wiodącego na wewnętrzny mogłoby skutkować obniżeniem jakości przeprowadzonego audytu. Rozporządzenie wykonawcze wskazuje wprost audytora wiodącego, a nie wewnętrznego.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

21.	KGHM Polska Miedź/ Związek Pracodawców Polska Miedź	Art. 15	Art. 1 pkt 20 ustawy zmieniającej, w zakresie art. 15 ust. 1b - Rekomenduje się doprecyzowanie sformułowania, zgodnie z którym nakazanie zlecenia audytu następuje jedynie w sytuacji, gdy podmiot kluczowy lub podmiot ważny nie daje należytej gwarancji wykonania audytu w terminie określonym w ustępie 1. Alternatywnie proponuje się jednoznacznie wskazanie katalogu przesłanek uzasadniających nakazanie takiego dodatkowego działania. Doprecyzowanie miałooby na celu wykluczenie interpretacji, zgodnie z którą organ właściwy ds. cyberbezpieczeństwa może nakazać przeprowadzenie innych dodatkowych audytów we wskazanym okresie referencyjnym.	Uwaga nieuwzględniona Dodatkowe audyty we wskazanym okresie referencyjnym są uprawnieniem nadzorczym organu właściwego do spraw cyberbezpieczeństwa. Takie uprawnienie nadzorcze wynika bezpośrednio z dyrektywy NIS 2.
22.	KGHM Polska Miedź S.A.	Art. 15 ust. 1b	Rekomenduje się doprecyzowanie sformułowania, zgodnie z którym nakazanie zlecenia audytu następuje jedynie w sytuacji, gdy podmiot kluczowy lub podmiot ważny nie daje należytej gwarancji wykonania audytu w terminie określonym w ust. 1. Alternatywnie proponuje się jednoznacznie wskazanie katalogu przesłanek uzasadniających nakazanie takiego dodatkowego działania. Adekwatnie do treści uwagi Doprecyzowanie miałooby na celu wykluczenie interpretacji, zgodnie z którą organ właściwy ds. cyberbezpieczeństwa może nakazać przeprowadzenie innych dodatkowych audytów we wskazanym okresie referencyjnym.	Uwaga częściowo uwzględniona Przepis zostanie doprecyzowany – organ będzie mógł nakazać audyt ad hoc w przypadku wystąpienia incydentu poważnego albo innego naruszenia wykonywania przepisów ustawy.
23.	PIPC	Art. 1 pkt 20 ustawy zmieniającej, w zakresie art. 15 ust. 1b	Rekomendujemy doprecyzowanie sformułowania, zgodnie z którym nakazanie zlecenia audytu następuje jedynie w sytuacji, gdy podmiot kluczowy lub podmiot ważny nie daje należytej gwarancji wykonania audytu w terminie określonym w ust. 1. Alternatywnie proponujemy jednoznaczne wskazanie katalogu przesłanek uzasadniających nakazanie takiego dodatkowego działania. Adekwatnie do treści uwagi Doprecyzowanie miałooby na celu wykluczenie interpretacji, zgodnie z którą organ właściwy ds. cyberbezpieczeństwa może nakazać przeprowadzenie innych dodatkowych audytów we wskazanym okresie referencyjnym.	Uwaga częściowo uwzględniona Przepis zostanie doprecyzowany – organ będzie mógł nakazać audyt ad hoc w przypadku wystąpienia incydentu poważnego albo innego naruszenia wykonywania przepisów ustawy.
24.	Związek Pracodawców Polska Miedź	Art. 1 pkt 20 ustawy zmieniającej, w zakresie art. 15 ust. 1b	Rekomenduje się doprecyzowanie sformułowania, zgodnie z którym nakazanie zlecenia audytu następuje jedynie w sytuacji, gdy podmiot kluczowy lub podmiot ważny nie daje należytej gwarancji wykonania audytu w terminie określonym w ust. 1. Alternatywnie proponuje się jednoznacznie wskazanie katalogu przesłanek uzasadniających nakazanie takiego dodatkowego działania. Adekwatnie do treści uwagi Doprecyzowanie miałooby na celu wykluczenie interpretacji, zgodnie z którą organ właściwy ds. cyberbezpieczeństwa może nakazać przeprowadzenie innych dodatkowych audytów we wskazanym okresie referencyjnym.	Uwaga częściowo uwzględniona Przepis zostanie doprecyzowany – organ będzie mógł nakazać audyt ad hoc w przypadku wystąpienia incydentu poważnego albo innego naruszenia wykonywania przepisów ustawy.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

25.	PERN SA	Art. 15	Konieczne doprecyzowanie: czy audyt systemu informacyjnego odnosi się do audytu zgodności z Ustawą o Krajowym Systemie Cyberbezpieczeństwa, Audyt zgodności z normą ISO 27001, lub audyt w formie przeprowadzonych pentestów.	Uwaga uwzględniona Audyt zgodności z ustawą. Uzasadnienie zostanie doprecyzowane w tym zakresie.
26.	PGE SA	Art. 15	Proponujemy dodanie w ustawie przepisu, który wskazywałby, że jeżeli podmiot posiada certyfikowany SZBI zgodnie z ISO27001 i SZCD zgodnie z ISO22301 dla całości działalności podmiotu, to audyt certyfikacyjny jest wystarczający dla zapewnienia zgodności. Zapis taki z jednej strony rozwinie rynek usług certyfikacyjnych, a z drugiej strony ograniczy obciążenia audytowe podmiotów certyfikujących SZBI i SZCD. Dodanie nowego ustępu w art. 15 w brzmieniu: <i>„Wymagania określone w ust. 1 uznaje się za spełnione, gdy podmiot kluczowy lub podmiot ważny przedstawia certyfikat zgodności Systemu Zarządzania Bezpieczeństwem Informacji z ISO/IEC 27001 oraz certyfikat zgodności Systemu Zarządzania Ciągłością Działania z ISO 22301, przy czym System Zarządzania Bezpieczeństwem Informacji oraz System Zarządzania Ciągłością Działania muszą obejmować swoim zakresem całą działalność podmiotu”</i>	Wyjaśnienie uwagi Podobny przepis wzbudził wątpliwości (pomimo wyjaśnienia w uzasadnieniu) i był interpretowany jako obowiązek wdrożenia konkretnych norm. Natomiast nie jest wykluczone, że certyfikowany SZBI na ISO 27001 oraz SZCD na ISO 22301 obejmie wymagania ustawowe.
27.	PGE SA	Art. 15 ust. 6	W związku ze zmianą pojęć stosowanych w ustawie, konieczne jest przeredagowanie art. 15 ust. 6 ustawy. Należy zastąpić pojęcie <i>operatora usługi kluczowej</i> oraz pojęcie <i>usługi kluczowej</i> na pojęcia podmiotu kluczowego lub podmiotu ważnego i pojęcie usługi świadczonej przez podmiot kluczowy lub podmiot ważny. ~~<i>Operator usługi kluczowej</i>~~ Podmiot kluczowy lub podmiot ważny, u którego w danym roku w stosunku do systemu informacyjnego wykorzystywanego do świadczenia usługi ~~kluczowej~~ przez podmiot kluczowy lub podmiot ważny został przeprowadzony przez osoby spełniające warunki określone w ust. 2 pkt 2 audyt wewnętrzny w zakresie bezpieczeństwa informacji, o którym mowa w przepisach wydanych na podstawie art. 18 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, nie ma obowiązku przeprowadzania audytu przez 2 lata. Istotne jest także zweryfikowanie całości ustawy, aby zachować spójność pojęciową aktu prawnego po wejściu w życie zmian przewidzianych projektem.	Uwaga uwzględniona
28.	Polska Wytwórnia Papierów Wartościowych	Art. 15	Uwaga do art. 1 pkt 20 projektu ustawy (art. 15 ust. 1 ustawy zmienianej). Polska Wytwórnia Papierów Wartościowych S.A. proponuje nadanie przepisowi art. 8a zawartemu w art. 1 pkt 13 projektu, następującego brzmienia: <i>„1. Podmiot kluczowy lub podmiot ważny ma obowiązek zapewnić przeprowadzenie, na własny koszt, audytu bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi, zwanego dalej „audytem”. Audyt przeprowadza się cyklicznie, z częstotliwością ustaloną w wyniku szacowanego ryzyka wystąpienia incydentu, jednak nie rzadziej niż co 3 lata.”.</i> Uzasadnienie: Polska Wytwórnia Papierów Wartościowych S.A. proponuje rozwiązanie, którego celem jest, po pierwsze, zwiększenie adekwatności działań podmiotów obowiązanych, poprzez wymóg przyjęcia	Uwaga częściowo uwzględniona Wydłużony został okres pomiędzy przeprowadzaniem audytów do 3 lat. Jednocześnie obecne brzmienie wskazuje, że audyt przeprowadzany powinien być co najmniej raz na 3 lata. Nie wyklucza to zatem przeprowadzania audytów częściej.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

			częstotliwości przeprowadzania audytu w zależności od stopnia szacowanego ryzyka wystąpienia incydentu dla danego systemu informacyjnego, po drugie, zachowanie okresu, w ramach którego, nie mniej jednak, obligatoryjne będzie przeprowadzenie takiego audytu, z jednoczesnym jego wydłużeniem z dwóch do trzech lat. Pozwoli to wyodrębnić te elementy bezpieczeństwa systemu informacyjnego, które wymagają częstszych audytów, ze względu na związane z nimi ryzyka, a jednocześnie pozostawi pewien standard dla audytów wszystkich elementów systemu bezpieczeństwa.	
29.	Osoba fizyczna	Art. 15	Zastosowano zapis dotyczący „audytu bezpieczeństwa systemu informacyjnego”, co wobec wprowadzonych zapisów wskazujących na obowiązek wdrożenia systemu zarządzania bezpieczeństwem informacji – w aktualnej wersji ustawy – w systemie informacyjnym, w noweli ustawy uKSC2 – w procesach, budzi wątpliwości co do realnych intencji. Proponuję dokonać weryfikacji i przyjąć spójne i konsekwentne podejście, co do podstawowego przedmiotu uKSC2	Uwaga uwzględniona Przeredagowano przepis wskazując system informacyjny wykorzystywany w procesie świadczenia usługi.
30.	PIKE i Mediakom	Art. 15	Obowiązkowy cykliczny audyt bezpieczeństwa systemu informacyjnego dla podmiotów ważnych nie występuje w dyrektywie NIS2 ani w przypadku podmiotów kluczowych (art. 32 ust. 2 pkt 2 oraz ust. 2 akapit drugi dyrektywy NIS2), ani podmiotów ważnych (art. 33 ust. 1 i 2 dyrektywy NIS2). Zgodnie z art. 32 ust. 2 pkt 2 dyrektywy NIS2, to właściwe organy powinny być uprawnione do objęcia podmiotu kluczowego regularnymi ukierunkowanymi audytami bezpieczeństwa. Wprowadzenie ogólnego obowiązku prowadzenia cyklicznych audytów bezpieczeństwa stanowi nadregulację. Jest to zaprzeczenie zasady proporcjonalności, ponieważ nie w przypadku każdego podmiotu kluczowego i ważnego będzie istniała potrzeba przeprowadzania takich audytów cyklicznie. Ponadto, zgodnie z art. 32 ust. 2 akapit drugi dyrektywy NIS2 „Ukierunkowane audyty bezpieczeństwa, o których mowa w akapicie pierwszym lit. b), opierają się na oszacowaniach ryzyka przeprowadzonych przez właściwy organ lub badany podmiot bądź na innych dostępnych informacjach dotyczących ryzyka”. Zatem regularne audyty bezpieczeństwa powinny być audytami ukierunkowanymi, a nie audytami obejmującymi za każdym razem cały system informacyjny wykorzystywany do świadczenia usługi. Ponadto, należy zaznaczyć, że w projekcie ustawy usunięto faktyczne różnice pomiędzy obrazem kontroli działalności podmiotów kluczowych i ważnych. W praktyce w projekcie ustawy istnieją tylko dwie różnice pomiędzy podmiotami kluczowymi i ważnymi: przesłanki wszczęcia kontroli oraz maksymalny wymiar kary. W pozostałym zakresie rozróżnienie na podmioty kluczowe i ważne nie ma praktycznego znaczenia. Obrazuje to skalę nadregulacji w przypadku projektu ustawy Art. 15. 1. <u>Organ właściwy do spraw bezpieczeństwa może nałożyć na ~~P~~podmiot kluczowy w drodze decyzji lub podmiot ważny ma</u> obowiązek ~~zapewnić~~ przeprowadzenia, na własny koszt, ~~ee~~ <u>najmniej</u> raz na <u>2-3</u> lata <u>lub rządzić</u>, audytu bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi, zwanego dalej „audytem”, <u>jeżeli przemawia za tym</u>	Uwaga częściowo uwzględniona Uwaga została uwzględniona w zakresie wyłączenia spod regularnych audytów podmiotów ważnych oraz wydłużenia regularnych audytów dla podmiotów kluczowych do 3 lat. W pozostałym zakresie należy wskazać, że obowiązek przeprowadzania audytu funkcjonuje na podstawie już obecnie obowiązującej ustawy. Jednocześnie państwa członkowskie mogą podejmować dalej idące środki niż przewiduje dyrektywa NIS2, jeżeli środki te są zgodne z celem dyrektywy. Związane jest to z harmonizacją minimalną. Ponadto wprowadzenie regulacji, że podmiot nie naruszył terminu jeśli zachował należyłą staranność w toku aktywnego poszukiwania audytora stanowiłoby pole do naruszeń i obejścia przepisów prawa. Ponadto stanowiłoby niezgodność z dyrektywą NIS2.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

			<u>charakter i częstotliwość występowania cyberzagrożeń w sektorze, w którym podmiot ten prowadzi działalność. Zakres audytu organ właściwy do spraw cyberbezpieczeństwa określa na podstawie wyników oszacowania ryzyka dla podmiotu kluczowego, wykonanego przez ten podmiot lub przez organ lub innych dostępnych informacjach dotyczących ryzyka.</u> <u>1a. Uznaje się, że podmiot kluczowy nie naruszył terminu przeprowadzenia audytu, o którym mowa w ust. 1, jeżeli do przeprowadzenia audytu dojdzie w terminie późniejszym, lecz podmiot kluczowy wykaże, że zachował należytą staranność w toku aktywnego poszukiwania audytora, spełniającego przesłanki określonego w art. 15 ust. 2-3.</u>	
31.	PIKE i Mediakom	Art. 15	Wydaje się, że art. 15 ust. 1b dotyczy audytu, o którym mowa w art. 32 ust. 2 lit. c i art. 33 ust. 2 lit. b dyrektywy NIS2. Niezbędne wydaje się określenie realistycznego terminu na przeprowadzenie takiego audytu. PIKE wnosi nadto o powstrzymanie się od nadregulacji i o wierne wdrożenie ww. przepisów dyrektywy NIS2. Art. 15 [...] 1b. Organ właściwy do spraw cyberbezpieczeństwa może nakazać, w drodze decyzji: <u>1) podmiotowi kluczowemu, przeprowadzenie audytu, o którym mowa w ust. 1, doraźnie i w uzasadnionych przypadkach w związku z wystąpieniem incydentu poważnego lub z naruszeniem przez podmiot kluczowy obowiązków określonych w ustawie, wraz z określeniem adekwatnego terminu przekazania sprawozdania z przeprowadzonego audytu, nie krótszego jednak niż 3 miesiące od dnia doręczenia podmiotowi kluczowemu decyzji ostatecznej.</u> <u>2) podmiotowi ważnemu przeprowadzenie audytu, o którym mowa w ust. 1, wraz z określeniem adekwatnego terminu przekazania sprawozdania z przeprowadzonego audytu, nie krótszego jednak niż 3 miesiące od dnia doręczenia podmiotowi kluczowemu decyzji ostatecznej, przy czym zakres audytu organ właściwy do spraw cyberbezpieczeństwa określa na podstawie wyników oszacowania ryzyka dla podmiotu ważnego, wykonanego przez ten podmiot lub przez organ lub innych dostępnych informacjach dotyczących ryzyka.</u> <u>1b¹. Uznaje się, że podmiot kluczowy i podmiot ważny nie naruszył terminu przeprowadzenia audytu, o którym mowa w ust. 1b, jeżeli do przeprowadzenia audytu dojdzie w terminie późniejszym niż określony zgodnie z ust. 1b, lecz podmiot ten wykaże, że zachował należytą staranność w toku aktywnego poszukiwania audytora, spełniającego przesłanki określonego w art. 15 ust. 2-3.</u>	Uwaga nieuwzględniona Wskazać należy, że organ właściwy do spraw cyberbezpieczeństwa zlecając w ramach czynności nadzorczych przeprowadzenie audytu określa termin jego przeprowadzenia. Wprowadzenie regulacji, że podmiot nie naruszył terminu jeśli zachował należytą staranność w toku aktywnego poszukiwania audytora stanowiłoby pole do naruszeń i obejścia przepisów prawa. Ponadto stanowiłoby niezgodność z dyrektywą NIS2. W pozostałym zakresie należy zauważyć, że państwa członkowskie mają swobodę we wdrażeniu dalej idących środków jeśli pozostają one w zgodności z celem dyrektywy.
32.	Urząd Marszałkowski Województwa Mazowieckiego (Wojewódzka Rada Dialogu Społecznego w	Art. 15	Audyty w stosunku do podmiotów ważnych w sprzeczności z dyrektywą NIS 2, która nie przewiduje regularnych audytów w stosunku do tych podmiotów, a jedynie do podmiotów ważnych. Postulat wyeliminowania konieczności przeprowadzenia audytów dla podmiotów ważnych.	Uwaga uwzględniona Zniesiono wymóg regularnego audytowania w stosunku do podmiotów ważnych.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

	województwie mazowieckim)			
33.	Urząd Miasta Gliwice	Art. 15 w zw. z art. 8	Zgodnie z art. 1 ust. 20) pkt a) projektu w art. 15 ust. 1 ustawy o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2023 r. poz. 913 i 1703) otrzymuje brzmienie: „1. Podmiot kluczowy lub podmiot ważny ma obowiązek zapewnić przeprowadzenie, na własny koszt, co najmniej raz na 2 lata, audytu bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi, zwanego dalej „audytem”.” Natomiast zgodnie z art. 1 ust. 12) projektu art. 8 ust. 2 ustawy o krajowym systemie cyberbezpieczeństwa otrzymuje brzmienie: "2. Wymagania, o których mowa w ust. 1, uznaje się za spełnione, gdy podmiot kluczowy i podmiot ważny zapewnia system zarządzania bezpieczeństwem informacji, z uwzględnieniem wymagań określonych w Polskiej Normie PN-EN ISO/IEC 27001 oraz PN-EN ISO/IEC 22301." Urząd Miejski w Gliwicach od 2015 r. utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zgodny z wymaganiami normy ISO/IEC 27001. System jest certyfikowany, aktualny certyfikat na zgodność z normą PN-EN ISO/IEC 27001:2017 jest ważny do 17 listopada 2024 r. W ramach nadzoru nad certyfikatem jednostka certyfikująca przeprowadza co roku audyt systemu zarządzania bezpieczeństwem informacji Urzędu. W związku z powyższym, proszę o wyjaśnienie czy przeprowadzenie audytu certyfikacyjnego SZBI na zgodność z normą ISO/IEC 27001 (oraz powiązanych audytów w ramach nadzoru nad certyfikatem) będzie tożsame z wyplenieniem obowiązku przeprowadzenia co najmniej raz na dwa lata audytu bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi? Wnoszę również o doprecyzowanie w tym zakresie zapisów art. 1 ust. 20 pkt. a) projektu ustawy.	Wyjaśnienie uwagi W dużej mierze certyfikat ISO 27001 wypełni wymogi ustawy. Kwestia ta zostanie szczegółowo rozpisana w uzasadnieniu.
34.	Polskie Stowarzyszenie Fotowoltaiki	Art. 15	Regularne audyty – NIS2 nie wprowadza obowiązków czasowych. Tymczasem Projekt przewiduje obowiązek przeprowadzenia audytu raz na dwa lata, bez względu na wcześniejszą ocenę ryzyka	Wyjaśnienie uwagi Określenie „regularne audyty” nakłada na państwa członkowskie obowiązek zapewnienia, że audyty te będą odbywały się co pewien – określony – czas. Pozostawienie nieostrego pojęcia „regularne” prowadziło do tego, że każdy podmiot mógłby uznać za regularny zupełnie inny czas. Tym samym prowadziło to do nieregularności, sprzeczności z dyrektywą oraz utrudnionym nadzorem i egzekwowaniem przepisów wobec podmiotów kluczowych. Miało to negatywny skutek na cały krajowy system cyberbezpieczeństwa.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

35.	APATOR SA	Art. 15	Art. 15 ust. 1 projektu – proponujemy, aby otrzymał brzmienie: Podmiot kluczowy lub podmiot ważny ma obowiązek zapewnić przeprowadzenie na własny koszt, co najmniej raz na 2 lata, audytu bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi, a także audytów bezpieczeństwa kluczowych dostawców produktów ICT i usług ICT mających kluczowe znaczenie z punktu widzenia bezpieczeństwa systemu informacyjnego podmiotu kluczowego lub podmiotu ważnego, zwanego dalej „audytem”. Uzasadnienie proponowanej zmiany: W naszej opinii, w celu rzetelnego i całościowego zweryfikowania prawdziwości twierdzeń dostawców usług, konieczne jest przeprowadzanie także w ich siedzibach lub miejscach prowadzenia działalności gospodarczej systematycznych audytów. Audyty powinny być przeprowadzane u producentów oprogramowania i dostawców, tak aby zminimalizować ryzyko nadużyć. Często bowiem producentem jest inny podmiot niż dostawca, który dodatkowo ma swoją siedzibę poza obszarem Unii Europejskiej, często w kraju, w którym standardy bezpieczeństwa zarządzania informacjami nie są znane lub stosowane.	Uwaga nieuwzględniona Taki obowiązek stanowi nieproporcjonalne obciążenie podmiotów kluczowych i podmiotów ważnych. Niemożliwe byłoby przeprowadzenie przez podmiot kluczowy, na własny koszt, audytu szbi dostawcy systemu operacyjnego. Ponadto zakres podmiotowy ustawy nie obejmuje obowiązków materialnych po stronie dostawców produktów/usług ICT.
36.	KIKE	Art. 15	Projekt właściwie nie różnicuje obowiązków podmiotów ważnych wobec podmiotów kluczowych. Jest to nie tylko sprzeczne z samą dyrektywą NIS 2 (która nie wymaga prowadzenia audytów przez podmioty ważne), ale z art. 67 i 68 Prawa przedsiębiorców. Izba postuluje przeanalizowanie Projektu pod kątem zmniejszenia obciążeń wobec podmiotów ważnych w stosunku do obowiązków nałożonych na podmioty kluczowe. Przede wszystkim należy usunąć: - obowiązek prowadzenia audytów z art. 15 uKSC przez podmioty ważne jako nieproporcjonalnego oraz stanowiącego przekroczenie dyrektywy NIS 2. Izba wskazuje, że nałożenie na mikro i małych przedsiębiorców telekomunikacyjnych obowiązek prowadzenia kosztownego audytu bezpieczeństwa (w skali krajowej) jest nieproporcjonalny i nieadekwatny. Wskazuję, że sam przepis art. 32 dyrektywy NIS 2 reguluje elastycznie obowiązek audytu (a więc nie na mocy ustawy, ale w indywidualnych sytuacjach) i to w dodatku tylko wobec podmiotów kluczowych a nie ważnych.	Uwaga uwzględniona Przepis został przeredagowany w ten sposób, że audytami regularnymi objęte będą wyłącznie podmioty kluczowe. Wobec podmiotów ważnych zastosowanie znajdą audyty zlecone w ramach nadzoru następczego.
37.	Ogólnopolska Federacja Przedsiębiorców i Pracodawców – przedsiębiorcy.pl	Art. 15	Polski projekt ustawy o KSC zaciera rozróżnienie podmiotów na kluczowe i ważne, gdyż przewiduje dla tychże podmiotów takie same obowiązki. Projektodawca krajowy nakłada na podmioty kluczowe i ważne obowiązek przeprowadzenia na ich koszt audytu bezpieczeństwa (art. 15 ust. 1 projektu ustawy o KSC) podczas, gdy w dotychczasowej wersji ustawy obowiązek przeprowadzenia audytu bezpieczeństwa dotyczył systemu informacyjnego wykorzystywanego jedynie do świadczenia usługi kluczowej.	Wyjaśnienie uwagi Przepis został zmieniony – obowiązkiem objęte zostaną wyłącznie podmioty kluczowe.
38.	Pracodawcy RP	Art. 15	Kolejną kwestią jest znacząco rozbudowany obszar audytów na gruncie NIS2, co będzie stanowić wyzwanie organizacyjne. Zgodnie z proponowaną treścią nowelizacji, podmioty objęte regulacją będą musiały regularnie przeprowadzać audyty bezpieczeństwa systemów informatycznych — nie rzadziej niż raz na 2	Wyjaśnienie uwagi Regularne audyty są niezbędne dla zapewnienia wysokiego poziomu bezpieczeństwa. Jednocześnie są one

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

			lata. Audyt ma być przeprowadzany na własny koszt podmiotu objętego audytem. To wymaga znaczących nakładów finansowych oraz zasobów ludzkich, aby zapewnić odpowiednią akredytację audytorów oraz przeprowadzenie badania zgodnie z wytycznymi i standardami dyrektywy NIS2. Ostatecznie, aby pokryć wydatki wynikające z nowych obowiązków, podmioty objęte regulacją w pewnym zakresie przeniosą koszty na konsumentów. Dodatkowo, konieczność przekazywania sprawozdań audytowych do organu odpowiedzialnego za cyberbezpieczeństwo w ciągu terminu 3 dni roboczych również przyczyni się do konieczności zwiększenia nakładów na bezpieczeństwo. Jednocześnie Nowelizacja wprowadzi możliwość przeprowadzania audytów ad hoc przez organy odpowiedzialne za cyberbezpieczeństwo. W konsekwencji istnieje ryzyko, że podmioty rynkowe zamiast skupiać się na rozwoju własnych produktów i usług — będą zmuszone do wydatkowania znaczącej części swojego budżetu na spełnianie nadmiernych wymogów stawianych przez regulację.	nakładane przez dyrektywę NIS 2 w przypadku podmiotów kluczowych. Zapewnienie regularności tych audytów jest konieczne do prawidłowego wdrożenia dyrektywy. Jednocześnie okres został wydłużony z 2 lat do 3. Przepis został również zmieniony w zakresie podmiotów ważnych – nie będą one już objęte regularnymi audytami, a wyłącznie audytami ad hoc przy nadzorze ex post. W przedmiocie przekazywania sprawozdań audytowych do organu w ciągu 3 dni roboczych należy wskazać, że jest to przekazywanie wyłącznie kopii, a wnioski z audytu należy realizować od dnia jego zakończenia.
39.	Stowarzyszenie Bezpieczeństwo Informacji w Telekomunikacji	Art. 15	Ustawa w art. 15 nakłada na podmioty kluczowe i podmioty ważne obowiązek poddania się audytowi bezpieczeństwa systemu informatycznego. Pierwszy taki audyt należy przeprowadzić w ciągu 12 miesięcy licząc od dnia uznania za podmiot kluczowy lub podmiot ważny. Następne audyty należy przeprowadzać co 2 lata. Audyt powinno przeprowadzać dwóch audytorów posiadających odpowiednie certyfikaty. Oznacza to, że w jednym czasie będzie zapotrzebowanie na kilkudziesięciu audytorów certyfikowanych. Należy spodziewać się, że w tym czasie podmiotowi kluczowemu i podmiotowi ważnemu bardzo trudno znaleźć audytorów posiadających właściwe uprawnienia, a ich usługi prawdopodobnie znacznie podrożeją. Dlatego proponuje się, aby dla podmiotów ważnych zwiększyć termin pierwszego audytu do 18 miesięcy natomiast terminy cyklicznych audytów zwiększyć do trzech lat.	Uwaga uwzględniona Zrezygnowano z obejmowania regularnymi audytami podmiotów ważnych, a w stosunku do podmiotów kluczowych audyty te będą przeprowadzane co 3 lata.
40.	Polska Izba Informatyki i Telekomunikacji	Art. 15	W zakresie decyzji dot. nakazu przeprowadzenia audytu należy doprecyzować w jakim trybie będzie wydawana decyzja. Koniecznym jest uzupełnienie przepisu o minimalny okres od dnia wydania decyzji na uruchomienie audytu, żeby organ nie wydał decyzji w poniedziałek z obowiązkiem przedstawienia sprawozdania w piątek.	Uwaga nieuwzględniona Przepis został doprecyzowany o warunki zlecenia takiego audytu. Są one związane np. z wystąpieniem incydentu poważnego. Organ może także określić zakres takiego audytu. Tym samym wprowadzenie sztywnego minimalnego okresu na przeprowadzenie audytu byłoby niecelowe i trudne do realizacji z uwagi na różny powód zlecenia audytu, różne potrzeby, pilność

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

				jego przeprowadzenia oraz zróżnicowany zakres.
41.	Konfederacja Lewiatan	Art. 15	Niekonstytucyjna forma komunikatu dla harmonogramów złożenia wniosków o wpis do wykazu podmiotów kluczowych i ważnych Jednostka redakcyjna: art. 15 w zw. z art. 14 ust. 2 projektu KSC Jednostka redakcyjna NIS2: art. 3 ust. 3 Uwaga: W art. 15 projektu KSC przewiduje się określenie harmonogramu złożenia wniosków o wpis do wykazu podmiotów kluczowych i podmiotów ważnych oraz rozpoczęcia korzystania przez te podmioty z systemu S46 w formie komunikatu. Niemniej, regulowanie terminu na realizację obowiązku ustawowego powinno mieć formę rozporządzenia, a nie komunikatu, który nie stanowi źródła prawa. Komunikat nie może bowiem decydować o obowiązkach obywateli i przedsiębiorców. Zgodnie z art. 87 ust. 1 Konstytucji RP, źródłami powszechnie obowiązującego prawa Rzeczypospolitej Polskiej są: Konstytucja, ustawy, ratyfikowane umowy międzynarodowe oraz rozporządzenia. W tym kontekście warto przywołać orzeczenie Trybunału Konstytucyjnego z 9 maja 2023 r. (sygn. akt SK 81/19), w którym stwierdzono niezgodność z ustawą zasadniczą komunikatów określających Program Szczepień Ochronnych na dany rok. ¹ . Komunikaty nie mogą bowiem kształtować praw jednostek. Do takiego kształtowania praw dojdzie w sytuacji, gdy określone daty graniczne wpisu do wykazu podmiotów kluczowych i podmiotów ważnych będą regulowane właśnie w formie komunikatu, a nie rozporządzenia. Konieczne jest zatem ograniczenie i doprecyzowanie przepisu art. 15 projektu KSC, aby zapewnić zgodność z konstytucyjnymi wymogami dotyczącymi źródeł powszechnie obowiązującego prawa. ² .	Wyjaśnienie uwagi Obowiązek wynika z przepisów ustawy. Komunikat stanowi jedynie czynność techniczną wskazującą, że można rozpocząć korzystanie z systemu. Dodatkowo komunikat ten ma charakter generalny (wobec wielu podmiotów określonych rodzajowo) i konkretny (dotyczy konkretnej sytuacji wpisania do wykazu po wejściu w życie ustawy). Przepisy prawa m. in. rozporządzenia mają charakter generalny i abstrakcyjny.
42.	Osoba fizyczna	Art. 15	W projekcie ustawy powinno być również napisane czy że podmiot wpisany obecnie do rejestru Operatorów Usługi Kluczowej, który ma już wykonany zerowy Audyt Bezpieczeństwa nie będzie musiał go wykonywać ponownie po wejściu w życie nowelizacji UKSC (12 miesięcy od wejścia w życie), tylko zachowywać dotychczasową ciągłość terminów.	Uwaga uwzględniona Kwestia zostanie uregulowana w przepisach dostosowujących.
43.	Związek Telewizji Kablowych Izba Gospodarcza	Art. 15	Na wstępie należy podnieść, że w dotychczasowej wersji art. 15 ustawy o KSC przewidziany jest obowiązek przeprowadzenia co dwa lata audytu bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej, ale w przedmiotowym przepisie nie przewidziano ponoszenia kosztów przez podmiot świadczący usługę kluczową.	Uwaga nieuwzględniona Dyrektywa NIS2 przewiduje tutaj możliwość, a nie obligatoryjność refundacji kosztów audytu przez państwo. Obecnie jest

¹⁾ Zgodnie z tym wyrokiem: Art. 17 ust. 11 ustawy z dnia 5 grudnia 2008 r. o zapobieganiu oraz zwalczaniu zakażeń i chorób zakaźnych u ludzi (Dz.U. z 2022 r. poz. 1657, ze zm.) w związku z § 5 rozporządzenia Ministra Zdrowia z dnia 18 sierpnia 2011 r. w sprawie obowiązkowych szczepień ochronnych (Dz.U. z 2022 r. poz. 2172) w zakresie, w jakim termin wymagalności obowiązkowych szczepień ochronnych, jak i liczba dawek poszczególnych obowiązkowych szczepień ochronnych, określone są w Programie Szczepień Ochronnych na dany rok, ogłaszanym przez Głównego Inspektora Sanitarnego w formie komunikatu, a nie przez ministra właściwego do spraw zdrowia, w drodze rozporządzenia, jest niezgodny z art. 47 w związku z art. 31 ust. 3 w związku z art. 87 Konstytucji Rzeczypospolitej Polskiej.

²⁾ Vide ust. 4 art. 15, zgodnie z którym: *W harmonogramie, o którym mowa w ust. 3, wskazuje się terminy dokonywania czynności przez poszczególne rodzaje podmiotów kluczowych i podmiotów ważnych.*

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

			Tymczasem w proponowanej nowej wersji art. 15 ust. 1 ustawy o KSC projektodawca wprost przewiduje obowiązek zapewnienia przez podmiot ważny lub kluczowy co dwa lata przeprowadzenia audytu bezpieczeństwa systemu informacyjnego na koszt podmiotu ważnego lub kluczowego, co już samo w sobie stanowi pogorszenie sytuacji finansowej obu tych grup podmiotów w zestawieniu z dotychczasową regulacją tegoż przepisu. W proponowanej regulacji projektodawca zupełnie pomija, iż prawodawca unijny przewiduje co prawda, że podmiot kluczowy lub podmiot ważny zapewnia przeprowadzenie rzeczonoego audytu na koszt podmiotu kluczowego lub ważnego, ale zarazem dopuszcza odstępstwo od ponoszenia kosztów przeprowadzanego audytu przez podmiot kluczowy lub ważny odniesione do wystąpienia należycie uzasadnionych przypadków, gdy organ właściwy do spraw cyberbezpieczeństwa postanowi inaczej, a mianowicie o nieponoszeniu tych kosztów przez podmiot kluczowy lub podmiot ważny (art. 32 ust. 2 zdanie ostatnie dyrektywy NIS 2, art. 33 ust. 2 zdanie ostatnie dyrektywy NIS 2). Pojawia się zatem uzasadnione pytanie, dlaczego to projektodawca pominął korzystną dla podmiotów poddanych audytowi, a dopuszczoną przez prawodawcę unijnego opcję odstąpienia od wymogu ponoszenia kosztów przeprowadzenia audytu bezpieczeństwa systemu informacyjnego przez podmiot kluczowy lub podmiot ważny w oparciu o odmienną decyzję organu właściwego do spraw cyberbezpieczeństwa w ściśle skonkretyzowanej sytuacji. W zaistniałej sytuacji proponujemy wprowadzenie zmiany art. 1 pkt. 20 lit. a projektu ustawy zmieniającej ustawę o KSC zasadzającej się w nadaniu proponowanej regulacji art. 15 ust. 1 ustawy o KSC oznaczenia zdania pierwszego oraz dodania zdania 2 w brzmieniu „<i>Organ właściwy do spraw cyberbezpieczeństwa w należycie uzasadnionych przypadkach może postanowić o nieponoszeniu przez podmiot kluczowy lub podmiot ważny kosztów przeprowadzenia audytu bezpieczeństwa systemu informacyjnego.</i>”.	to niemożliwe z uwagi na sytuację budżetową.
44.	Polska Izba Informatyki i Telekomunikacji	Art. 16	Z uwagi na objęcie przepisami bardzo szerokiego katalogu podmiotów, także niebędących dotychczas podmiotami krajowego systemu cyberbezpieczeństwa postulujemy wydłużenie terminów na implementację do 18 miesięcy na wdrożenie obowiązków oraz 24 miesiące na przeprowadzenie pierwszego audytu. Proponujemy też wskazanie daty dokonania wpisu do wykazu jako daty rozpoczynającej bieg terminu na realizację wymagań. Jest to data pewna, która nie będzie rodziła wątpliwości na etapie ewentualnych kontroli realizacji obowiązków. Należy zaznaczyć, że obecne brzmienie projektowanego przepisu może spowodować, że okres audytu będzie dotyczyć okresu w którym podmiot nie miał obowiązku realizacji obowiązków w zakresie cyberbezpieczeństwa jako podmiot kluczowy lub ważny.	Uwaga uwzględniona Terminy na wdrożenie przepisów oraz przeprowadzenie audytów zostały wydłużone.
45.	Konfederacja Lewiatan	Art. 16	Realizacja obowiązków od dnia wpisu do wykazu Jednostka redakcyjna: art. 16 ust. 1 „art. 16 otrzymuje brzmienie: „Art. 16. 1. Podmiot kluczowy i podmiot ważny:	Uwaga częściowo uwzględniona Wykaz podmiotów kluczowych i podmiotów ważnych ma charakter deklaratoryjny. Zgodnie z dyrektywą NIS2

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

			1) realizuje obowiązki, o których mowa w niniejszym rozdziale, 2) w terminie 6 miesięcy, zapewnia przeprowadzenie audytu, o którym mowa w art. 15 ust. 1, po raz pierwszy w terminie 12 miesięcy – <u>od dnia dokonania wpisu do wykazu, o którym mowa w art. 7 ust. 1.</u> Z uwagi na objęcie przepisami bardzo szerokiego katalogu podmiotów, także niebędących dotychczas podmiotami krajowego systemu cyberbezpieczeństwa postulujemy wydłużenie terminów na implementację do 12 miesięcy na wdrożenie obowiązków oraz 24 miesiące na przeprowadzenie pierwszego audytu. Potencjalne podmioty kluczowe lub podmioty ważne nie są w stanie przewidzieć na etapie składania wniosku czy zostaną jako takie podmioty zidentyfikowane, a w przypadku zaniechania samorejestracji – czy nie zostaną wpisane do wykazu z urzędu. Również możliwość dokonania takiego wpisu w dowolnym czasie wymusza konieczność zmiany brzmienia powyższego przepisu. Proponujemy też wskazanie daty dokonania wpisu do wykazu jako daty rozpoczynającej bieg terminu na realizację wymagań. Jest to data pewna, która nie będzie rodziła wątpliwości na etapie ewentualnych kontroli realizacji obowiązków.	podmioty mają realizować obowiązki w zakresie Cyberbezpieczeństwa niezależnie od tego czy państwo członkowskie wdrożyło mechanizmy samoidentyfikacji czy nie. Potencjalnie byłoby ryzyko tego, że podmiot celowo nie wpisałby się do wykazu i przez nie musiałby realizować obowiązków z zakresu Cyberbezpieczeństwa. Przepis zostanie zmieniony – termin na pierwszy audyt wyniesie – 24 mies.
46.	Osoba fizyczna	Art. 16 (nowa propozycja brzmienia)	Art. 16. Sankcje za naruszenia: 1. Podmioty, które nie przestrzegają przepisów niniejszej ustawy, podlegają następującym sankcjom: 1) Kary finansowe do 5% rocznych przychodów lub budżetu podmiotu, w zależności od skali i powagi naruszenia. 2) Odpowiedzialność karna dla członków zarządu lub innych osób odpowiedzialnych za bezpieczeństwo cybernetyczne. 3) Zakazy działalności lub świadczenia usług do czasu pełnego wdrożenia zaleconych środków naprawczych. 4) Publiczne ostrzeżenia o naruszeniach oraz obowiązek naprawy szkód wyrządzonych przez incydent.	Wyjaśnienie uwagi Sankcje za naruszenia zostały przewidziane w rozdziale 14 ustawy i zostały odpowiednio zmodyfikowane w taki sposób, aby zapewniały właściwe wdrożenie dyrektywy NIS 2. Przewidują zarówno kary finansowe oparte na % obrotu jak i kary finansowe dla kierownika podmiotu. W pozostałym zakresie organy właściwe do spraw cyberbezpieczeństwa sprawują nadzór nad podmiotami kluczowymi i podmiotami ważnymi. W związku z tym propozycje określone w niniejszej uwadze zostały już przez projektodawcę przewidziane w projekcie.
47.	Fundacja Open Allies	Art. 16	Terminy realizacji obowiązków przez podmioty kluczowe oraz podmioty ważne ustalone na 6 miesięcy oraz obowiązek przeprowadzenia pierwszego audytu w terminie 12 miesięcy – od dnia spełnienia przesłanek uznania za podmiot kluczowy lub podmiot ważny (art. 16), są bardzo wymagające. Zwracamy się o przedłużenie obydwóch terminów o 6 miesięcy – odpowiednio do 12 i 18 miesięcy. Zwracamy się również o doprecyzowanie, czy audyt, o którym mowa w art. 16 pkt 2 powinien być rozpoczęty czy zakończony w terminie wskazanym w omawianym przepisie.	Uwaga częściowo uwzględniona Przepis zostanie zmieniony – termin na pierwszy audyt wyniesie – 24 mies. Audyt ma być zakończony w terminie.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

48.	Zakład Wodociągów i Kanalizacji sp. z o.o.	Art. 16	W projekcie ustawy powinno być również napisane czy że podmiot wpisany obecnie do rejestru Operatorów Usługi Kluczowej, który ma już wykonany zerowy Audyt Bezpieczeństwa nie będzie musiał go wykonywać ponownie po wejściu w życie nowelizacji UKSC (12 miesięcy od wejścia w życie), tylko zachowywać dotychczasową ciągłość terminów.	Uwaga uwzględniona Przepisy przejściowe zostały preredagowane.
49.	Krajowi Producenci Leków	Art. 16	art. 16 otrzymuje brzmienie: „Art. 16. 1. Podmiot kluczowy i podmiot ważny: 1) realizuje obowiązki, o których mowa w niniejszym rozdziale, w terminie 6 miesięcy, 2) zapewnia przeprowadzenie audytu, o którym mowa w art. 15 ust. 1, po raz pierwszy w terminie 12 miesięcy – od dnia dokonania wpisu do wykazu, o którym mowa w art. 7 ust. 1. Uzasadnienie Postulujemy urealnienie terminu na realizację obowiązków wynikających z ustawy. Dzień spełnienia przesłanek uznania za podmiot kluczowy lub podmiot ważny jest terminem niepewnym, niedookreślonym. Potencjalne podmioty kluczowe lub podmioty ważne nie są w stanie przewidzieć na etapie składania wniosku czy zostaną jako takie podmioty zidentyfikowane, a w przypadku zaniechania samorejestracji – czy nie zostaną wpisane do wykazu z urzędu. Również możliwość dokonania takiego wpisu w dowolnym czasie wymusza konieczność zmiany brzmienia powyższego przepisu. Wskazanie, iż termin realizacji obowiązków zaczyna swój bieg od dnia dokonania wpisu do wykazu podmiotów kluczowych lub podmiotów ważnych pozwoli usunąć niepewność w tym zakresie po stronie adresatów tej ustawy.	Uwaga uwzględniona Przepis zostanie zmieniony – termin na pierwszy audyt wyniesie – 24 mies.
50.	Krzysztof Rożko i Wspólnicy Kancelaria Prawna sp. k.	Art. 16	UWAGA ZGŁOSZONA W RAMACH ZGŁOSZENIA LOBBINGOWEGO Zważywszy, że art. 10 pkt 4) projektu ustawy wdrażającej DORA przewiduje dodanie art. 16a do uKSC, zwracamy uwagę, by w art. 1 pkt 22 projektu nowelizacji uKSC, który przewiduje dodanie rozdziału 3a, zaczynającego się od art. 16a, uwzględnione zostały stosowne zmiany w numeracji przepisów.	Uwaga uwzględniona Będziemy pracować na rzecz rozgraniczenia projektów.
51.	Polska Izba Gospodarki Odpadami	Art. 16	Art. 1 ust. 21) w zakresie zmiany Art. 16 ust. 1. Pkt 1) – Wdrożenie SZBI zgodnego z normą ISO27001 i wdrożenie normy 22301 ciągłość działania ISO 22301 nie jest możliwe w terminie 6 miesięcy. Postuluję zapis 12 m-cy dla podmiotów ważnych dla ISO 27001 i 18m-cy dla ISO 22301 ISO22301. Podmioty działające w branży gospodarki odpadami są nieprzygotowane ani osobowo, ani zasobowo do wdrożenia w 6 miesięcy planów ciągłości działania. W związku z tym zgłaszamy postulat o wydłużeniu terminów wdrożenia. ISO27001 w branży gospodarki odpadami dotychczas nie był wdrażany, z doświadczeń firm wspierających podmioty czy audytujących okres potrzebny na wdrożenie ISO27001 to 12m-cy.	Uwaga częściowo uwzględniona Przepis zostanie zmieniony – termin na pierwszy audyt wyniesie – 24 mies.
52.	Polska Organizacja	Art. 16.1. tiret	zmiana określenie rozpoczęcia biegu terminu na „od dnia ujawnienia w wykazie podmiotów kluczowych i ważnych, o którym mowa w Art.7. ust.1”;	Uwaga nieuwzględniona Wpis w wykazie ma charakter deklaratoryjny – nie można od niego

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

	Handlu i Dystrybucji			uzależniać realizację obowiązków ustawowych.
53.	PGE SA	Art. 16 ust. 1 pkt 2 ustawy	Przy pozostawieniu obecnego brzmienia art. 16 ust. 1 pkt 2, po 12 miesiącach od wejścia w życie ustawy, w krótkim okresie będzie miało miejsce znaczące nagromadzenie audytów wynikających z ustawy. Należy rozważyć wprowadzenie przepisów przejściowych, które np. rozłożą wymaganie audytu dla obecnych operatorów usług kluczowych, np. przez zachowanie cyklu 2 lat.	Uwaga uwzględniona Zostanie wprowadzony odpowiedni przepis przejściowy.
54.	TAURON Polska Energia S.A	Art. 16 ust. 1	„Art. 16. 1. Podmiot kluczowy i podmiot ważny: 1) realizuje obowiązki, o których mowa w niniejszym rozdziale, w terminie 6 miesięcy, 2) zapewnia przeprowadzenie audytu, o którym mowa w art. 15 ust. 1, po raz pierwszy w terminie 12 miesięcy – od dnia spełnienia przesłanek uznania za podmiot kluczowy lub podmiot ważny. ” Ze względu na to, że wdrożenie znowelizowanych przepisów w podmiotach kluczowych i ważnych, w szczególności tych które nie są obecnie operatorami usług kluczowych wymaga dużych zasobów i jest to bardzo złożone przedsięwzięcie, proponujemy zmianę terminów. Dodatkowo w celu zapewnienia przejrzystości i pewności co do warunku od którego wskazane terminy należy zachować proponujemy aby termin ten był zależny od momentu wpisania podmiotu na listę podmiotów ważnych i kluczowych o których mowa nowelizacji. Proponowane brzmienie uwzględniające powyższe: „Art. 16. 1. Podmiot kluczowy i podmiot ważny: 1) realizuje obowiązki, o których mowa w niniejszym rozdziale, w terminie 12 miesięcy, 2) zapewnia przeprowadzenie audytu, o którym mowa w art. 15 ust. 1, po raz pierwszy w terminie 18 miesięcy – od dnia otrzymania zaświadczenia o wpisie potwierdzającego spełnienie przesłanek uznania za podmiot kluczowy lub podmiot ważny. ”	Uwaga nieuwzględniona Wpis w wykazie ma charakter deklaratoryjny – nie można od niego uzależniać realizację obowiązków ustawowych. Uwaga częściowo uwzględniona Przepis zostanie zmieniony – termin na pierwszy audyt wyniesie – 24 mies.
55.	Polska Izba Informatyki i Telekomunikacji	Art. 16a	Projekt ustawy przewiduje dodanie do ustawy o krajowym systemie cyberbezpieczeństwa szeregu przepisów z nowymi wymogami dla rejestrów nazw domen najwyższego poziomu (TLD) i podmiotów świadczących usługi rejestracji nazw domen (nowy art. 16a i następne). Nowo dodawane przepisy w kilku miejscach posługują się pojęciem „abonenta nazwy domeny”, nie definiując tego pojęcia. Brak definicji wynika zapewne z tego, że Projektodawca uznał, że jest to pojęcie występujące w obrocie gospodarczym, zrozumiałe i z tego względu nie wymagające definiowania i takie podejście jest poniekąd zrozumiałe. Niemniej jednak zwracamy uwagę na potencjalny problem związany z tym, że projektowana ustawa zmienia ustawę o krajowym systemie cyberbezpieczeństwa m.in. w taki sposób, że elementem systemu stają się przedsiębiorcy telekomunikacyjni (przedsiębiorcy komunikacji elektronicznej), w tym dostawcy publicznie dostępnych usług telekomunikacyjnych, których klientami są „abonenci” w rozumieniu ustawy – Prawo telekomunikacyjne (a w przyszłości ustawy – Prawo komunikacji elektronicznej).	Uwaga uwzględniona Wprowadzona zostanie definicja abonenta nazwy domeny.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

			Brak w ustawie o krajowym systemie cyberbezpieczeństwa definicji „abonenta nazwy domeny” może skutkować nieuzasadnionymi próbami stosowania na potrzeby nowego rozdziału 3a UKSC definicji „abonenta” z Prawa telekomunikacyjnego (w przyszłości Prawa komunikacji elektronicznej). I choć ryzyko takich nieuzasadnionych interpretacji nie wydaje się wysokie, to aby je całkowicie wyeliminować warto rozważyć albo wprowadzenie do UKSC definicji „abonenta nazwy domeny”, albo posłużenie się w przepisach rozdziału 3a uksc pojęciem innym, niż „abonent” nazwy domeny.	
56.	Cybermadeinpol and	Art. 26	W art. 26 w dodanym ust. 2b należy doprecyzować termin w którym zgoda wyrażona ustnie ma być udokumentowana.	Uwaga uwzględniona
57.	Polskie Towarzystwo Informatyczne	art. 26	W art. 26 w dodanym ust. 2b należy doprecyzować termin w którym zgoda wyrażona ustnie ma być udokumentowana	Uwaga uwzględniona Zostanie dodany przepis, że zgoda ma być udokumentowana niezwłocznie, nie później niż w terminie 24 godzin od jej dokonania.
58.	Cybermadeinpol and	Art. 26	W art.26 w nowym brzmieniu punktu 12 należy uzupełnić w punkcie d) brakujący nawias oraz dodać określenie „mających znaczenie” przed wyrażeniem „dla cyberbezpieczeństwa”.	Uwaga częściowo uwzględniona Uzupełniono nawias. Pojęcie „potencjalnego zdarzenia dla cyberbezpieczeństwa” jest zdefiniowanym pojęciem w dyrektywie NIS2 w związku z czym nie można go zmienić.
59.	Polskie Towarzystwo Informatyczne	art. 26	W art.26 w nowym brzmieniu punktu 12 należy uzupełnić w punkcie d) brakujący nawias oraz dodać określenie „mających znaczenie” przed wyrażeniem „dla cyberbezpieczeństwa”	Uwaga częściowo uwzględniona Uzupełniono nawias. Pojęcie „potencjalnego zdarzenia dla cyberbezpieczeństwa” jest zdefiniowanym pojęciem w dyrektywie NIS2 w związku z czym nie można go zmienić.
60.	Centrum Łukasiewicz	Art. 26	art. 26 pkt d) tiret 2. projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw „w ust. 6 pkt 1: - w lit. a wyrazy „11 i 12” zastępuje się wyrazami „10-13” - po lit. c dodaje się lit. ca-cc w brzmieniu: „ca) międzynarodowe instytuty badawcze, cb) Centrum Łukasiewicz cc)instytuty badawcze Centrum Łukasiewicz” W projekcie ustawy mylnie wpisano „instytuty badawcze Centrum Łukasiewicz”. Zgodnie z art 1 ust. 1 ustawy z dnia 21 lutego 2019 r. Sieć Badawczą Łukasiewicz tworzą Centrum Łukasiewicz oraz instytuty działające w ramach Sieci Badawczej Łukasiewicz. Ponadto w ustawie o szkolnictwie wyższym i nauce w art. 7 ust. 1 pkt 6a) i 6b) wpisano odpowiednio:	Uwaga uwzględniona

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

			pkt 6a „Centrum Łukasiewicz, działające na podstawie ustawy z dnia 21 lutego 2019 r. o Sieci Badawczej Łukasiewicz (Dz.U. z 2020 r. poz. 2098), pkt 6b „instytuty działające w ramach Sieci Badawczej Łukasiewicz, zwane dalej „instytutami Sieci Łukasiewicz”. „w ust. 6 pkt 1: - w lit. a wyrazy „11 i 12” zastępuje się wyrazami „10-13” - po lit. c dodaje się lit. ca-cc w brzmieniu: „ca) międzynarodowe instytuty badawcze, cb) Centrum Łukasiewicz cc)instytuty działające w ramach Sieci Badawczej Łukasiewicz”	
61.	Osoba fizyczna	Art. 26	Ust. 3 – w pkt 2 - Zastosowano zapis dot. zapewnia podmiotom ksc dynamicznej analizy ryzyka. Proponuję dokonać weryfikacji intencji, czy idzie o analizę ryzyka, czy o szacowanie ryzyka i przyjąć spójne i konsekwentne podejście.	Wyjaśnienie uwagi W tym przepisie celowo użyte jest pojęcie „dynamicznej analizy ryzyka”. Jest to istotne ze względu na zmiany ryzyka wraz z upływem czasu.
62.	Fundacja Bezpieczna Cyberprzestrzeń	Art. 26	Art. 1 pkt 26 lit. c, treść art. 26 ust 3 pkt 2 – co ustawodawca ma na myśli pisząc: „szacowanie ryzyka związanego z ujawnionym cyberzagrożeniem oraz zaistniałymi incydentami, w tym <u>zapewnianie podmiotom krajowego systemu cyberbezpieczeństwa dynamicznej analizy ryzyka</u>”? W jaki sposób CSIRT poziomu krajowego mają zapewnić dynamiczną ocenę ryzyka? Czy to znaczy, że mają ją przeprowadzić i podzielić się wynikami? Kto będzie przeprowadzał taką ocenę? Wydaje się, że poprzednie brzmienia tego przepisu lepiej odzwierciedlało merytorycznie i metodycznie cel.	Wyjaśnienie uwagi Dynamiczna analiza ryzyka jest pojęciem wykorzystywanym przez specjalistów zajmujących się ryzykiem i jest zrozumiałe. Ponadto należy to już do obecnych zadań CSIRT poziomu krajowego i nie wystąpiły problemy ze stosowaniem tego przepisu.
63.	PGE SA	Art. 26 ust. 3 pkt 2	Nie jest zdefiniowana „dynamiczna analiza ryzyka” – należy dodać definicję tego pojęcia w art. 2 ustawy lub usunąć przepis art. 26 ust. 3 pkt 2.	Uwaga nieuwzględniona Dynamiczna analiza ryzyka jest pojęciem wykorzystywanym przez specjalistów zajmujących się ryzykiem i jest zrozumiałe. Ponadto należy to już do obecnych zadań CSIRT poziomu krajowego i nie wystąpiły problemy ze stosowaniem tego przepisu.
64.	Fundacja Open Allies	Art. 26	Jednym z zadań CSIRT MON, CSIRT NASK i CSIRT GOV będzie „w odpowiednich przypadkach gromadzenie i analizowanie danych na potrzeby postępowań karnych.” W pewnych przypadkach dane mogą być zbierane przez odpowiedni CSIRT na podstawie ostrzeżeń lub zgłoszeń incydentów. Jeżeli jednak Projektodawca uważa, że CSIRT będą mogły domagać się uzupełnienia określonych danych od podmiotów ważnych i podmiotów kluczowych, należy wprowadzić obowiązek wobec przekazywania takich danych przez te podmioty.	Wyjaśnienie uwagi Chodzi o dane zebrane przy wspieraniu obsługi incydentu przez dany podmiot krajowego systemu cyberbezpieczeństwa w. O ewentualne dodatkowe informacje będą mogły na podstawie odrębnych przepisów wystąpić organy prowadzące dane postępowanie karne.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

65.	Osoba fizyczna	Art. 26	Ust. 3 pkt 9 – Zastosowano zapis „badania urządzenia informatycznego lub oprogramowania”. Proponuję dokonać weryfikacji intencji, czy może chodzić o „badanie produktów ICT, usług ICT i procesów ICT”. Zamienne stosowanie tych sformułowań jest częste w dokumencie, choć ich znaczenie jest zupełnie inne. Proponuję przyjąć spójne i konsekwentne podejście.	Uwaga uwzględniona Przepis zostanie zmieniony
66.	PFR	Art. 26	Zwracamy uwagę na rozbieżność w zapisie pomiędzy dodawanym pkt. 4c) ust. 7 art. 26 zmienianej ustawy, w brzmieniu: „4c) Polski Fundusz Rozwoju i inne instytucje rozwoju, o których mowa w art. 2 ust. 1 pkt 3-6 ustawy z dnia 4 lipca 2019 r. o systemie instytucji rozwoju;” a treścią Załącznika nr 1 do Ustawy, w którym do podmiotów kluczowych zalicza się m.in.: „Polski Fundusz Rozwoju oraz inne instytucje rozwoju, o których mowa w art. 2 ust. 1 <u>pkt 1</u> i 3-6 ustawy z dnia 4 lipca 2019 r. o systemie instytucji rozwoju.”	Uwaga uwzględniona
67.	Fundacja Bezpieczna Cyberprzestrzeń	Art. 32	Art. 1 pkt 30, treść art. 32 – wydaje się, że brak w przepisach ustawy informowania podmiotu kluczowego i ważnego o koordynacji incydentu poważnego przez CSIRT poziomu krajowego. W obliczu faktu, że koordynacja to zapewnienie aktualnej, ścisłej, istotnej dla sprawy i dotyczącej wybranych uczestników informacji włączenie w nią podmiotu, którego dotyczy incydent poważny jest niezbędne. Proponuje się dodać ust.1 (zmieniając numerację ustępów w tym artykule) o treści: „1. CSIRT MON, CSIRT NASK i CSIRT GOV informują podmiot kluczowy lub podmiot ważny o przejęciu koordynacji obsługi incydentu poważnego, który go dotyczy.”. Dla porównania CSIRT sektorowy może koordynować obsługę incydentów „w uzgodnieniu z podmiotami kluczowymi lub podmiotami, które ich dotyczą” (patrz art. 44 ust. 1b pkt 3)	Uwaga uwzględniona
68.	Fundacja Open Allies	Art. 32 i art. 33	Dyrektywa NIS2 nie przewiduje procedury przewidzianej w art. 32 – 33 nowelizowanej UKSC. Zwracamy się o uchylenie ww. przepisów. Jest to szczególnie istotne, gdyż zgodnie z art. 32 ust. 2 nowelizowanej UKSC – podmiot kluczowy lub podmiot ważny mogą zostać wezwani do usunięcia podatności, nie mając uprzednio wpływu na treść wezwania oraz możliwość kwestionowania jego treści. W przypadku pozostawienia ww. przepisów w projekcie ustawy, zwracamy się również o przedłużenie terminu, o którym mowa w art. 33 ust. 7 nowelizowanej UKSC. 7 dni na wniesienie zastrzeżeń do rekomendacji jest terminem zdecydowanie zbyt krótkim, w szczególności mając na uwadze przedmiot zagadnień mogących być przedmiotem rekomendacji. Wnosimy o ustalenie terminu 21 dni na wniesienie zastrzeżeń.	Uwaga częściowo uwzględniona Termin na wniesienie zastrzeżeń do rekomendacji zostanie wydłużony do 14 dni.
69.	ZBP	Art. 32 ust. 2	W trakcie koordynacji obsługi incydentu poważnego lub krytycznego CSIRT MON, CSIRT NASK lub CSIRT GOV może wystąpić do organu właściwego do spraw cyberbezpieczeństwa z wnioskiem o wezwanie podmiotu kluczowego lub podmiotu ważnego, aby w wyznaczonym terminie usunął podatności, które doprowadziły lub mogłyby doprowadzić do incydentu poważnego lub krytycznego.	Uwaga wyjaśniona Naszym zdaniem należy zachować w przepisie usunięcie podatności – podmiot powinien się dostosować do tego w zakresie, w jakim jest to możliwe.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

			W trakcie koordynacji obsługi incydentu poważnego lub krytycznego CSIRT MON, CSIRT NASK lub CSIRT GOV może wystąpić do organu właściwego do spraw cyberbezpieczeństwa z wnioskiem o wezwanie podmiotu kluczowego lub podmiotu ważnego, aby w wyznaczonym terminie usunął lub zmitygował podatności, które doprowadziły lub mogłyby doprowadzić do incydentu poważnego lub krytycznego. Proponowana zmiana ma na celu umożliwienie zmitygowania podatności, w przypadku gdy nie można jej usunąć. Przyjęcie takiej zmiany daje gwarancję, że podmiot kluczowy lub podmiot ważny będzie w stanie szybko wprowadzić środki naprawcze przy obsłudze incydentu. Poprzez mitygację rozumie się całokształt działań mających na celu ograniczenie możliwości materializacji ryzyka związaną ze zidentyfikowaną podatnością, bez usuwania przyczyny ich występowania.	
70.	Konfederacja Lewiatan	Art. 32	Działania techniczne i udostępnianie informacji Jednostka redakcyjna: art. 32 projektu KSC Jednostka redakcyjna NIS2: art. 10 Uwaga: Art. 32 ust. 1 CSIRT MON, CSIRT NASK i CSIRT GOV mogą wykonywać niezbędne działania techniczne związane z analizą zagrożeń, koordynacją obsługi incydentu poważnego i incydentu krytycznego. Choć jest to zrozumiałe w kontekście zapewnienia bezpieczeństwa, przepisy nie określają szczegółowo granic tych uprawnień ani warunków, które muszą być spełnione przy wykonywaniu takich działań. Brak precyzyjnych wytycznych może prowadzić do nadużyć i naruszeń praw podmiotów kontrolowanych. Zgodnie z art. 32 ust. 2 projektu KSC w trakcie koordynacji obsługi incydentu poważnego lub krytycznego, CSIRT MON, CSIRT NASK lub CSIRT GOV może wystąpić do organu właściwego do spraw cyberbezpieczeństwa z wnioskiem o wezwanie podmiotu kluczowego lub podmiotu ważnego, aby w wyznaczonym terminie usunął podatności, które doprowadziły lub mogłyby doprowadzić do incydentu poważnego lub krytycznego. Problemem jest brak przewidzianej ścieżki odwoławczej od takiego wezwania. Podmioty kluczowe i ważne nie mają możliwości zaskarżenia decyzji, co narusza zasadę prawa do obrony i do sprawiedliwego procesu (art. 45 Konstytucji RP). Zgodnie z art. 32 ust. 3 projektu KSC CSIRT MON, CSIRT NASK lub CSIRT GOV może wystąpić bezpośrednio do podmiotu kluczowego lub podmiotu ważnego o udostępnienie informacji technicznych związanych z incydentem poważnym lub krytycznym, które będą niezbędne do przeprowadzenia analizy lub koordynacji obsługi takiego incydentu. Takie żądanie może obejmować informacje stanowiące tajemnicę przedsiębiorstwa, co może naruszać prawa podmiotów kontrolowanych do ochrony informacji poufnych i własności intelektualnej (art. 64 Konstytucji RP). Ponadto, przepisy nie precyzują, w jaki sposób zapewniona będzie ochrona udostępnionych informacji oraz jakie będą konsekwencje ich nieuprawnionego ujawnienia. Zgodnie z art. 32 ust. 4 projektu KSC CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT sektorowe na podstawie informacji, o których mowa w art. 13 ust. 1 pkt 3 i 5 ustawy KSC,	Uwaga wyjaśniona Jest to normalne działanie zespołów CSIRT. Aby zespół CSIRT – jakkolwiek zresztą – mógł pomóc podmiotowi w poradzeniu sobie z incydentem poważnym/krytycznym to musi mieć prawo do żądania informacji niezbędnych do obsługi incydentu.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

			uzyskanych od podmiotu kluczowego lub podmiotu ważnego, mogą przekazywać im informacje o podatnościach i sposobie usunięcia podatności w wykorzystywanych technologiach. Choć przekazywanie takich informacji jest zrozumiałe z punktu widzenia poprawy bezpieczeństwa, brak jest gwarancji ochrony przed nadużyciem tych informacji przez osoby trzecie oraz zabezpieczeń przed ich niewłaściwym wykorzystaniem. Projektowane przepisy dotyczące uprawnień CSIRT MON, CSIRT NASK i CSIRT GOV w zakresie wykonywania działań technicznych oraz udostępniania informacji technicznych związanych z incydentami poważnymi i krytycznymi, budzą poważne wątpliwości co do ich zgodności z konstytucyjnymi standardami ochrony praw i wolności jednostek. Przede wszystkim, brak przewidzianej ścieżki odwoławczej dla podmiotów kontrolowanych narusza zasadę prawa do obrony i do sprawiedliwego procesu. Ponadto, możliwość żądania udostępnienia informacji stanowiących tajemnicę przedsiębiorstwa bez odpowiednich zabezpieczeń może naruszać prawa do ochrony informacji poufnych i własności intelektualnej. Niezbędne jest wprowadzenie zmian, które zapewnią zgodność z konstytucyjnymi standardami, w tym mechanizmów ochrony prawnej, transparentności działań oraz poszanowania praw podmiotów kontrolowanych. W szczególności, konieczne jest wprowadzenie procedury odwoławczej oraz ścisłych zabezpieczeń dotyczących ochrony udostępnianych informacji, aby przepisy te mogły skutecznie chronić interesy podmiotów kontrolowanych i zapewnić zgodność z zasadami konstytucyjnymi.	
71.	Polskie Stowarzyszenie Fotowoltaiki	Art. 32	Obowiązek udostępniania przez PK i PW informacji technicznych związanych z incydemtem poważnym lub krytycznym na żądanie CSIRT MON, CSIRT NASK lub CSIRT GOV w ramach koordynacji obsługi incydentu poważnego lub krytycznego. Ogólny wpływ regulacji: Obowiązek przekazania informacji na żądanie odpowiednich podmiotów. W ramach koordynacji obsługi incydentu poważnego lub krytycznego CSIRT MON, CSIRT NASK lub CSIRT GOV może wystąpić do organu właściwego do spraw cyberbezpieczeństwa z wnioskiem o wezwanie PK lub PW do terminowego usunięcia zidentyfikowanych podatności (pod rygorem nałożenia kary pieniężnej – zob. uwagi do art. 73 KSC wg Projektu) Wpływ na sektor energetyczny: Uwagi jw. – brak specyficznego wpływu na sektor energetyczny [Nadregulacja względem Dyrektywy NIS2] Uprawnienie CSIRT MON, CSIRT NASK lub CSIRT GOV do wystąpienia do organu właściwego do spraw cyberbezpieczeństwa z wnioskiem o wezwanie PK lub PW do terminowego usunięcia zidentyfikowanych	Wyjaśnienie uwagi Jest to normalne działanie zespołów CSIRT. Aby zespół CSIRT – jakkolwiek zresztą – mógł pomóc podmiotowi w poradeniu sobie z incydemtem poważnym/krytycznym to musi mieć prawo do żądania informacji niezbędnych do obsługi incydentu.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

			podatności pod rygorem nałożenia kary pieniężnej stanowi nadregulację względem wymogów wynikających z Dyrektywy NIS2 Rekomendacja: Zob. uwagi wskazane do art. 73	
72.	Polska Izba Informatyki i Telekomunikacji	Art. 33	Art. 33 – badanie produktów, usług, procesów ICT Z uwagi na potencjalne skutki prowadzenia badania, w tym także przerwanie lub zakłócenie działania usług, wnioskujemy o doprecyzowanie przepisów w zakresie ograniczenia możliwości prowadzenia takiego badania urządzeń lub oprogramowania wobec działających systemów teleinformatycznych służących do świadczenia określonych usług. Wydaje się, że intencją jest prowadzenie tego typu badań w warunkach laboratoryjnych, tudzież systemów wydzielonych na potrzeby badania, a nie zasobów działających w warunkach produkcyjnych i służących świadczeniu usług. Wnosimy o doprecyzowanie, że badanie, o którym mowa w art. 33 nie jest wykonywane wobec funkcjonujących systemów podmiotów krajowego systemu cyberbezpieczeństwa, ale w środowisku testowym zapewnianym przez dokonujący badania CSIRT. Jeśli natomiast takie działania miałyby być dopuszczalne, konieczne jest wprowadzenie przepisów dot. odpowiedzialności organu prowadzącego badanie za ew. przerwanie lub zakłócenie działania usługi, w tym dot. odpowiedzialności finansowej, także wobec stron trzecich.	Wyjaśnienie uwagi Ogólne przepisy o odpowiedzialności deliktowej Skarbu Państwa znajdują się w Kodeksie Cywilnym i nie ma potrzeby ich doprecyzowania.
73.	Konfederacja Lewiatan	Art. 33	Badanie produktów, usług, procesów ICT. Badanie oprogramowania bez gwarancji zabezpieczenia podmiotów, u których badanie miałoby następować Jednostka redakcyjna: art. 33 projektu KSC Jednostka redakcyjna NIS2: 20 ust. 1 Z uwagi na potencjalne skutki prowadzenia badania, w tym także przerwanie lub zakłócenie działania usług, wnioskujemy o doprecyzowanie przepisów w zakresie ograniczenia możliwości prowadzenia takiego badania urządzeń lub oprogramowania wobec działających systemów teleinformatycznych służących do świadczenia określonych usług. Wydaje się, że intencją jest prowadzenie tego typu badań w warunkach laboratoryjnych, tudzież systemów wydzielonych na potrzeby badania, a nie zasobów działających w warunkach produkcyjnych i służących świadczeniu usług. Wnosimy o doprecyzowanie, że badanie, o którym mowa w art. 33 nie jest wykonywane wobec funkcjonujących systemów podmiotów krajowego systemu cyberbezpieczeństwa, ale w środowisku testowym zapewnianym przez dokonujący badania CSIRT. Jeśli natomiast takie działania miałyby być dopuszczalne, konieczne jest wprowadzenie przepisów dot. odpowiedzialności organu prowadzącego badanie za ew. przerwanie lub zakłócenie działania usługi, w tym dot. odpowiedzialności finansowej, także wobec stron trzecich. Projektowane przepisy pozwalają na przeprowadzanie badań urządzeń informatycznych i oprogramowania na tzw. "żywym systemie", czyli w środowisku produkcyjnym, co może prowadzić do znaczących	Uwaga częściowo uwzględniona Zostanie dodany przepis zgodnie z którym badanie z art. 33 jest przeprowadzane w środowisku testowym. Wprowadzenie licencji ustawowej do przeprowadzania tego rodzaju badań jest konieczne, aby można było zidentyfikować podatności w produkcie/usłudze ICT.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

		zakłóceń w jego działaniu. Przepisy nie przewidują dodatkowych warunków ani zabezpieczeń dotyczących takich działań, co budzi poważne wątpliwości co do ich zgodności z zasadami ochrony praw i wolności jednostek. Zgodnie z art. 33 ust. 1 projektu KSC, CSIRT MON, CSIRT NASK lub CSIRT GOV mogą przeprowadzić badanie urządzenia informatycznego lub oprogramowania w celu identyfikacji podatności, której wykorzystanie może zagrozić w szczególności integralności, poufności, rozliczalności, autentyczności lub dostępności przetwarzanych danych, mających wpływ na bezpieczeństwo publiczne lub istotny interes bezpieczeństwa państwa. Projektowane przepisy dotyczące uprawnień CSIRT MON, CSIRT NASK i CSIRT GOV w zakresie badania urządzeń i oprogramowania budzą poważne wątpliwości co do ich zgodności z konstytucyjnymi standardami ochrony praw i wolności. Przepisy przyznają CSIRT szerokie uprawnienia do stosowania technik mających na celu: obserwację i analizę pracy urządzenia lub oprogramowania, uzyskanie dostępu do przetwarzanych danych, odtworzenie postaci źródłowej oprogramowania, zwielokrotnienie kodu programowego, translację jego formy, odtworzenie algorytmu przetwarzania danych, identyfikację realizowanych funkcji, usunięcie lub przełamanie zabezpieczeń przed badaniem, oraz identyfikację podatności i nieudokumentowanych funkcji. Tak szerokie uprawnienia mogą prowadzić do naruszenia prawa do prywatności (art. 47 Konstytucji RP) oraz ochrony danych osobowych (art. 51 Konstytucji RP). Przełamywanie zabezpieczeń systemów informacyjnych bez odpowiednich gwarancji ochrony prawnej budzi poważne wątpliwości co do zgodności z konstytucyjnymi standardami ochrony danych osobowych oraz integralności systemów informacyjnych. Ponadto, takie działania mogą naruszać prawa do ochrony własności intelektualnej (art. 64 Konstytucji RP) oraz prawa autorskie. Przepis ten stwierdza, że CSIRT prowadząc badanie, nie jest związany postanowieniami umów, w szczególności umów licencyjnych, które ograniczałyby możliwość przeprowadzenia badania. Takie sformułowanie budzi wątpliwości co do zgodności z zasadą ochrony własności (art. 64 Konstytucji RP) oraz zasadą rzetelnej legislacji (art. 2 Konstytucji RP). Naruszenie warunków umów licencyjnych bez zgody stron może prowadzić do poważnych konsekwencji prawnych i gospodarczych dla właścicieli oprogramowania oraz usług ICT. Przepis ten twierdzi, że badanie nie narusza autorskich praw osobistych oraz majątkowych oraz nie wymaga zgody licencjodawcy lub dysponenta produktu ICT, usługi ICT lub procesu ICT. Takie sformułowanie może być sprzeczne z art. 64 ust. 1 Konstytucji RP, który gwarantuje ochronę praw majątkowych, w tym praw autorskich. Pominięcie konieczności uzyskania zgody licencjodawcy na przeprowadzanie badań może naruszać umowne prawa stron oraz prowadzić do naruszeń prawa autorskiego i własności intelektualnej. Przepis ten stwierdza, że postanowienia umów sprzeczne z przepisami ust. 1–1d są nieważne. Taka generalna klauzula może prowadzić do niepewności prawnej i podważać zaufanie do państwa i jego prawa (art. 2 Konstytucji RP). Ograniczenie możliwości swobodnego zawierania umów i określania ich warunków może być sprzeczne z zasadą wolności gospodarczej (art. 20 i	

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

			art. 22 Konstytucji RP). Projektowane przepisy dotyczące uprawnień CSIRT MON, CSIRT NASK i CSIRT GOV w zakresie badania urządzeń i oprogramowania mogą prowadzić do poważnych naruszeń konstytucyjnych praw i wolności jednostek. Przede wszystkim, szerokie uprawnienia do przełamania zabezpieczeń, uzyskiwania dostępu do danych i analizowania kodu programowego bez odpowiednich gwarancji ochrony prawnej budzą poważne wątpliwości co do zgodności z prawem do prywatności, ochrony danych osobowych oraz własności intelektualnej. Brak związania CSIRT umowami licencyjnymi i postanowienia o nieważności sprzecznych postanowień umów mogą prowadzić do niepewności prawnej i podważać zasady wolności gospodarczej oraz ochrony własności. Niezbędne jest wprowadzenie zmian, które zapewnią zgodność z konstytucyjnymi standardami, w tym mechanizmów ochrony prawnej, transparentności działań oraz poszanowania praw majątkowych i autorskich podmiotów kontrolowanych. Tylko wtedy przepisy te będą mogły skutecznie chronić interesy podmiotów kontrolowanych i zapewnić zgodność z zasadami konstytucyjnymi.	
74.	Polskie Stowarzyszenie Fotowoltaiki	Art. 33	Projekt zakłada uprawnienie CSIRT MON, CSIRT NASK lub CSIRT GOV do przeprowadzenia badania produktu ICT, usługi ICT lub procesu ICT w celu identyfikacji podatności, przy czym skutek podatności nie jest zdefiniowany (otwarty katalog). Sam przedmiot badania może dotyczyć jakiegokolwiek produktu ICT, usługi ICT lub procesu ICT. Jednocześnie przepis nadaje uprawnienie organom do szerokiego katalogu czynności technicznych mających za przedmiot sprzęt i oprogramowanie, w tym dekompilowanie, przełamanie zabezpieczeń, odtwarzanie postaci źródłowej oprogramowania. Na podstawie badania, Pełnomocnik uprawniony jest do wydawania rekomendacji dotyczących stosowania produktów ICT, usług ICT lub procesów ICT. Szczegółowy zakres rekomendacji nie został jednak określony w Projekcie. Rekomendacje podlegają publikacji w BIP. Projekt nie uwzględnia uczestnictwa lub zawiadomienia PK, PW lub dostawcy produktu ICT, usługi ICT lub procesu ICT o przeprowadzeniu badania jak również, aby rekomendacje miały być tym podmiotom dostarczone. Tymczasem, podmiot krajowego systemu cyberbezpieczeństwa (np. PK lub PW) może wnieść do Pełnomocnika zastrzeżenia do rekomendacji dotyczących stosowania produktów ICT, usług ICT lub procesów ICT, z uwagi na ich negatywny wpływ na świadczoną usługę lub realizowane zadanie publiczne, nie później niż w terminie 7 dni od dnia otrzymania rekomendacji. Ponadto, podmiot krajowego systemu cyberbezpieczeństwa zobowiązany jest do uwzględnienia rekomendacji dotyczących stosowania produktów ICT, usług ICT lub procesów ICT przez podmiot krajowego systemu cyberbezpieczeństwa oraz przekazania informacji o sposobie i zakresie ich uwzględnienia. Projekt zakłada również obowiązek producenta produktu ICT, usługi ICT lub procesu ICT do przekazania dokumentacji na żądanie CSIRT MON, CSIRT NASK lub CSIRT GOV. Ogólny wpływ regulacji: Z uwagi na nieprzejrzyste przesłanki przeprowadzenia badania istnieje ryzyko arbitralnego poddawania produktu ICT, usługi ICT lub procesu ICT badaniu. Nieostre kryteria oceny	Wyjaśnienie uwagi Po pierwsze instytucja badania sprzętu lub oprogramowania funkcjonuje od 2018 r. Na podstawie ogólnych przepisów zespół CSIRT prowadzący badanie musi zachować w tajemnicy tajemnicę przedsiębiorstwa. Podmiot kluczowy/podmiot ważny może wnieść do Pełnomocnika zastrzeżenia do rekomendacji. Same rekomendacje mają charakter niewiążący. Przesłanką badania sprzętu/oprogramowania jest identyfikacja podatności zagrażającej bezpieczeństwu narodowemu. Pełnomocnik może też odwołać rekomendacje, szczególnie jeśli wpłyną zastrzeżenia.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

			produktów mogą w konsekwencji prowadzić do dyskryminacji określonych produktów i wykluczenia ich z rynku, poprzez rozpowszechnienie informacji w BIP. Ponadto, wobec braku zaangażowania w procedurę badania produktu ICT, usługi ICT lub procesu ICT konkretnego PK, PW lub dostawcy, wpływ tych podmiotów na wynik oraz ostateczną treść rekomendacji jest znikomy. Projekt nie precyzuje pojęcia dokumentacji, którą producent produktu ICT, usługi ICT lub procesu ICT jest zobowiązany przekazać organowi. Ponadto, postanowienia art. 33 KSC wg Projektu nie zawierają, na wzór innych postanowień Projektu, postanowień zgodnie z którymi informacje pozyskane od producenta lub wytworzone w ramach badania, stanowią tajemnicę prawnie chronioną i nie mogą być wykorzystane do realizacji innych zadań oraz podlegają zniszczeniu. Wpływ na sektor energetyczny: Uwagi jw. – brak specyficznego wpływu na sektor energetyczny [Nadregulacja względem Dyrektywy NIS2] Postanowienia Dyrektywy NIS2 nie obejmują obowiązku zapewnienia uprawnienia CSIRT do dokonywania badań urządzeń informatycznych lub oprogramowania, a jedynie przewidują wśród ich zadań monitorowanie i analizowanie cyberzagrożeń, podatności i incydentów na poziomie krajowym. Działania te wykraczają również poza pojęcie aktywnego, nieinwazyjnego skanowania publicznie dostępnych sieci i systemów informatycznych podmiotów kluczowych i ważnych (art. 11 ust. 3 Dyrektywy NIS2). Tym samym, postanowienia art. 33 KSC wg Projektu stanowią regulację wykraczającą poza zakres Dyrektywy NIS2. Rekomendacja: - wycofanie przepisów z Projektu. Alternatywnie: - doprecyzowanie kryteriów oceny urządzeń informatycznych i oprogramowania; - umożliwienie podmiotom krajowego systemu cyberbezpieczeństwa jak również dostawcom lub producentom wniesienie zastrzeżeń do rekomendacji przed publikacją w BIP; - doprecyzowania zakresu dokumentacji jaką producent produktu ICT, usługi ICT lub procesu ICT jest zobowiązany przekazać organowi oraz zapewnienia poufności przekazanych lub tworzonych przez organ w ramach badania informacji o produkcie ICT, usłudze ICT lub procesie ICT.	
75.	Konfederacja Lewiatan	Rozdział 6a	Nieograniczony i potencjalnie niewłaściwy dostęp do systemów informatycznych przez CSIRT-y Jednostka redakcyjna: rozdział 6a projektu ustawy KSC Jednostka redakcyjna NIS2: art. 20 ust. 1 Uwaga: Propozycja zawarta w rozdziale 6a ustawy KSC, umożliwiająca CSIRT MON, CSIRT NASK i CSIRT GOV przeprowadzanie dowolnych badań oprogramowania lub sprzętu w celu	Wyjaśnienie uwagi Odpowiedzialność odszkodowawcza Skarbu Państwa za działania organów administracji publicznej jest uregulowana w art. 417

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

			identyfikacji podatności, bez przestrzegania wymogów licencyjnych, budzi poważne zastrzeżenia. W świetle proponowanych przepisów, te jednostki będą mogły m.in. odtwarzać źródłową postać oprogramowania, powielać kod programowy, przełamywać zabezpieczenia, czy identyfikować nieudokumentowane funkcje. Brak w przepisach jakiegokolwiek odpowiedzialności Skarbu Państwa za potencjalne zniszczenie systemów lub danych podczas takich działań jest kolejnym aspektem, który budzi wątpliwości. To zaniechanie legislacyjne może prowadzić do poważnych konsekwencji finansowych i operacyjnych dla przedsiębiorstw posiadających kluczowe i ważne systemy informatyczne. Ostatecznie, brak odpowiednich zabezpieczeń i gwarancji, zarówno prawnych, jak i technicznych, dotyczących postępowania z uzyskanymi materiałami, pozostaje poważnym niedociągnięciem, które może osłabić zaufanie do krajowego systemu cyberbezpieczeństwa oraz prowadzić do dalszych nadużyć i szkód – przecież zespoły nie będą za każdym razem niszczyć dysków na których przechowywały dane materiały (co do zasady tylko fizyczne zniszczenie danych, daje gwarancje braku dostępu do nich).	Kodeksu cywilnego i nie ma potrzeby dublowania regulacji. Badanie z art. 33 ma na celu identyfikację podatności zagrażających bezpieczeństwu narodowemu. Wprowadzony zostanie przepis, zgodnie z którym badanie to odbywa się w środowisku testowym.
76.	ISSA Polska	Rozdział 6a	Propozycja zawarta w rozdziale 6a ustawy KSC, umożliwiająca CSIRT MON, CSIRT NASK i CSIRT GOV przeprowadzanie dowolnych badań oprogramowania lub sprzętu w celu identyfikacji podatności, bez przestrzegania wymogów licencyjnych, budzi poważne zastrzeżenia. Prawo do głębokiej analizy produktów ICT nie powinno podlegać dyskusji, taka analiza jest jednak prowadzona nie tylko przez CSIRT MON, CSIRT NASK i CSIRT GOV, ale również przez podmioty komercyjne, jeżeli analiza ryzyka w łańcuchu dostaw wykaże taką potrzebę. Działania takie realizowane przez podmioty komercyjne podlegają jednak każdorazowym uzgodnieniom z dostawcą produktu; ugodę o udostępnienie danych może uzyskać tylko ten, który udostępnił dane, a więc producent, udostępniającego na cele testów często kluczową dla swojej działalności własność intelektualną. Analogicznie na poziomie państwowym, w przypadku udostępnienia kluczowych informacji (np. kodu źródłowego) zawierane są bilateralne umowy chroniące prawa obu stron oraz sposób udostępnienia informacji oraz ich zabezpieczenia. W proponowanych przepisach brak odpowiednich zabezpieczeń i gwarancji, zarówno prawnych, jak i technicznych, dotyczących postępowania z weryfikowanymi materiałami, pozostaje poważnym niedociągnięciem, które może osłabić zaufanie do krajowego systemu cyberbezpieczeństwa oraz prowadzić do dalszych nadużyć i szkód – zespoły CSIRT MON, CSIRT NASK i CSIRT GOV nie są zobligowane do przestrzegania konkretnych wytycznych producenta w kwestii zabezpieczeń, brak jest również w przepisach jakiegokolwiek odpowiedzialności Skarbu Państwa za nieuprawnione ujawnienie lub wykorzystanie informacji. Zgodnie z art. 75 prawa autorskiego, przepisy wprowadzają określony zakres dozwolonego korzystania z programu komputerowego, w celach związanych z bezpieczeństwem (wykonywanie kopii, sprawdzanie współpracy programu z innymi programami). Należy rozważyć kwestię rozszerzenia przepisów zawartych w tym akcie o potrzeby wynikające z realizacji zadań przez podmioty krajowego systemu cyberbezpieczeństwa, przez zapisanie wprost normy bezwzględnie obowiązującej, o dopuszczalności takiego działania w ramach udzielonej licencji (w każdej formie bez względu na to, czy ma miejsce korzystanie z egzemplarza firmware	Wyjaśnienie uwagi Odpowiedzialność odszkodowawcza Skarbu Państwa za działania organów administracji publicznej jest uregulowana w art. 417 Kodeksu cywilnego i nie ma potrzeby dublowania regulacji. Badanie z art. 33 ma na celu identyfikację podatności zagrażających bezpieczeństwu narodowemu. Wprowadzony zostanie przepis, zgodnie z którym badanie to odbywa się w środowisku testowym.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

			w zakupionym produkcie czy chodzi o licencję na korzystanie z innego programu). Dlatego naszym zdaniem właściwszym podejściem byłoby określenie warunków, jakie powinny spełniać obowiązujące na terenie RP umowy licencyjne oraz zobowiązanie działających na polskim rynku firm do umożliwienia klientom oraz wybranym instytucjom prawa do przeprowadzania testów i analiz w oparciu o umowy zabezpieczające prawa własności intelektualnej i ochronę tajemnicy przedsiębiorstwa, zamiast ustawowego ich lekceważenia.	
77.	Amerykańska Izba Handlowa	Art. 33	Na gruncie obowiązującej ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (dalej: pr. aut.) istnieje podstawa, która pozwala na wykorzystanie utworów dla celów bezpieczeństwa publicznego (art. 33(2) pr. aut.). Przepis ten został jednak wyłączony w stosunku do programów komputerowych (zgodnie z art. 77 pr. aut.). Niezrozumiałym jest zatem intencja projektodawcy (także z powodu braku stosownego uzasadnienia) polegająca na dodaniu pkt. 1a-1e w art. 33 ust. 1 Ustawy, który daje podstawy do podjęcia czynności wkraczających w prawa autorskie twórcy programu komputerowego w ramach badań prowadzonych przez CSIRT MON, CSIRT NASK i CSIRT GOV – tj. uprawnienia pokrywające się z uprawnieniami wynikającymi z art. 33(2) pr. aut. (przy czym art. 33(2) pr. aut. przyznaje szersze uprawnienia niż projektowana nowelizacja). Zatem warto zastanowić się nad ewentualną zmianą pr. aut., polegającą na usunięciu wyłączenia wprowadzonego w art. 77 pr. aut., bez wprowadzania wyjątków w ustawach pobocznych. Takie działanie miałoby na celu zapewnienie przejrzystości prawa.	Uwaga nieuwzględniona Zmiany w Prawie autorskim wychodzą znacznie poza implementację dyrektywy NIS2 i kwestie Cyberbezpieczeństwa.
78.	Osoba fizyczna	Art. 33	Ust. 1 – zastosowano zapis „badanie produktu ICT, usługi ICT lub procesu ICT”, z kolei w art. 26 zastosowano „badania urządzenia informatycznego lub oprogramowania”. Proponuję dokonać weryfikacji intencji. Zamienne stosowanie tych sformułowań jest częste w dokumencie, choć ich znaczenie jest zupełnie inne. Proponuję przyjąć spójne i konsekwentne podejście.	Uwaga uwzględniona
79.	KWKR Konieczny Wierzbicki i Partnerzy S.K.A.	Art. 33	Proponowane zmiany w art. 33 uksc w zakresie dotyczącym rekomendacji pełnomocnika rządu ds. cyberbezpieczeństwa zdają się nie określać w sposób jednoznaczny i nie budzący wątpliwości interpretacyjnych kwestii nieuwzględnienia przez podmioty krajowego systemu cyberbezpieczeństwa rekomendacji wydanych przez pełnomocnika, w szczególności tego na czym polega „nieuwzględnienie rekomendacji”. Na gruncie dotychczasowego brzmienia tego przepisu powstały wątpliwości co do rozumienia zakresu pojęcia „nieuwzględnienia rekomendacji”, tzn. czy należy je traktować jako niewzięcie ich pod uwagę, nie rozpatrzenie w toku procesu (na co wskazuje interpretacja językowa) czy jako nie zastosowanie się do nich. Nieuwzględnienie rekomendacji, mimo ich formalnie niewiążącego charakteru, powoduje jednak powstanie określonych skutków prawnych, tj. daje podstawy do wystąpienia przez pełnomocnika do organu nadzoru nad podmiotem krajowego systemu cyberbezpieczeństwa, a z kolei taka informacja ze strony pełnomocnika może stanowić dla organu nadzoru podstawę np. do wszczęcia kontroli w podmiocie nadzorowanym. Nowelizacja uksc nie przesądza tych wątpliwości interpretacyjnych.	Wyjaśnienie uwagi Nie uwzględnienie rekomendacji należy rozumieć jako nie zastosowanie się do nich. Podmiot kluczowy i podmiot ważny ma do tego prawo. W przypadku kontroli podmiot musi wykazać zgodność z przepisami prawa powszechnie obowiązującego – np. że wypełnia wymogi z art. 8 ksc pomimo nieuwzględnienia rekomendacji.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

80.	ISAC-Kolej	Art. 34	Dla transportu kolejowego ten zapis, gdy powołany zostanie CSIRT dla podsektora transportu kolejowego jest niezrozumiały (dlaczego taki CSIRT ma współpracować z ULC, UKE czy KNF?). Ewentualnie zapis ten powinien odwoływać się do wszystkich regulatorów rynku (także UTK), a nie tylko ograniczać się do trzech.	Wyjaśnienie uwagi Jest to związane z art. 12 ust. 4 dyrektywy NIS2
81.	ISAC-Kolej	Art. 36a	„2) akredytowanych na podstawie art. 48 ustawy z dnia 15 marca 2010 r. o ochronie informacji niejawnych (Dz. U. z 2023 r. poz. 756, 1030 i 1532)”. Ustawa o ochronie informacji niejawnych jest z dnia 5 sierpnia 2010 roku a nie 15 marca 2010 roku.	Uwaga uwzględniona
82.	Konfederacja Lewiatan	Art. 36a-36d	Jednostka redakcyjna: Art. 36a – 36d Jednostka redakcyjna NIS2: art. 20 ust. 1 Uwaga: Projektowane przepisy dotyczące oceny bezpieczeństwa systemów informacyjnych, zawarte w art. 36a–36d, budzą liczne wątpliwości pod względem ich zgodności z konstytucyjnymi standardami ochrony praw i wolności jednostek. Przede wszystkim, art. 36b ust. 1 pkt 2 pozwala na przeprowadzenie oceny bezpieczeństwa systemu informacyjnego na zlecenie organu właściwego do spraw cyberbezpieczeństwa, bez konieczności uzyskania zgody podmiotu kontrolowanego. Taki poziom ingerencji może naruszać konstytucyjnie chronione prawa do prywatności (art. 47 Konstytucji RP) oraz prawa do ochrony własności (art. 64 Konstytucji RP). Przeprowadzanie testów bezpieczeństwa, które mogą obejmować przełamywanie zabezpieczeń systemów informacyjnych, stwarza ryzyko naruszenia integralności i poufności danych. To jest szczególnie niepokojące, ponieważ art. 36b ust. 4 i 5 projektu KSC zezwalają CSIRT na używanie urządzeń i programów komputerowych do przełamywania zabezpieczeń systemów informacyjnych. Brak odpowiednich mechanizmów ochrony prawnej i kontroli nad użyciem takich narzędzi może prowadzić do nieuzasadnionych naruszeń praw jednostek i podmiotów gospodarczych, co może być sprzeczne z zasadą ochrony prawnej prywatności i własności. Projektowane przepisy nie przewidują także mechanizmów odszkodowawczych w przypadku wystąpienia szkód wynikających z przeprowadzenia oceny bezpieczeństwa. Art. 36b ust. 2 projektu KSC stwierdza, że ocena bezpieczeństwa nie może prowadzić do nieodwracalnego zniszczenia danych przetwarzanych w systemie informacyjnym. Niemniej jednak, przepisy nie określają mechanizmu odszkodowawczego w przypadku, gdyby takie zniszczenie jednak miało miejsce. Brak takiego mechanizmu może być uznany za sprzeczny z art. 77 ust. 1 Konstytucji RP, który gwarantuje prawo do wynagrodzenia szkody wyrządzonej przez niezgodne z prawem działanie organów władzy publicznej. Kolejnym problemem jest brak transparentności w przepisach dotyczących trybu i warunków przeprowadzania oceny bezpieczeństwa. Art. 36b ust. 3 projektu KSC przewiduje, że CSIRT uzgadnia z podmiotem kontrolowanym tryb i ramowe warunki przeprowadzania oceny bezpieczeństwa, jednak brak jest precyzyjnych wytycznych dotyczących tego procesu. Brak transparentności może prowadzić do nadużyć i naruszeń praw podmiotów kontrolowanych, co	Uwaga wyjaśniona Możliwość przeprowadzenia oceny bezpieczeństwa wynika bezpośrednio z dyrektywy NIS2. Kwestie dotyczące odpowiedzialności odszkodowawczej Skarbu Państwa są zawarte w Kodeksie cywilnym i nie ma potrzeby dublowania tych rozwiązań.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

			może być sprzeczne z zasadą zaufania obywateli do państwa i jego prawa, wynikającą z art. 2 Konstytucji RP. Przepisy dotyczące używania urządzeń i programów komputerowych do przełamania zabezpieczeń systemów informacyjnych (art. 36b ust. 4 i 5 projektu KSC) mogą również prowadzić do naruszenia prawa do prywatności oraz ochrony danych osobowych. Przełamywanie zabezpieczeń bez odpowiednich gwarancji ochrony prawnej budzi poważne wątpliwości co do zgodności z art. 51 Konstytucji RP, który chroni dane osobowe i zobowiązuje organy publiczne do ochrony prywatności jednostki. Dodatkowo, informowanie o wykrytych podatnościach, jak przewiduje art. 36c ustawy o KSC, może prowadzić do naruszenia tajemnicy przedsiębiorstwa i innych chronionych informacji. Przepisy nie zawierają wystarczających zabezpieczeń, aby chronić te informacje przed nieuprawnionym ujawnieniem, co może być sprzeczne z art. 61 Konstytucji RP, gwarantującym prawo dostępu do informacji publicznej, ale z wyłączeniem informacji chronionych prawem. Podsumowując, projektowane przepisy dotyczące oceny bezpieczeństwa systemów informacyjnych wymagają istotnych zmian, aby zapewnić zgodność z konstytucyjnymi standardami ochrony praw i wolności jednostek. Niezbędne jest wprowadzenie mechanizmów odszkodowawczych, szczegółowych procedur gwarantujących transparentność i zgodność działań z obowiązującymi przepisami oraz mechanizmów weryfikacji poprawności działań kontrolnych. Tylko wtedy przepisy te będą mogły skutecznie chronić interesy podmiotów kontrolowanych i zapewnić zgodność z zasadami konstytucyjnymi.	
83.	Cybermadeinpol and	Art. 36b	W dodanym rozdziale 6a Ocena bezpieczeństwa w Art. 36b ust.4 wydaje się zbędny w związku z brzmieniem Art. 296b § 1a Kodeksu Karnego, gdyż cel tam wymieniony w całości pokrywa się z celem w jakim mogą działać wymienione CSIRT-y (działanie w celu zabezpieczenia systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej przed popełnieniem przestępstw).	Wyjaśnienie uwagi Przepis art. 36b ust. 4 ma zagwarantować wyraźną podstawę prawną do korzystania z oprogramowania przy przeprowadzaniu testów bezpieczeństwa.
84.	ISACA	Art. 36b	Art. 36b. 1. Ocena bezpieczeństwa systemu informacyjnego może być przeprowadzona: 1) za zgodą podmiotu krajowego systemu cyberbezpieczeństwa, wyrażoną w formie pisemnej lub formie elektronicznej pod rygorem nieważności lub 2) na zlecenie organu właściwego do spraw cyberbezpieczeństwa. "Doprecyzowanie pkt 2) o wskazanie rodzajów sytuacji, które mogą uzasadniać dokonanie oceny bezpieczeństwa systemu informacyjnego. Przykładowy katalog, który mógłby zostać zastosowany: 2) na zlecenie organu właściwego do spraw cyberbezpieczeństwa, gdy a) Występuje bieżący incydent cyberbezpieczeństwa, który zagraża bezpieczeństwu systemów informacyjnych podmiotów krajowego systemu bezpieczeństwa b) Istnieje realne i bezpośrednie zagrożenie, które może prowadzić do poważnych zakłóceń w funkcjonowaniu systemów informacyjnych podmiotów krajowego systemu bezpieczeństwa, a jego szybkie wykrycie i neutralizacja jest kluczowa dla ochrony interesów państwa i obywateli.	Uwaga częściowo uwzględniona Przed podjęciem decyzji o przeprowadzeniu oceny bezpieczeństwa organ właściwy do spraw Cyberbezpieczeństwa przeprowadzi szacowanie ryzyka odnośnie podmiotów, które powinny być ocenione.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

			c) Został ogłoszony stan wyjątkowy lub stan klęski żywiołowej, który uzasadnia potrzebę natychmiastowej oceny bezpieczeństwa systemów informacyjnych w celu ochrony zdrowia, życia, bezpieczeństwa publicznego lub porządku publicznego. d) Na podstawie przeprowadzonej analizy ryzyka stwierdzono wysokie prawdopodobieństwo wystąpienia incydentu cyberbezpieczeństwa, który mógłby mieć znaczący wpływ na bezpieczeństwo systemów informacyjnych podmiotu lub podmiotów krajowego systemu, a działania prewencyjne są niezbędne do minimalizacji tego ryzyka. "Doprecyzowanie pkt 2) art. 36b ust. 1 ustawy o krajowym systemie cyberbezpieczeństwa jest wskazane dla zapewnienia jasności i precyzji przepisów. Umożliwi to organowi właściwemu do spraw cyberbezpieczeństwa skuteczne i adekwatne reagowanie na sytuacje wymagające przeprowadzenia oceny bezpieczeństwa systemu informacyjnego. Sprecyzowanie rodzajów sytuacji, które mogą uzasadniać dokonanie takiej oceny, pozwoli na jednoznaczne określenie zakresu kompetencji organu oraz usprawni procedury działania w przypadkach zagrożeń. Dodatkowo, przyczyni się to do zwiększenia transparentności oraz przewidywalności działań podejmowanych przez organ właściwy do spraw cyberbezpieczeństwa.	
85.	ISACA	Art. 36b	3. W celu minimalizacji negatywnych następstw oceny bezpieczeństwa systemu informacyjnego CSIRT MON, CSIRT NASK, CSIRT GOV, lub CSIRT sektorowy uzgadnia z podmiotem krajowego systemu cyberbezpieczeństwa, w drodze porozumienia, tryb i ramowe warunki przeprowadzania tej oceny, w szczególności datę rozpoczęcia, harmonogram oraz zakres i rodzaj przeprowadzanych w ramach oceny bezpieczeństwa testów bezpieczeństwa. Uzupełnienie ust. o kolejne zdanie: W przypadku braku porozumienia w terminie 3 dni od poinformowania podmiotu o konieczności dokonania oceny na podstawie pkt 2) art. 36b ust. 1, odpowiedni CSIRT ustala te warunki jednostronnie, z uwzględnieniem konieczności ochrony interesów państwa i obywateli. Proponowana zmiana jest wskazana, aby zapewnić szybkie i skuteczne działanie w sytuacjach awaryjnych - ocenie bezpieczeństwa na zlecenie organu właściwego do spraw cyberbezpieczeństwa, takich jak incydenty cyberbezpieczeństwa lub stany wyjątkowe. Określenie terminu 3 dni na uzgodnienie warunków oceny z podmiotem krajowego systemu cyberbezpieczeństwa oraz umożliwienie odpowiednim CSIRT-om jednostronnego ustalania warunków w przypadku braku porozumienia, zapobiega opóźnieniom i zapewnia ochronę interesów państwa oraz obywateli.	Uwaga nieuwzględniona Zasadne wydaje się, żeby CSIRT oraz podmiot badany porozumiały się w sprawie oceny bezpieczeństwa.
86.	ISACA	Art. 36b	- kwestia nieuregulowania - "Propozycja dodania dodatkowego ust. w brzmieniu: Bez uszczerbku dla ust. 1 CSIRT MON, CSIRT NASK, CSIRT GOV, lub CSIRT sektorowy mogą prowadzić w granicach swojej odpowiedzialności aktywne, nieinwazyjne skanowanie publicznie dostępnych sieci i systemów informatycznych podmiotów kluczowych i ważnych. Takie skanowanie przeprowadza się w celu wykrycia sieci i systemów informatycznych podatnych na zagrożenia lub skonfigurowanych bez właściwego zabezpieczenia i poinformowania o tym podmiotów, których to dotyczy. Sposób prowadzenia takiego skanowania musi minimalizować	Wyjaśnienie uwagi Kwestia ta jest już zawarta w projekcie.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

			możliwość wystąpienia negatywnego wpływu na funkcjonowanie usług świadczonych przez te podmioty." "Dodanie dodatkowego ustępu jest wskazane w celu zapewnienia zgodności z implementowaną dyrektywą (Artykuł 11 ust 3 przedostatni akapit) oraz umożliwienia wczesnego wykrywania podatności. Implementacja przepisu umożliwia CSIRT-om prowadzenie aktywnego, nieinwazyjnego skanowania, co jest zgodne z wymaganiami dyrektywy. Regularne skanowanie publicznie dostępnych sieci i systemów informatycznych pozwala na szybkie wykrycie potencjalnych zagrożeń, co jest kluczowe dla prewencyjnego działania i ochrony przed cyberatakami."	
87.	Polska Izba Informatyki i Telekomunikacji	Art. 36b	Art. 36b - ocena bezpieczeństwa systemu informacyjnego Projektu ustawy zakłada dodanie do ustawy o krajowym systemie cyberbezpieczeństwa nowych przepisów (rozdział 6a, art. 36b i następne) dotyczących oceny bezpieczeństwa systemów informacyjnych. W ustawie ma się pojawić m.in. art. 36b ust. 1, który w projekcie ustawy ma następujące brzmienie (podkreślenie własne): <i>Art. 36b. 1. Ocena bezpieczeństwa systemu informacyjnego może być przeprowadzona:</i> <i>1) za zgodą podmiotu krajowego systemu cyberbezpieczeństwa, wyrażoną w formie pisemnej lub formie elektronicznej pod rygorem nieważności lub</i> <i>2) na zlecenie organu właściwego do spraw cyberbezpieczeństwa.</i> Zwracamy uwagę na konsekwencje posłużenia się spójnikiem „lub”, który w języku prawniczym jest alternatywą. Użycie spójnika „lub” oznacza, że projektowany przepis dopuszcza możliwość przeprowadzanie oceny bezpieczeństwa systemu informacyjnego na zlecenie organu (punkt 2), bez konieczności uzyskania zgody podmiotu, który ma zostać poddany ocenie (punkt 1). Jeśli obecna redakcja przepisu jest wynikiem błędu, to błąd ten powinien zostać poprawiony. Jeśli jednak obecna redakcja jest zabiegiem celowym, to jako Izba uznajemy za nieakceptowalne i szkodliwe rozwiązanie, które pozwala prowadzić ocenę bezpieczeństwa systemu informacyjnego danego podmiotu bez zgody i wiedzy tego podmiotu. Zgoda podmiotu, wobec którego ma zostać przeprowadzona ocena bezpieczeństwa systemu informacyjnego, musi być warunkiem <i>sine qua non</i> przeprowadzania takiej oceny, a podmiot kluczowy i podmiot ważny musi mieć możliwość niewyrażenia zgody na udział w ocenie, bez ponoszenia z tego tytułu negatywnych konsekwencji ze strony organów właściwych do spraw cyberbezpieczeństwa. Prowadzenie takiej oceny bez zgody albo co gorsza bez wiedzy podmiotu, który jest poddawany ocenie, oznaczałoby, że oceniany podmiot prowadzoną ocenę postrzegałby jako wrogi atak i reagowałby zgodnie z procedurami przewidzianymi na okoliczność ataku, włączając w to poinformowanie organów ścigania o podejrzeniu popełnienia albo usiłowania popełnienia przestępstwa. Oczywiście zrozumiałe jest, że nie wszyscy pracownicy podmiotu poddawanego ocenie muszą i powinni wiedzieć, że trwa ocena, niemniej jednak osoby decyzyjne w podmiocie kluczowym lub ważnym muszą mieć taką wiedzę i muszą mieć możliwość świadomego podjęcia decyzji, czy chcą, aby	Wyjaśnienie uwagi Zlecenie oceny bezpieczeństwa przez OWCyber jest działaniem nadzorczym i jako takie nie może tu być wymagana zgoda podmiotu.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

			kierowana przez nich organizacja brała udział w takim badaniu. Biorąc powyższe pod uwagę widzimy potrzebę preredagowania analizowanego przepisu tak, aby jednoznacznie wynikało z niego, że w każdym przypadku zgoda podmiotu kluczowego albo podmiotu ważnego jest warunkiem przeprowadzania oceny bezpieczeństwa systemu informacyjnego takiego podmiotu. Można to osiągnąć albo przez zastąpienie spójnika „lub” spójnikiem „oraz” albo przez nadanie analizowanemu przepisowi następującego brzmienia: <i>Art. 36b. 1. Ocena bezpieczeństwa systemu informacyjnego może być przeprowadzona na zlecenie organu właściwego do spraw cyberbezpieczeństwa, za uprzednią zgodą podmiotu krajowego systemu cyberbezpieczeństwa, wyrażoną w formie pisemnej lub formie elektronicznej pod rygorem nieważności.</i>	
88.	Polskie Stowarzyszenie Fotowoltaiki	Art. 36a-36d	Przepisy art. 36a-36b KSC wg Projektu wprowadzają uprawnienie do przeprowadzenia oceny bezpieczeństwa systemów informacyjnych wykorzystywanych przez podmioty krajowego systemu cyberbezpieczeństwa w celu identyfikacji podatności przez CSIRT MON, CSIRT NASK, CSIRT GOV lub (za zgodą jednego z poprzednich) CSIRT sektorowy. Oceny bezpieczeństwa nie przeprowadza się wobec podmiotów w zbiorach ABW i Agencji Wywiadu, oraz akredytowanych na podstawie ustawy o ochronie informacji niejawnych. Ocena bezpieczeństwa: - może być przeprowadzona (1) za zgodą podmiotu lub (2) na zlecenie organu właściwego ds. cyberbezpieczeństwa; - jest przeprowadzana z uwzględnieniem zasady minimalizacji zakłócenia pracy systemu informacyjnego lub ograniczenia jego dostępności i nie może prowadzić do nieodwracalnego zniszczenia danych - wymaga uzgodnienia warunków przeprowadzenia oceny z podmiotem; - wymaga sporządzenia i przekazania podmiotowi raportu zawierającego podsumowanie przeprowadzonych w ramach oceny bezpieczeństwa czynności oraz wskazanie wykrytych podatności systemu informacyjnego. Ogólny wpływ regulacji: Projekt dopuszcza możliwość przeprowadzenia oceny bezpieczeństwa systemu informacyjnego pomimo braku zgody podmiotu krajowego systemu cyberbezpieczeństwa (tj. na zlecenie organu właściwego). Pomimo określenia pewnych wymogów dot. przeprowadzania oceny bezpieczeństwa, proces ten może w sposób istotny wpływać na bieżącą działalność operacyjną PK i PW. Ponadto, na gruncie Projektu nie jest jasne, w jaki sposób ww. wymogi będą zapewniane przez podmiot przeprowadzający ocenę jak również jakimi uprawnieniami będzie dysponował PK lub PW w celu zapewnienia stosowania ww. wymogów. W rezultacie, istnieje ryzyko naruszenia integralności danych i systemów poddawanych ocenie bezpieczeństwa.	Wyjaśnienie uwagi Ocena bezpieczeństwa wynika z przepisów dyrektywy NIS2. W przypadku dokonania szkody przez CSIRT przeprowadzający ocenę to znajdują zastosowanie przesłanki odpowiedzialności odszkodowawczej Skarbu Państwa.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

			Niezależnie, wskazane przepisy nie przewidują odstępstwa od przeprowadzania oceny bezpieczeństwa systemów informacyjnych, które są przedmiotem odpowiedniej certyfikacji. Wobec tego rodzaju systemów brak uzasadnienia dla doraźnej kontroli w ramach oceny bezpieczeństwa. W końcu, należy podkreślić na szeroką definicję systemu informacyjnego na gruncie KSC wg Projektu, która obejmuje m.in. <i>urządzenie lub grupę połączonych urządzeń elektrycznych lub elektronicznych i oprogramowania zaprogramowanych w celu przetwarzania danych</i>. Wpływ na sektor energetyczny: Jak wskazano powyżej, proces przeprowadzenia oceny bezpieczeństwa może prowadzić do naruszenia integralności danych i systemów poddawanych ocenie bezpieczeństwa. Ma to szczególnie wpływ na zarządzanie siecią za pomocą inteligentnych systemów opomiarowania (<i>Smart Metering</i>) przez przedsiębiorstwa energetyczne. Smart Metering, zgodnie z Dyrektywą Parlamentu Europejskiego i Rady (UE) 2019/944 z dnia 5 czerwca 2019 roku w sprawie wspólnych zasad rynku wewnętrznego energii elektrycznej, polega na optymalizacji wykorzystania energii elektrycznej, między innymi przez dostarczanie usług w zakresie zarządzania energią, rozwój innowacyjnych formuł cenowych i stosowanie inteligentnych systemów opomiarowania, które są interoperacyjne. Podstawą działania Smart Meteringu są inteligentne liczniki energii elektrycznej. Komunikacja z systemami informatycznymi magazynującymi, agregującymi i przekazującymi dane odbywa się poprzez koncentratory danych. Do najważniejszych funkcji liczników należy m.in. automatyczny odczyt zdalny, wykrywanie awarii, możliwość zdalnego odcięcia i przywrócenia dostawy, monitorowanie zużycia w czasie rzeczywistym. Drugim elementem Smart Meteringu jest tzw. koncentrator danych, czyli urządzenie/oprogramowanie używane do pozyskiwania danych z liczników, przekazywania zgromadzonych danych, definiowanie harmonogramów odczytowych. Trzecim podstawowym elementem Smart Meteringu jest system informatyczny. Mając na uwadze powyższe, zwracamy uwagę, że projektowana procedura przeprowadzenia oceny bezpieczeństwa wprowadza ryzyko naruszenia integralności danych i systemów poddawanych ocenie bezpieczeństwa, co w konsekwencji może prowadzić do destabilizacji dostaw energii elektrycznej. Ponadto, ewentualne negatywne następstwa oceny bezpieczeństwa mogą narazić poszczególne podmioty na poniesienie istotnych nakładów finansowych oraz organizacyjnych dla przedsiębiorstwa. [Nadregulacja względem Dyrektywy NIS2] Uprawnienie do przeprowadzenia oceny bezpieczeństwa pomimo braku zgody podmiotu wykracza istotnie poza ramy Dyrektywy NIS2. Przewiduje ona uprawnienie CSIRT do przeprowadzania oceny bezpieczeństwa (tzw. <i>security scan</i>), ale na wniosek PK lub PW (art. 11 ust. 3 lit e Dyrektywy NIS2).	

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

			Ponadto postanowienia dot. oceny bezpieczeństwa zaproponowane w Projekcie z 3 lipca 2023 r. zostały w całości inkorporowane z nieznacznymi zmianami do Projektu. Projekt z 3 lipca 2023 r. nie przewidywał bowiem odstępstwa od wymogu pozyskania zgody podmiotu na przeprowadzanie oceny bezpieczeństwa (vide projekt nowego art. 36e ust. 1). Rekomendacja: - wyłączenie możliwości przeprowadzania oceny bezpieczeństwa na zlecenie organu właściwego ds. cyberbezpieczeństwa i bez zgody podmiotu krajowego systemu cyberbezpieczeństwa; Alternatywnie: - objęcie wyłączeniem w art. 36a ust. 3 KSC wg Projektu systemów informacyjnych, wobec których została wydana odpowiednia certyfikacja; - konkretyzacja zakresu systemów informatycznych, które mogą zostać objęte oceną bezpieczeństwa; - zapewnienie: • podmiotom krajowego systemu odpowiednich uprawnień cyberbezpieczeństwa w celu zagwarantowania prawidłowego przebiegu oceny bezpieczeństwa; • poufności przeprowadzanej oceny bezpieczeństwa równoległe do informacji i danych, które zostały w jej ramach wytworzone.	
89.	Cybermadeinpol and	Art. 36b	Art. 36b. 6. - zmiana brzmienia na: 6. Informacje uzyskane przez CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT sektorowy w wyniku przeprowadzania oceny bezpieczeństwa systemu informacyjnego stanowią tajemnicę prawnie chronioną i nie mogą być wykorzystane do realizacji innych zadań ustawowych CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT sektorowe oraz podlegają one niezwłocznemu trwałemu i nieodwracalnemu zniszczeniu, które przeprowadza komisja i które dokumentuje się protokołem zniszczenia tych informacji.	Uwaga uwzględniona Przepis zostanie zmieniony.
90.	Fundacja Bezpieczna Cyberprzestrzeń	Art. 36a	Art. 1 pkt 35, treść art. 36a ust. 1 – wydaje się, że w treści przepisu powinno się zastosować analogiczną terminologię, jak w przepisach art. 33 ust. 1, gdyż cel tych przepisów jest tożsamy tj. identyfikacja podatności. W związku z powyższym proponuje się art. 36a ust. 1 nadać następujące brzmienie: „1. CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT sektorowy mogą przeprowadzić ocenę bezpieczeństwa produktów ICT, usług ICT lub procesów ICT wykorzystywanych przez pomioty krajowego systemu cyberbezpieczeństwa.”. W pozostałych przepisach art. 36 analogicznie dokonać zmian (w odpowiedniej formie) wyrazów „systemu informacyjnego” na „, produktów ICT, usług ICT lub procesów ICT”. Ponadto w kontekście podobieństwa celu przepisów art. 33 i rozdziału 6a (co znajduje potwierdzenie w uzasadnieniu do ustawy w punkcie 2.13: „Celem oceny bezpieczeństwa jest pomoc w identyfikacji podatności. Ma ona charakter prewencyjny.”) prosimy o wyjaśnienie różnicy pomiędzy badaniem produktów ICT, usług ICT lub procesów ICT a oceną bezpieczeństwa systemu informacyjnego. Natomiast jeśli ta różnica nie jest jednoznaczna, proponuje się integrację (w raz z odpowiednim dostosowanie) art. 33 z przepisami Rozdziału 6a.c	Wyjaśnienie uwagi Art. 33 dotyczy testowania pojedynczych elementów systemów – czyli produktów czy usług ICT. Ocena bezpieczeństwa dotyczy oceny samych systemów.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

91.	Osoba fizyczna	Art. 36a	Ust. 1 – Zastosowano zapis „ocenę bezpieczeństwa systemów informacyjnych”, z kolei w art. 26 zastosowano „badania urządzenia informatycznego lub oprogramowania”, a w art. 33 zastosowano zapis „badanie produktu ICT, usługi ICT lub procesu ICT”. Proponuję dokonać weryfikacji intencji, co zdefiniowania przedmiotu, celu i zakresu oceny. Proponuję przyjąć spójne i konsekwentne podejście.	Wyjaśnienie uwagi Art. 33 dotyczy badania elementu systemu, a ocena bezpieczeństwa dotyczy badania systemów.
92.	Polska Izba Gospodarki Odpadami	Art. 36b	Art. 1 ust. 35) w zakresie dodanego Art. 36b ust. 1. Pkt 1) KSC – proponujemy wykreślenie formę elektroniczną zgody na przeprowadzenie oceny bezpieczeństwa systemu informacyjnego.	Uwaga nieuwzględniona Naszym zdaniem należy promować formę elektroniczną, zwłaszcza, że podmiot może skorzystać z darmowych podpisów elektronicznych jak podpis osobisty czy podpis zaufany.
93.	Rada Bezpieczeństwa Biznesowego Grupy MiSOT	Art. 36b	Art 36b. 4. CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT sektorowy o może wytwarzać lub pozyskiwać ogólnie dostępne urządzenia lub programy komputerowe, o których mowa w art. 269b ustawy z dnia 6 czerwca 1997 r. – Kodeks karny (Dz. U. z 2024 r. poz. 17), oraz ich używać w celu określenia podatności ocenianego systemu informacyjnego na możliwość popełnienia przestępstw, o których mowa w art. 165 § 1 pkt 4, art. 267 § 3, art. 268a § 1 albo § 2 w związku z § 1, art. 269 § 1 i 2 albo art. 269a ustawy z dnia 6 czerwca 1997 r. – Kodeks karny.”. Uzasadnienie: Artykuł 36b w brzmieniu z projektu dopuszcza każde narzędzie do przełamывania zabezpieczeń. Informujemy zatem, że są narzędzia, które nie są dostępne na rynku. Mogą z tych narzędzi korzystać jedynie Państwa lub wywiady typu PRISM czy PEGASUS. Nie jesteśmy w stanie bronić się przed tymi narzędziami, zwłaszcza jeżeli idzie o wywiady sojusznicze. Nie ma też sensu wprowadzać takiego zwolnienia dla CSIRTów. Uznajemy, że CSIRT powinien dokonywać oceny bezpieczeństwa, ale z użyciem takich narzędzi, które sam wytworzy lub będzie w stanie uzyskać w sposób, który uzyskałby każdy cyberprzestępca. Dlatego proponujemy zmianę zapisu gwarantującą zakaz używania w stosunku do podmiotów ważnych i kluczowych narzędzi przełamывania zabezpieczeń dostępnych tylko dla Rządów. Nie trzeba tego sprawdzać, nie jesteśmy na to odporni. Dlatego proponujemy zapis “ogólnie dostępnych”.	Uwaga nieuwzględniona Takie brzmienie przepisu spowoduje, że nie można będzie przeprowadzać testów bezpieczeństwa za pomocą mało dostępnych programów, które dla niektórych grup np. hakywistów mogą być dostępne.
94.	Cybermadeinpol and	Art. 36b	Art. 36b. 6. - zmiana brzmienia na: 6. Informacje uzyskane przez CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT sektorowy w wyniku przeprowadzania oceny bezpieczeństwa systemu informacyjnego stanowią tajemnicę prawnie chronioną i nie mogą być wykorzystane do realizacji innych zadań ustawowych CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT sektorowe oraz podlegają one niezwłocznemu trwałemu i nieodwracalnemu zniszczeniu, które przeprowadza komisja i które dokumentuje się protokołem zniszczenia tych informacji.	Uwaga uwzględniona Przepis zostanie zmieniony.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

95.	Polska Izba Gospodarki Odpadami	Art. 36b	Art. 1 ust. 35) w zakresie dodanego Art. 36b ust. 7. KSC – proponujemy uwzględnić dodatkowo w składzie komisji przedstawicieli podmiotu, w stosunku do którego prowadzona jest ocena, którzy nie mogliby uczestniczyć w komisyjnym zniszczeniu informacji w przypadku przełamania zabezpieczeń.	Uwaga nieuwzględniona Takie brzmienie może naruszyć ochronę informacji w CSIRT przeprowadzających badanie.
96.	Polskie Towarzystwo Informatyczne	Art. 36b	W dodanym rozdziale 6a Ocena bezpieczeństwa Art. 36b ust. 4 wydaje się zbędny w związku z brzmieniem Art. 296b § 1a Kodeksu Karnego, gdyż cel tam wymieniony w całości pokrywa się z celem w jakim mogą działać wymienione CSIRT-y (działanie w celu zabezpieczenia systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej przed popełnieniem przestępstw).	Uwaga nieuwzględniona Przepis ma zapewnić wyraźną podstawę prawną do podejmowania tego typu działań.
97.	Stowarzyszenie Absolwentów Studiów Cyberbezpieczeństwa MBA	Art. 36b	W projektowanym przepisie art. 36b pkt 5 odpowiednie CISRT-y przy wykorzystywaniu narzędzi, tzw. exploitów mogą dokonać przełamania zabezpieczeń infrastruktury i uzyskać informacje chronioną lub dokonać ekspansji na sieci technologiczne. W przypadku działań związanych z testami penetracyjnymi, działania takie w środowisku produkcyjnym automatyki przemysłowej grozi uszkodzeniem, zniszczeniem procesu technologicznego, a w skrajnych warunkach katastrofą. Warto nadmienić, że ustawodawca nie wymaga od CSIRTu wskazania narzędzi oraz miejsc w infrastrukturze, gdzie będzie wykonywany test penetracyjny. W związku z powyższym rodzi się ryzyko pozostawienia tzw. backdoor-a (tylnych drzwi), w przypadku używania exploitów, które mogą posiadać w sobie takie luki (np. incydent związany z backdoorem Webshell C99, który miał ukryte tylne drzwi dla autora tego skryptu). Dodatkowo w związku z licznymi incydentami bezpieczeństwa z wykorzystywaniem oprogramowania NSO Group - Pegasus, przepis może być wykorzystywany do inwigilacji przez organ władzy dość szerokiej listy podmiotów KSC. W związku z powyższym ramowe warunki testów powinny uwzględniać opisane wyżej wyzwaenia dla systemów przemysłowych odpowiednie kompetencje osób przeprowadzających testy bezpieczeństwa, szczegółową checklistę zadań, wykaz narzędzi oraz testy powinny być nagrywane. Należy też uwzględnić infrastruktury teleinformatyczne wyższego ryzyka, które nie powinny być badane w sposób aktywny.	Wyjaśnienie uwagi Przed podjęciem oceny bezpieczeństwa CSIRT zawiera porozumienie z podmiotem – siłą rzeczy wtedy podmiot wie o prowadzonym badaniu. W porozumieniu określa się też rodzaje prowadzonych testów.
98.	ISSA Polska	Art. 36b	W art. 36b pkt 5 odpowiednie CISRT-y przy wykorzystywaniu narzędzi, tzw. Exploitów mogą dokonać przełamania zabezpieczeń infrastruktury i uzyskać informacje chronioną lub dokonać ekspansji na sieci technologiczne. W przypadku działań związanych z testami penetracyjnymi, działania takie w środowisku produkcyjnym automatyki przemysłowej grozi uszkodzeniem, zniszczeniem procesu technologicznego, a w skrajnych warunkach katastrofą. Warto nadmienić, że ustawodawca nie wymaga od CSIRTu wskazania narzędzi oraz miejsc w infrastrukturze, gdzie będzie wykonywany test penetracyjny. W związku z powyższym rodzi się ryzyko pozostawienia tzw. backdoor-a (tylnych drzwi), w przypadku używania exploitów, które mogą posiadać w sobie takie luki (np. incydent związany z backdoorem Webshell C99, który miał ukryte tylne drzwi dla autora tego skryptu).	Wyjaśnienie uwagi Przed podjęciem oceny bezpieczeństwa CSIRT zawiera porozumienie z podmiotem – siłą rzeczy wtedy podmiot wie o prowadzonym badaniu. W porozumieniu określa się też rodzaje prowadzonych testów.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

			Dodatkowo w związku z licznymi incydentami bezpieczeństwa z wykorzystywaniem oprogramowania NSO Group - Pegasus, przepis może być wykorzystywany do inwigilacji przez organ władzy dość szerokiej listy podmiotów KSC. W związku z powyższym ramowe warunki testów powinny uwzględniać odpowiednie kompetencje osób przeprowadzających testy bezpieczeństwa, szczegółową checklistę zadań, wykaz narzędzi oraz testy powinny być nagrywane. Należy też uwzględnić infrastruktury teleinformatyczne wyższego ryzyka, które nie powinny być badane w sposób aktywny.	
99.	Związek Telewizji Kablowych Izba Gospodarcza	Art. 36b	Błąd redakcyjnej natury W art. 1 pkt. 35 projektu ustawy zmieniającej ustawę o KSC w art. 36 b ust. 4 ustawy o KSC po słowie „sektorowy” należy skreślić zbędną literę „o”.	Uwaga uwzględniona Litera „o” zostanie usunięta
100.	Cybermadeinpol and	Art. 39	Art. 39 5. - zmiana brzmienia na: 5. Dane, o których mowa w ust. 3 i 4, są usuwane lub niszczone w sposób trwały i nieodwracalny lub anonimizowane przez CSIRT MON, CSIRT NASK i sektorowy zespół cyberbezpieczeństwa niezwłocznie po stwierdzeniu, że nie są niezbędne do realizacji zadań, o których mowa w art. 26 ust. 3 pkt 1–11, 14 i 15 i ust. 5–8 oraz art. 44 ust. 1–3.	Wyjaśnienie uwagi Zgodnie z uwagą UODO pozostawimy jedynie pojęcie anonimizacji.
101.	Cybermadeinpol and	Art. 39	Art. 39 6. - zmiana brzmienia na: 6. Dane, o których mowa w ust. 3 i 4, niezbędne do realizacji zadań, o których mowa w art. 26 ust. 3 pkt 1–11, 14 i 15 i ust. 5–8 oraz art. 44 ust. 1–3, są usuwane lub niszczone w sposób trwały i nieodwracalny lub anonimizowane przez CSIRT MON, CSIRT NASK i sektorowy zespół cyberbezpieczeństwa w terminie 5 lat od zakończenia obsługi incydentu, którego dotyczą.	Wyjaśnienie uwagi Zgodnie z uwagą UODO pozostawimy jedynie pojęcie anonimizacji.
102.	ZBP	Art. 39 ust. 1-3 oraz ust. 7-8	1. W celu realizacji zadań, o których mowa w art. 26 ust. 3 pkt 1-11, 14 i 15 i ust. 5-8 oraz art. 44 ust. 1-3, CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT Sektorowe przetwarzają dane pozyskane w związku z incydentami i cyberzagrożeniami, w tym dane osobowe, obejmujące także dane określone w art. 9 ust. 1 i art. 10 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), zwanego dalej "rozporządzeniem 2016/679", w zakresie i w celu niezbędnym do realizacji tych zadań. 2. CSIRT MON, CSIRT NASK i CSIRT Sektorowe, przetwarzając dane osobowe określone w art. 9 ust. 1 i art. 10 rozporządzenia 2016/679, prowadzą analizę ryzyka, stosują środki ochrony przed złośliwym oprogramowaniem oraz mechanizmy kontroli dostępu, a także opracowują procedury bezpiecznej wymiany informacji. 3. CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT sektorowe przetwarzają dane osobowe pozyskane w związku z incydentami i zagrożeniami cyberbezpieczeństwa:	Uwaga nieuwzględniona Nie planuje się takich zmian.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

		1) dotyczące użytkowników systemów informacyjnych oraz użytkowników telekomunikacyjnych urządzeń końcowych; 2) dotyczące telekomunikacyjnych urządzeń końcowych w rozumieniu art. 2 pkt 43 ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne; „3) gromadzone przez podmioty kluczowe i podmioty ważne w związku ze świadczeniem usług; 4) dotyczące podmiotów zgłaszających incydent zgodnie z art. 30 ust. 1.”, [...] 7. W celu realizacji zadań określonych w ustawie CSIRT MON, CSIRT NASK, CSIRT GOV i sektorowe zespoły cyberbezpieczeństwa mogą przekazywać sobie wzajemnie dane, o których mowa w ust. 3, w zakresie niezbędnym do realizacji tych zadań i współpracować z organem właściwym do spraw ochrony danych osobowych. 8. Przetwarzanie przez CSIRT MON, CSIRT NASK i CSIRT sektorowe zespoły cyberbezpieczeństwa danych, o których mowa w ust. 3, nie wymaga realizacji obowiązków wynikających z art. 15, art. 16, art. 18 ust. 1 lit. a i d oraz art. 19 zdanie drugie rozporządzenia 2016/679, jeżeli uniemożliwiłoby to realizację zadań CSIRT NASK, CSIRT MON i CSIRT sektorowych, o których mowa w art. 26 ust. 3 pkt 1–11, 14 i 15 i ust. 5–8 oraz art. 44 ust. 1–3, i jest możliwe, gdy CSIRT MON, CSIRT NASK i CSIRT sektorowe prowadzą analizę ryzyka, stosują środki ochrony przed złośliwym oprogramowaniem, stosują mechanizmy kontroli dostępu oraz opracowują procedury bezpiecznej wymiany informacji 1. W celu realizacji zadań, o których mowa w art. 13, art. 26 ust. 3 pkt 1-11, 14 i 15 i ust. 5-8 oraz art. 44 ust. 1-3, CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT Sektorowe oraz centrum wymiany i analiz informacji przetwarzają dane pozyskane w związku z incydentami i cyberzagrożeniami, w tym dane osobowe, obejmujące także dane określone w art. 9 ust. 1 i art. 10 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), zwanego dalej "rozporządzeniem 2016/679", w zakresie i w celu niezbędnym do realizacji tych zadań. 2. CSIRT MON, CSIRT NASK i CSIRT Sektorowe oraz centrum wymiany i analiz informacji przetwarzając dane osobowe określone w art. 9 ust. 1 i art. 10 rozporządzenia 2016/679, prowadzą analizę ryzyka, stosują środki ochrony przed złośliwym oprogramowaniem oraz mechanizmy kontroli dostępu, a także opracowują procedury bezpiecznej wymiany informacji. 3. CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT sektorowe oraz centrum wymiany i analiz informacji przetwarzają dane osobowe pozyskane w związku z incydentami i zagrożeniami cyberbezpieczeństwa: 1) dotyczące użytkowników systemów informacyjnych oraz użytkowników telekomunikacyjnych urządzeń końcowych;	

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

			2) dotyczące telekomunikacyjnych urządzeń końcowych w rozumieniu art. 2 pkt 43 ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne; 3) gromadzone przez podmioty kluczowe i podmioty ważne w związku ze świadczeniem usług; 4) dotyczące podmiotów zgłaszających incydent zgodnie z art. 30 ust. 1., [...] 7. W celu realizacji zadań określonych w ustawie CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT sektorowe ~~zespoły cyberbezpieczeństwa~~ oraz centrum wymiany i analiz informacji mogą przekazywać sobie wzajemnie dane, o których mowa w ust. 3, w zakresie niezbędnym do realizacji tych zadań i współpracować z organem właściwym do spraw ochrony danych osobowych. 8. Przetwarzanie przez CSIRT MON, CSIRT NASK, CSIRT sektorowe ~~zespoły cyberbezpieczeństwa~~ oraz centrum wymiany i analiz informacji danych, o których mowa w ust. 3, nie wymaga realizacji obowiązków wynikających z art. 15, art. 16, art. 18 ust. 1 lit. a i d oraz art. 19 zdanie drugie rozporządzenia 2016/679, jeżeli uniemożliwiłoby to realizację zadań CSIRT NASK, CSIRT MON, CSIRT sektorowych oraz centrum wymiany i analiz informacji o których mowa w art. 13, art. 26 ust. 3 pkt 1–11, 14 i 15 i ust. 5–8 oraz art. 44 ust. 1–3, i jest możliwe, gdy CSIRT MON, CSIRT NASK, CSIRT sektorowe oraz centrum wymiany i analiz informacji, prowadzą analizę ryzyka, stosują środki ochrony przed złośliwym oprogramowaniem, stosują mechanizmy kontroli dostępu oraz opracowują procedury bezpiecznej wymiany informacji W związku z wprowadzeniem do treści UKSC oraz ustawy – Prawo Bankowe definicji centrum wymiany i analizy informacji oraz zakresu jego działań, konieczne jest zapewnienie odpowiednio doprecyzowanej podstawy przetwarzania danych osobowych przez ten podmiot oraz wymiany informacji z tym podmiotem.	
103.	Konfederacja Lewiatan	Art. 39a	Nieproporcjonalne uprawnienia Ministra Cyfryzacji do dostępu do wrażliwych danych osobowych (art. 39a ustawy KSC) Jednostka redakcyjna: art. 39a KSC Jednostka redakcyjna NIS2: nie dotyczy Uwaga: Art. 39a ustawy KSC, który upoważnia Ministra Cyfryzacji do dostępu do danych osobowych o szczególnie wrażliwym charakterze, budzi poważne obawy dotyczące prywatności i ochrony danych osobowych. Mowa tutaj o danych, których przetwarzanie jest szczegółowo regulowane przez art. 9 ust. 1 i art. 10 RODO, obejmujących informacje o rasie, orientacji seksualnej, poglądach politycznych, przekonaniach religijnych, przynależności do związków zawodowych, a także dane genetyczne, biometryczne oraz zdrowotne. Chociaż koncepcja serwisu umożliwiającego użytkownikom weryfikację, czy ich dane zostały w sposób nieuprawniony ujawnione, jest wartościowa, to jednak zapisy pozwalające na dostęp do tak delikatnych informacji przez organ administracji publicznej, bez wyraźnych, restrykcyjnych zabezpieczeń i ograniczeń, są niepokojące. Jest to szczególnie problematyczne w świetle wymagań RODO, które	Uwaga uwzględniona Przepis został zmieniony w ten sposób, że stanowić będzie art. 26c jako zadanie CSIRT NASK, a uzupełniać go będzie art. 39 w zmienionym brzmieniu. Doprecyzowano również uzasadnienie w tym zakresie.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

			nakłada na państwa członkowskie obowiązek zapewnienia wysokiego poziomu ochrony danych osobowych, w szczególności tych o wrażliwym charakterze. Brak jasnych mechanizmów kontrolnych, przejrzystości działań oraz odpowiednich środków zabezpieczających te dane przed nadużyciem stanowi realne zagrożenie dla praw i wolności obywateli, co może prowadzić do nadmiernej inwigilacji i naruszenia prywatności przez państwo. Tego typu uprawnienia powinny być otoczone szczególną ostrożnością i zabezpieczone solidnymi gwarancjami proceduralnymi oraz nadzorcami, aby zapobiec jakimkolwiek nadużyciom.	
104.	ISSA Polska	Art. 39a	Art. 39a ustawy KSC, który upoważnia Ministra Cyfryzacji do dostępu do danych osobowych o szczególnie wrażliwym charakterze, budzi poważne obawy dotyczące prywatności i ochrony danych osobowych. Mowa tutaj o danych, których przetwarzanie jest szczegółowo regulowane przez art. 9 ust. 1 i art. 10 RODO, obejmujących informacje o rasie, orientacji seksualnej, poglądach politycznych, przekonaniach religijnych, przynależności do związków zawodowych, a także dane genetyczne, biometryczne oraz zdrowotne. Chociaż koncepcja serwisu umożliwiającego użytkownikom weryfikację, czy ich dane zostały w sposób nieuprawniony ujawnione, jest wartościowa, to jednak zapisy pozwalające na dostęp do tak delikatnych informacji przez organ administracji publicznej, bez wyraźnych, restrykcyjnych zabezpieczeń i ograniczeń, są niepokojące. Jest to szczególnie problematyczne w świetle wymagań RODO, które nakłada na państwa członkowskie obowiązek zapewnienia wysokiego poziomu ochrony danych osobowych, w szczególności tych o wrażliwym charakterze. Brak jasnych mechanizmów kontrolnych, przejrzystości działań oraz odpowiednich środków zabezpieczających te dane przed nadużyciem stanowi realne zagrożenie dla praw i wolności obywateli, co może prowadzić do nadmiernej inwigilacji i naruszenia prywatności przez państwo. Tego typu uprawnienia powinny być otoczone szczególną ostrożnością i zabezpieczone solidnymi gwarancjami proceduralnymi oraz nadzorcami, aby zapobiec jakimkolwiek nadużyciom.	Uwaga uwzględniona Przepis został zmieniony w ten sposób, że stanowić będzie art. 26c jako zadanie CSIRT NASK, a uzupełniać go będzie art. 39 w zmienionym brzmieniu. Doprecyzowano również uzasadnienie w tym zakresie.
105.	Stowarzyszenie Absolwentów Studiów Cyberbezpieczeństwa MBA	Art. 39a	Przepis art. 39a ustawy KSC, który upoważnia Ministra Cyfryzacji do dostępu do danych osobowych o szczególnie wrażliwym charakterze, budzi poważne obawy dotyczące prywatności i ochrony danych osobowych. Mowa tutaj o danych, których przetwarzanie jest szczegółowo regulowane przez art. 9 ust. 1 i art. 10 RODO, obejmujących informacje o rasie, orientacji seksualnej, poglądach politycznych, przekonaniach religijnych, przynależności do związków zawodowych, a także dane genetyczne, biometryczne oraz zdrowotne. Chociaż koncepcja serwisu umożliwiającego użytkownikom weryfikację, czy ich dane zostały w sposób nieuprawniony ujawnione, jest wartościowa, to jednak przepisy pozwalające na dostęp do danych szczególnie wrażliwych przez organ administracji publicznej, bez wyraźnych, restrykcyjnych zabezpieczeń i ograniczeń, są niepokojące. Jest to szczególnie problematyczne w świetle wymagań RODO, które nakłada na państwa członkowskie obowiązek zapewnienia wysokiego poziomu ochrony danych osobowych, w szczególności tych o wrażliwym charakterze.	Uwaga uwzględniona Przepis został zmieniony w ten sposób, że stanowić będzie art. 26c jako zadanie CSIRT NASK, a uzupełniać go będzie art. 39 w zmienionym brzmieniu. Doprecyzowano również uzasadnienie w tym zakresie.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

			Brak jasnych mechanizmów kontrolnych, przejrzystości działań oraz odpowiednich środków zabezpieczających te dane przed nadużyciem stanowi realne zagrożenie dla praw i wolności obywateli, co może prowadzić do nadmiernej inwigilacji i naruszenia prywatności przez państwo. Tego typu uprawnienia powinny być otoczone szczególną ostrożnością i zabezpieczone solidnymi gwarancjami proceduralnymi oraz nadzorcami, aby zapobiec jakimkolwiek nadużyciom.	
106.	Fundacja Bezpieczna Cyberprzestrzeń	Art. 40	Art. 1 pkt 40 lit. b, treść art. 40 pkt. 9a – proponuje się nadanie sektorowi i tym samym punktowi 9a nazwy odpowiadającej przepisom ustawy o zbiorowym zaopatrzeniu w wodę i odprowadzaniu ścieków tj. „9a. dla sektora zbiorowego odprowadzania ścieków – minister właściwy do spraw go[?]pod[rki wod[?]j;”.	Uwaga uwzględniona
107.	Osoba fizyczna	Art. 40	Wg mnie woda pitna i Ścieki powinny tworzyć wspólny sektor. <u>Uzasadnienie:</u> Większość podmiotów kluczowych z tych sektorów wykonują działalność w obydwu sektorach. Jeżeli to będą dwa różne sektory i będą miały dwa CSIRT sektorowe to może zaistnieć obowiązek wysyłania informacji o incydentach i późniejszych raportów do dwóch CSIRT sektorowych.	Uwaga nieuwzględniona Dyrektywa NIS2 traktuje te sektory odrębnie.
108.	Fundacja Bezpieczna Cyberprzestrzeń	Art. 41	Art. 1 pkt 40 dotyczy Art. 41, który w propozycji nowelizacji ma odnosić się zgodnie z proponowaną zmianą w literze a) tylko do podmiotów kluczowych, natomiast zostały wymienione podmioty ważne w punktach 9d) do 9g).	Uwaga uwzględniona
109.	ISAC-Kolej	Art. 41	Organami właściwymi do spraw cyberbezpieczeństwa dla podmiotów działających w sektorach lub podsektorach regulowanych powinien być regulator danego rynku. Tak jak dla sektora bankowego i infrastruktury rynków finansowych organem właściwym jest KNF, a dla sektora infrastruktury cyfrowej podsektora komunikacji elektronicznej UKE, tak dla sektora transportu kolejowego powinien być Urząd Transportu Kolejowego (UTK). Warto rozważyć by organy właściwe były określone w załączniku nr 1 i być przypisane do podmiotu działającego w danym sektorze lub podsektorze	Uwaga nieuwzględniona Minister Infrastruktury pełni tę rolę od kilku lat i zbudował już ku temu odpowiednie kompetencje.
110.	Polska Izba Informatyki i Telekomunikacji	Art. 41	Art. 41 – organy właściwe do spraw cyberbezpieczeństwa Przyjęta na gruncie ustawy o krajowym systemie cyberbezpieczeństwa logika wyznaczania organów właściwych do spraw cyberbezpieczeństwa wydaje się nie uwzględniać w wystarczającym stopniu realiów rynkowych i faktu, że wiele przedsiębiorstwa prowadzi równolegle działalność w dwóch lub większej ilości sektorów. Logika przyjęta w ustawie powoduje, że wielosektorowe podmioty kluczowe i ważne będą jednocześnie podlegać kontroli i nadzorowi dwóch, trzech albo większej ilości organów właściwych, co jest rozwiązaniem dalekim od optymalnego. Tytułem przykładu wyobraźmy sobie przedsiębiorcę telekomunikacyjnego, który nie tylko świadczy usługi telekomunikacyjne i dostarcza sieć telekomunikacyjną, ale jednocześnie świadczy usługi DNS i CDN (co jest stosunkowo powszechną praktyką na rynku telekomunikacyjnym), a na dodatek sprzedaje energię elektryczną. Od razu zaznaczmy również, że nie jest to przykład teoretyczny, bowiem istnieją podmioty, które prowadzą działalność w takim właśnie zakresie i nie	Wyjaśnienie uwagi Multisektorowość wynika z samej dyrektywy NIS2. W projekcie zostaną zaproponowane rozwiązania, które umożliwią wspólne prowadzenie działań nadzorczych przez organy właściwe do spraw Cyberbezpieczeństwa.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

			są to przypadki odosobnione (spadająca rentowność działalności telekomunikacyjnej zmusza przedsiębiorców telekomunikacyjnych do szukania przychodów na innych rynkach). Podmiot taki, jako potencjalny podmiot kluczowy, zgodnie z przepisami ustawy będzie podlegał kontroli i nadzorowi co najmniej trzech organów właściwych: • Prezesa Urzędu Komunikacji Elektronicznej – jako podmiot kluczowy z podsektora komunikacji elektronicznej; • ministra właściwego ds. informatyzacji – jako podmiot kluczowy świadczący usługi takie jak DNS czy CDN; • ministra właściwego ds. energii – jako podmiot kluczowy sprzedający energię elektryczną. W praktyce pojawią się podmioty kluczowe podlegające nawet większej licznie organów. Z powodów oczywistych sytuacja, w której ten sam podmiot ma podlegać dwóm, trzem albo większej ilości organów kontroli i nadzoru nie jest sytuacją optymalną, w szczególności, że każdy z tych organów będzie przecież mógł i chciał egzekwować swoje kompetencje w tym samym obszarze, czyli w obszarze wymogów związanych z cyberbezpieczeństwem. Konflikty, sprzeczności a co najmniej brak spójności są wręcz wpisane w taki model. Szczególnie kłopotliwy może być fakt, że nawet w sektorze „infrastruktura cyfrowa” pojawią się dwa organy (Prezes UKE dla podsektora komunikacja elektroniczna i Minister Cyfryzacji dla pozostałej części infrastruktury cyfrowej), które będą miały kompetencje kontrolne i nadzorcze wobec bardzo zbliżonych usług i obszarów. Przykładowo usługa dostępu do Internetu to na gruncie UKSC będzie obszarem zainteresowania Prezesa UKE, ale już usługi DNS i CDN (które technicznie są powiązane z usługą dostępu do sieci Internet i transmisją danych) ma być przedmiotem kontroli i nadzoru ze strony Ministra Cyfryzacji. Żeby dopełnić obrazek trzeba też przypomnieć, że Prezes UKE jest organem nadzorowanym przez Ministra Cyfryzacji. Prosimy Projektodawcę o ponowne przeanalizowanie tego rozwiązania i tam gdzie to możliwe uproszczenie systemu tak, aby wyeliminować albo ograniczyć do minimum przypadki, w których ten sam podmiot kluczowy albo podmiot ważny podlega w zakresie cyberbezpieczeństwa więcej niż jednemu organowi. W szczególności prosimy o uproszczenie systemu dla podmiotów działających w sektorze „infrastruktura cyfrowa”, tak, aby dla całego tego sektora był tylko jeden organ właściwy. Organem tym powinien być Prezes UKE, biorąc pod uwagę doświadczenie Urzędu Komunikacji Elektronicznej w sprawowaniu nadzoru nad rynkiem telekomunikacyjnym.	
111.	Fundacja Bezpieczna Cyberprzestrzeń	Art. 41b	Art. 1 pkt 41, treść art. 41b ust. 1 – wydaje się, że Szef Agencji Bezpieczeństwa Wewnętrznego nie powinien pełnić roli organu właściwego, biorąc pod uwagę zadania organów właściwych wskazane w przepisach art. 42 – art. 44f. Rozdzielenie funkcji zarządczych, operacyjnych (którymi Szef ABW dysponuje poprzez będący w strukturze ABW CSIRT GOV) i kontrolnych jest jedną z kluczowych zasad bezpieczeństwa. Wydaje się, że objęcie szczególnym nadzorem podmiotów wskazanych w tym przepisie może być dokonane na podstawie innych ustaw np. o zarządzaniu kryzysowym lub ustawy o ABW. Wydaje się, że rolę organu właściwego należy	Uwaga uwzględniona Rolę tę będzie pełnił Minister właściwy do spraw informatyzacji.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

			przypisać ministrowi-członkowi Rady Ministrów właściwemu do spraw koordynowania działalności służb specjalnych lub Prezesowi Rady Ministrów lub integracji ust. 1 i ust. 2 art. 41b i powierzenie roli organu właściwego dla połączonego zbioru podmiotów ministrowi właściwemu do spraw informatyzacji. Ponadto niejasne jest sformułowanie w pkt. 1 „z wyjątkiem wymienionych w ust. 5 i 6”. W przywoływanym art. 9 ustawy o finansach publicznych nie ma takiej jednostki redakcyjnej, podobnie jak w projektowanym art. 41b.	
112.	Osoba fizyczna	Art. 41-41b	Ust. 1 – Zastosowano we wprowadzeniu zapisy określające organy właściwe dla typów podmiotów, odpowiednio kluczowych, ważnych i w sektorze administracji publicznej. Podmioty kluczowe i ważne są typowane z załącznika 1 i 2 ze względu na wielkość. Proponuję zdefiniować organy właściwe dla sektorów bez względu na typ podmiotów.	Uwaga uwzględniona
113.	Polskie Stowarzyszenie Fotowoltaiki	Art. 43 ust. 1	Obowiązek udzielania przez podmiot, o którym mowa w Załączniku nr 1 lub nr 2 informacji w celu wstępnej oceny możliwości kwalifikacji jako PK lub PW. Ogólny wpływ regulacji: <i>Brak istotnego wpływu</i> Wpływ na sektor energetyczny jw. – brak specyficznego wpływu na sektor energetyczny	Wyjaśnienie uwagi Dziękujemy za zgłoszenie uwagi.
114.	Akademia Górniczo-Hutnicza	Art. 44	Wskazane jest rozszerzenie zakresu podmiotów mogących pełnić zadania CSIRT sektorowego. Art 44a i 44b wskazują, że zadania CSIRT sektorowego mogą zostać powierzone “jednostce [...] podległej albo przez [...] nadzorowanej” przez Organ właściwy do spraw cyberbezpieczeństwa albo Minister będący organem właściwym do spraw cyberbezpieczeństwa dla kilku sektorów lub podsektorów. Wskazane jest, aby rozszerzyć ten katalog również dopuszczając do pełnienia zadań CSIRT sektorowego inne podmioty publiczne i/lub komercyjne, które spełnią warunki określone przez Organ właściwy do spraw cyberbezpieczeństwa.	Wyjaśnienie uwagi CSIRT sektorowym może być także państwowa osoba prawna, która posiada takie zdolności. Powierzenie zadania publicznego w postaci funkcjonowania CSIRT sektorowego podmiotom prywatny rodzi pytania o m. in. o poufność przekazywanych tak wrażliwych informacji. Potencjalnie CSIRTem sektorowym byłby podmiot – konkurent podmiotów kluczowych i ważnych z tego samego sektora. Ograniczałoby to zaufanie przy zgłaszaniu incydentów.
115.	Osoba fizyczna	Art. 44	Ust. 1 – zastosowano zapisy wskazujące zakres zadań CSIRT sektorowego. Proponuję w wyliczeniu dodać: „1) przyjmowanie zgłoszeń o potencjalnych zdarzeniach dla cyberbezpieczeństwa, 2) przyjmowanie zgłoszeń o wczesnych ostrzeżeniach”. Proponowany dodatkowy zakres zadań wynika wprost z zapisów uKSC2 sformułowanych w innym miejscu jako obowiązki raportowe podmiotów. (ref. Art. 11 ust.1).	Uwaga uwzględniona
116.	ZBP	Art. 44	CSIRT sektorowy może, w szczególności: (...)	Uwaga nieuwzględniona

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

		ust. 1b pkt 4	1b. w ramach reagowania na incydent poważny wystąpić do organu właściwego do spraw cyberbezpieczeństwa z wnioskiem o wezwanie podmiotu kluczowego i podmiotu ważnego, aby w wyznaczonym terminie usunął podatności, które doprowadziły lub mogłyby doprowadzić do incydentu poważnego. CSIRT sektorowy informuje o złożeniu wniosku właściwy CSIRT MON, CSIRT NASK albo CSIRT GOV; CSIRT sektorowy może, w szczególności: (...) 1b. w ramach reagowania na incydent poważny wystąpić do organu właściwego do spraw cyberbezpieczeństwa z wnioskiem o wezwanie podmiotu kluczowego i podmiotu ważnego, aby w wyznaczonym terminie usunął lub zmitygował podatności, które doprowadziły lub mogłyby doprowadzić do incydentu poważnego. CSIRT sektorowy informuje o złożeniu wniosku właściwy CSIRT MON, CSIRT NASK albo CSIRT GOV; Proponowana zmiana ma na celu umożliwienie zmitygowania podatności, w przypadku gdy nie można jej usunąć. Przyjęcie takiej zmiany daje gwarancje, że podmiot kluczowy lub podmiot ważny będzie w stanie szybko wprowadzić środki naprawcze przy obsłudze incydentu. Poprzez mitygację rozumie się całokształt działań mających na celu ograniczenie możliwości materializacji ryzyka związaną ze zidentyfikowaną podatnością, bez usuwania przyczyny ich występowania.	Podmiot w miarę możliwości powinien usunąć podatność.
117.	Konfederacja Lewiatan	Art. 44a	Kontrowersje wokół możliwości powierzenia funkcji CSIRT sektorowego państwowym osobom prawnym (art. 44a ustawy KSC) Jednostka redakcyjna: art. 44a projektu KSC Jednostka redakcyjna NIS2: art. 15 Uwaga: Projekt nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa, który zakłada możliwość powierzenia funkcji CSIRT sektorowego różnorodnym państwowym osobom prawnym, wzbudza poważne wątpliwości co do skuteczności i właściwości takiego rozwiązania. Zgodnie z art. 44a ustawy KSC, funkcję tę mogą pełnić m.in. agencje wykonawcze, instytucje kultury, jednostki naukowe Polskiej Akademii Nauk, uczelnie publiczne oraz parki narodowe. Przykładowo mogą to być takie podmioty jak: Polski Instytut Sztuki Filmowej; Narodowy Instytut Fryderyka Chopina; Zakład Narodowy imienia Ossolińskich; Akademia Kopernikańska; uczelnia publiczna; Instytut Współpracy Polsko-Węgierskiej im. Wacława Felczaka; Instytut Rozwoju Języka Polskiego im. świętego Maksymiliana Marii Kolbego; czy dowolne przedsiębiorstwo państwowe. Przekazanie odpowiedzialności za cyberbezpieczeństwo sektora tak zróżnicowanym podmiotom, które często nie mają odpowiednich kompetencji, doświadczenia, ani struktur do efektywnego zarządzania kwestiami bezpieczeństwa informacyjnego, stawia pod znakiem zapytania racjonalność i efektywność takiego rozwiązania. Cyberbezpieczeństwo wymaga specjalistycznej wiedzy i narzędzi, a także szybkiej reakcji na incydenty, co w przypadku wielu wymienionych instytucji może być trudne do osiągnięcia. Nawet potencjalna możliwość powierzenia takich funkcji może budzić poważne zastrzeżenia.	Wyjaśnienie uwagi Odpowiedzialność za utworzenie CSIRT sektorowych spoczywa na organach właściwych, które najlepiej znają swój sektor i są w stanie wskazać podmiot dostosowany do pełnienia tych zadań. Proponowane rozwiązanie zapewni im elastyczność w doborze takich podmiotów. Oparte jest na rozwiązaniach w zakresie sektorowych zespołów cyberbezpieczeństwa na podstawie których funkcjonuje m.in. Centrum e-zdrowia.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

118.	ISSA Polska	Art. 44a-44c	Kontrowersje wokół możliwości powierzenia funkcji CSIRT sektorowego państwowym osobom prawnym (art. 44a – 44c ustawy KSC) Zgodnie z art. 2 pkt. 3a ustawy o KSC definicja CSIRT sektorowy to Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego, działający na poziomie sektora lub podsektora (...). Pojęcie to zastępuje wcześniejsze sformułowanie „sektorowy zespół cyberbezpieczeństwa”. Jest to podmiot, który obok głównych CSIRT (NASK, GOV, MON) bierze udział w komunikacji dotyczącej obsługi incydentu przez podmioty kluczowe i ważne. Brak jest zapisów w ustawie, które precyzują CSIRT sektorowy będzie właściwy dla podmiotów, które będą kwalifikowały się do działalności w różnych sektorach lub podsektorach. Będzie to miało wpływ na obowiązki dotyczące zgłaszania incydentów poważnych sformułowane w art. 11 ust. 1 pkt. 2 ustawy o KSC (zwłaszcza w sytuacji powołania CSIRT sektorowych przed uruchomieniem pełnej funkcjonalności systemu do obsługi tego typu komunikacji). Dodatkowo nie ma zapisu o powołaniu CSIRT w formie prawnej, która umożliwi konsultacje przyjętego zakresu poszczególnych CSIRT sektorowych. Zgodnie z art. 44 ust. 1 w dotychczasowym brzmieniu, jasno wskazano, że organ właściwy ds. cyberbezpieczeństwa ustanawia sektorowy zespół ds. cyberbezpieczeństwa. Po zmianach, zapewnia jego funkcjonowanie. Zmiana stylistyczna pomijająca sposób utworzenia CSIRT sektorowego, w powiązaniu z wprowadzonym art. 44a – 44c może budzić wątpliwości o to, na ile w praktyce CSIRT sektorowe będą faktycznie funkcjonowały jako struktura podnosząca efektywność działania organów krajowego systemu cyberbezpieczeństwa, a na ile będą dublowały zadania organów właściwych ds. cyberbezpieczeństwa lub CSIRT poziomu krajowego. W dotychczasowych przepisach zespoły ds. cyberbezpieczeństwa były strukturami wyodrębnionymi pomocniczo. Projekt nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa, który zakłada możliwość powierzenia funkcji CSIRT sektorowego różnorodnym państwowym osobom prawnym, wzbudza poważne wątpliwości co do skuteczności i właściwości takiego rozwiązania. Zgodnie z art. 44a ustawy KSC, funkcję tę mogą pełnić m.in. agencje wykonawcze, instytucje kultury, jednostki naukowe Polskiej Akademii Nauk, uczelnie publiczne oraz parki narodowe. Przykładowo mogą to być takie podmioty jak: Polski Instytut Filmu i Teatru; Narodowy Instytut Fryderyka Chopia; Narodowy Instytut im. Oskara Łozińskiego; Akademia Kopernikańska; Uniwersytet Publiczny; Instytut Współpracy Polsko-Węgry im. Włodzisława Fijałki; Instytut Rozwoju Języka Polski im. świętego Maksymiliana Marii Kolbego; czy dowolne przedsiębiorstwo państwowe. Przekazanie odpowiedzialności za cyberbezpieczeństwo sektora tak zróżnicowanym podmiotom, które często nie mają odpowiednich kompetencji, doświadczenia, ani struktur do efektywnego zarządzania kwestiami bezpieczeństwa informacyjnego, stawia pod znakiem zapytania racjonalność i efektywność takiego rozwiązania.	Wyjaśnienie uwagi Odpowiedzialność za utworzenie CSIRT sektorowych spoczywa na organach właściwych, które najlepiej znają swój sektor i są w stanie wskazać podmiot dostosowany do pełnienia tych zadań. Proponowane rozwiązanie zapewni im elastyczność w doborze takich podmiotów. Oparte jest na rozwiązaniach w zakresie sektorowych zespołów cyberbezpieczeństwa na podstawie których funkcjonuje m.in. Centrum e-zdrowia.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

			Przepisy w obecnym brzmieniu na tyle komplikują strukturę krajowego systemu cyberbezpieczeństwa, że z pewnością nie pozwalają uznać, żeby cel w postaci uporządkowania struktury organów, o którym mowa w uzasadnieniu projektu ustawy, został osiągnięty. Cyberbezpieczeństwo wymaga specjalistycznej wiedzy i narzędzi, a także szybkiej reakcji na incydenty, co w przypadku wielu wymienionych instytucji może być trudne do osiągnięcia. Nawet potencjalna możliwość powierzenia takich funkcji może budzić poważne zastrzeżenia.	
119.	Osoba fizyczna	Art. 45	Ust. 1 p.9 – Zastosowano zapis dotyczący ustanowienia struktur komunikacyjnych na potrzeby wykrywania kryzysów, reagowania kryzysowego i zarządzania kryzysowego. Wskazany zakres działań jest realizowany na podstawie przepisów ustawy o zarządzaniu kryzysowym i nie ma zastosowania w uKSC2. Na potrzeby ustawy uKSC2 i w jej przedmiotowym kontekście i zakresie proponuję zmodyfikować zapis poprzez dodanie sformułowania „w cyberbezpieczeństwie” do postaci „wykrywania kryzysów w cyberbezpieczeństwie, reagowania kryzysowego w cyberbezpieczeństwie i zarządzania kryzysowego w cyberbezpieczeństwie” (ref. Art. 2 p.11, art. 45a)	Uwaga uwzględniona
120.	PGE SA	Art. 1 pkt 47 projekt u, Art. 45a ustawy	Czy będą dostępne procedury komunikacji na wypadek wystąpienia incydentu na dużą skalę?	Wyjaśnienie uwagi Kwestie te zostaną określone w Krajowym Planie reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę.
121.	Osoba fizyczna	Art. 46	Art. 46 Zagadnienia stosowania systemu art. 46 (S46): 14.1. Ust. 1 p.1 – Zastosowany zapis definiujący zakres funkcjonalny systemu art. 46 (S46), jako wspierającego, wskazując w pkt 1 – „współpracę podmiotów wchodzących w skład krajowego systemu cyberbezpieczeństwa”. Proponuję zweryfikować intencjonalny zakres zapisów tego punktu i zdecydować o jego ostatecznym kształcie. Proponuję, aby zakres współpracy podmiotów obejmował: 1) wszystkie typy podmiotów, tzn. podmioty instytucjonalne, „zarządzające KSC” – Pełnomocnik, Kolegium PPK, organy właściwe, minister wł. ds. informatyzacji oraz CSIRT krajowe i CSIRT sektorowe, a także podmioty kluczowe i ważne, 2) wymianę informacji o zdarzeniach, cyberzagrożeniach, incydentach, sposobach postępowania i reagowania itp. przekazywanie dokumentów, rekomendacji, zaleć, poleceń zabezpieczających itp. Jeśli intencje aktualnego zapisu nie pokrywają wskazanego zakresu, to proponuję wprowadzić stosowne modyfikacje, aby zapewnić możliwość wszechstronnej komunikacji i współpracy wszystkim podmiotom KSC.	Uwaga uwzględniona
122.	Osoba fizyczna	Art.46	Ust. 5 – Zastosowano zapis wskazujący metody uwierzytelniania określone w art. 20a ust.1 Ustawy o informatyzacji Proponuję odwołanie do art. 20a bez wskazywania ust. Tak	Wyjaśnienie uwagi W przepisie tym zostanie wskazane odwołanie także do uwierzytelniania wieloskładnikowego.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

			zdefiniowane metody uwierzytelniania zapewnią spójne podejście realizacji funkcji wszystkich publicznych systemów informacyjnych/teleinformatycznych.	
123.	Osoba fizyczna	Art. 46	Ust. 8 – Zastosowano zapis wskazujący, że minister wł. ds. informatyzacji udostępni wykaz usług świadczonych przez podmioty kluczowe i ważne, który będzie stosowany w systemie S46. Takie postawie kwestii katalogu usług jest niewłaściwe ze względu fakt, że wiele zapisów ustawy uKSC2 wprost odwołuje się do usług, stawia wymagania względem nich i ich bezpieczeństwa. Definicja usługi, czym jest usługa, jak ją rozumieć, szczególnie w powiązaniu do rodzajów podmiotów, wskazanych w załącznikach 1 i 2 NIS2/uKSC2, jest kluczową kwestią dla dobrego rozumienia i implementacji zapisów ustawy uKSC2. Zastosowanie katalogu usług w systemie S46 powinno być traktowane jako wtórne względem pierwotnego, ww. kontekstu. Proponuję zdefiniować katalog usług na potrzeby interpretacji i implementacji ustawy uKSC2.	Uwaga nieuwzględniona Dyrektywa NIS2 odeszła od podejścia opartego na usługach i przeszła do podejścia opartego na podmiotach. Dlatego podmioty kluczowe i ważne muszą zabezpieczyć wszystkie swoje systemy, a nie tylko te związane z konkretną usługą. W związku z tym nie trzeba wskazywać katalogu usług na potrzeby przepisów.
124.	Osoba fizyczna	Art. 46	Proponuję, żeby wszelkie dokumenty, rekomendacje, zalecenia itp., kierowane przez organy właściwe, ministra wł. ds. cyfryzacji, Pełnomocnika, Kolegium do podmiotów KSC były umieszczane poza BIP danego organu, również w S46, co zapewni natychmiastowe powiadomienie adresatów o ich zamieszczeniu i dostęp bez szukania w BIP. (ref. Art. 8 ust.3, art. 15 ust.1a, art. 31 ust.3, art. 33 ust.4c, art. 35 ust.5, art. 37 ust.2, art. 44e ust.2, art. 46 ust. 7 i 8, art. 53c ust.3, 67a ust.2, art. 67b ust.6, ust.17, art. 67f, art. 67g ust.4, ust.15	Uwaga częściowo uwzględniona Te dokumenty mogą być publikowane wS46, natomiast jako akty administracji powinny być opublikowane czy to w BIP – urzędowym publikatorze, czy to w Monitorze Polskim.
125.	ZBP	Art. 46 ust. 2	CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT sektorowe, organy właściwe do spraw cyberbezpieczeństwa oraz Prezes Urzędu Ochrony Danych Osobowych korzystają z systemu teleinformatycznego w celu realizacji swoich zadań ustawowych CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT sektorowe, organy właściwe do spraw cyberbezpieczeństwa, centrum wymiany i analiz informacji oraz Prezes Urzędu Ochrony Danych Osobowych korzystają z systemu teleinformatycznego w celu realizacji swoich zadań ustawowych. Proponowana zmiana ma na celu umożliwienie centrum wymiany i analiz informacji dostępu do systemu „S-46” co pozwoliłoby na bezpośrednie przekazywanie podmiotom sektora finansowego informacji na temat incydentów, podatności i zagrożeń bez wprowadzania obowiązku ich uczestniczenia w systemie.	Uwaga nieuwzględniona ISACi w polskiej praktyce nie są podmiotami, a porozumieniami. Nie są jednostkami organizacyjnymi. Trudno byłoby je podłączyć do systemu.
126.	Konfederacja Lewiatan	Art. 46 ust. 4	Zakres korzystania z S46 przez podmioty kluczowe i ważne Jednostka redakcyjna: Art. 46 ust. 4 W art. 46 ust. 4 wskazano ogólnie, że: <i>Podmioty kluczowe i podmioty ważne, inne niż w ust. 2, korzystają z systemu teleinformatycznego w zakresie, o którym mowa w ust. 1, po uzyskaniu wpisu w wykazie podmiotów kluczowych i podmiotów ważnych.</i> W naszej ocenie przepis ten wymaga doprecyzowania w świetle faktycznych obowiązków podmiotów kluczowych i ważnych wynikających z przepisów art. 8-15. W szczególności	Wyjaśnienie uwagi Zakres korzystania z S46 będzie wyznaczony przez obowiązki danego podmiotu. Równocześnie chcemy aby wiele dodatkowych informacji takich jak ostrzeżenia czy rekomendacje było przekazywanych podmiotom krajowego

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

			podmioty takie nie są uprawnione/zobowiązane do realizacji poniższych zadań przypisanych do S46: 2) generowanie i przekazywanie rekomendacji dotyczących działań podnoszących poziom cyberbezpieczeństwa; 3) szacowanie ryzyka na poziomie krajowym; 4) ostrzeganie o cyberzagrożeniach; 5) czynności nadzorcze organów właściwych do spraw cyberbezpieczeństwa;	systemu cyberbezpieczeństwa za pośrednictwem systemu S46.
127.	Rada Bezpieczeństwa Biznesowego Grupy MiSOT	Art. 46	Art 46 „6. Podmioty kluczowe i podmioty ważne obowiązane są zapewnić zgodność swoich systemów informacyjnych z minimalnymi wymaganiami technicznymi i funkcjonalnymi korzystania z systemu teleinformatycznego, o którym mowa w ust. 1, w terminie 3 miesięcy podmioty kluczowe i 6 miesięcy podmioty ważne od udostępnienia tych wymagań.”. Uzasadnienie: Proponujemy zmianę z uwagi na liczebność personelu u mikroprzedsiębiorców. 3 miesiące w przypadku dostosowania się do wymagań od momentu ich publikacji może okazać nieosiągalne w przypadku podmiotów telekomunikacyjnych w skali mikro.	Uwaga uwzględniona
128.	Polskie Stowarzyszenie Fotowoltaiki	Art. 43 ust. 4	[Systemy teleinformatyczne wykorzystywane do celów KSC] Obowiązek PK i PW: - korzystania z systemu teleinformatycznego po uzyskaniu wpisu w wykazie podmiotów kluczowych i podmiotów ważnych w celu (1) współpracy podmiotów wchodzących w skład krajowego systemu cyberbezpieczeństwa; (2) zgłaszania i obsługi incydentów – tj. systemu S46; - zapewnienia zgodności swoich systemów informacyjnych z minimalnymi wymaganiami technicznymi i funkcjonalnymi korzystania z systemu (S46) w terminie 3 miesięcy od udostępnienia tych wymagań. Ogólny wpływ regulacji: Zastosowanie systemu informatycznego lub wdrożenie dodatkowych wymagań w celu zapewnienia zgodności swoich systemem z systemem, o którym mowa w art. 46 może wymagać dodatkowych nakładów finansowych oraz personelu ze strony podmiotów zobowiązanych. Brak możliwości oceny rzeczywistego wpływu regulacji. Wpływ na sektor energetyczny: jw. – brak specyficznego wpływu na sektor energetyczny	Wyjaśnienie uwagi Przewiduje się, że S46 będzie dostępny w modelu chmurowym.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

129.	Konfederacja Lewiatan	Art. 46 ust. 6	Termin dostosowania do S46 Jednostka redakcyjna: Art. 46 ust. 6 Niejasna jest relacja wymagań technicznych, do których należy się dostosować w ciągu 3 miesięcy od ich publikacji do terminu rozpoczęcia korzystania z systemu w ciągu 2 tygodni od wpisu do wykazu (wyżej uwagi do art. 9), a także art. 46 ust. 4 (korzystanie po wpisie) oraz art. 15 dotyczącego komunikatu o harmonogramie rozpoczęcia korzystania. W szczególności nie jest jasne czy przed spełnieniem wymagań technicznych (które zostaną opublikowane w nieznanym terminie po wejściu w życie ustawy) możliwe będzie prawidłowe korzystanie z S46. Kwestie te nie zostały wyjaśnione w uzasadnieniu i w naszej ocenie wymagają jednoznacznego rozstrzygnięcia. Ponadto sygnalizujemy, że na obecnym etapie nie jest możliwe odniesienie się do tego czy 3 miesięczny termin na wdrożenie wymagań będzie wystarczający. Nie są bowiem znane jakiegokolwiek założenia techniczne (poza tym, że ma to być wersja chmurowa) dot. nowej wersji S46 i tym samym nie jest jasne jakiego rodzaju zmian będzie wymagało dostosowanie. Zauważamy, że dokonywanie istotnych zmian w systemach informatycznych dużych podmiotów jest wielokrotnie zadaniem skomplikowanych, które wymaga wielomiesięcznych przygotowań oraz zapewnienia odpowiedniego budżetu. Z tego względu wnioskujemy o wydłużenie terminu na dostosowanie do 6 miesięcy, z możliwością ewentualnego wcześniejszego zgłoszenia gotowości.	Wyjaśnienie uwagi Przepisy zostaną uszójnione.
130.	Polska Izba Informatyki i Telekomunikacji	Art. 46	Art. 46 ust. 1 pkt 7 – S46 i zgłaszanie naruszeń danych osobowych Projekt ustawy przewiduje dodanie do art. 46 ust. 1 ustawy o krajowym systemie cyberbezpieczeństwa nowego punktu 7, który w połączeniu ze zdaniem wprowadzającym może być odczytywany w ten sposób, że system S46 ma wspierać m.in. dokonywanie zgłoszeń naruszenia ochrony danych osobowych, o których mowa w art. 33 RODO. Niestety projektowany przepis jest dosyć ogólny i prowokuje szereg pytań, które będą musiały doczekać się odpowiedzi w toku dalszych prac legislacyjnych. Nieznana jest ani kierunkowa intencja Projektodawcy (jaki cel ten przepis ma realizować?) ani to, czy podmioty kluczowe i ważne będą prawnie zobowiązane do zgłaszania Prezesowi Urzędu Ochrony Danych Osobowych naruszeń bezpieczeństwa danych osobowych wyłącznie za pośrednictwem S46 (zastępując tym samym istniejące i działające mechanizmy zgłaszania naruszeń) czy też może S46 ma być narzędziem, z którego podmioty kluczowe i ważne mogą, ale nie muszą korzystać do zgłaszania naruszeń danych osobowych? Jako Izba prosimy o dialog w tym zakresie, tak aby przyszłe przepisy w tym zakresie uwzględniały doświadczenia wypracowane przez Inspektorów Ochrony Danych Osobowych zdobyte przez lata stosowania przepisów o ochronie danych osobowych. Nie można również zapominać, że przedsiębiorcy telekomunikacyjni znajdują się w tym zakresie w szczególnej sytuacji, bo muszą stosować nie tylko horyzontalne przepisy RODO, ale związani są również przepisami sektorowymi, a konkretnie wciąż obowiązującą dyrektywą 2002/58/WE z dnia 12 lipca	Wyjaśnienie uwagi Celem jest to, aby podmioty kluczowe/ważne miały możliwość zgłaszania naruszeń odo za pomocą S46 – ma to być uprawnienie, jedno okienko.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

			2002 r. dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa e-Privacy) i wydanym na jej podstawie rozporządzeniem Komisji (UE) nr 611/2013 z dnia 24 czerwca 2013 r. w sprawie środków mających zastosowanie przy powiadamianiu o przypadkach naruszenia danych osobowych, na mocy dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady o prywatności i łączności elektronicznej. Konsekwencją tych przepisów jest art. 174a ustawy – Prawo telekomunikacyjne, który wprost stanowi, że dostawca publicznie dostępnych usług telekomunikacyjnych zawiadamia Prezesa Urzędu Ochrony Danych Osobowych o naruszeniu danych osobowych w terminie i na zasadach określonych w rozporządzeniu Komisji (UE) nr 611/2013 z dnia 24 czerwca 2013 r. w sprawie środków mających zastosowanie przy powiadamianiu o przypadkach naruszenia danych osobowych.	
131.	Polska Izba Informatyki i Telekomunikacji	Art. 46	Art. 46 ust. 4 – zakres korzystania z S46 przez podmioty kluczowe i ważne W art. 46 ust. 4 wskazano ogólnie, że: <i>Podmioty kluczowe i podmioty ważne, inne niż w ust. 2, korzystają z systemu teleinformatycznego w zakresie, o którym mowa w ust. 1, po uzyskaniu wpisu w wykazie podmiotów kluczowych i podmiotów ważnych.</i> W naszej ocenie przepis ten wymaga doprecyzowania w świetle faktycznych obowiązków podmiotów kluczowych i ważnych wynikających z przepisów art. 8-15. W szczególności podmioty takie nie są uprawnione/zobowiązane do realizacji poniższych zadań przypisanych do S46: 2) generowanie i przekazywanie rekomendacji dotyczących działań podnoszących poziom cyberbezpieczeństwa; 4) szacowanie ryzyka na poziomie krajowym; 5) ostrzeganie o cyberzagrożeniach; 6) czynności nadzorcze organów właściwych do spraw cyberbezpieczeństwa;	Uwaga uwzględniona
132.	Polska Izba Informatyki i Telekomunikacji	Art. 46	Art. 46 ust. 6 – termin dostosowania do S46 Niejasna jest relacja wymagań technicznych, do których należy się dostosować w ciągu 3 miesięcy od ich publikacji do terminu rozpoczęcia korzystania z systemu w ciągu 2 tygodni od wpisu do wykazu (wyżej uwagi do art. 9), a także art. 46 ust. 4 (korzystanie po wpisie) oraz art. 15 dotyczącego komunikatu o harmonogramie rozpoczęcia korzystania. W szczególności nie jest jasne czy przed spełnieniem wymagań technicznych (które zostaną opublikowane w nieznanym terminie po wejściu w życie ustawy) możliwe będzie prawidłowe korzystanie z S46. Kwestie te nie zostały wyjaśnione w uzasadnieniu i w naszej ocenie wymagają jednoznacznego rozstrzygnięcia. Ponadto sygnalizujemy, że na obecnym etapie nie jest możliwe odniesienie się do tego, czy 3-miesięczny termin na wdrożenie wymagań będzie wystarczający. Nie są bowiem znane jakiegokolwiek założenia techniczne (poza tym, że ma to być wersja chmurowa) dot. nowej wersji S46 i tym samym nie jest jasne jakiego rodzaju zmian będzie wymagało dostosowanie. Zauważamy, że dokonywanie istotnych zmian w systemach informatycznych dużych podmiotów jest wielokrotnie zadaniem skomplikowanych, które wymaga wielomiesięcznych przygotowań	Uwaga uwzględniona Terminy zostaną przeanalizowane i poprawione. Zapewnienie zgodności – intencją była właśnie kompatybilność.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

			oraz zapewnienia odpowiedniego budżetu. Dlatego postulujemy dokonanie konsultacji wymagań przed ich publikacją. Dodatkowo należy wskazać, że proponowane nowelizacją brzmienie art. 46 ust. 6 – „zapewnienie zgodności systemów informacyjnych” wskazuje na postanowienia znacząco ograniczające swobodę działalności gospodarczej, w ocenie Izby podmioty zobowiązane do podłączenia się do s46 powinny zapewnić kompatybilność swojego systemu z s46. Obecne brzmienie art. 46 ust. 6 oznacza, że to minister ds. informatyzacji będzie decydował o kształcie systemów informatycznych służących do komunikacji w zakresie zadań wynikających z ksc bez możliwości uwzględnienia jakichkolwiek zmian przez podmioty zobowiązane związanych ze specyfiką działalności danego podmiotu. Z tego względu wnioskujemy o wydłużenie terminu na dostosowanie wskazanego w ustawie do 6 miesięcy, z możliwością ewentualnego wcześniejszego zgłoszenia gotowości. Jednocześnie należy rozważyć wprowadzenie możliwości wskazania przez Ministra dłuższego terminu, w samych wymaganiach.	
133.	Osoba fizyczna	Art. 47	Ust. 3 – Zastosowany zapis dotyczący udostępniania jednostkom podległym lub nadzorowanym przez ministra wł. ds. informatyzacji, realizującym zadania ministra, danych z wykazu podmiotów kluczowych i ważnych. Proponuję rozszerzenie zapisu o udostępnianie również danych z systemu S46.	Uwaga nieuwzględniona Zakres udostępniania danych z systemu jest określony w art. 46.
134.	Konfederacja Lewiatan	Art. 53	Zastosowanie procedur zawieszenia działalności bez zachowania gwarancji proceduralnych znanych z NIS2 Jednostka redakcyjna: art. 53 projektu KSC Jednostka redakcyjna NIS2: art. 32 ust. 5 Uwaga: Zgodnie z art. 32 ust. 5 dyrektywy NIS2, tymczasowe zawieszenie lub zakaz prowadzenia działalności powinno być stosowane z zachowaniem odpowiednich gwarancji proceduralnych, zgodnych z ogólnymi zasadami prawa Unii Europejskiej oraz z Kartą Praw Podstawowych Unii Europejskiej. Do tych gwarancji należą prawo do skutecznej ochrony prawnej, rzetelny proces sądowy, domniemanie niewinności oraz prawo do obrony. Zaproponowana implementacja tego przepisu w art. 53 ust. 8 i kolejnych projektu ustawy nie zawiera takich gwarancji proceduralnych. Trudno uznać za gwarancję proceduralną samą możliwość przedstawienia swojego stanowiska przed organem do spraw cyberbezpieczeństwa, gdyż to ten sam organ (lub inny działający na jego wniosek) podejmuje decyzję o cofnięciu, zawieszeniu odpowiedniej koncesji lub wykreśleniu z rejestru.	Uwaga uwzględniona Przed zastosowaniem środków, o których mowa w art. 53 ust. 8 muszą być zastosowane inne środki nadzoru na które podmiotowi przysługuje skarga do sądu administracyjnego. Stosuje się w takiej sytuacji przepisy ustawy – Prawo o postępowaniu przed sądami administracyjnymi. Zastosowanie ma zatem art. 61 tej ustawy dający możliwość wstrzymania wykonania postanowień decyzji lub innej czynności z zakresu administracji publicznej do czasu rozstrzygnięcia. Dopiero po rozpatrzeniu sprawy przez sąd organ może wszcząć środki nadzorcze określone w art. 53 ust. 8 projektu ustawy. Przepis ten został zmodyfikowany oraz w odrębnym przepisie (art. 53e) została dodana procedura, która

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

				wiąże się z realizacją uprawnień nadzorczych.
135.	PIKE i Mediakom	Art. 53	Art. 53 ust. 3 pkt 2 - Przepis ustawy stanowi, że nadzór nad podmiotami ważnymi ma charakter następczy „w szczególności w przypadku uzasadnionego podejrzenia, że zachodzi możliwość naruszenia przepisów ustawy”. Tymczasem takie podejrzenie jest koniecznym warunkiem przeprowadzenia kontroli podmiotu ważnego, zgodnie z art. 33 ust. 1 i motywem 122 dyrektyw NIS2. Art. 53 [...] 3. Organy właściwe do spraw cyberbezpieczeństwa za pomocą działań nadzorczych sprawują nadzór o charakterze: 1) prewencyjnym i następczym nad podmiotami kluczowymi; 2) następczym nad podmiotami ważnymi, ~~w szczególności~~ w przypadku uzasadnionego podejrzenia, że zachodzi możliwość naruszenia przepisów ustawy.	Uwaga nieuwzględniona Uzasadnione podejrzenie, że zachodzi naruszenie przepisów ustawy jest główną przesłanką wszczęcia nadzoru następczego nad podmiotem ważnym, ale może być to również szereg innych przyczyn. Jednym z przykładów będzie potwierdzona sytuacja wystąpienia incydentu.
136.	PIKE i Mediakom	Art. 53	Art. 53 ust. 5 pkt 6 - PIKE stoi na stanowisku, że „urzędnik monitorujący, [wyznaczony] do nadzorowania wykonywania obowiązków, o których mowa w rozdziale 3” może być wyznaczony, jak wskazuje art. 32 ust. 4 lit. g dyrektywy NIS2 na oznaczony okres oraz powinien mieć ściśle określone zadania. Wymogu ścisłego określenia zadań brakuje w omawianym przepisie. Ponadto, obecność takiego urzędnika monitorującego stanowi poszerzenie czasu prowadzenia kontroli u przedsiębiorcy, którego nie wlicza się do limitu 48 dni na przeprowadzenie takiej kontroli. Należy zatem ustanowić górny limit obecności takiego urzędnika monitorującego u podmiotu kluczowego. Postulat do rozważenia: uzupełnienie przepisu o wymagania dla urzędnika aby posiadał certyfikat dostępu do informacji niejawnych lub przynajmniej zastrzeżenia potencjalnej odpowiedzialności urzędnika za ujawnienie tajemnicy przedsiębiorstwa. Art. 53 [...] 5. W celu egzekwowania przepisów ustawy organ właściwy do spraw cyberbezpieczeństwa w stosunku do podmiotów kluczowych, może: [...] 6) wyznaczyć, w drodze decyzji, na określony czas, <u>nie dłuższy jednak niż 10 dni roboczych</u>, spośród osób zatrudnionych w urzędzie obsługującym ten organ, urzędnika monitorującego do nadzorowania wykonywania obowiązków, o których mowa w rozdziale 3, <u>wskazując ściśle określone zadania, które urzędnik powinien realizować w tym czasie</u>;	Uwaga częściowo uwzględniona Przepis pkt 6 otrzymał brzmienie „wyznaczyć, w drodze decyzji, na określony czas, nie dłuższy niż miesiąc, spośród osób zatrudnionych w urzędzie obsługującym ten organ, urzędnika monitorującego do nadzorowania wykonywania obowiązków, o których mowa w rozdziale 3, wskazując ściśle określone zadania, które urzędnik powinien realizować w tym czasie”. Jednocześnie należy zauważyć, że urzędnik monitorujący nie realizuje czynności kontrolnych a zatem zarzut poszerzenia czasu prowadzenia kontroli jest niezasadny.
137.	PIKE i Mediakom	Art. 53	Art. 53 ust. 7 Przepis przewiduje niezwykle daleko idące środki wymierzone przeciwko przedsiębiorcy. Od wszystkich tych środków powinno z całą pewnością przysługiwać prawo do wniesienia skargi do sądu. 7. Postępowanie, o którym mowa w ust. 5, jest jednoinstancyjne, a na decyzję organu właściwego do spraw cyberbezpieczeństwa przysługuje skarga do sądu administracyjnego. Nakaz, o którym mowa w ust. 5 pkt 1, jest inną czynnością z zakresu administracji publicznej, na którą przysługuje skarga do sądu administracyjnego.	Uwaga uwzględniona

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

138.	PIKE i Mediakom	Art. 53 ust. 13	Biorąc pod uwagę, że przepis ten dotyczy niezwykle daleko idących sankcji, równoznacznych z zawieszeniem prowadzenia działalności w obszarach kluczowych dla gospodarki, w opinii PIKE niedopuszczalna jest rezygnacja przez organ z poinformowania „o wstępnych ustaleniach” równoznacznych z ostrzeżeniem, że organ ten rozważa zastosowanie środków tymczasowych określonych w art. 53 ust. 8. Wykreślenie art. 53 ust. 13.	Uwaga nieuwzględniona Przepis wdraża dyrektywę NIS2, która również przewiduje wyjątek we wstępnym informowaniu.
139.	PIKE i Mediakom	Art. 53 ust. 15	Dyrektywa NIS2 w swoim art. 33 nie przewiduje możliwości nałożenia na podmiot ważny obowiązku przeprowadzania regularnych audytów bezpieczeństwa (o czym jest mowa w uwadze do art. 15 ust. 1) ani możliwości ustanowienia urzędnika monitorującego. Te obowiązki są wyjątkowo dotkliwe, więc Izba postuluje o rezygnację z ich wprowadzania w stosunku do podmiotów ważnych, skoro dyrektywa NIS2 tego nie wymaga. Art. 53 [...] 15. Organ właściwy do spraw cyberbezpieczeństwa sprawując nadzór w stosunku do podmiotu ważnego stosuje odpowiednio ust. 2 ~~i 4-14~~ , 4, 5 pkt 1-5, 6-7, 9-14, uwzględniając postanowienia określone w ust. 3 pkt 2.	Uwaga uwzględniona Art. 53 ust. 15 został przeredagowany w ten sposób, że wskazano wprost, które przepisy mają zastosowanie do podmiotów ważnych.
140.	Amerykańska Izba Handlowa	Art. 53	Projekt wykracza poza zakres dyrektywy poprzez przyznanie organowi właściwemu do spraw cyberbezpieczeństwa niezwykle szerokich uprawnień wykonawczych, zarówno wobec podmiotów kluczowych, jak i ważnych. W szczególności uprawnienia te obejmują środki tak dolegliwe jak: a) żądanie zawieszenia, ograniczenia zakresu lub cofnięcia koncesji przyznanej podmiotowi przez właściwy organ, cofnięcia pozwolenia na prowadzenie działalności lub usunięcia podmiotu z rejestru działalności regulowanej (art. 53 ust. 8 pkt 1-3 wprowadzane do uksc), b) zwrócenie się do sądu o nałożenie tymczasowego zakazu pełnienia funkcji przez osoby kierujące podmiotem kluczowym (art. 53 ust. 8 pkt 4 wprowadzane do uksc), c) powołanie w drodze decyzji na określony czas spośród osób zatrudnionych w biurze obsługującym organ inspektora monitorującego wykonywanie obowiązków wymienionych w rozdziale 3 uksc (art. 53 ust. 5 pkt 6 wprowadzany do uksc). Przyznanie organom administracyjnym tak szerokich uprawnień wykonawczych może prowadzić do nadmiernej ingerencji w działalność podmiotów kluczowych i ważnych, a przez to do zaburzeń ich normalnym funkcjonowaniu. Stoiśmy na stanowisku, że konieczne jest ponowne rozważenie proponowanych przepisów, aby znaleźć bardziej zrównoważone podejście, które w zgodzie z zasadą proporcjonalności zapewni egzekwowanie standardów cyberbezpieczeństwa bezpieczeństwo, przy jednoczesnej minimalizacji ryzyka nadmiernych obciążeń i zakłóceń w bieżącym funkcjonowaniu podmiotów kluczowych i ważnych. Ponadto sugerujemy rozważenie sformułowania wprowadzanego do art. 53 ust. 10 uksc katalogu kryteriów oceny naruszenia przepisów Ustawy w sposób otwarty. Z uwagi na podobieństwo katalogu do przepisów Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne	Wyjaśnienie uwagi Art. 53 ust. 8 pkt 1 projektu wdraża art. 32 ust. 5 pkt 1 lit. a dyrektywy NIS2: <i>5. Jeżeli środki z zakresu egzekwowania przepisów zastosowane na podstawie ust. 4 lit. a)–d) i f) okażą się nieskuteczne, państwa członkowskie zapewniają, by ich właściwe organy były uprawnione do wyznaczenia terminu, do którego podmiot kluczowy jest zobowiązany podjąć działania konieczne do usunięcia uchybień lub zapewnienia zgodności z wymogami określonymi przez te organy. Jeżeli żądane działanie nie zostanie podjęte w wyznaczonym terminie, państwa członkowskie zapewniają, by właściwe organy były uprawnione do:</i> <i>a) tymczasowego zawieszenia lub zwrócenia się do organu, który przyznał certyfikację lub udzielił zezwolenia, lub do sądu, zgodnie z prawem krajowym, o tymczasowe zawieszenie certyfikacji lub zezwolenia na niektóre lub wszystkie odpowiednie usługi świadczone bądź na część lub całość</i>

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

			rozporządzenie o ochronie danych „RODO”), można rozważyć dodanie przepisu analogicznego do art. 83 ust. 2 lit. k RODO, tj. oceny naruszenia pod względem „wszelkich innych obciążających lub łagodzących czynników mających zastosowanie do okoliczności sprawy, takich jak osiągnięte bezpośrednio lub pośrednio w związku z naruszeniem korzyści finansowe lub uniknięte straty” (lub w brzmieniu innym, zbliżonym). Dodanie takiego kryterium pozwoli na uwzględnienie szerokiego spektrum okoliczności występujących w sprawie.	<i>działalności prowadzonej przez podmiot kluczowy;</i> Art. 53 ust. 8 pkt 2 projektu wdraża art. art. 32 ust. 5 pkt 1 lit. b dyrektywy NIS2: <i>5. Jeżeli środki z zakresu egzekwowania przepisów zastosowane na podstawie ust. 4 lit. a)–d) i f) okażą się nieskuteczne, państwa członkowskie zapewniają, by ich właściwe organy były uprawnione do wyznaczenia terminu, do którego podmiot kluczowy jest zobowiązany podjąć działania konieczne do usunięcia uchybień lub zapewnienia zgodności z wymogami określonymi przez te organy. Jeżeli żądane działanie nie zostanie podjęte w wyznaczonym terminie, państwa członkowskie zapewniają, by właściwe organy były uprawnione do:</i> <i>b) zwrócenia się do właściwych instytucji lub sądów, zgodnie z prawem krajowym, o nałożenie tymczasowego zakazu pełnienia funkcji zarządczych w tym podmiocie kluczowym na osobę fizyczną wykonującą obowiązki zarządcze na poziomie dyrektora generalnego lub przedstawiciela prawnego w tym podmiocie.</i> Art. 53 ust. 5 pkt 6 projektu wdraża art. 32 ust. 4 lit. g dyrektywy NIS2: 4. Państwa członkowskie zapewniają, aby wykonując uprawnienia w zakresie egzekwowania przepisów wobec podmiotów kluczowych, ich właściwe organy były uprawnione co najmniej do: g) wyznaczenia urzędnika monitorującego – ze ściśle określonymi zadaniami na oznaczony okres – do nadzorowania przestrzegania przez dane podmioty art. 21 i 23.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

				Mając powyższe na uwadze należy wskazać, że przepisy te stanowią bezpośrednie wdrożenie postanowień dyrektywy NIS2. Również w zakresie propozycji zmiany art. 53 ust. 10 projektodawca zwraca uwagę, że przepis ten stanowi wdrożenie do porządku krajowego katalogu przesłanek bezpośrednio wskazanych w NIS2.
141.	Związek Cyfrowa Polska	Art. 53	Projekt wykracza poza założenia dyrektywy, przyznając władzom szersze uprawnienia egzekucyjne zarówno wobec podmiotów kluczowych, jak i ważnych. Organ właściwy do spraw cyberbezpieczeństwa w myśl projektu może bowiem: • żądać zawieszenia, ograniczenia zakresu lub cofnięcia licencji lub autoryzacji przyznanej jednostce, lub usunięcie jednostki z rejestru działalności regulowanej, • żądać tymczasowego zakazu pełnienia funkcji przez szefa podmiotu kluczowego lub ważnego, • powołać decyzją na określony czas spośród osób zatrudnionych w biurze obsługującym organ inspektora monitorującego wykonywanie obowiązków wymienionych w rozdziale 3, • wymagać od podmiotów kluczowych i ważnych przeprowadzenia audytów bezpieczeństwa oraz oceny bezpieczeństwa systemów informacyjnych. Należy w tym miejscu zauważyć, że przyznanie władzom szerszych uprawnień egzekucyjnych może prowadzić do nadmiernej ingerencji w działalność podmiotów kluczowych i ważnych, a przez to do destabilizacji ich funkcjonowania. Sugerujemy ponowne rozważenie proponowanych przepisów, aby znaleźć bardziej zrównoważone podejście, które zapewni bezpieczeństwo, jednocześnie minimalizując ryzyko nadmiernych obciążeń i zakłóceń dla podmiotów kluczowych i ważnych.	Wyjaśnienie uwagi Przepisy stanowią bezpośrednie wdrożenie dyrektywy NIS 2 i są niezbędnym środkiem nadzorczym przysługującym organom właściwym do spraw cyberbezpieczeństwa. Jednocześnie zagwarantowana została możliwość wstrzymania się z realizacją tych uprawnień do czasu rozstrzygnięcia przez sąd skargi złożonej przez podmiot kluczowy na środki nadzorcze zastosowane wcześniej.
142.	Fundacja Bezpieczna Cyberprzestrzeń	Art. 53	Art. 1 pkt 56, treść art. 53 ust 9 „Środków, o których mowa w ust. 8, nie stosuje się do podmiotów publicznych.” – jest to sprzeczne z ideą NIS2, która wszystkie podmioty miała równać w obowiązkach i konsekwencjach za ich łamanie lub zaniechanie.	Uwaga nieuwzględniona Wyłączenie z zakresu stosowania środków o których mowa w art. 53 ust. 8 podmiotów publicznych wynika bezpośrednio z dyrektywy NIS2, a zatem stanowi zgodność z prawem unijnym.
143.	ISACA	Art. 53	Art. 53 ust 9 - ust. 9 należy nadać brzmienie „Środków, o których mowa w ust. 8 pkt 1-3, nie stosuje się do podmiotów publicznych”. - Podmioty publiczne są zaliczone do podmiotów kluczowych – należy je traktować jednolicie z innymi podmiotami.	Uwaga nieuwzględniona Wyłączenie z zakresu stosowania środków o których mowa w art. 53 ust. 8 podmiotów publicznych wynika bezpośrednio z dyrektywy NIS2, a zatem stanowi zgodność z prawem unijnym.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

144.	Związek Telewizji Kablowych Izba Gospodarcza	Art. 53	Niezrozumiała jest projektowana regulacja art. 53 ust. 9 ustawy o KSC, wedle której na okoliczność niezastosowania się przed podmiot kluczowy do nakazu, o którym mowa w art. 53 ust. 5 pkt. 1 ustawy o KSC lub postanowień decyzji, o której mowa w art. 53 ust. 5 pkt. 2-5 lub 6 zostało wyłączone uprawnienie organu właściwego do spraw cyberbezpieczeństwa zwrócenia się do sądu o nałożenie tymczasowego zakazu zajmowania stanowiska przez osoby kierujące podmiotem kluczowym, którym jest podmiot publiczny. Nie wiadomo dlaczego projektodawca pragnie w omawianych przypadkach „chronić” osoby zajmujące kierownicze stanowiska w podmiotach publicznych będących podmiotami kluczowymi. Niewątpliwie bowiem zapewnienie takiej „ochrony” osobom kierującym podmiotami publicznymi w stosunku do osób na stanowiskach kierowniczych w podmiotach kluczowych nie będących podmiotami publicznymi świadczy o nierównym traktowaniu tych osób, co jest prawnie niedopuszczalne w świetle regulacji art. 32 ust. 1 w zw. z art. 8 Konstytucji RP gwarantującej równość wobec prawa wszystkich osób oraz przyznającej konstytucyjne prawo do równego traktowania przez władze publiczne. Proponujemy zatem wprowadzenie zmiany do art. 1 pkt. 56 projektu ustawy zmieniającej ustawę o KSC zasadzającej się w nadaniu nowego brzmienia art. 53 ust. 9 ustawy o KSC „Środków, o których mowa w ust. 8 pkt. 1-3 nie stosuje się do podmiotów publicznych.”.	Uwaga nieuwzględniona Wyłączenie z zakresu stosowania środków o których mowa w art. 53 ust. 8 podmiotów publicznych wynika bezpośrednio z dyrektywy NIS2, a zatem stanowi zgodność z prawem unijnym.
145.	KGHM Polska Miedź S.A.	Art. 53 ust. 4 i 5 lit. a)	Rekomenduje się, aby także w zakresie nakazania podjęcia określonych czynności dotyczących obsługi incydentu lub wydania ostrzeżenia, które mogą nakładać na podmiot określone czynności, również następowało w formie decyzji administracyjnej. Adekwatnie do treści uwagi	Uwaga nieuwzględniona Incydent może mieć dynamiczny charakter i wprowadzenie tutaj decyzji administracyjnej może utrudnić skuteczną reakcję. Proponujemy model innej czynności z zakresu administracji publicznej.
146.	PIPC	Art. 53 ust. 4 i 5 lit. a)	Rekomendujemy, aby także w zakresie nakazania podjęcia określonych czynności dotyczących obsługi incydentu lub wydania ostrzeżenia, które mogą nakładać na podmiot określone czynności, również następowało w formie decyzji administracyjnej.	Uwaga nieuwzględniona Incydent może mieć dynamiczny charakter i wprowadzenie tutaj decyzji administracyjnej może utrudnić skuteczną reakcję. Proponujemy model innej czynności z zakresu administracji publicznej.
147.	KGHM Polska Miedź S.A.	Art. 53 ust. 8	W zakresie stosowanych środków rekomendujemy, aby dokładnie wskazać kiedy faktycznie te środki będą mogły być zastosowane, w szczególności w sytuacji, gdy podmiot złoży skargę do WSA i zostanie uwzględniony wniosek złożony w trybie art. 61 ustawy - Prawo o postępowaniu przed sądami administracyjnymi z dnia 30 sierpnia 2002 r. (Dz. U. z 2023 r. poz. 1634 z późn. zm.).	Uwaga uwzględniona Doprecyzowano przepisy oraz uzasadnienie
148.	PIPC	Art. 53 ust. 8	W zakresie stosowanych środków rekomendujemy, aby dokładnie wskazać, kiedy faktycznie te środki będą mogły być zastosowane, w szczególności w sytuacji, gdy podmiot złoży skargę do WSA i zostanie uwzględniony wniosek złożony w trybie art. 61 ustawy - Prawo o postępowaniu	Uwaga uwzględniona Doprecyzowano przepisy oraz uzasadnienie.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

			przed sądami administracyjnymi z dnia 30 sierpnia 2002 r. (t.j. Dz. U. z 2023 r. poz. 1634 z późn. zm.). Adekwatnie do treści uwagi	
149.	KIKE	Art. 53	Poprawienie art. 53 uKSC w zakresie kontroli podmiotów ważnych, aby przebieg kontroli i jej wyniki dotyczyły następnych incydentów a nie działań prewencyjnych. W tym zakresie Projekt jest niekonsekwentny, gdyż z jednej strony deklaruje wobec podmiotów ważnych następny charakter kontroli, a jednocześnie dopuszcza działania związane z prewencją.	Uwaga uwzględniona Przepis został przeredagowany w ten sposób, że doprecyzowano które środki nadzoru sprawowane są odpowiednio do podmiotów ważnych z uwzględnieniem następczego charakteru nadzoru.
150.	KIKE	Art. 53	Zmianę art. 53 ust. 3 pkt 2 uKSC w zakresie nadzoru nad podmiotami ważnymi. Przepis ten powinien wyraźnie wskazywać, że nadzór ma miejsce wyłącznie w sytuacji uzasadnionego podejrzenia, że zachodzi możliwość naruszenia przepisów uKSC. Obecny zapis sugeruje, że nadzór ten jest nieograniczony, a kwestia podejrzenia naruszenia przepisów uKSC jest jedynie przykładowa.	Uwaga wyjaśniona Art. 53 ust. 3 pkt 2 wprost wskazuje, że nadzór nad podmiotami ważnymi sprawowany jest następco. Jednocześnie doprecyzowano, że może być on następco stosowany również wtedy, gdy istnieje uzasadnione podejrzenie, że zachodzi możliwość naruszenia przepisów uKSC. Będą jednak sytuacje, kiedy to nie podejrzenie, a fakt będzie wymuszał wszczęcie nadzoru nad podmiotem. Z tego względu zawężenie nadzoru wyłącznie do uzasadnionego podejrzenia byłoby niezgodne z dyrektywą NIS 2 i celem dyrektywy oraz ustawy.
151.	Konfederacja Lewiatan	Art. 53	Art. 53 ust. 2 pkt 1 projektu KSC nie przewiduje przeprowadzania kontroli doraźnych przez organy właściwe do spraw cyberbezpieczeństwa – a żaden inny przepis nie przewiduje takiej kontroli (także przepisy ustawy – Prawo przedsiębiorców). Zgodnie z art. 7 Konstytucji RP, organy władzy publicznej działają na podstawie i w granicach prawa. Brak wskazania kontroli doraźnych w przepisach podważa możliwość powołania się na te przepisy. Art. 53 ust. 2 pkt 3 projektu KSC przewiduje ocenę bezpieczeństwa systemu informacyjnego podmiotów ważnych jako nadzór o charakterze ex ante, a nie ex post. W konsekwencji, podmioty mogą być niepotrzebnie obciążane dodatkowymi obowiązkami, co narusza ich prawo do swobodnego prowadzenia działalności gospodarczej (art. 22 Konstytucji RP). Dyrektywa NIS2, w szczególności motyw 58 oraz art. 29, przewiduje nadzór ex post wobec podmiotów ważnych, co podkreśla, że nadzór ten powinien być stosowany głównie po wystąpieniu incydentu lub naruszenia, a nie przed (jak proponuje się to w art. 53 ust. 2 pkt 3 projektu KSC). Projekt ustawy nie precyzuje formy poszczególnych czynności, takich jak zlecenie CSIRT, wnioski o udzielenie	Uwagi częściowo uwzględnione i w pozostałym zakresie wyjaśnione: 1) Kontrole doraźne – dodany został art. 59c; 2) Ocena bezpieczeństwa systemu informacyjnego - projekt wyraźnie wskazuje, że środki nadzoru nad podmiotami ważnymi prowadzone są ex post - mają charakter następco. Dopuszczalna jest sytuacja, w której podmiot podejmuje takie działania z uwagi na uzasadnione podejrzenie. Ocena bezpieczeństwa systemu

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

			dostępu do danych, czy postanowienia. Brak jasności w tej kwestii narusza zasadę pewności prawa (art. 2 Konstytucji RP), która wymaga, aby przepisy były precyzyjne i przewidywalne. Nieokreśloność formy czynności administracyjnych może prowadzić do arbitralności działań administracji, co jest sprzeczne z zasadą demokratycznego państwa prawa. W szczególności art. 53 ust. 5 pkt 1 projektu KSC przewiduje możliwość nakazania podjęcia określonych czynności dotyczących obsługi incydentu bez formy decyzji administracyjnej. Takie rozwiązanie narusza prawo do ochrony praw majątkowych (art. 64 Konstytucji RP) oraz prawo do sądu (art. 45 Konstytucji RP), ponieważ podmioty nie mają możliwości zaskarżenia takiego nakazu. Nakazy ingerujące w podstawowe swobody prowadzenia działalności gospodarczej powinny być wydawane w formie decyzji administracyjnej, aby zapewnić podmiotom prawo do obrony i kontroli sądowej. Brak możliwości złożenia wniosku o ponowne rozpatrzenie sprawy, przewidziany w art. 53 ust. 7 projektu KSC, budzi wątpliwości w kontekście art. 78 Konstytucji RP, który gwarantuje każdemu prawo do zaskarżenia decyzji wydanej w pierwszej instancji. Ograniczona rola sądownictwa administracyjnego i brak kompetencji do zajmowania się kompleksową tematyką cyberbezpieczeństwa dodatkowo potęgują te wątpliwości ponieważ podmioty nie mają realnej możliwości obrony swoich praw w pełnym postępowaniu administracyjnym. Wymóg przedstawienia wstępnego stanowiska w ciągu 7 dni, o którym mowa w art. 53 ust. 11-12 projektu KSC, nie zastępuje rzetelnego, sprawiedliwego postępowania administracyjnego, w którym podmiot ma prawo do obrony swoich praw	informacyjnego podmiotu ważnego będzie miała również charakter następczy. Obowiązek ten wynika bezpośrednio z NIS 2 - art. 33 ust. 2 lit. c; 3) Forma czynności - częściowo została przewidziana forma decyzji administracyjnej a częściowo zrezygnowano z tej formy np. przy poleceniu obsługi incydentu. Jest to uzasadnione tym, że obsługa incydentu powinna być prowadzona niezwłocznie, a wprowadzenie procedury administracyjnej znacznie wydłuży okres implementacji rozwiązań niezbędnych do obsługi incydentu. Również w interesie podmiotu powinno być szybkie wdrożenie działań, które pozwolą zminimalizować szkody wyrządzone incydemem; 4) Jednoinstancyjne postępowanie – zarzut ograniczenia prawa do zaskarżenia decyzji wydanej w pierwszej instancji jest niezasadny. Przewidziane zostało bowiem zaskarżenie do sądu administracyjnego. Postępowanie sądowoadministracyjne cechuje się dwuinstancyjnością. Brak możliwości złożenia wniosku o ponowne rozpatrzenie sprawy podyktowane jest potrzebą zapewnienia skuteczności przepisów. Jednocześnie zagwarantowana droga sądowa w pełni realizuje konstytucyjne prawo do sądu.
152.	Konfederacja Lewiatan	Art. 53	Na podstawie art. 53 ust. 4 ustawy KSC, w przypadku uzasadnionego podejrzenia naruszenia przepisów ustawy przez podmiot kluczowy, organ właściwy do spraw cyberbezpieczeństwa kieruje do tego podmiotu pismo w formie elektronicznej z ostrzeżeniem, wskazując czynności, jakie należy podjąć w celu zapobiegnięcia lub zaprzestania naruszania przepisów ustawy. Następnie, zgodnie z art. 76b ust. 1 te same ustawy, organ może nałożyć na podmiot kluczowy	Wyjaśnienie uwagi Przede wszystkim należy zauważyć, że mechanizm ten jest fakultatywny – organ po dokonaniu analizy konkretnej sprawy może

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

			okresową karę pieniężną w wysokości od 500 zł do 100 000 zł za każdy dzień opóźnienia w wykonaniu czynności określonych w ostrzeżeniu. Jednakże, należy podkreślić, że ostrzeżenie, o którym mowa w art. 53 ust. 4 projektu KSC, nie stanowi decyzji administracyjnej ani postanowienia. Forma prawna tego dokumentu nie jest jasno określona w przepisach. Brak precyzyjnego zdefiniowania formy prawnej ostrzeżenia rodzi poważne wątpliwości co do jego charakteru i skutków prawnych. Podmiot, który otrzymał takie ostrzeżenie, może zostać obciążony wysoką karą dzienną aż do 100 000 zł, co stanowi poważne obciążenie finansowe. Nakładanie takiej kary na podstawie dokumentu, który nie ma jednoznacznie określonej formy prawnej, łamie podstawowe zasady praworządności i demokratycznego państwa prawa, przewidziane w Konstytucji RP. W demokratycznym państwie prawa każda ingerencja organu administracji publicznej w prawa i obowiązki obywateli musi być jasna, precyzyjna i oparta na jednoznacznych przepisach prawnych. Zgodnie z art. 2 Konstytucji RP, Rzeczpospolita Polska jest demokratycznym państwem prawnym, urzeczywistniającym zasady sprawiedliwości społecznej. W demokratycznym państwie prawa każda ingerencja organu administracji publicznej w prawa i obowiązki obywateli musi być jasna, precyzyjna i oparta na jednoznacznych przepisach prawnych. Ponadto, zgodnie z art. 7 Konstytucji RP, organy władzy publicznej działają na podstawie i w granicach prawa. Nakładanie kary na podstawie ostrzeżenia, którego forma prawna nie jest jasno określona, stoi w sprzeczności z tymi fundamentalnymi zasadami.	podjąć inne czynności nadzorcze zanim przejdzie do przepisów o karach. Ponadto środki nadzorcze mają różną formę w zależności od charakteru czynności jakich dotyczą - ostrzeżenie (podobnie jak nakaz obsługi incydentu) musi być wydane szybko, bez hamulcowej procedury. Wynika to z faktu, że celem ostrzeżenia jest przede wszystkim zapobieganie naruszeniom lub zapobieganie pogłębianiu tych naruszeń. Tym samym ostrzeżenie oraz nakaz dot. incydentów stanowi inną czynność z zakresu administracji publicznej.
153.	Konfederacja Lewiatan	Art. 53 ust. 8	Nieproporcjonalność nadzoru i rygory sankcji Jednostka redakcyjna: art. 53 ust. 8 projektu KSC Jednostka redakcyjna NIS2: art. 20 ust. 1 Uwaga: Artykuł 53 ust. 8 ustawy KSC wprowadza niezmiernie surowe sankcje, pozwalające organom nadzoru cyberbezpieczeństwa na zawieszenie, ograniczenie lub cofnięcie koncesji do czasu usunięcia przez podmiot kluczowy lub ważny stwierdzonych uchybień lub zaprzestania naruszeń. Co więcej, umożliwia to również wykreślenie podmiotu z rejestru (np. z rejestru przedsiębiorców telekomunikacyjnych Prezesa Urzędu Komunikacji Elektronicznej), co w praktyce może oznaczać natychmiastowe i całkowite zaprzestanie prowadzenia działalności przez danego przedsiębiorcę, jak na przykład w przypadku przedsiębiorcy telekomunikacyjnego, który musiałby natychmiast przerwać świadczenie usług telekomunikacyjnych. Tak drastyczne uprawnienia nadzorcze mogą prowadzić do nadmiernie surowych konsekwencji dla podmiotów, których naruszenia mogą być stosunkowo niewielkie, jak na przykład nieprzeprowadzenie audytu bezpieczeństwa. Wprowadzenie takiego mechanizmu, który może efektywnie „zamknąć” działalność podmiotu na podstawie stwierdzenia administracyjnego bez adekwatnego procesu sądowego lub bez możliwości skutecznego odwołania, jest wysoce nieproporcjonalne. Przewidziane sankcje mogą nie tylko nieodwracalnie zaszkodzić firmom, które z różnych przyczyn mogą czasowo nie spełniać określonych wymogów, ale również destabilizować sektory gospodarki, wpływając na gospodarkę narodową i bezpieczeństwo usług. Odpowiednie byłoby	Uwaga uwzględniona Z przepisu wykreślone zostało odpowiednie zastosowanie w stosunku do podmiotów ważnych oraz uprawnienie do zwracania się do właściwego organu o wykreślenie z rejestru.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

			zatem przemyślenie skali sankcji oraz wprowadzenie bardziej zrównoważonych i proporcjonalnych środków naprawczych, które pozwoliłyby na kontynuację działalności przy jednoczesnym zapewnieniu odpowiednich działań naprawczych, zamiast automatycznego i drastycznego zakończenia działalności.	
154.	ISSA Polska	Art. 53 ust. 8	Artykuł 53 ust. 8 ustawy KSC wprowadza niezmiernie surowe sankcje, pozwalające organom nadzoru cyberbezpieczeństwa na zawieszenie, ograniczenie lub cofnięcie koncesji do czasu usunięcia przez podmiot kluczowy lub ważny stwierdzonych uchybień lub zaprzestania naruszeń. Co więcej, umożliwia to również wykreślenie podmiotu z rejestru (np. z rejestru przedsiębiorców telekomunikacyjnych Prezesa Urzędu Komunikacji Elektronicznej), co w praktyce może oznaczać natychmiastowe i całkowite zaprzestanie prowadzenia działalności przez danego przedsiębiorcę, jak na przykład w przypadku przedsiębiorcy telekomunikacyjnego, który musiałby natychmiast przerwać świadczenie usług telekomunikacyjnych. Tak drastyczne uprawnienia nadzorcze mogą prowadzić do nadmiernie surowych konsekwencji dla podmiotów, których naruszenia mogą być stosunkowo niewielkie, jak na przykład nieprzeprowadzenie audytu bezpieczeństwa. Wprowadzenie takiego mechanizmu, który może efektywnie „zamknąć” działalność podmiotu na podstawie stwierdzenia administracyjnego bez adekwatnego procesu sądowego lub bez możliwości skutecznego odwołania, jest wysoce nieproporcjonalne. Przewidziane sankcje mogą nie tylko nieodwracalnie zaszkodzić firmom, które z różnych przyczyn mogą czasowo nie spełniać określonych wymogów, ale również destabilizować sektory gospodarki, wpływając na gospodarkę narodową i bezpieczeństwo usług. Odpowiednie byłoby zatem przemyślenie skali sankcji oraz wprowadzenie bardziej zrównoważonych i proporcjonalnych środków naprawczych, które pozwoliłyby na kontynuację działalności przy jednoczesnym zapewnieniu odpowiednich działań naprawczych, zamiast automatycznego i drastycznego zakończenia działalności.	Uwaga uwzględniona Z przepisu wykreślone zostało odpowiednie zastosowanie w stosunku do podmiotów ważnych oraz uprawnienie do zwracania się do właściwego organu o wykreślenie z rejestru działalności regulowanej, a także cofnięcie koncesji.
155.	KIKE	Art. 54 ust. 8	Izba wskazuje również, że czynności z art. 53 uKSC w zakresie wykreślenia podmiotu z rejestrów działalności gospodarczej powinny być czynnościami, od których przysługuje odwołanie do sądu administracyjnego. Jest to bowiem czynność władcza organu państwowego mająca doniosłe skutki dla podmiotu gospodarczego i powinna podlegać kontroli sądowej. Co więcej, sama „decyzja o wykreśleniu” (a właściwie to powinno być postanowienie administracyjne) powinno podlegać analizie pod kątem adekwatności i proporcjonalności tego środka. Obecna propozycja sugeruje, że organ ds. cyberbezpieczeństwa ma pełną uznaniowość w zakresie zwrócenia się do właściwego organu o wykreślenie z rejestru prowadzenia działalności gospodarczej, a organ ten ma się do tego żądania zastosować. Zdaniem Izby, jeżeli wykreślenie z rejestru działalności gospodarczej nie będzie poddane kontroli sądowej należy usunąć z Projektu tę kompetencję.	Wyjaśnienie uwagi Przepis został zmieniony, wykreślono m.in. środek nadzorczy w postaci wykreślenia podmiotu z rejestru działalności regulowanej.
156.	Konfederacja Lewiatan	Art. 53 ust. 11	Artykuł 53 ust. 11 projektu ustawy proponuje procedurę wstępnego informowania o działaniach mających na celu wydanie decyzji lub podjęcie działań polegających na tymczasowym zawieszeniu działalności. Jednakże zgodnie z art. 32 ust. 8 NIS2, istnieje wymóg szczegółowego uzasadnienia zastosowanych środków z zakresu egzekwowania przepisów. W związku z tym nie jest jasne, w jakim stopniu działania organów właściwych do spraw cyberbezpieczeństwa będą	Uwaga uwzględniona Przepis został zmodyfikowany o obowiązek szczegółowego uzasadnienia.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

			należycie uzasadniane, co stanowi bezwzględny warunek umożliwiający polemikę z danym rozstrzygnięciem.	
157.	Związek Pracodawców Polska Miedź	Art. 1 pkt 56 ustawy zmieniającej, w zakresie art. 53 ust. 4 i 5 lit. a)	Rekomenduje się, aby także w zakresie nakazania podjęcia określonych czynności dotyczących obsługi incydentu lub wydania ostrzeżenia, które mogą nakładać na podmiot określone czynności, również następowało w formie decyzji administracyjnej.	Uwaga nieuwzględniona Incydent może mieć dynamiczny charakter i wprowadzenie tutaj decyzji administracyjnej może utrudnić skuteczną reakcję. Wydanie nakazu jest inną czynnością z zakresu administracji publicznej.
158.	Związek Pracodawców Polska Miedź	Art. 1 pkt 56 ustawy zmieniającej, w zakresie art. 53 ust. 8	W zakresie stosowanych środków rekomendujemy, aby dokładnie wskazać kiedy faktycznie te środki będą mogły być zastosowane, w szczególności w sytuacji, gdy podmiot złoży skargę do WSA i zostanie uwzględniony wniosek złożony w trybie art. 61 ustawy - Prawo o postępowaniu przed sądami administracyjnymi z dnia 30 sierpnia 2002 r. (Dz. U. z 2023 r. poz. 1634 z późn. zm.).	Uwaga uwzględniona Doprecyzowano przepisy i uzasadnienie.
159.	Polska Izba Przemysłu Chemicznego	Art. 53	Art. 1 pkt 56 ustawy zmieniającej, w zakresie art. 53 ust. 4 i 5 lit. a) - Rekomendujemy, aby także w zakresie nakazania podjęcia określonych czynności dotyczących obsługi incydentu lub wydania ostrzeżenia, które mogą nakładać na podmiot określone czynności, również następowało w formie decyzji administracyjnej.	Uwaga nieuwzględniona środki nadzorcze mają różną formę w zależności od charakteru czynności jakich dotyczą – ostrzeżenie (podobnie jak nakaz obsługi incydentu) musi być wydane szybko, bez hamulcowej procedury. Wynika to z faktu, że celem ostrzeżenia jest przede wszystkim zapobieganie naruszeniom lub zapobieganie pogłębianiu tych naruszeń. Incydent może mieć dynamiczny charakter zatem wprowadzenie decyzji administracyjnej może utrudniać szybkość i skuteczną reakcję. Tym samym ostrzeżenie oraz nakaz dot. incydentów stanowi inną czynność z zakresu administracji publicznej.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

160.	Polskie Stowarzyszenie Fotowoltaiki	Art. 53	Zgodnie z Projektem, nadzór w wykonaniu obowiązków w zakresie cyberbezpieczeństwa sprawowany ma być przez organy właściwe ds. cyberbezpieczeństwa: - w odniesieniu do PK: prewencyjnie i następczo; - w odniesieniu do PW: następczo. Uprawnienia organu właściwego ds. cyberbezpieczeństwa: - przeprowadzanie kontroli; - zobowiązanie do przeprowadzenia audytu; - zlecenie odpowiedniemu CSIRT oceny bezpieczeństwa systemu informacyjnego PK lub PW; - wystąpienie z wnioskiem o udzielenie informacji dot. wdrożenia środków technicznych i organizacyjnych; - wystąpienie z wnioskiem o udzielenie dostępu do danych, dokumentów i informacji; - wystąpienie z wnioskiem o przedstawienie dowodów realizacji wymogów, o których mowa w art. 8 ust. 1. Uprawnienia organu właściwego ds. cyberbezpieczeństwa do nakazania/wyznaczenia w drodze decyzji (ust. 5): - podjęcia określonych czynności dot. obsługi incydentu; - zaniechania naruszania ustawy; - zapewnienia zgodności systemu zarządzania bezpieczeństwem informacji zgodnie z art. 8 lub realizacji obowiązku zgłaszania incydentu poważnego; - odpowiedniego poinformowania odbiorców usług o cyberzagrożeniu; - wdrożenia zaleceń wydanych w wyniku audytu; - urzędnika monitorującego do nadzorowania wykonywania obowiązków, o których mowa w rozdziale 3; - podania do wiadomości publicznej informacji o naruszeniach przepisów ustawy; - nałożenie kary pieniężnej; - podanie do publicznej wiadomości informacji o incydencie poważnym; wraz z zobowiązaniem PK lub PW do usunięcia uchybień lub zapewnienia zgodności z wymogami określonymi przez organ. Dodatkowe uprawnienia organu właściwego w razie niezastosowania do nakazu lub decyzji: - zwrócenie się o zawieszenie, ograniczenie lub cofnięcie koncepcji;	Uwaga uwzględniona Wprowadzono odpowiednie zmiany z przepisach w zakresie określonym w rekomendacjach podmiotu zgłaszającego uwagi.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

		- zwrócenie się o wykreślenie z rejestru działalności regulowanej; - zwrócenie się o cofnięcie zezwolenia na prowadzenie działalności gospodarczej; - zwrócenie się do sądu o nałożenie tymczasowego zakazu zajmowania stanowiska przez osoby kierujące podmiotem kluczowym. Ogólny wpływ regulacji: Szeroki katalog uprawnień organu właściwego względem PK i PW. Obowiązek realizacji nakazanego działania pod groźbą nałożenia kary pieniężnej zgodnie z art. 73 KSC wg Projektu. Możliwe do podjęcia przez organ właściwy środki w postaci zwrócenia się o wycofanie koncesji, zezwolenia na wykonywanie działalności gospodarczej mogą nieść za sobą poważne konsekwencje dla działalności prowadzonej przez PK i PW Wpływ na sektor energetyczny: jw. – brak specyficznego wpływu na sektor energetyczny [Nadregulacja względem Dyrektywy NIS2] Przepisy Projektu zarówno wykraczają istotnie poza zakres Dyrektywy NIS2 jak również zawierają nieprecyzyjne określenia w postanowieniach dotyczących odpowiedzialności PK, PW i osób fizycznych: - Projekt przewiduje możliwość wyznaczenia w drodze decyzji względem PW urzędnika monitorującego do nadzorowania wykonywania obowiązków dot. cyberbezpieczeństwa, podczas gdy Dyrektywa NIS2 nie obejmuje tego środka względem PW (vide art. 33 ust. 4 Dyrektywy NIS2) - środki w postaci zwrócenia się o wycofanie koncesji, zezwolenia na wykonywanie działalności gospodarczej, o których mowa w art. 53 ust. 8 KSC wg Projektu przewidziane są w Dyrektywie NIS2 jedynie w odniesieniu do PK. Dyrektywa NIS2 nie przewiduje ich stosowania względem PW - ponadto, w odniesieniu do PK, Dyrektywa NIS2 przewiduje, że zezwolenia na świadczenie określonych usług powinny być tymczasowe – tymczasem przepisy Projektu przewidują możliwość całkowitego cofnięcia zezwolenia do czasu usunięcia naruszenia. Cofnięcie może skutkować koniecznością przeprowadzenia przez zainteresowany podmiot na nowo odrębnych postępowań administracyjnych w celu uzyskania odpowiedniego zezwolenia, koncesji. W rezultacie, ten środek egzekwowania przepisów nie będzie miał w praktyce „tymczasowego” charakteru ; - w art. 53 ust. 8 pkt 4 KSC wg Projektu wprowadzono możliwość zwrócenia się do sądu o nałożenie tymczasowego zakazu zajmowania stanowiska przez osoby kierujące podmiotem kluczowym. Nie wskazano jednak jakiego stanowiska i w jakim podmiocie zakaz ma dotyczyć. Dyrektywa NIS2 ogranicza się przy tym wyłącznie do wskazania zakazu zajmowania stanowiska kierowniczego w przedmiotowym PK ; - zgodnie z art. 32 ust. 4(g) Dyrektywy NIS2 – środek w postaci oddelegowania urzędnika monitorującego powinien ściśle określać jego zadania oraz okres	

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

			wyznaczenia urzędnika, tymczasem zakres monitorowania urzędnika określony w art. 53 ust. 5 pkt 6 KSC wg Projektu obejmuje ogólnie wykonywanie obowiązków, o których mowa w rozdziale 3. W rezultacie, może to skutkować rozszerzeniem kompetencji urzędnika monitorującego poza zakres wyznaczony w Dyrektywie NIS2. Rekomendacje: Dostosowanie zakresu środków - prawnych o których mowa w art. 53 KSC wg Projektu do zakresu Dyrektywy NIS2, w celu zachowania minimalnego charakteru implementacji, w szczególności: - wyłączenie możliwości wyznaczenia urzędnika monitorującego do nadzorowania wykonywania obowiązków dot. cyberbezpieczeństwa względem PW; - wyłączenie zastosowania art. 53 ust. 8 KSC wg Projektu względem PW; - ograniczenie zakresu delegacji urzędnika monitorującego do nadzorowania wykonywania obowiązków dot. cyberbezpieczeństwa na podstawie art. 53 ust. 5 pkt 6 KSC wg Projektu.	
161.	Polska Organizacja Handlu i Dystrybucji	Art. 53	Art. 53.12 zmiana na „nie później niż w terminie 14 dni (...)”	Uwaga nieuwzględniona Termin 7 dni jest terminem wystarczającym na przekazanie stanowiska w stosunku do informacji o wstępnych ustaleniach organu właściwego do spraw cyberbezpieczeństwa.
162.	Osoba fizyczna	Art. 53a-b	Zastosowano pojęcie „metodyki nadzoru”. Proponuję zamieść na inną formą takich opracowań, jak np. metody, techniki, sposoby itp. Metodyka jest rozwiązaniem organizacyjnym znacznie bardziej złożonym niż metoda, jest definiowana jako metoda realizacji metod. Zdaje się, że do realizacji nadzoru wystarczające będą wskazane metody, techniki, sposoby itp. Proponuję rozważyć i zastosować odpowiednio do potrzeb.	Wyjaśnienie uwagi Nazewnictwo wynika wprost z wdrażanej dyrektywy NIS2.
163.	Osoba fizyczna	Art. 53b	Zastosowano zapisy wskazujące na prowadzenie przez organy właściwe analizy ryzyka dla konkretnych podmiotów, przy czym zakres tej analizy obejmuje zagadnienia wykraczające poza zakres przedmiotowy i merytoryczny ustawy uKSC2 i kwestie cyberbezpieczeństwa, jak np. 1) znaczenie usługi dla bezpieczeństwa narodowego i porządku publicznego, 2) wpływ usługi na gospodarkę, 4) potencjalne skutki incydentu takie jak straty finansowe szkody wizerunkowe, utrata danych osobowych lub zakłócenia w funkcjonowaniu systemów i infrastruktury. W zakresie ustawy uKSC2 jest ryzyko cyberbezpieczeństwa oraz prowadzenia anlizy, a raczej szacowania ryzyka w zakresie cyberbezpieczeństwa. Wskazany w przepisie zakres analizy/szacowania ryzyka odnosi się do zagadnień BIA (analizy wpływu na biznes/działalność) i to na poziomie krajowym, co leży w gestii systemu zarządzania kryzysowego. Przywołując propozycję pkt. 3.2 powyżej: Kwestia bezpieczeństwa usług podmiotów, szczególnie usług kluczowych dla krytycznej działalności społecznej i gospodarczej i bezpieczeństwa państwa, realizowanych z wykorzystaniem infrastruktury (krytycznej) przez podmioty określane operatorami infrastruktury krytycznej jest w jurysdykcji organów zarządzania kryzysowego i ustawy o zarządzaniu kryzysowym. Proponuję, aby kwestie bezpieczeństwa, ciągłości, stabilności i jakości pozostałych,	Uwaga nieuwzględniona Wskazane elementy analizy ryzyka są zdaniem projektodawcy ściśle związane z obszarem tematycznym ustawy. Cyberbezpieczeństwa nie sposób jest odłączyć od kwestii związanych z bezpieczeństwem narodowym, porządkiem publicznym, gospodarką i społeczeństwem, a także pozostałymi zagadnieniami związanymi ze stratami finansowymi, szkodami wizerunkowymi czy zakłóceniami w funkcjonowaniu systemów i infrastruktury. Elementy te oddziałują bowiem silnie na funkcjonowanie państwa na poziomie ekonomicznym i społecznym. W związku z tym uwzględnienie tych

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

			nie krytycznych, usług ważnych, istotnych dla państwa, odpowiadających sektorom, podsektorom i rodzajom działalności podmiotów wskazanych w załącznikach 1 i 2 NIS2/uKSC2 zostały zaadresowane w znowelizowanej ustawie o zarządzaniu kryzysowym, implementującej CER i zapewniającej integrację regulacji NIS2-CER oraz uKSC2-uZK	elementów w analizie ryzyka przy tworzeniu hierarchii priorytetów w sprawowaniu nadzoru po stworzeniu metodyki w ocenie projektodawcy są konieczne. Jednocześnie projektodawca nie wyklucza, że analizie będą poddane inne elementy dlatego posłużył się sformułowaniem „w szczególności”. Metodyki nadzoru oraz hierarchizacja nie są ponadto obligatoryjne a mają jedynie na celu sprawniejsze zarządzanie zadaniami i ich prawidłową realizację.
164.	Polska Organizacja Handlu i Dystrybucji	Art. 53c	Uprawnienia organu do przekazywania informacji powinny być ograniczone do przypadków związanych z zarządzaniem incydentami.	Uwaga nieuwzględniona Organ nadzorczy powinien mieć zdolność do pozyskiwania informacji niezbędnych do prowadzenia działań nadzorczych. Przepis ma na celu umożliwienie prowadzenia skutecznego i prawidłowego nadzoru i kontroli nad podmiotami. Zakres nadzoru jest zdecydowanie szerszy niż zarządzanie incydentami, zatem uwaga co do ograniczenia przepisu jest niezasadna.
165.	Grupa MiSOT	Art. 53c	Art. 53c. „3. Żądanie sporządza się w postaci elektronicznej i przekazuje na adres do doręczeń elektronicznych, a w przypadku braku adresu do doręczeń elektronicznych, żądanie sporządza się w formie pisemnej i nadaje za pośrednictwem operatora świadczącego pocztowe usługi powszechne na terytorium Rzeczypospolitej na adres siedziby podmiotu, do którego jest kierowane. Uzasadnienie: Obecnie mamy przesunięty termin dotyczący e-doręczeń. Czy, biorąc pod uwagę możliwe terminy uchwalenia nowelizacji KSC, jesteście Państwo pewni, że terminy e-doręczeń nie zostaną przesunięte raz jeszcze? Poza tym obecne terminy e-doręczeń daleko wybiegają poza terminy, o których mówimy w kontekście KSC. Jeżeli KSC wejdzie w życie terminowo, czyli w październiku br., ten przepis sprawi przedsiębiorcom kłopot.	Uwaga nieuwzględniona Przepis został przeredagowany w ten sposób, że dopuszczalne będzie przekazanie żądania na adres do doręczeń elektronicznych albo przez system, o którym mowa w art. 46 ust. 1 pkt 6.
166.	Polskie Stowarzyszenie Fotowoltaiki	Art. 53c	Art. 53c - Obowiązek przekazywania informacji przez PK i PW na żądanie organu właściwego] - Obowiązek dotyczy: danych, informacji i dokumentów niezbędnych do wykonywania przez organ jego uprawnień i obowiązków z zakresu sprawowania nadzoru i kontroli, określonych w ustawie. - Projekt przewiduje wskazanie terminu przekazania danych, informacji lub dokumentów adekwatnego do zakresu tego żądania, nie krótszego niż 7 dni.	Uwaga nieuwzględniona W ocenie projektodawcy określenie minimalnego czasu na przekazanie danych, informacji i dokumentów na poziomie 7 dni jest czasem adekwatnym. Organ właściwy do spraw cyberbezpieczeństwa może

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

			Ogólny wpływ regulacji: PK i PW w razie skierowania żądania udzielenia danych lub informacji będą zobowiązane do dostarczenia ich organowi właściwemu ds. cyberbezpieczeństwa we wskazanym terminie. Wpływ na sektor energetyczny: jw. – brak specyficznego wpływu na sektor energetyczny [Nadregulacja względem Dyrektywy NIS2] Dyrektywa NIS2 przewiduje uprawnienie organów właściwych ds. cyberbezpieczeństwa do żądania od PK i PW odpowiednich danych i informacji (vide art. 32 ust. 2 lit. e-f Dyrektywy NIS2). Dyrektywa NIS2 nie precyzuje dodatkowych wymogów żądania innych niż wskazanie celu wniosku i określenie żądanych informacji (art. 32 ust. 3 Dyrektywy NIS2), w szczególności terminu realizacji żądania. Przepis art. 53c KSC wg Projektu wskazuje w tym miejscu na adekwatny termin. Tak nieprecyzyjne określenie terminu jaki powinien zostać wyznaczony przez organ przy jednoczesnym szerokim katalogu informacji o jakie organ ten może wnioskować może skutkować wyznaczaniem zbyt krótkiego terminu, do którego PK i PW nie będzie w stanie się dostosować z przyczyn technicznych lub organizacyjnych. Zwracamy przy tym uwagę, że niewykonanie obowiązku dostarczenia żądanych informacji może być przedmiotem kary pieniężnej na podstawie art. 73 KSC wg Projektu. Wskazanie tej podstawy nałożenia kary pieniężnej wykracza poza zakres wymagany na gruncie Dyrektywy NIS2 (zob. uwagi do art. 73 KSC wg Projektu). Rekomendacja: - wydłużenie minimalnego terminu na realizację żądania informacji i danych przez organ właściwy; - ograniczenie zakresu podstaw nałożenia kary pieniężnej (zob. uwagi do Art. 73 KSC wg Projektu)	sprawować nadzór, który będzie miał charakter pilny – czekanie 14 dni na dane, informacje czy dokumenty jest terminem nieadekwatnym do zakresu nadzoru. Dotyczyć to będzie również sytuacji, w której nadzór sprawowany będzie wobec mniejszego podmiotu, w nieznacznym zakresie. Na podstawie stanu faktycznego i zakresu prowadzonego nadzoru organ właściwy do spraw cyberbezpieczeństwa będzie określał termin. Musi być on odpowiednio długi dla podmiotu nadzorowanego ale jednocześnie odpowiednio krótki aby nie przedłużać prowadzonego nadzoru, który również jest uciążliwy dla podmiotu.
167.	Związek Telewizji Kablowych (ZTKIG)	Art. 53c i art. 43	Nie sposób zgodzić się z zamysłem projektodawcy, który zmieniając zapisy dotyczące tzw. wezwania miękkiego z jednej strony odsyła do stosowania odpowiedniego do tej instytucji regulacji art. 53 c ust. 2 ustawy o KSC (nowe brzmienie art. 43 ust. 1 zd. 2 ustawy o KSC), z drugiej zaś strony uchyla poświęconą wezwaniu miękkiemu regulację art. 43 ust. 3- 5 ustawy o KSC. Przede wszystkim w sytuacji wezwania miękkiego, kiedy to podmiot nie jest obciążony obowiązkiem pozytywnego ustosunkowania się do jego treści nie jest dopuszczalne zastosowanie przepisu o zagrożeniu karą w przypadku braku terminowej odpowiedzi na przekazane żądanie (art. 53 c ust. 2 pkt. 7 ustawy o KSC). Po drugie, nie sposób zgodzić się ze skróceniem terminu na reakcję na wezwanie miękkie z 14 dni od jego otrzymania (art.43 ust. 3 ustawy o KSC), do raptem co najmniej 7 dni od jego otrzymania (art. 53 c ust. 2 pkt. 5 ustawy o KSC). Po trzecie, nie można także zaakceptować propozycji, wedle której wykreśleniu uległaby regulacja art. 43 ust. 4 ustawy o KSC przewidująca, iż podmiot może udzielić odpowiedzi na wezwanie miękkie lub też odmówić udzielenia odpowiedzi na przedmiotowe wezwanie. Po czwarte, nie sposób zaakceptować propozycji uchylenia przepisu art. 43 ust. 5 ustawy o KSC przewidującej, iż wystosowanie wezwania miękkiego oraz brak na nie odpowiedzi nie wpływa na możliwość wszczęcia postępowania administracyjnego lub postępowania kontrolnego. Co więcej,	Uwaga nieuwzględniona Nowe brzmienie przepisu tj. art. 53c jest niezbędne z uwagi na konieczność zapewnienia skuteczności przepisów, w tym w szczególności szybkiego i efektywnego realizowania zadań nadzorczych przez organ właściwy do spraw cyberbezpieczeństwa. Przepis ten ma na celu także realizować główne założenie implementowanej dyrektywy NIS 2, czyli podnoszenie cyberbezpieczeństwa. Dodatkowo to organ właściwy do spraw cyberbezpieczeństwa będzie określał termin, może być on wobec tego dłuższy niż 7 dni – w zależności od stanu faktycznego.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

			uważamy, iż regulację art. 43 ustawy o KSC należy uzupełnić o obowiązek pouczenia adresata takiego wezwania miękkiego o treści art. 43 ust. 4 i ust. 5 ustawy o KSC. Proponowane zatem rozwiązanie przez projektodawcę znacząco pogarsza sytuację podmiotu, do którego skierowano wezwanie miękkie, zwiększając tym samym jego niepewność prawną co do praw i obowiązków tegoż podmiotu w razie otrzymania przedmiotowego wezwania, czemu zapobiega utrzymanie w mocy regulacji art. 43 ust. 3-5 ustawy o KSC. yW reasumpcji omówienia instytucji wezwania miękkiego wnioskujemy o: 1/ zmianę art. 1 pkt. 43 lit. a projektu ustawy zmieniającej ustawę o KSC, w ten sposób, że: a/ w proponowanym art. 43 ust. 1 zd. 2 ustawy o KSC otrzyma nowe brzmienie: „Przepis art. 53 c ust. 2 pkt.1-4 i 6 oraz ust. 3 stosuje się odpowiednio.”, b/ w proponowanym art. 43 ust. 1 ustawy o KSC dodaje się zdanie 3 w brzmieniu „We wniosku o udzielenie informacji, o którym mowa w zd. 1 organ właściwy do spraw cyberbezpieczeństwa umieszcza także pouczenie o treści art. 43 ust. 4 i ust. 5.”,	
168.	Konfederacja Lewiatan	Art. 53c ust. 2 pkt 5	W związku z potencjalnie szerokim zakresem niezbędnych do zgromadzenia i przekazania danych wnioskujemy o dookreślenie, że wskazanie terminu jest proporcjonalne do zakresu żądania, a minimalny termin jest określany na 14 dni, a nie 7 jak w projekcie	Uwaga nieuwzględniona W ocenie projektodawcy termin 7 dni jest terminem wystarczającym na przekazanie danych, informacji i dokumentów. Zwrócić uwagę należy również na fakt, że jest to termin minimalny - tzn. organ nie może żądać przekazania mu dokumentów w terminie krótszym niż 7 dni - zatem jeśli wnioskował będzie o informacje w szerokim zakresie z pewnością termin ten ulegnie odpowiedniemu wydłużeniu.
169.	Polska Izba Informatyki i Telekomunikacji	Art. 53c	Zgodnie z art. 32 ust. 3 dyrektywy NIS2 właściwe organy wykonując swoje uprawnienia wskazane w art. 32 ust. 2 lit. e), f) g), tj. uprawnienia do wnioskowania o udzielenie informacji, udzielenie dostępu oraz przedstawienie dowodów realizacji polityki cyberbezpieczeństwa, podają cel wniosku i określają informacje, o które wnoszą. Tym samym wymogi określone w art. 53c powinny mieć zastosowanie zarówno do wniosków o udzielenie informacji, wniosków o udzielenie dostępu jak również wniosków o przedstawienie dowodów realizacji polityki bezpieczeństwa. Tym samym wnioskujemy o wskazanie w art. 53c ust. 1, że wymogi tam określone dotyczą również obok żądania przekazania danych, informacji i dokumentów: <i>żądania uzyskiwania dostępu do danych, dokumentów i informacji koniecznych do wykonania nadzoru oraz dowodów realizacji wymogów, o których mowa w art. 8 ust. 1.</i>	Uwaga uwzględniona Przepis zostanie doprecyzowany o wskazane w uwadze kwestie.
170.	Polska Izba Informatyki i	Art. 53c	Art. 53c ust. 2 pkt 5 – termin przekazania danych, informacji i dokumentów	Uwaga nieuwzględniona W ocenie projektodawcy określenie minimalnego czasu na przekazanie danych,

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

	Telekomunikacji		W związku z potencjalnie szerokim zakresem niezbędnych do zgromadzenia i przekazania danych wnioskujemy o dookreślenie, że wskazanie terminu jest proporcjonalne do zakresu żądania, a minimalny termin jest określany na 14 dni, a nie 7 jak w projekcie.	informacji i dokumentów na poziomie 7 dni jest czasem adekwatnym. Organ właściwy do spraw cyberbezpieczeństwa może sprawować nadzór, który będzie miał charakter pilny – czekanie 14 dni na dane, informacje czy dokumenty jest terminem nieadekwatnym do zakresu nadzoru. Dotyczyć to będzie również sytuacji, w której nadzór sprawowany będzie wobec mniejszego podmiotu, w nieznacznym zakresie. Na podstawie stanu faktycznego i zakresu prowadzonego nadzoru Organ właściwy do spraw cyberbezpieczeństwa będzie określał termin. Musi być on odpowiednio długi dla podmiotu nadzorowanego ale jednocześnie odpowiednio krótki aby nie przedłużać prowadzonego nadzoru, który również jest uciążliwy dla podmiotu.
171.	Konfederacja Lewiatan	Art. 53d	Z uwagi na bardzo szerokie, projektowane uprawnienia urzędnika monitorującego, wnioskujemy, aby w szczególności w przypadku pkt 1 (swobodny wstęp i poruszanie się po terenie bez obowiązku uzyskania przepustki) oraz pkt 5 (przeprowadzenie oględzin), czynności te odbywały się po wcześniejszym zawiadomieniu podmiotu kluczowego. Jest to istotne w celu umożliwienia prawidłowego wykonywania czynności urzędnika.	Uwaga uwzględniona Przepis został przeredagowany w ten sposób, że w pkt 1 niezbędna będzie przepustka, a w pkt 5 zawiadomienie podmiotu kluczowego.
172.	Polskie Stowarzyszenie Fotowoltaiki	Art. 53d	Art. 53d [Uprawnienia urzędnika monitorującego oddelegowanego do PK lub PW] Uprawnienia urzędnika monitorującego obejmują: - swobodny wstęp i poruszanie się po terenie PK/PW; - wglądu do dokumentów dot. PK/PW; - przetwarzanie danych osobowych; - żądanie wyjaśnień; - przeprowadzanie oględzin urządzeń, nośników, systemów informacyjnych Ogólny wpływ regulacji: W związku z szerszym niż określono w Dyrektywie NIS2 zakresem możliwej delegacji urzędnika monitorującego (zob. uwag wskazane odnośnie do art. 53 KSC wg Projektu), uprawnienia urzędnika monitorującego mogą wykraczać poza to co niezbędne dla weryfikacji stwierdzonej nieprawidłowości w zakresie cyberbezpieczeństwa. Projekt nie zawiera również jakichkolwiek przepisów zapewniających - brak negatywnego wpływu na działalność PK lub PW (jak w przypadku art. 36a-36d); - wymogu odpowiednich kompetencji specjalistycznych od urzędnika nadzorującego. Wpływ na sektor energetyczny: jw. – brak specyficznego wpływu na sektor energetyczny [Nadregulacja względem Dyrektywy NIS2] Dyrektywa NIS2 nie zawiera postanowień w zakresie uprawnień urzędnika monitorującego oddelegowanego do nadzorowania wykonania obowiązków	Uwaga częściowo uwzględniona Wprowadzono korektę do odesłania oraz zmodyfikowano przepis pod kątem obowiązku uzyskania przepustki, zawiadomienia podmiotu oraz obowiązku urzędnika do przestrzegania tajemnicy prawnie chronionej odrębnymi przepisami. Urzędnik monitorujący nie będzie wyznaczany do nadzoru podmiotu ważnego. Wprowadzenie wymogu posiadania specjalistycznej wiedzy jest niemożliwe z uwagi na nieprecyzyjność tego kryterium, a jego doprecyzowanie nie odpowiadałoby wymaganiom praktyki. Specjalistyczna

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

			w zakresie cyberbezpieczeństwa. Z uwagi jednak na określenie tego środka jedynie względem PK, przepis art. 53d mający zastosowanie również do PW stanowi w rezultacie nadregulację względem Dyrektywy NIS2. Ponadto, Projekt zawiera błąd legislacyjny – błędne odwołanie do urzędnika monitorującego, „o którym mowa w art. 53 ust. 5 pkt 7” -właściwe odniesienie do art. 53 ust. 5 pkt 6 KSC wg Projektu. Rekomendacje: - zapewnienie wymogu posiadania specjalistycznej wiedzy przez urzędnika monitorującego; - korekta odniesienia do art. 53 ust. 5 pkt 6; - odnośnie do stosowania środka w postaci wyznaczenia urzędnika monitorującego względem PW oraz zakresu jego zadań – zob. uwagi do art. 53 KSC wg Projektu.	wiedza musiałaby być zależna od zakresu działania nadzorczego i specyfiki podmiotu nadzorowanego – nie jest możliwe doprecyzowanie zakresu tej wiedzy przed zbadaniem jakiego naruszenia czy możliwego naruszenia dotyczyć ma nadzór. Byłoby to również utrudnienie dla organu właściwego do spraw cyberbezpieczeństwa, który może mierzyć się z brakami kadrowymi osób o określonych kwalifikacjach, które byłyby ustanowione wprost w ustawie. Organ właściwy do spraw cyberbezpieczeństwa będzie musiał określać zadania takiego urzędnika monitorującego i to na ich podstawie będzie dopierał właściwą osobę, która będzie pełniła funkcję urzędnika monitorującego.
173.	Polska Izba Informatyki i Telekomunikacji	Art. 53d	Z uwagi na bardzo szerokie, projektowane uprawnienia urzędnika monitorującego, wnioskujemy, aby w szczególności w przypadku pkt 1 (swobodny wstęp i poruszanie się po terenie bez obowiązku uzyskania przepustki) oraz pkt 5 (przeprowadzenie oględzin), czynności te odbywały się po wcześniejszym zawiadomieniu podmiotu kluczowego. Jest to istotne w celu umożliwienia prawidłowego wykonywania czynności urzędnika. W zakresie uprawnienia do swobodnego wstępu bez obowiązku uzyskania przepustki dostrzegamy sprzeczność z normą ISO 27001. Kontrola dostępu jest jednym z wymogów ISO27001, na które powołuje się niniejszy akt prawny. Zgodnie z tym standardem i najlepszymi praktykami z zakresu cyberbezpieczeństwa i socjotechniki na wstęp i poruszanie się po siedzibie spółki niezbędne jest uzyskanie przepustki. W związku z powyższym dostrzegamy konieczność zmiany poprzez wykreślenie punktu lub zmianę na: 1) wstępu i poruszania się po terenie podmiotu kluczowego za uzyskaniem przepustki. Ponieważ urzędnik monitorujący byłby sui generis „kuratorem” podmiotu kluczowego należy rozważyć czy nie powinno się doprecyzować, że pracownik taki powinien mieć poświadczenie bezpieczeństwa co najmniej o klauzuli "tajne", a decyzja o której mowa w przepisie powinna wskazywać ściśle określone zadania jakie ma wykonywać taki „kurator” zgodnie z art. 32 ust. 4 lit g NIS2 albo przynajmniej wprowadzenie możliwości odpowiedzialności za ujawnienie tajemnicy przedsiębiorstwa	Uwaga częściowo uwzględniona Przepis został przeredagowany w ten sposób, że urzędnik monitorujący zobowiązany będzie uzyskać przepustkę. W zakresie pkt 5 konieczne będzie wcześniejsze zawiadomienie podmiotu. Urzędnik monitorujący będzie ponosił odpowiedzialność za ujawnienie tajemnicy prawnie chronionej na zasadzie przepisów prawa powszechnie obowiązującego. Należy mieć na uwadze również fakt, że urzędnik monitorujący będzie ponosił odpowiedzialność wynikającą z kodeksu pracy jako że zadania nadzorcze będzie sprawował w ramach zatrudnienia w organie właściwym do spraw cyberbezpieczeństwa.
174.	Fundacja Bezpieczna Cyberprzestrzeń	Art. 53d	Art. 1 pkt 57, treść art. 53d – przedstawione w tym artykule przepisy, zwłaszcza ust. 1 pkt 1 i dalszych, jeśli są konsekwencją wykorzystania tych uprawnień, stoją w sprzeczności z wymaganiami postawionymi podmiotom kluczowym i podmiotom ważnym w art. 8, w tym w	Wyjaśnienie uwagi Dokonano odpowiednich zmian w przepisie – urzędnik monitorujący będzie m.in.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

			szczegółności wymogiem wdrożenia systemu zarządzania bezpieczeństwem informacji oraz środków technicznych i organizacyjnych zmniejszających ryzyko. Przepis sam w sobie tworzy wyłom w systemie bezpieczeństwa organizacji. Oczywiście znane są organy kontrolne z podobnymi uprawnieniami, ale z reguły te uprawnienia są wsparte odpowiednimi przepisami wykonawczymi np. w sprawie określenia wzoru umundurowania, legitymacji służbowych itp., na podstawie których następowałaby niezawodna identyfikacja osoby kontrolującej i przysługujących jej uprawnień. Proponuje się usunięcie art. 53d ust. 1 pkt 1 lub nadanie mu następującej treści: „1) poruszania się po terenie podmiotu kluczowego,”.	obowiązany posiadać przepustkę. Dodatkowo doprecyzowano przepis uprawniający do wyznaczenia urzędnika monitorującego – określono w nim okres na który można wyznaczyć urzędnika, a także obowiązek ścisłego określenia jego zadań. Urzędnik monitorujący zatem będzie mógł korzystać ze swoich uprawnień w celu realizacji ściśle określonych w decyzji o wyznaczeniu zadań.
175.	Fundacja Open Allies	Art. 53d	Zwracamy się o modyfikację uprawnień urzędnika monitorującego. Naszym zdaniem nadmiarowe jest uprawnienie urzędnika monitorującego do działań <i>bez obowiązku uzyskiwania przepustki</i> . Art. 53d ust. 1 pkt 1 powinien brzmieć: „ <i>swobodnego wstępu i poruszania się po terenie podmiotu kluczowego bez obowiązku uzyskiwania przepustki</i> ”. W szczególności u podmiotów kluczowych, z wielu branż, znajdują się pomieszczenia, do których wstęp jest ściśle ograniczony i monitorowany. Jako przykład możemy wskazać data center lub, z innego sektora, laboratoria farmaceutyczne. Urzędnik monitorujący może mieć ustawowe uprawnienie wstępu do wszystkich pomieszczeń – jednak dostęp nie powinien odbywać się dowolnie, lecz w sposób obowiązujący u danego podmiotu (np. określony w regulaminie wewnętrznym), z uwzględnieniem zasad odpowiedniego bezpieczeństwa. Ponadto, zwracamy się o uzupełnienie warunków, jakie urzędnik monitorujący powinien spełniać. Naszym zdaniem urzędnik monitorujący powinien gwarantować ochronę danych osobowych, informacji stanowiących tajemnicę przedsiębiorstwa, oraz tam, gdzie jest to uzasadnione, tajemnicę telekomunikacyjną. Odpowiednie przepisy powinny znaleźć się w art. 53d ust. .1, zaś urzędnik monitorujący, przed podjęciem czynności, powinien przekazać podmiotowi ważnemu lub kluczowemu odpowiednie oświadczenia.	Uwaga częściowo uwzględniona Urzędnik monitorujący będzie zobowiązany uzyskać przepustkę, a uprawnienie, o którym mowa w pkt 5 tego przepisu będzie realizowane po uprzednim zawiadomieniu podmiotu. Jednocześnie wskazać należy, że urzędnik monitorujący zobowiązany jest do realizacji powierzonych zadań z zachowaniem przepisów o tajemnicy prawnie chronionej. Tyczy się to zarówno tajemnicy zawodowej, tajemnicy przedsiębiorcy i innych regulowanych odrębnymi przepisami. Urzędnik monitorujący wykonuje swoje czynności będąc zatrudnionym w organie właściwym do spraw cyberbezpieczeństwa, wiąza go zatem również przepisy wynikające z kodeksu pracy w zakresie obowiązków i odpowiedzialności pracowniczej.
176.	Osoba fizyczna	Art. 53d	W propozycji zapisów art. 53d.1. zamieszczono zapisy mogące naruszać postanowienia innych ustaw i przepisów krajowych czy unijnych, dotyczących działalności między innymi związanymi z IK, czy: - Tajemnicy lekarskiej, - Tajemnicy adwokackiej, - Tajemnic handlowych, - Informacji poufnych w ramach stosunków pracy, - Tajemnic służbowych pracowników administracji publicznej.	Uwaga częściowo uwzględniona W ocenie projektodawcy nakaz zachowania tajemnicy prawnie chronionej jest wystarczający, aby zapewnić przestrzeganie tych tajemnic. Proponowany przepis jest wdrożeniem postanowień dyrektywy NIS 2, która nakłada na państwa członkowskie obowiązek wyposażenia urzędnika

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

			Nakaz zachowania tajemnicy prawnie chronionej, nie jest w tym przypadku wystarczający. Podobnie zapis, który stanowi o możliwości odstąpienia od uzyskania przepustki. Przepustka jest instrumentem identyfikacji osoby i w sytuacjach, przykładowo, poruszania się po jednostkach służb mundurowych, czy medycznych jest instrumentem niezbędnym. Czynności kontrolne nie mogą burzyć porządku organizacyjnego służb bezpieczeństwa czy organizacji pracy, przykładowo placówek medycznych czy mundurowych.	monitorującego w kompetencje, które pozwolą na prawidłowe i skuteczne realizowanie jego zadań. Wyposażając urzędnika monitorującego w kompetencje ,o których mowa w art. 53d kierowano się w szczególności uprawnieniami, jakie przysługują osobom wykonującym kontrolę. Są to uprawnienia na tyle podstawowe i niezbędne, że bez nich nie jest możliwe, aby urzędnik monitorujący prawidłowo realizował powierzone mu zadania. Przepis jest zatem wzorowany na obecnie obowiązującym art. 55 ustawy o krajowym systemie cyberbezpieczeństwa, a dodatkowo wprost nakazuje zachowanie tajemnicy prawnie chronionej. Tym samym nie można zgodzić się, że uprawnienia urzędnika naruszają postanowienia innych ustaw oraz mogą zagrażać zachowaniu tajemnicy zawodowej, służbowej czy informacji poufnych. W szczególności wskazać należy, że każda tajemnica zawodowa oraz zagadnienia związane z jej ujawnianiem i ochroną podlega właściwym ustawom i innym aktom prawnym. W przypadku tajemnicy zawodowej nie można również wyklądać możliwości zwolnienia z niej w sposób rozszerzający. Właściwe akty prawne przewidują ponadto sposób postępowania w przypadku, kiedy tajemnica zawodowa może zostać naruszona. Ponadto urzędnik monitorujący będzie pracownikiem zatrudnionym w organie właściwym do spraw cyberbezpieczeństwa, który również związany jest tajemnicą w odniesieniu do zadań, które realizuje i informacji, które w ramach realizacji zadań pozyskuje.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

				W zakresie uzyskiwania przepustki przez urzędnika monitorującego uwaga została uwzględniona.
177.	Związek Pracodawców Technologii Cyfrowych Lewiatan	Art. 53d	Oczywiście w tym przypadku należy także rozważyć elementy związane ze sprawowaniem nadzoru zwłaszcza opisanymi w art. 53d. Czy urzędnik monitorujący uda się za granicę aby bez przepustki poruszać się po terenie podmiotu kluczowego i przeprowadzać oględziny urządzeń, nośników i systemów informacyjnych? Czy urzędnik monitorujący z innego kraju UE będzie mógł wkroczyć bez przepustki na teren CPD na terenie Polski i dokonywać oględzin? Jak takie oględziny związane z prewencyjną kontrolą podmiotu X będą wyglądały u dostawcy chmury obliczeniowej, gdzie przetwarzają także podmioty Y i Z? A może także podmiot U, który nie jest polskim podmiotem? Wreszcie jak wygląda odpowiedzialność w przypadku kiedy urzędnik monitorujący dokonując oględzin doprowadzi do incydentu bezpieczeństwa, zwłaszcza kiedy przetwarzanie będzie miało miejsce w infrastrukturze innego podmiotu, a incydent dotyczy podmiotu trzeciego, niebędącego przedmiotem kontroli? Uważamy, że projekt uksc powinien być bardzo dokładnie przejrany pod kątem różnych scenariuszy przetwarzania, tak aby oddawał rzeczywistość technologiczną, a także relacje nadzoru opisane w innych aktach prawnych powiązanych z Dyrektywą NIS 2	Uwaga uwzględniona Urzędnik monitorujący przed rozpoczęciem wykonywania swoich zadań będzie musiał uzyskać przepustkę. Dodatkowo przepis został uzupełniony o bezpośrednie wskazanie, że odpowiednio stosuje się art. 58. Zatem czynności urzędnika monitorującego będą opisane w protokole. Jednocześnie wskazać należy, że urzędnik monitorujący będzie wykonywał swoje zadania jako pracownik organu właściwego do spraw cyberbezpieczeństwa – w związku z tym wszelką odpowiedzialność za szkody będzie ponosił przede wszystkim na podstawie Kodeksu Pracy.
178.	Polska Organizacja Handlu i Dystrybucji	Art. 54	Limit czasu trwania kontroli wobec podmiotu kontrolowanego na poziomie 48 dni roboczych jest nadmiarowy. Uzasadniony limit to max 20 dni.	Uwaga nieuwzględniona Krajowy System Cyberbezpieczeństwa będzie obejmował swoim zakresem bardzo dużą – w stosunku do obecnego stanu – liczbę podmiotów. Tym samym liczba podmiotów kontrolowanych będzie wielokrotnie większa niż jest organów właściwych i ich pracowników, którzy będą wykonywać funkcje kontrolne. Ograniczenie czasowe, które określone jest w prawie przedsiębiorców znacznie utrudni prawidłową – a nie jedynie pobieżną – realizację czynności kontrolnych. Dodatkowo wskazać należy, że specyfika naruszeń ustawy i ich wpływ na ciągłość działania, łańcuch dostaw, ochronę danych i bezpieczeństwo państwa prowadzi do wniosku, że kontrola pełni istotną funkcję. Naruszenia dokonywane przez mikroprzedsiębiorcę, małego czy średniego

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

				przedsiębiorcę mogą być równie dotkliwie, a rozróżnienie czasu kontroli w tych podmiotach może nie zawsze być adekwatne do skali naruszenia i niezbędności działań, jakie należy podjąć.
179.	PGE SA	Art. 1 pkt 57 projektu, Art. 53d ust. 1. pkt 1 oraz Art. 55 pkt 1 ustawy	Nie jest dopuszczalne, by na teren zakładu wchodziły osoby bez przepustki, ze względu na bezpieczeństwo infrastruktury krytycznej, jak i osób, które chcą wejść na teren. Wymagane jest, by osoba prowadząca czynności poruszała się po terenie zakładu w obecności pracownika, który będzie mógł ją ewentualnie wprowadzić do miejsc objętych systemem kontroli dostępu oraz ostrzegał o miejscach niebezpiecznych.	Uwaga uwzględniona Urzędnik monitorujący przed rozpoczęciem wykonywania swoich zadań będzie musiał uzyskać przepustkę.
180.	Cybermadein Poland	Art. 56	W art. 56 w dodanym ust.3 wskazany wymóg tłumaczenia dokumentacji przez podmiot kontrolowany należy doprecyzować w sposób następujący: „Tłumaczenie powinno być wykonane przez tłumacza przysięgłego”.	Uwaga nieuwzględniona Nałożenie obligatoryjnego obowiązku polegającego na tym, że tłumaczenie może być dokonane wyłącznie przez tłumacza przysięgłego stanowi dodatkowe, nieuzasadnione, obciążenie finansowe podmiotów. Wskazać należy, że zakres dokonania tłumaczenia może być bardzo szeroki co generowałoby znaczne koszty po stronie podmiotu. W związku z tym projektodawca postanowił nie narzucać sposobu dokonania tłumaczenia przez podmiot.
181.	Polska Izba Informatyki i Telekomunikacji	Art. 56	Wnioskujemy o doprecyzowanie przepisu o wskazanie, że tłumaczenia są przygotowywane na uzasadniony wniosek organu kontrolującego, w którym wskazany jest związek wniosku z faktycznym zakresem kontroli oraz zakres w jakim dany dokument miałby zostać przetłumaczony. W naszej ocenie wyłączone z tego zakresu powinny zostać dokumenty zawierające normy techniczne. Tłumaczenie tego typu dokumentów (których często nie realizuje nawet PKN wdrażając normy europejskie) byłoby obowiązkiem bardzo kosztownym i czasochłonnym dla podmiotu kontrolowanego. W powszechnym obrocie często wykorzystywane są wersje w języku angielskim.	Uwaga częściowo uwzględniona Przepis został doprecyzowany o zakres tłumaczenia, związek z kontrolą oraz określenie terminu na przedstawienie tłumaczenia. W pozostałym zakresie należy wskazać, że w Polsce językiem urzędowym jest język polski (art. 27 Konstytucji RP). Podmioty wykonujące zadania publiczne na terytorium

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

				Polski dokonują wszelkich czynności urzędowych w języku polskim (chyba że przepisy szczególne stanowią inaczej). Obliguje je do tego art. 5 ust. 1 ustawy o języku polskim. Konsekwentnie organ właściwy do spraw cyberbezpieczeństwa, m.in. prowadząc kontrolę, wykonuje swoje działania w języku polskim. Przekłada się to na obowiązki podmiotów kontrolowanych. Tożsame podejście dotyczące obciążeniem kosztami tłumaczenia podmiotu kontrolowanego wynika z Ordynacji podatkowej. Zgodnie z art. 287 Ordynacji podatkowej kontrolowany, jego pracownik oraz osoba współdziałająca z kontrolowanym muszą na wezwanie kontrolujących przedłożyć tłumaczenie na język polski dokumentacji sporządzonej w języku obcym, a dotyczącej spraw będących przedmiotem kontroli podatkowej. Kontrolowany wykonuje przekłady na własny koszt.
182.	Konfederacja Lewiatan	Art. 56	Wnioskujemy o doprecyzowanie przepisu o wskazanie, że tłumaczenia są przygotowywane na uzasadniony wniosek organu kontrolującego, w którym wskazany jest związek wniosku z faktycznym zakresem kontroli oraz zakres w jakim dany dokument miałby zostać przetłumaczony. W naszej ocenie wyłączone z tego zakresu powinny zostać dokumenty zawierające normy techniczne. Tłumaczenie tego typu dokumentów (których często nie realizuje nawet PKN wdrażając normy europejskie) byłoby obowiązkiem bardzo kosztownym i czasochłonnym dla podmiotu kontrolowanego. W powszechnym obrocie często wykorzystywane są wersje w języku angielskim.	Uwaga częściowo uwzględniona Przepis został doprecyzowany o zakres tłumaczenia, związek z kontrolą oraz określenie terminu na przedstawienie tłumaczenia. W pozostałym zakresie należy wskazać, że w Polsce językiem urzędowym jest język polski (art. 27 Konstytucji RP). Podmioty wykonujące zadania publiczne na terytorium Polski dokonują wszelkich czynności urzędowych w języku polskim (chyba że przepisy szczególne stanowią inaczej). Obliguje je do tego art. 5 ust. 1 ustawy o języku polskim. Konsekwentnie organ właściwy do spraw cyberbezpieczeństwa, m.in. prowadząc kontrolę, wykonuje swoje

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

				działania w języku polskim. Przekłada się to na obowiązki podmiotów kontrolowanych. Tożsame podejście dotyczące obciążeniem kosztami tłumaczenia podmiotu kontrolowanego wynika z Ordynacji podatkowej. Zgodnie z art. 287 Ordynacji podatkowej kontrolowany, jego pracownik oraz osoba współdziałająca z kontrolowanym muszą na wezwanie kontrolujących przedłożyć tłumaczenie na język polski dokumentacji sporządzonej w języku obcym, a dotyczącej spraw będących przedmiotem kontroli podatkowej. Kontrolowany wykonuje przekłady na własny koszt.
183.	Związek Telewizji Kablowych Izba Gospodarcza	Art. 56	Nie sposób zgodzić się z wymogiem tłumaczenia dokumentacji na potrzeby kontroli na koszt podmiotu kontrolowanego. Przerzucenie kosztu tłumaczenia dokumentacji na podmiot kontrolowany nie znajduje oparcia w dyrektywie NIS 2, stąd obciążenie kosztami tłumaczenia dokumentacji podmiotu kontrolowanego stanowi kolejny przykład obciążania przedsiębiorców kosztami, które winny obciążać państwo polskie, gdyż to ono zainteresowane jest przeprowadzaniem czynności kontrolnych w swoim własnym interesie. Takie rozwiązanie jest nie do pogodzenia z konstytucją zasadą sprawiedliwości społecznej (art. 2 w zw. z art. 8 Konstytucji RP). Proponujemy zatem zmianę art. 1 pkt. 59 ustawy zmieniającej ustawę o KSC w ten sposób, że w dodawanym art. 56 ust. 3 zd. 2 otrzymuje nowe brzmienie: „<i>Tłumaczenie dokumentacji wykonuje na własny koszt organ prowadzący czynności kontrolne lub też tłumaczenia dokumentacji dokonuje podmiot kontrolowany na koszt organu prowadzącego czynności kontrolne.</i>”.	Uwaga nieuwzględniona W Polsce językiem urzędowym jest język polski. Podmioty wykonujące zadania publiczne na terytorium Polski dokonują wszelkich czynności urzędowych w języku polskim (chyba że przepisy stanowią inaczej) Konsekwentnie organ właściwy do spraw cyberbezpieczeństwa wykonuje swoje działania w języku polskim. Przekłada się to na obowiązki podmiotów kontrolowanych. Tożsame podejście dotyczące obciążeniem kosztami tłumaczenia podmiotu kontrolowanego wynika z Ordynacji podatkowej. Zgodnie z art. 287 Ordynacji podatkowej kontrolowany, jego pracownik oraz osoba współdziałająca z kontrolowanym muszą na wezwanie kontrolujących przedłożyć tłumaczenie na język polski dokumentacji sporządzonej w języku obcym, a dotyczącej spraw będących przedmiotem kontroli. Kontrolowany wykonuje przekłady na własny koszt.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

184.	Polskie Stowarzyszenie Fotowoltaiki	Art. 56	Art. 55-56 - [Uprawnienia osoby przeprowadzającej kontrolę w PK lub PW] Uprawnienia urzędnika kontrolującego obejmują: - wgląd w wstęp i porównanie po trzecie; - wgląd do dokumentów dot. działalności kontrolowanego; - sporządzanie kopii, odpisów wyłączeń z dokumentów; - przetwarzanie danych osobowych; - żądanie wyjaśnień; - przeprowadzenie oględzin urządzeń, obiektów, systemów i formacji; - żądanie przedstawienia tłumaczenia na język polski sporządzonej w języku obcym dokumentacji przedłożonej przez podmiot kontrolowany (tłumaczenie na koszt kontrolowanego) [Obowiązki kontrolowanych przedsiębiorców] Obowiązek PK i PW: - zapewnienia warunków niezbędnych do prawidłowego przeprowadzenia kontroli; - potwierdzania za zgodność z oryginałem porównania kopii i wydruków; Projekt nie wprowadza zmian do art. 55 i 56 KSC z wyłączeniem obowiązku wykonania przez podmiot kontrolowany tłumaczenia dokumentacji na język polski na jego koszt. Wpływ na sektor energetyczny: jw. – brak specyficznego wpływu na sektor energetyczny Dyrektywa NIS2 nie wprowadza dalej idących regulacji dot. obowiązków PK lub PW oraz uprawnień urzędników w razie przeprowadzanych kontroli. Ponadto, Dyrektywa NIS2 nie nakłada w żadnym wypadku obowiązku dostarczania organowi kontrolującemu tłumaczenia jakiegokolwiek dokumentacji. W tym miejscu wskazujemy, że: - przepis nie precyzuje zakresu pojęcia dokumentacji; - sporządzenie dokumentacji pochodzących od podmiotów trzecich, w tym dostawców produktów ICT, usług ICT i procesów ICT może być znacznie utrudnione, a ponadto wymagać autoryzacji zgodności z oryginalną treścią przez takich dostawców. W końcu, korzystanie przez podmiot kontrolowany z tłumaczenia – opracowania – dokumentacji wchodzi w zakres autorskich praw zależnych i może wymagać zgody uprawnionego. W efekcie, realizacja obowiązku określonego w Projekcie może nieść ryzyko naruszenia autorskich praw podmiotu trzeciego. Rekomendacja: - wycofanie obowiązku dostarczenia tłumaczenia dokumentacji na język polski na żądanie organu kontrolującego.	Uwaga nieuwzględniona Wskazać należy, że projekt ma na celu nie tylko wdrożenie postanowień dyrektywy NIS2, ale jest efektem przeglądu funkcjonowania przepisów obecnie obowiązującej ustawy. Jednocześnie zwraca uwagę fakt, że w Polsce językiem urzędowym jest język polski. Podmioty wykonujące zadania publiczne na terytorium Polski dokonują wszelkich czynności urzędowych w języku polskim (chyba że przepisy stanowią inaczej) Konsekwentnie organ właściwy do spraw cyberbezpieczeństwa wykonuje swoje działania w języku polskim. Przekłada się to na obowiązki podmiotów kontrolowanych. Tożsame podejście dotyczące tłumaczenia i obciążeniem kosztami tłumaczenia podmiotu kontrolowanego wynika z Ordynacji podatkowej. Zgodnie z art. 287 Ordynacji podatkowej kontrolowany, jego pracownik oraz osoba współdziałająca z kontrolowanym muszą na wezwanie kontrolujących przedłożyć tłumaczenie na język polski dokumentacji sporządzonej w języku obcym, a dotyczącej spraw będących przedmiotem kontroli. Kontrolowany wykonuje przekłady na własny koszt.
185.	Polskie Towarzystwo Informatyczne	Art. 56	W art. 56 w dodanym ust. 3 wskazany wymóg tłumaczenia dokumentacji przez podmiot kontrolowany należy doprecyzować w sposób następujący: „Tłumaczenie powinno być wykonane przez tłumacza przysięgłego” ze względu na konieczność wiernego przetłumaczenia takiej dokumentacji	Uwaga nieuwzględniona Nałożenie obligatoryjnego obowiązku polegającego na tym, że tłumaczenie może być dokonane wyłącznie przez tłumacza przysięgłego stanowi dodatkowe, nieuzasadnione, obciążenie finansowe podmiotów. Wskazać należy, że zakres dokonania tłumaczenia może być bardzo szeroki co generowałoby znaczne koszty po stronie podmiotu. W związku z tym

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

				projektodawca postanowił nie narzucać sposobu dokonania tłumaczenia przez podmiot.
186.	ZBP	Art. 56 ust. 2	Czas trwania kontroli realizowanej wobec podmiotów kluczowych lub podmiotów ważnych będących przedsiębiorcami w jednym roku kalendarzowym nie może przekroczyć 48 dni roboczych.”; Powyższe ograniczenie może dotyczyć przebywania przedstawicieli organu kontrolującego w podmiotach kontrolowanych i absorbowania zasobów kadrowych tych podmiotów, ale czas ten nie będzie wystarczający na przeanalizowanie rozwiązań informatycznych i sporządzenie wymaganej dokumentacji.	Uwaga nieuwzględniona Należy wskazać, że projektowana ustawa wydłuży w stosunku do stanu obecnego czas przeprowadzenia kontroli czyniąc tym samym wyłom od ogólnych zasad kontroli wynikających z ustawy – Prawo przedsiębiorców. Czyni to jedynie w zakresie niezbędnym i koniecznym dla skuteczności i prawidłowości prowadzonej kontroli i realizowanych zadań. W ocenie projektodawcy jest to termin wystarczający na przeprowadzenie wszystkich czynności związanych z kontrolą.
187.	PERN SA - SOC	Art. 56 ust. 3	Powinny zostać uwzględnione przypadki gdy dostarczona dokumentacja stanowi tajemnicę przedsiębiorstwa i nie powinna być tłumaczona przez kancelarię zewnętrzną. Art. 1 pkt 59 (art. 56 ust. 3 ustawy) – projektowane brzmienie przepisu powinno zostać uzupełnione o wyłączenie spod jego zakresu dokumentacji objętych tajemnicą przedsiębiorstwa;	Uwaga uwzględniona Doprecyzowano, że zlecenie tłumaczenia dokumentacji podmiotom trzecim powinno odbywać się z poszanowaniem tajemnicy prawnie chronionej na podstawie odrębnych przepisów.
188.	ZBP	Art. 56 ust.3	Organ przeprowadzający kontrolę może żądać od podmiotu kontrolowanego przedstawienia tłumaczenia na język polski sporządzonej w języku obcym dokumentacji przedłożonej przez podmiot kontrolowany. Tłumaczenie dokumentacji podmiot kontrolowany jest obowiązany wykonać na własny koszt. Uwaga ogólna Tłumaczenie dokumentacji (zwłaszcza technicznej , która może być liczona w setkach stron) może być czasochłonne i generować duże koszty po stronie podmiotów kontrolowanych. Sugerujemy dodanie przepisów jednoznacznie zabezpieczających dostarczenie wraz z tłumaczeniem oryginałów dokumentacji tłumaczonej.	Uwaga częściowo uwzględniona Przepis został przeredagowany w ten sposób, aby zminimalizować obciążenia finansowe podmiotu kontrolowanego. Podmiot kontrolujący będzie musiał wskazać zakres dokumentów, które należy przetłumaczyć, ich związek z prowadzoną kontrolą oraz określić termin przetłumaczenia dokumentacji biorąc pod uwagę zakres koniecznego tłumaczenia. Jednocześnie nie budzi wątpliwości, że podmiot dostarcza dokumentację niezbędną do przeprowadzenia kontroli, a jedynie na żądanie podmiotu dostarcza również tłumaczenie.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

189.	PERN SA -SOC	Art. 58 ust. 11	Czy biorąc pod uwagę stopień informatyzacji, nie można zrezygnować z formy papierowej ? Uzgadnianie dokumentów i umów może zająć wiele czasu. Art. 1 pkt 60 (art. 58 ust. 11 pkt 1 ustawy) – rozważenia wymaga kwestia rezygnacji ze sporządzania protokołu kontroli w postaci papierowej na rzecz wyłącznie postaci elektronicznej, co w dobie informatyzacji powinno być zasadą;	Uwaga nieuwzględniona Przepis przewiduje dwie dopuszczalne postaci – elektroniczną oraz papierową i nie narzuca żadnej z tych form. Mogą istnieć szczególne przypadki w których konieczne będzie forma papierowa.
190.	Konfederacja Lewiatan	Art. 58	Zgodnie z art. 58 ust. 4 projektu KSC, "Kontrolowany ma prawo odmówić podpisania protokołu kontroli oraz złożyć umotywowane pisemne zastrzeżenia do tego protokołu w terminie 7 dni od dnia przedstawienia mu go do podpisu." Wydłużenie terminu na zgłoszenie zastrzeżeń do protokołu kontroli do minimum 14 dni jest uzasadnione z uwagi na złożoność materii kontroli, potrzebę konsultacji i zbierania informacji oraz porównanie z analogicznymi przepisami w innych ustawach. Dodatkowo, projektowane przepisy powinny uwzględniać bardziej szczegółowe procedury odwoławcze, dostęp do informacji, mechanizmy kontrolne oraz kwestie proceduralne, aby skutecznie zagwarantować prawa podmiotów kontrolowanych. Proponowany termin 7 dni jest zbyt krótki, aby kontrolowany podmiot mógł dokładnie przeanalizować protokół, skonsultować się z odpowiednimi specjalistami oraz przygotować umotywowane zastrzeżenia. Wydłużenie tego terminu jest niezbędne dla zapewnienia rzetelności procesu kontroli oraz ochrony praw kontrolowanych podmiotów.	Uwaga nieuwzględniona W ocenie projektodawcy termin 7 dni na zgłoszenie zastrzeżeń jest terminem wystarczającym i odpowiednim biorąc pod uwagę również inne przepisy prawa powszechnie obowiązującego, takie jak np. art. 40 ustawy o kontroli w administracji rządowej – Kierownik jednostki kontrolowanej ma prawo do zgłoszenia, w terminie 7 dni roboczych od dnia otrzymania projektu, umotywowanych pisemnych zastrzeżeń do projektu wystąpienia pokontrolnego.
191.	KIKE	Art. 59	Jednocześnie postuluję, aby w art. 59 uKSC doprecyzować termin w jakim podmiot ma wykonać zalecenia pokontrolne. Obecny zapis daje organowi całkowitą dowolność co w związku z sankcją finansową za ich niewykonanie może prowadzić do nadużyć lub wyznaczania nierealnych terminów.	Uwaga uwzględniona Doprecyzowano, że organ właściwy przekazując zalecenia pokontrolne wzywające do usunięcia nieprawidłowości wskazuje termin ich usunięcia uwzględniając zakres i rodzaj naruszeń.
192.	PIKE i Mediakom	Art. 59	Zauważalną i nierzadką praktyką organów kontrolujących przedsiębiorców telekomunikacyjnych, w szczególności Prezesa Urzędu Komunikacji Elektronicznej oraz Ministra Cyfryzacji (kontrolującego podmioty świadczące usługi DNS i IXP), jest wydawanie zaleceń pokontrolnych zawierających <u>wymogi, które nie znajdują oparcia w przepisach prawa</u> . Taka praktyka, w połączeniu z wysokimi karami za sam brak zastosowania się do zaleceń pokontrolnych w określonym terminie, powinna się koniecznie skończyć. Jest ona ewidentnie sprzeczna z motywem 143 dyrektywy NIS2 (prawo do skutecznego środka prawnego i rzetelnego procesu sądowego, domniemania niewinności oraz prawa do obrony). Należy zatem zrezygnować całkowicie z wydawania zaleceń pokontrolnych na gruncie ustawy o krajowym systemie cyberbezpieczeństwa i poprzestać na wskazaniu uchybień, które podmiot kluczowy i podmiot ważny powinny usunąć. <u>Alternatywnie, jako wariant minimum, należy umożliwić wnoszenie odwołania do niezależnego sądu od zaleceń pokontrolnych – i to takiego sądu, który może rozpatrzyć sprawę merytorycznie i zmienić zalecenia pokontrolne.</u>	Uwaga nieuwzględniona Z uwagi na charakter zaleceń pokontrolnych nie przysługuje od nich odwołanie. W przypadku nałożenia kary za niewykonanie zaleceń podmiot może złożyć skargę do sądu administracyjnego. Jednocześnie należy wskazać, że w innych ustawach, które regulują zagadnienia związane z kontrolą nie przewidziano instytucji odwołania od zaleceń pokontrolnych. Podmiot ma za to prawo złożenia zastrzeżeń do protokołu kontroli.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

			Art. 59. 1. Jeżeli na podstawie informacji zgromadzonych w toku kontroli organ właściwy do spraw cyberbezpieczeństwa uzna, że mogło dojść do naruszenia przepisów ustawy przez podmiot kontrolowany, <u>przekazuje</u> <u>wydaje</u> zalecenia pokontrolne, <u>w formie decyzji, wzywając do usunięcia nieprawidłowości. wskazujące nieprawidłowości, które podmiot kontrolowany powinien usunąć. Dobór środków zmierzających do usunięcia nieprawidłowości należy do podmiotu kontrolowanego.</u> 2. Od zaleceń pokontrolnych <u>nie przysługują środki odwoławcze przysługuje odwołanie do Sądu Okręgowego w Warszawie - Sądu Ochrony Konkurencji i Konsumentów.</u> 3. Podmiot kontrolowany, w wyznaczonym terminie, informuje organ właściwy do spraw cyberbezpieczeństwa lub ministra właściwego do spraw informatyzacji o sposobie wykonania zaleceń	
193.	Cybermadeinpol and	Art. 59	Art. 59. P. 2. - proponujemy przewidzenie w ustawie środków odwoławczych, np. Zgodnie z procedurami opisanymi dla kontroli przez CSIRT.	Uwaga nieuwzględniona Z uwagi na charakter zaleceń pokontrolnych nie przysługuje od nich odwołanie. W przypadku nałożenia kary za niewykonanie zaleceń podmiot może złożyć skargę do sądu administracyjnego. Jednocześnie należy wskazać, że w innych ustawach, które regulują zagadnienia związane z kontrolą nie przewidziano instytucji odwołania od zaleceń pokontrolnych. Podmiot ma za to prawo złożenia zastrzeżeń do protokołu kontroli.
194.	Grupa MiSOT	Art. 59	Niezwykle niepożądanym rozwiązaniem w KSC jest brak środków odwoławczych od zaleceń pokontrolnych. Zdarza się, że organy kontrolujące umieszczają w zaleceniach pokontrolnych wymogi, które nie mają oparcia w przepisach. Z kolei brak wdrożenia zaleceń pokontrolnych zagrożony jest (bardzo wysoką) karą administracyjną (art. 59 ust. 2). Niedopuszczalna powinna być sytuacja, gdy od zaleceń pokontrolnych nie przysługuje chociażby skarga do sądu administracyjnego lub odwołanie do Sądu Ochrony Konkurencji i Konsumentów, ponieważ może to prowadzić (i aktualnie zdarza się na gruncie obowiązujących przepisów, że prowadzi!) do nakładania na przedsiębiorców obowiązków bez podstawy prawnej i bez możliwości wniesienia odwołania.	Uwaga nieuwzględniona Z uwagi na charakter zaleceń pokontrolnych nie przysługuje od nich odwołanie. W przypadku nałożenia kary za niewykonanie zaleceń podmiot może złożyć skargę do sądu administracyjnego. Jednocześnie należy wskazać, że w innych ustawach, które regulują zagadnienia związane z kontrolą nie przewidziano instytucji odwołania od zaleceń pokontrolnych. Podmiot ma za to prawo złożenia zastrzeżeń do protokołu kontroli.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

195.	Fundacja Bezpieczna Cyberprzestrzeń	Art. 59	Fundacja zwraca się o wprowadzenie prawa podmiotu kontrolowanego do kwestionowania zaleceń pokontrolnych. Wedle proponowanych przepisów, podmiot kontrolowany ma nie tylko obowiązek wykonania zaleceń pokontrolnych, ale również poinformowania organu kontrolującego o sposobie wykonania. Niewykonanie zaleceń pokontrolnych jest z kolei zagrożone karą. Prowadzi to do konstatacji, że organ kontrolujący może wydać dowolne zalecenia pokontrolne – a podmiot kontrolowany ma obowiązek się do nich zastosować, bez możliwości odwołania. Zwracamy się o wprowadzenie procedury odwoławczej od zaleceń pokontrolnych.	Uwaga nieuwzględniona Z uwagi na charakter zaleceń pokontrolnych nie przysługuje od nich odwołanie. W przypadku nałożenia kary za niewykonanie zaleceń podmiot może złożyć skargę do sądu administracyjnego. Jednocześnie należy wskazać, że w innych ustawach, które regulują zagadnienia związane z kontrolą nie przewidziano instytucji odwołania od zaleceń pokontrolnych. Podmiot ma za to prawo złożenia zastrzeżeń do protokołu kontroli.
196.	Polskie Stowarzyszenie Fotowoltaiki	Art. 59	[Wdrożenie zaleceń pokontrolnych] Obowiązek wdrożenia przez PK i PW oraz poinformowania o wdrożeniu zaleceń pokontrolnych wzywających do usunięcia nieprawidłowości. Przepis nie określa minimalnego terminu wdrożenia oraz innych wymogów mających zastosowanie do zalecenia pokontrolnego. Ogólny wpływ regulacji: Przepis zobowiązuje PK i PW do wdrożenia zaleceń pokontrolnych oraz poinformowania o tym organu właściwego. Wpływ na sektor energetyczny: jw. – brak specyficznego wpływu na sektor energetyczny. [Stosunek względem Dyrektywy NIS2] Przepis stanowi implementację postanowień Dyrektywy NIS2 dotyczących uprawnień organów właściwych do wydawania wiążących poleceń – lub nakazów zobowiązujących dane podmioty do naprawienia stwierdzonych uchybień lub usunięcia naruszeń dyrektywy (vide art. 32 ust. 4 Dyrektywy NIS2). [Nadregulacja względem Dyrektywy NIS2] Zwracamy uwagę, że niewdrożenie zaleceń pokontrolnych może stanowić podstawę nałożenia kary pieniężnej na podstawie art. 73 KSC wg Projektu. Pomimo, że taka podstawa nałożenia kary pieniężnej wykracza poza zakres Dyrektywy NIS2 (zob. uwagi do art. 73 KSC wg Projektu), brak ustawowego wymogu określenia terminu realizacji wdrożenia zaleceń, może skutkować uznaniowym wyznaczaniem zbyt krótkiego terminu lub wszczynaniem postępowania przeciwko PK i PW. Podobnie, Projekt nie precyzuje obowiązku wskazania charakteru naruszenia oraz innych informacji niezbędnych dla jego usunięcia. Rekomendacja: Dookreślenie wymogów zalecenia pokontrolnego, w tym minimalnego (dostatecznego) terminu wdrożenia zaleceń oraz wskazania podstawy oraz natury zidentyfikowanego naruszenia.	Uwaga nieuwzględniona Wdrożenie terminu na realizację zaleceń pokontrolnych jest niemożliwe z uwagi na różny charakter naruszeń oraz zaleceń. Termin będzie różny w zależności od podmiotu, przypadku, charakteru naruszeń.
197.	Konfederacja Lewiatan	Art. 61	<i>Superfluum</i> ustawowe w zakresie upoważnienia dyrektora, zastępcy dyrektora departamentu lub naczelnika wydziału Jednostka redakcyjna: art. 61 ust. 6 projektu KSC Jednostka redakcyjna NIS2: nie dotyczy	Wyjaśnienie uwagi Status Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa jest niejasny. Stąd nie jest możliwe upoważnianie pracowników do wykonywania zadań Pełnomocnika na

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

			Uwaga: Z Zgodnie z art. 268a Kodeksu postępowania administracyjnego (kpa), organ administracji publicznej, któremu przysługuje prawo do wydawania decyzji administracyjnych, może upoważnić do tego inną osobę. Upoważnienie takie musi być wyraźnie określone w przepisach prawa lub wynikać z upoważnienia ustawowego. Oznacza to, że delegowanie kompetencji musi być jasno sprecyzowane i wynikać bezpośrednio z norm prawnych. Art. 268a kpa już teraz precyzyjnie reguluje możliwość delegowania kompetencji w ramach administracji publicznej. Wprowadzenie dodatkowych przepisów, które pozwalają pełnomocnikowi ds. cyberbezpieczeństwa upoważniać dyrektora, zastępcę dyrektora lub naczelnika do realizacji swoich zadań, jest zbędne, ponieważ art. 268a kpa wystarczająco normuje te kwestie. Przepis art. 61 ust. 6 projektu KSC jest więc zbędny, gdyż dodaje regulacje, które są już wystarczająco uregulowane w istniejących przepisach prawa. Przepis ten powinien zostać ograniczony lub usunięty, aby uniknąć nadmiarowości legislacyjnej i zapewnić przejrzystość regulacji prawnych.	podstawie Kodeksu postępowania administracyjnego.
198.	Konfederacja Lewiatan	Art. 61	Brak ograniczenia zakresu uprawnień Pełnomocnika do żądania pomocy Jednostka redakcyjna: art. 61 ust. 7 projektu KSC Jednostka redakcyjna NIS2: 32 Uwaga: Proponowany przepis nie precyzuje ograniczeń zakresu pomocy, jaką organy administracji rządowej oraz jednostki organizacyjne mają obowiązek udzielać Pełnomocnikowi. Przykładem bardziej precyzyjnego sformułowania jest art. 9 ustawy o obronie ojczyzny, który wskazuje, że pomoc ma być udzielana "w zakresie swojego działania". Brak takiego ograniczenia może prowadzić do niejasności i nadmiernego obciążenia tych organów obowiązkami, które mogą wykraczać poza ich podstawowe zadania i kompetencje. Przepis ten, w obecnym brzmieniu, może kolidować z innymi regulacjami prawnymi dotyczącymi ochrony danych osobowych, tajemnicy służbowej czy poufności informacji. Bez odpowiednich ograniczeń, organy administracji rządowej mogą być zmuszone do udostępniania informacji, które są chronione innymi przepisami prawa, co może prowadzić do naruszeń prawa i sankcji. Dodatkowo, przepis ten nie zawiera żadnych mechanizmów kontrolnych ani proceduralnych, które zapewniałyby właściwe zarządzanie udzielaniem pomocy. Wprowadzenie takich mechanizmów pozwoliłoby na lepsze monitorowanie i koordynowanie działań oraz zapobieganie potencjalnym nadużyciom. Obecny brak precyzyjnych ograniczeń i mechanizmów kontrolnych może prowadzić do niejasności i potencjalnych problemów w praktycznym stosowaniu tego przepisu.	Wyjaśnienie uwagi W wielu rozporządzeniach ustanawiających Pełnomocników Rządu zawarte jest uprawnienie pełnomocnika do żądania pomocy od jednostek administracji rządowej. Należy zauważyć, że jest to pełnomocnik rządu dlatego administracja rządowa powinna go wspierać w wykonywaniu jego zadań.
199.	Fundacja Bezpieczna Cyberprzestrzeń	Art. 62	Art. 1 pkt 64, treść art. 62 ust. 3 – jakie będą źródła finansowania zakupów realizowanych na podstawie tego przepisu?	Wyjaśnienie uwagi Źródłem sfinansowania będzie cz. 27 budżetu państwa.
200.	Polska Izba Informatyki i	Art. 62	Art. 62 ust. 3 – zakupy na rzecz podmiotów publicznych Izba wnioskuje o usunięcie albo ograniczenie możliwości dokonywania zakupów produktów ICT, usług ICT lub procesów ICT przez Pełnomocnika na rzecz podmiotów publicznych. Uprawnienie	Wyjaśnienie uwagi Chodzi o to, żeby Pełnomocnik mógł dokonywać tańszych hurtowych zakupów.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

	Telekomunikacji		to może spowodować, że uszczuplone zostaną możliwości konkurowania o zlecenia podmiotów publicznych, a Pełnomocnik zostanie pośrednikiem w zakupach mającym charakter Operatora Sieci obejmującej podmioty publiczne. Podobne pomysły były przedmiotem ostrej krytyki poprzednich projektów ustawy i w znacznym stopniu przyczyniły się do ich pogrzebania.	
201.	Osoba fizyczna	Art. 62a	Ust. 5 i 6 – Zastosowano zapisy przywołujące niestosowany dotychczas byt, jakim jest „cyberprzestrzeń”. Proponuję zweryfikować intencję wprowadzenia tego nowego pojęcia i bytu. Jeśli ma to być zamiennik/synonim „systemów informacyjnych”, to należy dokonać stosownej korekty, jeśli natomiast wprowadzenie tego pojęcia jest celowe, to proponuję zweryfikowanie całej konstrukcji krajowego systemu cyberbezpieczeństwa i zapisów ustawy uKSC2 w ramach przededefiniowania podstawowego przedmiotu ustawy, jakim powinna być cyberprzestrzeń (rozumiana jako sieć połączonych sieci i systemów informatycznych (NIS2) lub jako sieć połączonych systemów informacyjnych) i bezpieczeństwo cyberprzestrzeni.	Wyjaśnienie uwagi Pojęcie cyberprzestrzeni występuje m. in. w ustawie z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej. Art. 2 ust. 1b ustawy wskazuje, że przez cyberprzestrzeń, o której mowa w ust. 1, rozumie się przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne, określone w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, wraz z powiązaniem między nimi oraz relacjami z użytkownikami. Ustawa z dnia 21 czerwca 2002 r. o stanie wyjątkowym. Art. 2 ust. 1a. przez cyberprzestrzeń, o której mowa w ust. 1, rozumie się przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne, określone w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, wraz z powiązaniem między nimi oraz relacjami z użytkownikami.
202.	Konfederacja Lewiatan	Art. 64	Brak udziału Prezesa Urzędu Komunikacji Elektronicznej w pracach Kolegium ds. Cyberbezpieczeństwa a także w pracach Połączonego Centrum Operacyjnego Cyberbezpieczeństwa Jednostka redakcyjna: art. 62a i 66 projektu KSC Jednostka redakcyjna NIS2: 13 ust. 1 Uwaga: Zgodnie z art. 66 ustawy o krajowym systemie cyberbezpieczeństwa, Kolegium ds. Cyberbezpieczeństwa stanowi organ doradczy w sprawach dotyczących krajowego systemu	Wyjaśnienie uwagi Prezes UKE jako organ właściwy do spraw Cyberbezpieczeństwa będzie miał swojego przedstawiciela w PCOC.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

			cyberbezpieczeństwa. Kolegium to ma na celu koordynację działań na rzecz poprawy cyberbezpieczeństwa na poziomie krajowym oraz zapewnienie spójności działań podejmowanych przez różne podmioty zaangażowane w ochronę cyberprzestrzeni. Prezes Urzędu Komunikacji Elektronicznej (UKE) posiada szczególne kompetencje oraz wiedzę w zakresie zarządzania i regulacji rynku telekomunikacyjnego. Jego doświadczenie i znajomość specyfiki sektora telekomunikacyjnego są nieocenione w kontekście tworzenia i wdrażania polityki cyberbezpieczeństwa. Prezes UKE będzie odpowiedzialny za nadzór nad procesem wymiany urządzeń i infrastruktury telekomunikacyjnej dostawcy uznanego za dostawcę wysokiego ryzyka. W ramach tego zadania, Prezes UKE będzie musiał współpracować z podmiotami krajowego systemu cyberbezpieczeństwa, aby zapewnić, że wymiana ta nie wpłynie negatywnie na ciągłość działania sieci oraz na poziom bezpieczeństwa telekomunikacyjnego. Włączenie Prezesa UKE w pracę Kolegium ds. Cyberbezpieczeństwa umożliwi skuteczniejszą koordynację tych działań oraz szybsze reagowanie na potencjalne zagrożenia. Zgodnie z art. 192 ustawy Prawo telekomunikacyjne, Prezes UKE jest odpowiedzialny za podejmowanie działań mających na celu zapewnienie bezpieczeństwa publicznego oraz ochrony interesów użytkowników końcowych. Jego udział w Kolegium ds. Cyberbezpieczeństwa jest więc naturalnym rozszerzeniem jego obowiązków i kompetencji w zakresie ochrony infrastruktury krytycznej telekomunikacyjnej. Obecność Prezesa UKE w Kolegium ds. Cyberbezpieczeństwa pozwoli na zapewnienie spójności działań podejmowanych przez różne podmioty w zakresie cyberbezpieczeństwa. Prezes UKE, jako członek Kolegium, będzie mógł lepiej koordynować działania telekomunikacyjne z innymi obszarami cyberbezpieczeństwa, co jest kluczowe w przypadku złożonych zagrożeń cybernetycznych, które często obejmują wiele sektorów. Artykuł 66 ustawy o krajowym systemie cyberbezpieczeństwa przewiduje możliwość powoływania do Kolegium przedstawicieli różnych organów administracji publicznej, którzy mają istotne znaczenie dla bezpieczeństwa cyberprzestrzeni. Biorąc pod uwagę kluczową rolę Prezesa UKE w nadzorze nad telekomunikacją oraz jego zaangażowanie w działania związane z bezpieczeństwem tej infrastruktury, włączenie go do Kolegium jest w pełni uzasadnione. Włączenie Prezesa Urzędu Komunikacji Elektronicznej do Kolegium ds. Cyberbezpieczeństwa oraz do Połączonego Centrum Operacyjnego Cyberbezpieczeństwa jest nie tylko logiczne, ale również niezbędne dla zapewnienia skutecznej i spójnej ochrony cyberprzestrzeni w Polsce. Jego doświadczenie, kompetencje oraz nowe obowiązki związane z nadzorem nad wymianą urządzeń i infrastruktury telekomunikacyjnej dostawców wysokiego ryzyka stanowią silne argumenty za jego udziałem w tych pracach. Zapewni to lepszą koordynację działań, zwiększy efektywność podejmowanych środków oraz przyczyni się do podniesienia poziomu bezpieczeństwa telekomunikacyjnego w kraju.	
203.	Federacja Przedsiębiorców Polskich	Art. 65	W art. 65 w ust. 1 w pkt 8 proponuje się następujące brzmienie:	Uwaga nieuwzględniona w związku z nieuwzględnieniem uwagi dot. definicji funkcji krytycznych.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. II

			8) decyzji w sprawie uznania dostawcy sprzętu lub oprogramowania o funkcjach krytycznych, określonych w wykazie kategorii funkcji oraz komponentów krytycznych dla bezpieczeństwa sieci i usług, za dostawcę wysokiego ryzyka; Kolegium, o którym mowa w art. 64 ustawy o KSC, będzie wydawać opinię w sprawie dostawcy wysokiego ryzyka. W konsekwencji przepis art. 65 ust. 1 powinien być uzupełniony o punkt 8 poprzez wskazanie, że Kolegium podejmuje decyzje w sprawie uznania danego dostawcy sprzętu lub oprogramowania o funkcjach krytycznych, za dostawcę wysokiego ryzyka. To precyzyjne określenie jest kluczowe, aby zapewnić, że tylko te elementy, które mają bezpośredni wpływ na bezpieczeństwo sieci i usług, będą podlegały szczególnym procedurom oceny i ewentualnym restrykcjom. Podkreślenie funkcji i komponentów krytycznych ma na celu uniknięcie niepotrzebnych obciążeń dla dostawców, których produkty i usługi nie mają bezpośredniego wpływu na bezpieczeństwo sieci i usług. Skupienie się na funkcjach i komponentach krytycznych pozwoli na bardziej precyzyjne i efektywne zarządzanie ryzykiem, ograniczając niepotrzebne koszty i zakłócenia dla dostawców oraz użytkowników końcowych.	
204.	Krzysztof Rożko i Wspólnicy Kancelaria Prawna sp. k.	Art. 65	UWAGA ZGŁOSZONA W RAMACH ZGŁOSZENIA LOBBINGOWEGO Niniejszy przepis przewiduje dodanie w art. 65 ust. 1 nowego pkt 8). Zwracamy uwagę, że w projekcie ustawy wdrażającej DORA na podstawie art.10 pkt 5, w art. 65 ust. 1 uKSC również proponuje się dodanie pkt 8), który jednak odnosi się do odmiennej materii. Wobec powyższego postulujemy odpowiednie skoordynowanie treści projektowanych przepisów.	Uwaga uwzględniona Projekty zostaną wzajemnie uspołnione.
205.	Krzysztof Rożko i Wspólnicy Kancelaria Prawna sp. k.	Art. 66	UWAGA ZGŁOSZONA W RAMACH ZGŁOSZENIA LOBBINGOWEGO Projekt ustawy wdrażającej DORA przewiduje uwzględnienie w art. 66 ust. 4 pkt. 5 uKSC Przewodniczącego Komisji Nadzoru Finansowego, jako uczestnika posiedzeń Kolegium. W projekcie nowelizacji uKSC w art. 1 pkt 68 lit. a) również uwzględniony został Przewodniczący Komisji Nadzoru Finansowego jako uczestnik posiedzeń Kolegium. Wobec powyższego postulujemy odpowiednie skoordynowanie treści projektowanych przepisów.	Uwaga uwzględniona Projekty zostaną wzajemnie uspołnione.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

Lp.	Zgłaszający uwagę	Jednostka redakcyjna	Treść uwagi	Stanowisko Ministra Cyfryzacji
1.	Apator	Art. 67a	Art. 67a ust. 1 Projektu proponujemy, aby otrzymał brzmienie: Pełnomocnik może wydać rekomendacje określające środki techniczne i organizacyjne stosowane w celu zwiększania poziomu bezpieczeństwa systemów informacyjnych podmiotów krajowego systemu cyberbezpieczeństwa. W rekomendacjach Pełnomocnik może wskazać kategorie podmiotów, do których kierowane są rekomendacje. Rekomendacje powinny wskazywać m.in. to, że warunkiem nawiązania współpracy przez podmioty kluczowe oraz podmioty ważne jest to, aby podmioty, z którymi taka współpraca ma być lub jest nawiązana miały swoją siedzibę lub prowadziły działalność w państwach, które spełniają łącznie co najmniej poniższe warunki: posiadają demokratycznie wybrany rząd, co obejmuje m.in. istnienie niezależnej opozycji, wolne wybory, w wyniku których można zastąpić obecny rząd oraz funkcjonującą zasadę tzw. kontroli i równowagi; posiadają system sądowny, podporządkowany bpośród niej i gromadzi politycznej, przestrzegane są w nich obowiązujące zasady, zwyczaje i zasady praworządności, takie jak prawo do sprawiedliwego procesu, w tym prawo do sądu; których przepisy prawne i polityki publiczne regulują sprawy tworzące; które dbają o ochronę własności i terytorium; które nie naruszają prawa międzynarodowego w sposób długotrwały lub systemowy; które utrzymują partnerskie stosunki z Rzeczpospolitą Polską i nie prowadzą działalności sprzecznej z podstawowymi interesami RP lub jej państw sojusznich. Uzasadnienie proponowanej zmian: W naszej opinii, biorąc pod uwagę obecną sytuację geopolityczną oraz zagrożenia na świecie, celowe by było, na wzór innych państw, wyraźne wskazanie, że również polski ustawodawca nie będzie akceptował nawiązywania lub kontynuowania przez podmioty kluczowe lub podmioty ważne, które prowadzą swoją działalność na terytorium RP, współpracy z podmiotami pochodzącymi z państw, w których nie są przestrzegane elementarne standardy wynikające z prawa międzynarodowego, a także które prowadzą wrogą i zagrażającą ogólnoswiatowemu pokojowi politykę.	Uwaga nieuwzględniona Rekomendacje będą miały charakter niewiążący i zostanie to podkreślone w przepisie.
2.	Konfederacja Lewiatan	Art. 67a	Wiążąca forma rekomendacji Pełnomocnika pomimo rzekomo niewiążącej formy Jednostka redakcyjna: art. 67a projektu KSC Jednostka redakcyjna NIS2: nie dotyczy Uwaga: W myśl przepisów Konstytucji RP, obywatelom przysługuje prawo do sądu, a także prawo do odwołania się od decyzji organów administracyjnych. Art. 45 Konstytucji RP stanowi, że każdy ma prawo do sprawiedliwego i jawnego rozpatrzenia sprawy przez właściwy, niezależny, bezstronny i niezawisły sąd. Przepisy zawarte w art. 67a ustawy o krajowym systemie cyberbezpieczeństwa nie przewidują jednak żadnej ścieżki odwoławczej od wydawanych przez Pełnomocnika rekomendacji. Brak możliwości odwołania się od decyzji organu publicznego stanowi naruszenie fundamentalnego prawa do sądu. Art. 67a ust. 1 projektu KSC umożliwia bowiem Pełnomocnikowi wydawanie rekomendacji, które określają środki techniczne i organizacyjne stosowane w celu zwiększania poziomu bezpieczeństwa systemów informacyjnych. Przepisy nie precyzują jednak, w jakiej formie mają być wydawane te rekomendacje, co może prowadzić do niejasności i niejednoznaczności w ich interpretacji. Konstytucja RP w art. 2 zapewnia, że Rzeczpospolita Polska jest demokratycznym państwem prawnym, urzeczywistniającym zasady sprawiedliwości społecznej, co wymaga, aby przepisy prawa były jasne, precyzyjne i zrozumiałe dla	Uwaga uwzględniona Rekomendacje będą miały charakter niewiążący i zostanie to podkreślone w przepisie.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			obywateli. Brak jednoznacznej formy rekomendacji może prowadzić do ich dowolnej interpretacji i stosowania. Zgodnie z art. 78 Konstytucji RP, każda ze stron ma prawo do zaskarżania orzeczeń i decyzji wydanych w pierwszej instancji. Tymczasem art. 67a projektu KSC nie przewiduje obowiązku doręczania rekomendacji podmiotom krajowego systemu cyberbezpieczeństwa. Udostępnianie rekomendacji jedynie w Biuletynie Informacji Publicznej na stronie podmiotowej Pełnomocnika może być niewystarczające do skutecznego powiadomienia zainteresowanych podmiotów, co stanowi naruszenie prawa do rzetelnej informacji i możliwości odwołania się od wydanych rekomendacji. Art. 67a ust. 1 projektu KSC pozwala Pełnomocnikowi na wydawanie rekomendacji dotyczących szerokiego spektrum środków technicznych i organizacyjnych związanych z bezpieczeństwem systemów informacyjnych. Ogólnikowa forma tych rekomendacji sprawia, że mogą one dotyczyć praktycznie każdego aspektu związanego z cyberbezpieczeństwem. Tak szeroko zakrojona kompetencja Pełnomocnika bez szczegółowych wytycznych i ograniczeń może prowadzić do nadużyć oraz braku przejrzystości w funkcjonowaniu systemu cyberbezpieczeństwa. Konstytucja RP w art. 7 stanowi, że organy władzy publicznej działają na podstawie i w granicach prawa, co oznacza, że kompetencje organów administracyjnych muszą być wyraźnie określone i ograniczone.	
3.	Polskie Stowarzyszenie Fotowoltaiki	Art. 67a	[Rekomendacje Pełnomocnika dot. środków technicznych i organizacyjnych] Obowiązek uwzględnienia przez podmiot krajowego systemu cyberbezpieczeństwa skierowanych do niego rekomendacji Pełnomocnika określających środki techniczne i organizacyjne stosowane w celu zwiększania poziomu bezpieczeństwa systemów informacyjnych. Ogólny wpływ regulacji: Podmioty krajowego systemu cyberbezpieczeństwa, w tym PK i PW, powinny uwzględniać rekomendacje Pełnomocnika w zarządzaniu ryzykiem, w razie, gdy są do niego skierowane. W zależności od przedmiotu rekomendacji, uwzględnienie ich w zarządzaniu ryzyka może wymagać poniesienia przez PK lub PW istotnych nakładów finansowych oraz organizacyjnych dla przedsiębiorstwa. Rekomendacje Pełnomocnika nie mają wiążącego charakteru (vide Uzasadnienie Projektu s. 58). Wpływ na sektor energetyczny: jw. – brak specyficznego wpływu na sektor energetyczny [Nadregulacja względem Dyrektywy NIS2] Zarówno kwestia funkcjonowania Pełnomocnika, jak i jego uprawnienie do wydawania rekomendacji nie znajduje podstawy w Dyrektywie NIS2. Ponadto, z uwagi na brak związania podmiotów krajowego systemu cyberbezpieczeństwa rekomendacjami Pełnomocnika, w praktyce nie mogą one nie mieć istotnego znaczenia dla oceny zgodności PK i PK z wymogami wynikającymi z KSC Brak wdrożenia rekomendacji nie oznacza automatycznie naruszenia obowiązku wdrożenia odpowiednich środków technicznych o organizacyjnych w celu zwiększania poziomu bezpieczeństwa systemów informacyjnych. Rekomendacja: Z uwagi na naturę instytucji Pełnomocnika jako jednostki wspierającej administrację rządową, rekomendowane ograniczenie zakresu jego działań względem podmiotów prywatnych.	Uwaga wyjaśniona Rekomendacje Pełnomocnika będą miały charakter niewiążący dla podmiotów prywatnych.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

4.	Polska Izba Informatyki i Telekomunikacji	Art. 67a	Art. 67a – rekomendacje Pełnomocnika Projekt ustawy przewiduje dodanie do ustawy o krajowym systemie cyberbezpieczeństwa nowego art. 67a, który daje Pełnomocnikowi kompetencję do wydawania rekomendacji określających środki techniczne i organizacyjne stosowane w celu zwiększania poziomu bezpieczeństwa systemów informacyjnych podmiotów krajowego systemu cyberbezpieczeństwa. Nowo dodawany przepis określa również podstawowe aspekty związane z wydaniem, udostępnieniem i wykonywaniem rekomendacji. W związku z powyższym zwracamy uwagę, że w ustawie o krajowym systemie cyberbezpieczeństwa już dzisiaj funkcjonują przepisy art. 33 ust. 4 – 9, które upoważniają Pełnomocnika do wydawania, zmieniania i odwoływania rekomendacji dotyczących stosowania produktów ICT, usług ICT lub procesów ICT, w szczególności w zakresie wpływu na bezpieczeństwo publiczne lub istotny interes bezpieczeństwa państwa. Przepisy te określają również tryb wydawania rekomendacji, sposób ich udostępniania i dostępne środki odwoławcze. Podkreślić trzeba, że projekt ustawy przewiduje wprowadzenie szeregu zmian do art. 33 ust. 4 – 9 ustawy o krajowym systemie cyberbezpieczeństwa, jednocześnie zakładając utrzymanie w mocy tych przepisów. W efekcie dodanie do ustawy o krajowym systemie cyberbezpieczeństwa art. 67a, z jednoczesnym utrzymaniem w mocy art. 33 ust. 4 - 9 ustawy, spowoduje, że ta sama instytucja i narzędzie, czyli rekomendacje Pełnomocnika, będą regulowane zestawem dwóch różnych przepisów tej samej ustawy. A podkreślić trzeba, że dodawany art. 67a i zmieniany art. 33 ust. 4 nieco odmiennie opisują procedurę wydawania, udostępniania i wykonywania rekomendacji Pełnomocnika i cel, któremu te rekomendacje mają służyć. Jeśli jest to błąd to błąd ten należy poprawić. Jeśli natomiast intencją Projektodawcy było stworzenie dwóch różnych narzędzi prawnych, z których każdy nazywa się „rekomendacjami Pełnomocnika” to taki zabieg należy ocenić krytycznie, gdyż taka konstrukcja będzie powodowała liczne wątpliwości i spory praktyczne. Jeśli zamierzeniem było oddanie w ręce Pełnomocnika dwóch różnych narzędzi to musi to znaleźć odzwierciedlenie w przepisach ustawy, która powinna wyraźnie rozgraniczać (również na poziomie nazewnictwa) oba instrumenty.	Uwaga wyjaśniona Są to różne rekomendacje i różne stany faktyczne.
5.	Polska Izba Informatyki i Telekomunikacji	Art. 67b	Art. 67b ust. 1 – podmioty, do których może być kierowana decyzja HRV Według projektu skutki decyzji dot. dostawcy wysokiego ryzyka mogą zostać skierowane do podmiotów kluczowych lub ważnych, z wyłączeniem podsektora komunikacji elektronicznej lub do przedsiębiorców telekomunikacyjnych. W ten sposób precyzyjnie wyłączone zostały podmioty świadczące usługę komunikacji interpersonalnej niewykorzystującej numerów, które należą do podsektora komunikacji elektronicznej, ale mogą nie być przedsiębiorcami telekomunikacyjnymi. Uzasadnienie nie odnosi się do tego czy jest to zabieg celowy i z jakich wynika przesłanek. Należy więc wprost przesądzić o objęciu wszystkich podmiotów podsektora komunikacji elektronicznej potencjalnymi skutkami wydania decyzji dot. dostawcy wysokiego ryzyka.	Uwaga uwzględniona Postępowanie dotyczące dostawcy wysokiego ryzyka (HRV) będzie mogło dotyczyć także dostawcy dla podmiotów świadczących usługę komunikacji interpersonalnej niewykorzystującej numerów OTT-1.
6.	Polska Izba Informatyki i Telekomunikacji	Art. 67b	Art. 67b – przegląd decyzji HRV Postulujemy, aby wprowadzić zasadę cyklicznego przeglądu wydanych decyzji dot. dostawcy wysokiego ryzyka. Przegląd wydanej decyzji powinien się odbywać po okresie nie krótszym niż czas wynikający z decyzji (w tym przypadku 4 lata).	Uwaga nieuwzględniona

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			Kwestia ta wydaje się bardzo ważna, z uwagi na bardzo doniosłe skutki wydania decyzji HRV, a także dynamikę zmian technicznych i poza-technicznych mogących skutkować zmianą okoliczności będących podstawą do wydania pierwotnej decyzji.	
7.	Polska Izba Informatyki i Telekomunikacji	Art. 67 b	Art. 67b – notyfikacja techniczna Wyjaśnienia wymaga wyrażone w uzasadnieniu utrzymanie założenia dot. braku uzasadnienia dla dokonania notyfikacji technicznej w zakresie przepisów. Zauważamy, że w biegu prac nad poprzednią nowelizacją uznawano taką potrzebę, a dopiero na finalnym etapie podejście to zostało zmodyfikowane bez przedstawienia szerszego uzasadnienia. Z uwagi na doniosłość projektowanych przepisów uważamy, że kwestia ta powinna zostać w pełni wyjaśniona, szczególnie, że odnotowaliśmy, że część krajów UE takich notyfikacji dokonywała, w tym: Belgia, Estonia, Finlandia, Francja, Hiszpania, Słowenia. Wnosimy więc uzupełnienie uzasadnienia o wskazanie przyczyn uznania braku zasadności notyfikacji.	Uwaga wyjaśniona Notyfikacji technicznej może podlegać sama decyzja HRV, stąd przepisy ustawy nie muszą być notyfikowane.
8.	Amerykańska Izba Handlowa	Art. 67b	Wprowadzany do uksc Art. 67b ust. 9 wskazuje na możliwość przedstawienia stanowiska tylko przez izbę gospodarczą. Stoimy na stanowisku, że katalog podmiotów uprawnionych powinien zostać poszerzony także o organizacje pracodawców (związki branżowe). Zakładamy, że jest to zgodne z intencją prawodawcy zmierzającą do możliwości uzyskania opinii reprezentatywnych przedstawicieli branży. Biorąc pod uwagę fundamentalne znaczenie zachowania cyberbezpieczeństwa przez podmioty infrastruktury krytycznej w Polsce, w naszej opinii termin wyznaczonych dla tych podmiotów na wycofanie produktów ICT, rodzajów usług ICT i konkretnych procesów ICT w zakresie objętym decyzją, dostarczanych przez dostawcę wysokiego ryzyka, powinien wynosić 1 rok.	Uwaga częściowo uwzględniona Związki pracodawców zostaną uwzględnione w art. 67b ust. 9 projektu.
9.	ISSA Polska	Art. 67b	Nieadekwatność mechanizmu dostawcy wysokiego ryzyka do ograniczenia ryzyka w łańcuchu dostaw Procedura dotycząca dostawcy wysokiego ryzyka wprowadzana w art 67b, na gruncie wiedzy merytorycznej z dziedziny cyberbezpieczeństwa nie może być uznana za skuteczne narzędzie ograniczenia ryzyka w łańcuchu dostaw. Kryteria geopolityczne proponowane w ustawie nie korelują w żaden sposób z poziomem bezpieczeństwa usług, produktów i procesów – co znajduje potwierdzenie w analizie poważnych światowych incydentów (przykładowo - przedmiotem skutecznego ataku ze strony Rosji została część infrastruktury jednego z ukraińskich operatorów telekomunikacyjnych, dostarczana akurat przez europejskiego dostawcę). Dodatkowo, proponowany mechanizm zakłada, że poziom ryzyka reprezentowany przez każdy podmiot uczestniczący w łańcuchu dostaw jest stały w czasie, ignorując rzeczywisty wpływ działań dostawców na zarządzanie ryzykiem i poziom bezpieczeństwa dostarczanych usług, produktów i procesów ICT i to w perspektywie wieloletniej. Nie uwzględnia też w ogóle możliwości wprowadzenia po stronie podmiotów krajowego systemu cyberbezpieczeństwa środków ograniczających ryzyko, w sposób nieuzasadniony narzucając konkretną - a być może nie optymalną - strategię postępowania z ryzykiem. Na rynkach z ograniczoną liczbą dostawców (np. produkcja, telekomunikacja, energetyka) usunięcie któregośkolwiek z dostawców z rynku powoduje w konsekwencji automatyczne obniżenie, a nie zwiększenie poziomu bezpieczeństwa. W sytuacji braku w proponowanej ustawie jakichkolwiek standardów określających wymagany poziom bezpieczeństwa rozwiązań w poszczególnych sektorach, ustawowe ograniczanie konkurencji (z tworzeniem monopolu włącznie) powoduje zanik jakiegokolwiek motywacji producentów do udoskonalania rozwiązań pod względem bezpieczeństwa. Jest to tym bardziej realne i niebezpieczne, że kryteria przewidziane w ustawie wykorzystują kryteria geopolityczne, co de facto wyklucza część dostawców z działania mechanizmu, tym	Uwaga wyjaśniona Postępowanie w sprawie uznania za dostawcę wysokiego ryzyka ma na celu zabezpieczenie polskiej gospodarki i polskiego społeczeństwa przed dostawcą sprzętu lub oprogramowania, który stwarza poważne zagrożenie dla bezpieczeństwa państwa, obronności, bezpieczeństwa i porządku publicznego lub zdrowia i życia ludzi. W ramach postępowania administracyjnego będą brane pod uwagę zarówno aspekty techniczne związane z dostarczaniem przez dostawcę sprzętem i oprogramowaniem jak również aspekty nietechniczne związane z dostawcą. Dostawca wysokiego ryzyka może ukryć podatności w dostarczonym sprzęcie i w ten sposób zagrozić bezpieczeństwu państwa.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			samym tworząc grupę podmiotów posiadających często uprzywilejowany dostęp do krajowej infrastruktury krytycznej, a nie objętych żadnymi wymaganiami lub sankcjami w zakresie bezpieczeństwa. Powyższe założenia powodują, że mechanizm dostawcy wysokiego ryzyka zyskuje charakter międzypaństwowych sankcji ekonomicznych, a nie mechanizmu krajowego systemu cyberbezpieczeństwa i jako taki powinien być dyskutowany i ewentualnie regulowany poza ustawą o KSC. W zakresie przedmiotowym ustawy o krajowym systemie cyberbezpieczeństwa proponujemy, zgodnie z dyrektywą NIS2, pozostawienie obowiązku szacowania ryzyka i jego mitygacji - wraz z decyzją co do doboru środków mitygujących - po stronie podmiotów kluczowych i ważnych.	
10.	ISSA Polska	Art. 67b	Nadmierne rozszerzenie zakresu wykluczenia dostawcy na wszystkie podmioty ważne i kluczowe Wprowadzenie w projekcie ustawy KSC procedury wykluczenia dostawcy obejmującej wszystkie podmioty kluczowe i ważne, a nie tylko sektor telekomunikacyjny, jak to ma miejsce w 5G Toolbox i dyrektywie NIS2, stanowi przejaw nadmiarowej regulacji. Proponowany zakres wprowadza rygorystyczne regulacje dla około 35 000 podmiotów z różnorodnych sektorów, co jest rozwiązaniem niespotykanym w Unii Europejskiej i mogącym prowadzić do poważnych konsekwencji operacyjnych i finansowych dla szerokiego spektrum przedsiębiorstw. Sektory takie jak administracja publiczna, zdrowie, bankowość, energetyka, a także nauka i produkcja (w tym żywności i chemikaliów), znajdują się wśród tych, które będą musiały zastosować się do procedury dostawcy wysokiego ryzyka (DWR), co oznacza całkowite wyeliminowanie i zastąpienie urzędów oraz oprogramowania wykluczonego dostawcy w ciągu zaledwie 7 lat. To nie tylko stwarza ryzyko znaczących przerw w działalności, ale także narzuca ogromne koszty związane z wymianą sprzętu i oprogramowania, bez przewidzianego odszkodowania dla dotkniętych tym podmiotów. Tak szerokie zastosowanie procedury DWR bez proporcjonalnej oceny ryzyka i specyfiki każdego sektora jest nieadekwatne i może prowadzić do nadmiernego obciążenia podmiotów, które niekoniecznie są wrażliwe na zagrożenia związane z wykorzystaniem technologii od określonych dostawców. Co więcej, brak rekompensaty za wymianę sprzętu może spowodować poważne obciążenia finansowe dla wielu przedsiębiorstw, co z kolei może wpłynąć negatywnie na całą gospodarkę. Art. 67c różnicuje również obowiązki przedsiębiorców telekomunikacyjnych i pozostałych podmiotów kluczowych i ważnych w zakresie wycofania z użytkowania produktów, usług i procesów objętych decyzją, w sposób arbitralny i nieuzasadniony określając różne terminy ich wycofania. Takie podejście może zostać uznane za dyskryminujące, nie widzimy również merytorycznego uzasadnienia do różnicowania terminów wycofania - niezależnie od kwestionowanej wcześniej adekwatności takiego podejścia do zarządzania ryzykiem w łańcuchu dostaw. Projektowany akt nie uwzględnia również w wystarczającym stopniu powiązania zmian dotyczących analizy ryzyka w łańcuchu dostaw jakie są potrzebne w przepisach prawa zamówień publicznych. Szereg podmiotów krajowego systemu cyberbezpieczeństwa nie kupuje usług ani produktów ICT w warunkach pełnej swobody biznesowej i dokonuje wyboru (zwłaszcza w zakresie automatyki przemysłowej i systemów do obsługi infrastruktury) w warunkach ograniczonej liczby dostawców i umów zawieranych na czas dłuższy niż wskazany w przepisach okres „wyjścia” z danego rozwiązania (5 lub 7 lat wymienione w art. 67c ust. 5). Projektowane przepisy nie wprowadzają ustawowego prawa do „zerwania” zawartej umowy, co oznacza, że w przypadku umów serwisowych lub dostaw kolejnych wersji oprogramowania, podmioty kluczowe i ważne mogą ponieść wydatek, który nie znajdzie pokrycia w	Uwaga wyjaśniona Postępowanie w sprawie uznania za dostawcę wysokiego ryzyka ma na celu zabezpieczenie polskiej gospodarki i polskiego społeczeństwa przed dostawcą sprzętu lub oprogramowania, który stwarza poważne zagrożenie dla bezpieczeństwa państwa, obronności, bezpieczeństwa i porządku publicznego lub zdrowia i życia ludzi. Postępowanie umożliwia badanie dostawcy sprzętu lub oprogramowania dla wszystkich sektorów gospodarki wskazanych w ustawie. Jest to wskazane z uwagi na to, że każdy podmiot kluczowy i podmiot ważny musi dbać o bezpieczeństwo łańcuchów dostaw. Podmioty kluczowe i podmioty ważne mają istotny charakter dla funkcjonowania współczesnej gospodarki i społeczeństwa informacyjnego. Zakłócenie funkcjonowania tych podmiotów poprzez atak przez łańcuch dostaw może spowodować niepowetowane straty. Na gruncie prawa cywilnego niewykonanie umowy w związku z obowiązkiem wycofania sprzętu/oprogramowania pochodzącego od dostawcy wysokiego ryzyka należy traktować jako spowodowany siłą wyższą.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			otrzymanym produkcie lub usłudze. Ma to określone konsekwencje z punktu widzenia gospodarności wydatkowania środków publicznych. Potrzebne jest doprecyzowanie tych kwestii w celu uniknięcia (przynajmniej częściowo) strat z tym związanych. Jest oczywiście możliwość podjęcia próby zawarcia odpowiednich zapisów w zawieranych umowach, jednak wówczas istnieje ryzyko niezłożenia oferty przez żadnego dostawcę. Przepisy powinny wprowadzać miernik staranności wymagany od podmiotów, które dokonują zakupów lub doprecyzować zapisy prawa zamówień publicznych co do uprawnień dotyczących możliwości odstąpienia od zawartej umowy. Projekt zmienia jedynie art. 226 ust. 1 prawa zamówień publicznych. Jest to niewystarczające. Ponadto zmiany dokonywane art. 8 projektowanego aktu w art. 226 ust. 1 pkt. 19 prawa zamówień publicznych, tworzą obowiązek odrzucenia oferty, która obejmuje typ produktu określony w decyzji wydanej na podstawie art. 67b ust. 15 projektowanej zmiany do Ustawy o KSC. Decyzja taka powinna dotyczyć dostawcy. Obecne zapisy eliminują możliwość zakupu produktu innych dostawców, których nie dotyczy wydana decyzja. Należy również rozszerzyć zapis Art. 67c o przeprowadzenie analizy ryzyka i zastosowanie komplementarnych środków zaradczych w celu obniżenia poziomu ryzyka, jeśli to jest możliwe oraz jego monitorowania monitorować poziom ryzyka.	Odnosnie kwestii zerwania umowy w związku z wycofaniem sprzętu lub oprogramowania - obecne Prawo zamówień publicznych (dalej zwane – PZP) umożliwia zamawiającemu odstąpienie od umowy, jeżeli dalsze jej wykonywanie może zagrazić podstawowemu interesowi bezpieczeństwa państwa lub bezpieczeństwu publicznemu (art. 456 ust. 1 pkt 1 PZP). Zdaniem projektodawcy ryzyka stwarzanego przez dostawcę wysokiego ryzyka nie da się inaczej zmitigować jak tylko poprzez wycofanie sprzętu lub oprogramowania.
11.	ISSA polska	Art. 67b	Niezgodne z NIS2 i normami ETSI narzucenie podmiotom KSC wyników analizy ryzyka w zakresie sieci 5G Nowelizacja ustawy nakłada w art 8 na podmioty kluczowe lub ważne obowiązek prowadzenia systematycznego szacowania ryzyka wystąpienia incydentu. Każda analiza ryzyka obejmuje w szczególności klasyfikację zasobów ze względu na wpływ na procesy wpływające na świadczenie usług przez ten podmiot. Szczególnym przypadkiem takiego szacowania ryzyka jest sieć telefonii komórkowej piątej generacji (5G). Szacowania tego - łącznie z kategoryzacją zasobów - zgodnie z zapisami ustawy wdrażającymi NIS2 powinni dokonać operatorzy takiej sieci, będący podmiotami kluczowymi. W oparciu o przeprowadzone szacowanie operatorzy są zobowiązani do wdrożenia odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych. Niestety w załączniku nr 3 do Ustawy ustawodawca narzuca wynik kategoryzacji funkcji sieci 5G, której powinien dokonać podmiot kluczowy. Jest to nie tylko niezgodne z dyrektywą NIS2 i art 8 ustawy, ale kategoryzacja ta jest również błędna merytorycznie, ponieważ: - podczas szacowania ryzyka kategoryzacja poszczególnych zasobów jest względna, czyli dotyczy wpływu poszczególnych zasobów na realizację usługi świadczonej przez konkretny podmiot w porównaniu do pozostałych zasobów, - niedopuszczalna jest kategoryzacja wszystkich zasobów na tym samym, najwyższym poziomie, co przewiduje Załącznik 3, klasyfikujący jako krytyczne WSZYSTKIE funkcje sieci 5G. Tak wykonana kategoryzacja jest sprzeczna z przewidzianą w NIS2 i art 8 zasadą proporcjonalności, jest również niezgodna z normami technicznymi, na bazie których działa sieć 5G (np. ETSI TR 121 915 – V.15.0.0). Zgodnie z przedstawionym diagramem pochodzącym z normy ETSI TR 121 915 – V.15.0.0, poszczególne funkcje sieciowe posiadają różny poziom istotności, przy czym jako funkcje krytyczne uznawane są przede wszystkim AUSF, UDM i ARPF W związku z powyższym, w przypadku pozostawienia mechanizmu dostawcy wysokiego ryzyka, postulujemy usunięcie Załącznika 3 oraz zmianę brzmienia: - Art. 67c. ust 2 na „Przedsiębiorcy telekomunikacyjni, o których mowa w art. 67b ust. 1 pkt 2, wycofują w ciągu 5 lat typy produktów ICT, rodzaje usług ICT, konkretne procesy ICT wskazane w decyzji i określone, zgodnie z przeprowadzonym przez przedsiębiorcę szacowaniem ryzyka, jako krytyczne dla bezpieczeństwa sieci i usług” - Art. 67c ust 5. na „W przypadku, gdy podmioty, o których	Uwaga wyjaśniona Dyrektywa NIS 2 nie zabrania państwom członkowskim dbania o swoje bezpieczeństwo w sposób, który uważają za słuszne. Normy ETSI nie są wiążące dla państwa.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			mowa w art. 67b ust. 1, do których stosuje się ustawę z dnia 11 września 2019 r. – Prawo zamówień publicznych, nabyły, w drodze zamówienia publicznego, przed dniem ogłoszenia lub udostępnienia informacji o decyzji, o której mowa w art. 67b ust. 15, produkt ICT, usługę ICT lub proces ICT określone w tej decyzji, mogą korzystać z tych produktów, usług lub procesów nie dłużej niż 7 lat od dnia ogłoszenia lub udostępnienia informacji o decyzji, o której mowa w art. 67b ust. 15, a w przypadku produktów ICT, usług ICT lub procesów ICT wykorzystywanych do wykonywania funkcji krytycznych określonych w przeprowadzonych przez te podmioty szacowaniu ryzyka, nie dłużej niż 5 lat.” Powyższe propozycje obejmują również zmianę w celu realizacji postulatu ujednolicenia i urealnienia czasu wycofania elementów krytycznych.	
12.	ISSA Polska	Art. 67b	Strony postępowania w sprawie dostawcy wysokiego ryzyka W art. 67b ust. 3 ustawy o KSC jako stronę postępowania wskazuje się jedynie dostawcę, którego dotyczy postępowanie w sprawie uznania za dostawcę wysokiego ryzyka. Stroną takiego postępowania powinien móc być również podmiot, który korzysta z produktów lub usług takiego dostawcy, w celu umożliwienia zgłoszenia kwestii związanych ze skutkami wycofania towaru lub usługi ze stosowania (i faktycznej możliwości zastąpienia dostarczanego rozwiązania).	Uwaga wyjaśniona Z uwagi na charakter tego postępowania wyłączono część przepisów Kodeksu postępowania administracyjnego. Przede wszystkim nie jest możliwe przeprowadzenie postępowania administracyjnego przy udziale wszystkich podmiotów, które wykorzystują sprzęt lub oprogramowanie pochodzące od danego dostawcy.
13.	Federacja Przedsiębiorców Polskich	Art. 67b	W art. 67b ust. 1 proponuje się następujące brzmienie: <i>1. Minister właściwy do spraw informatyzacji, w celu ochrony bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego, może wszcząć z urzędu albo na wniosek przewodniczącego Kolegium, postępowanie w sprawie uznania dostawcy produktów ICT, usług ICT lub procesów ICT o funkcjach krytycznych, zwanego dalej dostawcą sprzętu lub oprogramowania o funkcjach krytycznych, które jest wykorzystywane przez podmioty kluczowe lub podmioty ważne w sektorach zarządzanie usługami ICT i dostawców usług cyfrowych, o których mowa w załączniku nr 1 i 2 do ustawy.</i> Przepis art. 67b przewiduje przeprowadzenie przez ministra właściwego do spraw informatyzacji, w celu ochrony ważnego interesu państwowego, postępowania w sprawie uznania dostawcy sprzętu lub oprogramowania o funkcjach krytycznych za dostawcę wysokiego ryzyka. W proponowanym kształcie przepis art. 67b ust. 1 spełnia wymagania określone w dokumencie przygotowanym przez Network and Information System Cooperation Group („NISCG”), który ustalił zestaw narzędzi obejmujący środki ograniczające ryzyko, które mają służyć eliminacji zidentyfikowanych zagrożeń dla cyberbezpieczeństwa na szczeblu krajowym i unijnym dla sieci 5G. Zestaw opisanych środków zawiera raport z 29 stycznia 2020 „Cybersecurity of 5G networks EU Toolbox of risk mitigating measures” (“Toolbox”, https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures). Chodzi w szczególności o zgodność ze środkiem określonym jako SM03, który stanowi, że: "Ocena profilu ryzyka dostawców i zastosowanie ograniczeń do dostawców uznanych za wysokiego ryzyka ma następować w odniesieniu do kluczowych aktywów" (s. 12 Toolbox). Mechanizm oceny powinien więc dotyczyć „key assets”, które to pojęcie jest wyjaśnione na s. 21 Toolbox. Przepis precyzyjnie określa, że nie chodzi o dostawcę każdego sprzętu lub oprogramowania, ale „o funkcjach krytycznych”. Treść przepisu jest zgodna także z oceną realizacji Toolbox w krajach członkowskich UE zawartą w dokumencie z lipca 2020	Uwaga wyjaśniona Zdaniem projektodawcy zasadne jest aby postępowanie w sprawie uznania za dostawcę wysokiego ryzyka dotyczyło dostawców dla wszystkich podmiotów kluczowych lub podmiotów ważnych. Nie można ograniczać się jedynie do funkcji krytycznych, ponieważ przez ukryte podatności w urządzeniach końcowych też można doprowadzić na przykład do incydentu krytycznego.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			r. NIS Cooperation Group pt. Report of Member States' Progress in Implementing the EU Toolbox on 5G Cybersecurity (s. 7, 11 tego raportu), jak również oceną zawartą w sprawozdaniu z czerwca 2023 roku dotyczącym działań państw członkowskich w zakresie wdrażania unijnego zestawu narzędzi dotyczących cyberbezpieczeństwa sieci 5G (NIS Cooperation Group: Progress in implementing the EU Toolbox on 5G Cybersecurity).sProponowane w przepisie art. 67b ust. 1 określenie „dostawcy sprzętu lub oprogramowania o funkcjach krytycznych” będzie obejmować tylko dostawców wrażliwych elementów sieci, zgodnie z zaleceniami Grupy Współpracy NIS (zob. sprawozdanie Grupy Współpracy ds. Bezpieczeństwa Sieci i Informacji z postępów państw członkowskich we wdrażaniu zestawu narzędzi UE w zakresie cyberbezpieczeństwa 5G, lipiec 2020 r., s. 16), a nie każdego producenta, dystrybutora lub importera produktów, usług lub procesów ICT. Konieczne jest precyzyjne określenie w tym przepisie, że dostawcą sprzętu lub oprogramowania jest nie każdy dostawca produktów ICT, usług ICT lub procesów w ICT, ale tylko dostawca produktów ICT, usług ICT lub procesów ICT o funkcjach krytycznych.	
14.	Federacja Przedsiębiorców Polskich	Art. 67b	W art. 67b ust. 2 proponuje się następujące brzmienie:<i>2. Do postępowania w sprawie uznania za dostawcę wysokiego ryzyka stosuje się przepisy ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego.</i> Z uwagi na to, że projektowane przepisy będą ograniczać swobodę prowadzenia działalności gospodarczej przez podmioty zobowiązane do wycofania wskazanych w decyzji administracyjnej typów produktów i usług oraz wpłyną na konkurencję na rynku tych produktów i usług, konieczne jest zagwarantowanie transparentnego i rzetelnego postępowania administracyjnego. Przepisy te mogą mieć dalekosiężne konsekwencje dla podmiotów gospodarczych, zarówno w kontekście bezpośrednich kosztów związanych z wycofaniem produktów i usług, jak i w kontekście zmian rynkowych wynikających z ograniczenia dostępności określonych produktów i usług. Do postępowania w sprawie uznania dostawcy za dostawcę wysokiego ryzyka będą więc miały zastosowanie przepisy kodeksu postępowania administracyjnego (KPA). Jest to kluczowe, aby zapewnić, że proces ten będzie przeprowadzony w sposób sprawiedliwy i zgodny z obowiązującymi standardami prawnymi, co z kolei zwiększy zaufanie do podejmowanych decyzji. Przestrzeganie przepisów KPA gwarantuje, że wszystkie strony postępowania będą miały równe prawa i będą mogły skutecznie bronić swoich interesów.tDostawca sprzętu lub oprogramowania będzie brał udział w postępowaniu na prawach strony, co oznacza, że będzie miał możliwość przedstawienia swoich argumentów, dowodów oraz składania wniosków. Projekt nie przewiduje wyłączenia stosowania jakichkolwiek przepisów KPA, co jest kluczowe dla zapewnienia pełnej ochrony praw dostawców. W szczególności zastosowanie ma art. 28 KPA, zgodnie z którym stroną jest każdy, czyjego interesu prawnego lub obowiązku dotyczy postępowanie albo kto żąda czynności organu ze względu na swój interes prawny lub obowiązek.eArt. 31 KPA, który dotyczy udziału organizacji społecznej w postępowaniu administracyjnym, również będzie miał zastosowanie. Umożliwia to organizacjom społecznym, które działają na rzecz ochrony interesów publicznych, uczestniczenie w postępowaniu. Jest to istotne, ponieważ organizacje te mogą dostarczyć dodatkowych informacji i perspektyw, które mogą być kluczowe dla pełnej i rzetelnej oceny sytuacji.ePonadto, transparentność i rzetelność postępowania administracyjnego są niezbędne do zapewnienia, że decyzje podejmowane w sprawie uznania dostawcy za dostawcę wysokiego ryzyka będą miały solidne podstawy prawne i faktyczne.	Uwaga wyjaśniona Przy wielu potencjalnych stronach postępowania niemożliwe byłoby skuteczne przeprowadzenie postępowania administracyjnego. Jednocześnie w projekcie zapewnia się możliwość przedstawienia opinii w sprawie dostawcy, wobec którego wszczęto postępowanie przez izby gospodarcze.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			W praktyce oznacza to, że każde postępowanie powinno być przeprowadzone w sposób jawny, z możliwością wglądu w dokumenty i dowody przedstawiane przez strony, oraz z zapewnieniem możliwości odwołania się od decyzji administracyjnych. Wprowadzenie przepisów zapewniających transparentność i rzetelność postępowania administracyjnego ma również na celu zapobieganie potencjalnym nadużyciom i arbitralności w podejmowaniu decyzji. Gwarantuje to, że proces wycofywania produktów i usług będzie oparty na obiektywnych kryteriach i rzetelnej analizie ryzyka, a nie na subiektywnych ocenach czy presjach politycznych.	
15.	PTI	Art. 67b	W dodanym do zmienianej ustawy art. 67b ust.1określającym uprawnienie Ministra właściwego ds. informatyzacji do wszczęcia postępowania w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, proponuje się ograniczyć zakres podmiotów w stosunku do których decyzja taka może być wydana jedynie do podmiotów kluczowych. Przesłanką do takiej zmiany jest zarówno szacowana liczba podmiotów ważnych która mogłaby zostać objęta skutkami takiej decyzji, jak i możliwość jej faktycznego wykonania przez te podmioty nProponowany zapis art. 67b ust.1 p 1): „ <i>podmioty kluczowe, z wyłączeniem podsektora ko-munikacji elektronicznej lub</i> ”	Uwaga nieuwzględniona Także podmioty ważne są obowiązane do dbania o bezpieczeństwo łańcuchów dostaw, stąd wyłączenie ich z obowiązku wycofania sprzętu lub oprogramowania pochodzącego od dostawcy wysokiego ryzyka jawi się jako działanie niezasadne i niecelowe.
16.	PTI	Art. 67b	Pkt 70, art. 67b, ust 11 ppkt 4): „ <i>liczby i rodzajów wykrytych podatności i incydentów dotyczących typów produktów ICT lub rodzajów usług ICT lub konkretnych procesów ICT dostarczanych przez dostawcę sprzętu lub oprogramowania oraz sposobu i czasu ich eliminowania;</i> ” – kryterium jest nieprecyzyjne; wykryte przez kogo? W jakim okresie? – zapis wymaga doprecyzowania	Uwaga wyjaśniona Wiedza o podatnościach i incydentach związanych z konkretnym dostawcą będzie pochodzić od zespołów CSIRT czy np. z publicznych baz CVE.
17.	PTI	Art. 67b	Pkt 70, art. 67b, ust 11 ppkt 5): „trybu i zakresu, w jakim dostawca sprzętu lub oprogramowania sprawuje nadzór nad procesem wytwarzania i dostarczania sprzętu lub oprogramowania dla podmiotów,” – kryterium jest nieprecyzyjne. Co oznacza „trybu i zakresu”? jaki tryb jest akceptowalny? Czy jeśli wiodący europejski dostawca sprzętu telekomunikacyjnego ma 6000 dostawców w łańcuchu dostaw, to należy uznać, że sprawuje wystarczający nadzór? A nie będzie on wystarczający, jeśli dotyczyłoby to dostawcy azjatyckiego? Kryterium jest skrajnie nieprecyzyjne. Należy rozważyć jego wykreślenie	Uwaga wyjaśniona Chodzi o analizę tego co się dzieje z wytwarzaniem produktów w ramach łańcuchów dostaw – czy dostawca ma odpowiednią wiedzę i wymagania wobec dostarczanych dla niego produktów czy też ma niskie wymagania jakościowe.
18.	Przedsiębiorcy.pl	Art. 67b	III.1 Wylimitowanie możliwości udziału podmiotów kluczowych w charakterze strony postępowania w przedmiocie uznania dostawcy za dostawcę wysokiego ryzyka Podkreślenia wymaga fakt, że w postępowaniu w sprawie uznania za dostawcę wysokiego ryzyka (art. 67b ust. 1 projektu ustawy o KSC), stroną postępowania jest jedynie dostawca wysokiego ryzyka. Wyłączono tutaj bowiem zastosowanie art. 28 kpa stanowiącego, że: „stroną jest każdy, czyjego interesu prawnego lub obowiązku dotyczy postępowanie”. Wyłączony jest tutaj zatem podmiot kluczowy lub podmiot ważny, który korzysta z oprogramowania takiego dostawcy wysokiego ryzyka. Podmioty te powinny mieć prawo wziąć udział w tym postępowaniu, gdyż zwyczajnie mają w tym interes prawny. Wyjątkiem jest tutaj przedsiębiorca komunikacji elektronicznej, który spełnia określony w przepisach projektu ustawy census majątkowy (co najmniej dwudziestotysięczna krotność przeciętnego wynagrodzenia w gospodarce narodowej wskazanego w ostatnim komunikacie Prezesa GUS). Jest to uregulowanie zaburzające zasadę równowagi, zwłaszcza biorąc pod uwagę fakt, że decyzja o wycofaniu sprzętu, zgodnie z projektem ustawy	Uwaga wyjaśniona Przy wielu potencjalnych stronach postępowania niemożliwe byłoby skuteczne przeprowadzenie postępowania administracyjnego. Jednocześnie w projekcie zapewnia się możliwość przedstawienia opinii w sprawie dostawcy wobec którego wszczęto postępowanie przez izby gospodarcze.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			ma dotyczyć 18 branż, a nie tylko branży telekomunikacyjnej. W tym postępowaniu wyłączono również przepis art. 31 kpa i tym samym wyeliminowano udział organizacji społecznych, co również zasługuje na krytykę. Udział organizacji społecznych wyłączony również został w postępowaniu administracyjnym, w którym rozpatrywana będzie skarga na decyzję o uznaniu dostawcy za dostawcę wysokiego ryzyka (art. 67b ust. 15 projektu ustawy o KSC). Warto także wskazać na niepokojący fakt, że wyrok sądu administracyjnego, który rozpatruje skargę doręczany jest skarżącemu z częścią uzasadnienia, która nie zawiera informacji niejawnych. Skarżący nie posiada zatem do końca wiedzy o motywach wykluczenia go jako dostawcy produktów lub usług dla danego podmiotu kluczowego lub ważnego.	
19.	Federacja Przedsiębiorców Polskich	Art. 67b ust. 3	Art. 67b ust.3 otrzymuje następujące brzmienie: <i>3. Stroną postępowania jest każdy, czyjego interesu prawnego lub obowiązku dotyczy postępowanie w sprawie uznania za dostawcę wysokiego ryzyka albo kto żąda czynności organu ze względu na swój interes prawny lub obowiązek.</i> Określenie strony jest zgodne ze zdefiniowaniem strony w art. 28 KPA, który stanowi, że stroną jest każdy, czyjego interesu prawnego lub obowiązku dotyczy postępowanie albo kto żąda czynności organu ze względu na swój interes prawny lub obowiązek. Zapewni to ochronę swoich praw przez podmioty zainteresowane udziałem w tym postępowaniu. Szczególnie jest to ważne dla podmiotów, których może dotyczyć decyzja wydana w postępowaniu w sprawie uznania danego dostawcy za dostawcę wysokiego ryzyka.	Uwaga wyjaśniona Przy wielu potencjalnych stronach postępowania niemożliwe byłoby skuteczne przeprowadzenie postępowania administracyjnego. Jednocześnie w projekcie zapewnia się możliwość przedstawienia opinii w sprawie dostawcy wobec którego wszczęto postępowanie przez izby gospodarcze.
20.	Federacja Przedsiębiorców Polskich	Art. 67b ust. 4	Proponuje się wykreślenie art. 67b ust. 4 Stroną postępowania powinien być każdy podmiot, czyjego interesu prawnego lub obowiązku dotyczy postępowanie albo kto żąda czynności organu ze względu na swój interes prawny lub obowiązek. Zapewni to ochronę swoich praw przez podmioty zainteresowane udziałem w tym postępowaniu. Szczególnie jest to ważne dla podmiotów, których może dotyczyć decyzja wydana w postępowaniu w sprawie uznania danego dostawcy za dostawcę wysokiego ryzyka.	Uwaga wyjaśniona Przy wielu potencjalnych stronach postępowania niemożliwe byłoby skuteczne przeprowadzenie postępowania administracyjnego. Jednocześnie w projekcie zapewnia się możliwość przedstawienia opinii w sprawie dostawcy wobec którego wszczęto postępowanie przez izby gospodarcze.
21.	Federacja Przedsiębiorców Polskich	Art. 67b ust. 5	W art. 67b ust. 5 powinien zostać wykreślony. <i>5. Za poprzedni rok obrotowy uznaje się rok, przed którym postępowanie zostało wszczęte. Za ostatni komunikat Prezesa Głównego Urzędu Statystycznego uznaje się ostatni komunikat Prezesa Głównego Urzędu Statystycznego przed wszczęciem postępowania.</i> Skreślenie ust. 5 w art. 67b jest konsekwencją zmiany w art. 67b ust. 4, czyli usunięcia kryterium przychodu jako kryterium udziału w postępowaniu zainteresowanego podmiotu.	Uwaga nieuwzględniona W związku z nieuwzględnieniem uwagi do art. 67b ust. 4 projektu.
22.	Federacja Przedsiębiorców Polskich	Art. 67b ust. 8:	W art. 67b skreśla się ust. 8 w brzmieniu: <i>8. Jeżeli dostawcą sprzętu lub oprogramowania jest strona niemająca siedziby na terytorium państwa członkowskiego Unii Europejskiej, Konfederacji Szwajcarskiej albo państwa członkowskiego Europejskiego Porozumienia o Wolnym Handlu (EFTA) – stronie umowy o Europejskim Obszarze Gospodarczym</i>	Uwaga nieuwzględniona Przepis ma zapewnić możliwość skutecznego doręczenia zawiadomienia o wszczęciu postępowania wobec dostawcy,

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			zawiadomienie, o którym mowa w ust. 6, udostępnia się w Biuletynie Informacji Publicznej na stronie podmiotowej ministra właściwego do spraw informatyzacji. Udostępnienie ma skutek doręczenia po upływie 14 dni od dnia jego dokonania. Uregulowanie to jest odstępstwem od podstawowych zasad obowiązujących w KPA. Postanowienia art. 67b ust. 8 w obecnym kształcie mogą zostać uznane za dyskryminujące dla krajów, które nie posiadają siedziby na terytorium wskazanym w tym przepisie. Mogą być także sprzeczne z dwustronnymi umowami Polski z innymi krajami, które zakazują tego rodzaju dyskryminacji.	który nie ma siedziby na terenie UE, EFTA/EOG, itd.
23.	Związek Cyfrowa Polska	Art. 67b ust. 9	Art. 67b ust 9 – postulujemy o poszerzenie katalogu podmiotów, które <i>mogą przedstawić ministrowi właściwemu do spraw informatyzacji stanowisko co do dostawcy sprzętu lub oprogramowania, wobec którego wszczęto postępowanie, oraz dostarczanych przez niego produktów ICT, usług ICT oraz procesów ICT</i> , również o Związki Pracodawców, działających na podstawie Ustawy z dnia 23 maja 1991 r. o organizacjach pracodawców.	Uwaga uwzględniona Przepis zostanie zmieniony.
24.	Federacja Przedsiębiorców Polskich	Art. 67b ust. 10	Proponuje się następujące brzmienie art. 67b przepis ust. 10: <i>10. Przed rozstrzygnięciem sprawy minister właściwy do spraw informatyzacji zasięga opinii Kolegium. Kolegium przekazuje opinię w terminie 3 miesięcy od dnia wystąpienia o opinię. Okresu od dnia wystąpienia o opinię do dnia jej otrzymania nie wlicza się do terminu załatwienia sprawy.</i> W stosunku do wersji przewidzianej w projekcie ustawy, zmiana polega na wykreśleniu zdania: „Przepisu art. 106 § 5 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego nie stosuje się.” Nowe brzmienie art. 67b ust. 10 oznacza więc, że na przygotowaną przez Kolegium opinię będzie przysługiwać zażalenie, co będzie zgodne właśnie z art. 106 § 5 KPA, który stanowi, że zajęcie stanowiska przez ten organ następuje w drodze postanowienia, na które służy stronie zażalenie. Zapewni to transparentność postępowania i możliwość korzystania z podstawowych praw przewidzianych przez KPA dla uczestników postępowania, a przede wszystkim możliwość weryfikacji stanowisk organów administracyjnych w drodze złożenia na nie zażalenia przez strony tego postępowania.	Uwaga nieuwzględniona Kolegium do Spraw Cyberbezpieczeństwa nie jest organem administracji publicznej więc nie może wydawać postanowień. Stąd został wyłączony art. 106 § 5 KPA.
25.	Federacja Przedsiębiorców Polskich	Art. 67 ust. 11	Proponuje się następujące brzmienie art. 67b ust. 11: <i>11. Opinia, o której mowa w ust. 10 uwzględnia:</i> <i>1) analizę zagrożeń bezpieczeństwa narodowego o charakterze ekonomicznym, wywiadowczym i terrorystycznym oraz zagrożeń dla realizacji zobowiązań sojuszniczych i europejskich, jakie stanowi sprzęt i oprogramowanie;</i> <i>2) sprawdzenie przedsiębiorcy, w tym na podstawie danych zawartych w rejestrach, ewidencjach, kartotekach, także niedostępnych powszechnie, które obejmuje:</i> <i>a) strukturę kapitału oraz powiązania kapitałowe przedsiębiorcy, źródła pochodzenia środków finansowych i sytuację finansową,</i> <i>b) strukturę organizacyjną,</i> <i>c) prawodawstwo w zakresie ochrony danych osobowych, zwłaszcza tam, gdzie nie ma porozumień w zakresie ochrony danych między UE i danym państwem;</i> <i>3) tryb, zakres i rodzaje powiązań dostawcy sprzętu lub oprogramowania z podmiotami określonymi w załączniku do rozporządzenia Rady (UE) 2019/796 z dnia 17 maja 2019 r. w sprawie środków</i>	Uwaga nieuwzględniona Sprawdzenie przedsiębiorcy w rejestrach/kartotekach może w niewystarczający sposób identyfikować zagrożenia związane z konkretnym dostawcą.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

		<i>ograniczających w celu zwalczania cyberataków zagrażających Unii lub jej państwom członkowskim (Dz. Urz. UE L 129I z 17.5.2019, str. 1–12, z późn. zm.);</i> <i>4) liczby i rodzajów wykrytych podatności i incydentów dotyczących typów produktów ICT lub rodzajów usług ICT lub konkretnych procesów ICT dostarczanych przez dostawcę sprzętu lub oprogramowania oraz sposobu i czasu ich eliminowania;</i> <i>5) tryb i zakres, w jakim dostawca sprzętu lub oprogramowania sprawuje nadzór nad procesem wytwarzania i dostarczania sprzętu lub oprogramowania dla podmiotów, o których mowa w ust. 1 pkt 1–2, oraz ryzyka dla procesu wytwarzania i dostarczania sprzętu lub oprogramowania;</i> <i>6) treści wydanych wcześniej rekomendacji, o których mowa w art. 33 ust. 4, dotyczących sprzętu lub oprogramowania danego dostawcy.</i> Postanowienia art. 67b ust. 11 zawierają wskazanie kryteriów, które będą podstawą do wydania opinii Kolegium. W ramach opinii będzie przeprowadzona kompleksowa analiza dostawcy sprzętu lub oprogramowania na podstawie zarówno aspektów technicznych, jak i nietechnicznych. Zaproponowane w art. 67b ust. 11 kryteria są analogiczne do obowiązujących już w innych krajach, takich jak Austria czy Słowenia. Analiza zagrożeń bezpieczeństwa narodowego (pkt 1) obejmuje ocenę potencjalnych ryzyk związanych z bezpieczeństwem ekonomicznym, wywiadowczym i terrorystycznym oraz zobowiązaniami sojuszniczymi i europejskimi. Wprowadzenie tak szerokiej analizy ma na celu dokładne zidentyfikowanie wszystkich możliwych zagrożeń, które mogą wynikać z działalności dostawcy sprzętu lub oprogramowania. Sprawdzenie przedsiębiorcy (pkt 2) na podstawie różnych źródeł, w tym rejestrów i ewidencji, pozwala na dokładne poznanie struktury kapitałowej, powiązań kapitałowych, źródeł finansowania oraz struktury organizacyjnej dostawcy. Szczególna uwaga poświęcona jest prawodawstwu w zakresie ochrony danych osobowych, co jest kluczowe w kontekście zgodności z przepisami UE, zwłaszcza tam, gdzie nie ma porozumień o ochronie danych z danym państwem. Ocena powiązań dostawcy (pkt 3) z podmiotami określonymi w rozporządzeniu Rady (UE) 2019/796 jest istotna dla zrozumienia potencjalnych zagrożeń związanych z cyberatakami, które mogą zagrażać Unii lub jej państwom członkowskim. Taka analiza pomaga w identyfikacji dostawców, którzy mogą być powiązani z podmiotami uznanymi za ryzykowne. Analiza liczby i rodzaju wykrytych podatności oraz incydentów (pkt 4) dotyczących produktów i usług ICT dostarczanych przez dostawcę jest kluczowa dla oceny jego wiarygodności i zdolności do szybkiego i skutecznego reagowania na zagrożenia. Sposób i czas eliminacji tych podatności stanowi ważny wskaźnik poziomu bezpieczeństwa oferowanego przez dostawcę. Ocena trybu i zakresu nadzoru nad procesem wytwarzania i dostarczania sprzętu lub oprogramowania (pkt 5) jest istotna dla zrozumienia, w jaki sposób dostawca zarządza ryzykami związanymi z produkcją i dostarczaniem swoich produktów. Takie informacje pomagają ocenić, czy dostawca jest w stanie utrzymać odpowiedni poziom bezpieczeństwa w całym procesie produkcyjnym. Wreszcie, uwzględnienie treści wydanych wcześniej rekomendacji (pkt 6) dotyczących sprzętu lub oprogramowania danego dostawcy zapewnia, że wszelkie wcześniejsze oceny i zalecenia są brane pod uwagę przy podejmowaniu decyzji. To pomaga w zachowaniu ciągłości i spójności w podejmowaniu decyzji dotyczących bezpieczeństwa. Postanowienia obowiązujące od 1 listopada 2021	

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			r. austriackiej ustawy prawo telekomunikacyjne (Telekommunikationsgesetz - TKG 2021, zob. § 45 ust. 3 pkt 1-3), nie wymieniają przesłanek w postaci zdolności ingerencji państwa trzeciego w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania, ani prawdopodobieństwa, z jakim dostawca sprzętu lub oprogramowania znajduje się pod kontrolą państwa spoza terytorium Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego. Jednakże, uwzględnienie takich kryteriów w polskim prawodawstwie jest uzasadnione ze względu na specyficzne zagrożenia i kontekst geopolityczny, w jakim funkcjonują polscy dostawcy i konsumenci usług ICT. Skupienie się na tych sześciu kryteriach zapewnia, że decyzje o uznaniu dostawcy za dostawcę wysokiego ryzyka będą podejmowane na podstawie solidnych i obiektywnych przesłanek, co zwiększa transparentność i przewidywalność procesu decyzyjnego oraz przyczynia się do wzmocnienia bezpieczeństwa cybernetycznego w Polsce.	
26.	Federacja Przedsiębiorców Polskich	Art. 67b ust. 13	Proponuje się następujące brzmienie art. 67b ust. 13 pkt : <i>1) przewodniczący Kolegium powołuje zespół w celu opracowania projektu opinii w sprawie uznania dostawcy za dostawcę wysokiego ryzyka, zwany dalej „zespołem opiniującym”, w skład którego wchodzi przedstawiciele członków Kolegium wskazani przez przewodniczącego Kolegium oraz przedstawiciele podmiotu który nabywa lub posiada produkty ICT, procesy ICT lub oprogramowanie ICT podlegające ocenie, zainteresowane izby gospodarcze lub inne organizacje zrzeszające podmioty z branży ICT, a także przedstawiciele dostawcy sprzętu lub oprogramowania podlegającego ocenie;</i> Przewidziany w art. 67b ust. 13 pkt 1 skład osobowy zespołu opiniującego jest analogiczny do funkcjonujących w Niemczech, Austrii i Finlandii, gdzie w procesie oceny dostawców wysokiego ryzyka uczestniczą również apolityczni przedstawiciele izb gospodarczych, producentów, dostawców i operatorów. Taka struktura zespołu opiniującego zapewnia, że ocena dostawców jest przeprowadzana w sposób rzetelny i obiektywny, z uwzględnieniem szerokiego spektrum perspektyw i interesów różnych podmiotów. Każdy członek zespołu opiniującego przygotowuje stanowisko w zakresie swojej właściwości. To znaczy, że przedstawiciele różnych grup interesariuszy mogą dostarczyć istotnych informacji i wiedzy specjalistycznej, które są niezbędne do dokładnej oceny ryzyka związanego z dostawcą sprzętu lub oprogramowania. Dzięki temu proces oceny jest bardziej wszechstronny i obejmuje różnorodne aspekty techniczne, ekonomiczne oraz prawne. Włączenie przedstawicieli podmiotu, który nabywa lub posiada produkty ICT, procesy ICT lub oprogramowanie ICT podlegające ocenie, jest kluczowe, ponieważ to oni są bezpośrednio zainteresowani bezpieczeństwem i niezawodnością dostarczanych produktów i usług. Ich udział w zespole opiniującym zapewnia, że ocena ryzyka będzie uwzględniać rzeczywiste zagrożenia i wyzwania, z jakimi mogą się spotkać użytkownicy końcowi. Zainteresowane izby gospodarcze oraz inne organizacje zrzeszające podmioty z branży ICT wnoszą do zespołu opiniującego perspektywę sektora, co jest niezbędne do zrozumienia szerszych implikacji gospodarczych i rynkowych. Organizacje te mogą również dostarczyć informacji na temat najlepszych praktyk i standardów obowiązujących w branży, co przyczynia się do podniesienia jakości oceny. Włączenie przedstawicieli dostawcy sprzętu lub oprogramowania podlegającego ocenie jest istotne dla zapewnienia, że proces oceny jest przejrzysty i sprawiedliwy. Dostawcy mają możliwość przedstawienia	Uwaga nieuwzględniona Izby gospodarcze będą mogły przedstawić stanowisko w sprawie dostawcy wobec którego wszczęto postępowanie. Dostawca sprzętu lub oprogramowania będzie mógł się wypowiedzieć w postępowaniu jako strona postępowania. Uprawnienia te konsumują uwagę.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			swoich argumentów i dowodów, co pozwala na pełne uwzględnienie wszystkich istotnych informacji przy podejmowaniu decyzji. Analogiczne rozwiązania funkcjonujące w Niemczech, Austrii i Finlandii pokazują, że takie podejście jest skuteczne i sprawdzone. W tych krajach, proces oceny dostawców wysokiego ryzyka angażuje szerokie grono interesariuszy, co przyczynia się do bardziej zrównoważonych i przemyślanych decyzji. Każdy członek zespołu opiniującego przygotowuje stanowisko w zakresie swojej właściwości, co zapewnia, że ocena jest wszechstronna i uwzględnia wszystkie istotne aspekty ryzyka. Taki system promuje rzetelność i obiektywizm w procesie oceny, co jest kluczowe dla zachowania wysokiego poziomu bezpieczeństwa i zaufania do systemu oceny dostawców wysokiego ryzyka.	
27.	Federacja Przedsiębiorców Polskich	Art. 67b ust. 14	W art. 67b po przepisie ust. 14 proponuje się dodanie ust. 14a w następującym brzmieniu: <i>14a. W ciągu miesiąca od otrzymania opinii Kolegium, dostawca sprzętu lub oprogramowania o funkcjach krytycznych, którego dotyczy ta opinia, może przedstawić środki naprawcze i plan naprawczy. Środki naprawcze powinny wskazywać sposób usunięcia sformułowanych w opinii Kolegium zagrożeń dla obronności, bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego lub życia i zdrowia ludzi. Plan naprawczy powinien przedstawiać harmonogram realizacji poszczególnych środków naprawczych. W przypadku zaakceptowania środków naprawczych i planu naprawczego, Kolegium zmienia ocenę. Do czasu zakończenia postępowania w sprawie zaakceptowania środków naprawczych i planu naprawczego, minister właściwy do spraw informatyzacji nie wydaje decyzji o której mowa w art. 67b ust. 15.</i> Postanowienia art. 67b ust. 14a przewidują możliwość podjęcia właściwych środków naprawczych przez dostawcę sprzętu lub oprogramowania, którego dotyczy postępowanie w sprawie uznania za dostawcę wysokiego ryzyka. Zważywszy na daleko idące skutki decyzji – zarówno dla dostawcy, jak i dla jego klientów zobowiązanych do zaprzestania użytkowania rozwiązań objętych decyzją – decyzja powinna stanowić <i>ultima ratio</i>, czyli być podejmowana dopiero wtedy, gdy inne, mniej dotkliwe, ale możliwe środki naprawcze okazały bezskuteczne. Biorąc pod uwagę fakt, że wydanie decyzji, na podstawie projektowanego art. 67b ust. 15 będzie stanowić przejaw dużego ograniczenia (o ile nie zupełnego wyłączenia) swobody działalności gospodarczej, to wprowadzenie rozwiązań mniej uciążliwych należy uznać za konieczne w kontekście art. 31 ust. 3 Konstytucji i wywodzonej z tego przepisy zasady proporcjonalności. Prawodawca powinien dążyć do wprowadzenia regulacji, które w jak najmniejszym stopniu ograniczą konstytucyjne wolności i prawa jednostek, a doprowadzą do ochrony tych samych wartości (bezpieczeństwo państwa). Proponowane rozwiązanie jest zbliżone do rozwiązań funkcjonujących w innych państwach członkowskich UE (przykładowo – § 244a fińskiej ustawy o usługach łączności elektronicznej).	Uwaga nieuwzględniona W przypadku dostawcy wysokiego ryzyka mamy do czynienia z podmiotem który poważnie zagraża bezpieczeństwu państwa. W tym przypadku stopniowe wycofanie sprzętu lub oprogramowania od takiego dostawcy jest jedyną możliwością zmitigowania ryzyk stwarzanych przez takiego dostawcę.
28.	Federacja Przedsiębiorców Polskich	Art. 67b ust. 15	Proponuje się następujące brzmienie art. 67b ust. 15: <i>15. Minister właściwy do spraw informatyzacji, w drodze decyzji na okres nie dłuższy niż 24 miesiące, po wcześniejszym jej zaakceptowaniu przez ministra właściwego do spraw rozwoju i technologii, ministra spraw wewnętrznych, ministra obrony narodowej, ministra sprawiedliwości oraz wyrażenia pozytywnej opinii przez Prezesa Urzędu Ochrony Konkurencji i Konsumentów, uznaje dostawcę sprzętu lub oprogramowania o funkcjach krytycznych, za dostawcę wysokiego ryzyka, jeżeli dostawca ten stanowi poważne zagrożenie dla obronności, bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego, lub życia i zdrowia ludzi.</i>	Uwaga nieuwzględniona Decyzja ministra właściwego do spraw informatyzacji będzie poprzedzona opinią rządowego Kolegium do Spraw Cyberbezpieczeństwa. Ponadto w przygotowywaniu opinii będzie uczestniczył także Prezes UOKiK.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			Po przeprowadzeniu postępowania powinna być wydana decyzja w sprawie uznania dostawcy sprzętu lub oprogramowania o funkcjach krytycznych za dostawcę wysokiego ryzyka. Decyzja nie powinna być podejmowana jednoosobowo przez ministra właściwego do spraw informatyzacji. Z uwagi na wpływ tej decyzji na stosunki międzynarodowe z innymi państwami czy bezpieczeństwo wewnętrzne oraz skomplikowany charakter prawny, powinny uczestniczyć w jej podejmowaniu także inni ministrowie odpowiedzialni za obszary istotne z perspektywy chronionych wartości (obronność, bezpieczeństwo i porządek publiczny, zdrowie i życie ludzi) lub za obszary właściwe merytorycznie z perspektywy sektora, którego dotyczy decyzja (rozwój i technologia). Będzie to zgodne z analogicznymi rozwiązaniami funkcjonującymi w innych krajach UE. Przykładowo decyzja taka w Niemczech jest podejmowana przy udziale federalnego ministerstwa spraw wewnętrznych, zagranicznych i gospodarki (Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme, Dziennik Nr 25 z 27.05.2021, s. 1122, https://www.bundesanzeiger-verlag.de). Pozytywną opinię powinien wyrazić także Prezes Urzędu Ochrony Konkurencji i Konsumentów. Decyzja w sprawie uznania za dostawcę wysokiego ryzyka może bowiem, poprzez ograniczenie możliwości oferowania określonych produktów lub usług przez tego dostawcę, wpływać istotnie na konkurencję na rynku oraz korzystanie z usług przez użytkowników. Konsekwencją takiego – częściowego lub całkowitego – wykluczenia z rynku dostawcy czy dostawców, może być wzrost cen infrastruktury telekomunikacyjnej, a w konsekwencji wzrost cen świadczonych dla indywidulanych klientów usług telekomunikacyjnych. Wyłączenie możliwości prowadzenie działalności gospodarczej danego rodzaju (a do tego sprowadzałoby się dla dostawcy wydanie decyzji na podstawie projektowanego art. 67b ust. 15), nie może być przy tym bezterminowe. Regulacja powinna w szczególności uwzględniać wpływ bardzo szybkiego rozwoju technologicznego i dynamicznych zmian w zakresie zagrożeń związanych z cyberbezpieczeństwem na aktualność decyzji. Z tego względu regulacja powinna wymuszać przegląd aktualnych uwarunkowań, i stosownie do przypadku – dokonanie zmian w wydanej decyzji, wydanie nowej decyzji albo uznanie, że nie zachodzi już potrzeba wydawania w omawianym zakresie kolejnej decyzji. Uregulowania takie występują w innych krajach UE, np. w Austrii i Słowenii.	
29.	ZBP	Art. 67b ust. 15 i 16	Minister właściwy do spraw informatyzacji, w drodze decyzji, uznaje dostawcę sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, jeżeli dostawca ten stanowi poważne zagrożenie dla obronności, bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego, lub życia i zdrowia ludzi. Decyzja, o której mowa w ust. 15, zawiera w szczególności wskazanie typów produktów ICT, rodzajów usług ICT lub konkretnych procesów ICT pochodzących od dostawcy sprzętu lub oprogramowania uwzględnionych w postępowaniu w sprawie uznania za dostawcę wysokiego ryzyka. Uwaga ogólna: Należy zwrócić uwagę, że w związku z wejściem w życie wskazanych przepisów, uzasadnione jest wprowadzenie uregulowań, które zabezpieczą realnie przed określaniem „dostawców wysokiego ryzyka” (i wskazanie typów produktów ICT, rodzajów usług ICT lub konkretnych procesów ICT) na polecenie lub pod wpływem obcych służb zabezpieczających własne interesy finansowe, pozostające w konflikcie interesów z interesami podatników polskich. Przykład z tych bardziej znanych „wojen lobbystów”, odnoszących się do wcześniejszych zmian tej samej ustawy: https://spidersweb.pl/plus/2021/11/huawei-budowa-sieci-5g-w-polsce-stany-zjednoczone-chiny-siec-aukcja	Uwaga wyjaśniona Decyzja będzie podejmowana przez ministra właściwego do spraw informatyzacji, który jest niezależny od obcych wpływów.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

30.	Federacja Przedsiębiorców Polskich	Art. 67b ust. 18	Proponuje się skreślenie art. 67b ust. 18. <i>Decyzja, o której mowa w ust. 15, podlega natychmiastowemu wykonaniu.</i> Decyzja nie powinna być natychmiast wykonalna z uwagi na istotne skutki gospodarcze oraz prawo do sprawiedliwego procesu. Natychmiastowe wykonanie decyzji nakładałoby na podmioty gospodarcze obowiązek natychmiastowego zaprzestania nabywania nowego sprzętu lub oprogramowania oraz rozpoczęcia procedury wycofania już nabytego sprzętu lub oprogramowania. Taki wymóg może prowadzić do znacznych kosztów oraz zakłóceń w działalności przedsiębiorstw, co może mieć negatywny wpływ na ich funkcjonowanie oraz stabilność finansową.ŚPrzed wszystkim jednak, ze względu na to, że postępowania sądowe w praktyce trwają nawet kilka lat, późniejsze nawet korzystne rozstrzygnięcie sądowe nie będzie miało znaczenia, gdyż do tego czasu sprzęt lub usługi zostaną zakupione od innych dostawców. W praktyce oznacza to, że przedsiębiorstwa, które zostałyby zmuszone do natychmiastowego wykonania decyzji, mogą ponieść nieodwracalne straty, zanim będą miały szansę na uzyskanie sądowego rozstrzygnięcia. Naruszy to gwarantowane konstytucyjnie i traktatów prawo do sprawiedliwego rozpatrzenia sprawy przez sąd. Artykuł 45 ust. 1 w zw. z art. 31 ust. 3 Konstytucji RP stanowi, że każdy ma prawo do sprawiedliwego rozpatrzenia sprawy przez sąd w rozsądnym terminie. Podobne gwarancje znajdują się w art. 47 w zw. z art. 52 ust. 1 i 3 Karty Praw Podstawowych UE oraz art. 6 w zw. z art. 13 Europejskiej Konwencji Praw Człowieka. Wymóg natychmiastowego wykonania decyzji administracyjnej, która może mieć daleko idące skutki gospodarcze, naruszałby te fundamentalne prawa.aWprowadzenie możliwości natychmiastowego wykonania decyzji mogłoby również prowadzić do sytuacji, w której przedsiębiorstwa nie miałyby realnej szansy na obronę swoich interesów przed sądem. Nawet jeśli sąd ostatecznie uznałby, że decyzja administracyjna była niesłuszna, przedsiębiorstwa mogłyby już ponieść nieodwracalne straty, których nie da się naprawić. Taka sytuacja byłaby niezgodna z zasadą proporcjonalności, która wymaga, aby ograniczenia nakładane na podmioty gospodarcze były adekwatne i konieczne do osiągnięcia zamierzonych celów.eSkreślenie ust. 18 ma na celu zapewnienie, że decyzje administracyjne dotyczące uznania dostawcy za dostawcę wysokiego ryzyka będą podlegały procedurom odwoławczym i kontrolnym zgodnie z zasadami sprawiedliwości proceduralnej. Pozwoli to na bardziej zrównoważone podejście, które uwzględnia zarówno potrzeby bezpieczeństwa narodowego, jak i prawa przedsiębiorstw do sprawiedliwego procesu i ochrony swoich interesów gospodarczych.aPodsumowując, skreślenie ust. 18 jest konieczne, aby zapewnić zgodność z podstawowymi zasadami prawa i ochrony praw człowieka. Umożliwi to przedsiębiorstwom pełne korzystanie z prawa do obrony swoich interesów przed sądem oraz zabezpieczy je przed nieodwracalnymi skutkami natychmiastowych decyzji administracyjnych.	Uwaga wyjaśniona Z uwagi na to, że dostawca wysokiego ryzyka jest podmiotem, który bezpośrednio zagraża bezpieczeństwu państwa uznano, że należy niezwłocznie wykonać decyzję dotyczące tego dostawcy i dzięki temu zmitygować zagrożenia pochodzące od niego.
31.	Fundacja Rozwoju Obrotu Bezgotówkowego	Art. 67b	W stosunku do sektora finansowego zastosowanie będą miały postanowienia art. 67b i n. Projektu, dotyczące postępowania w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Zgodnie z nowym brzmieniem 67b ust. 1 postępowanie będzie także dotyczyć sprzętu i usług dostarczanego dla podmiotów z sektora bankowości i infrastruktura rynków finansowych, których zgodnie z Oceną Skutków Regulacji („OSR”) jest aż 547. Sposób i zakres nakładanych obowiązków budzi jednak wątpliwości.	Uwaga wyjaśniona Sektor bankowy również powinien podlegać obowiązkom w zakresie wycofania sprzętu lub oprogramowania pochodzącego od dostawcy wysokiego ryzyka.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

32.	Fundacja Rozwoju Obrotu Bezgotówkowego	Art. 67b	Zgodnie z art. 67b ust. 1, Projektu postępowanie w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka będzie dotyczyć sprzętu lub oprogramowania, które jest wykorzystywane przez podmioty kluczowe lub podmioty ważne. W obecnym brzmieniu wskazany przepis bardzo poszerza zakres stosowania ustawy o krajowym systemie cyberbezpieczeństwa. Dotyczy bowiem podmiotów kluczowych lub podmiotów ważnych, co oznacza, że odnosi się także do sektora bankowości i infrastruktury rynków finansowych. W sumie zakres regulacji obejmie ok. 38 000 podmiotów. Będzie to więc zdecydowanie więcej niż przewidywała to poprzednia wersja nowelizacji, a także więcej niż w innych krajach np. Niemczech czy Francji. Projekt nowelizacji wykracza zakresem podmiotowym i przedmiotowym poza zakres stosowania Toolbox 5G. Postanowienia art. 67b ust. 1 odwołują się do definicji produktów, usług i procesów ICT, czyli wszystkich elementów sieci lub systemów teleinformatycznych, podczas gdy 5G Toolbox dotyczy technologii telekomunikacyjnej 5G. Sektor finansowy jest sektorem silnie regulowanym, co naturalnie rozumiemy i wspieramy w takim zakresie, w jakim czyni to rynek bezpiecznym dla konsumentów oraz podmiotów gospodarczych. Jednak nadregulacja może przyczynić się do wprowadzenia dodatkowych barier oraz obciążeń finansowych dla jego uczestników.	Uwaga wyjaśniona Sektor bankowy również powinien podlegać obowiązkom w zakresie wycofania sprzętu lub oprogramowania pochodzącego od dostawcy wysokiego ryzyka.
33.	Hikvision	Art. 67b	W imieniu firmy Hikvision1, światowego lidera w dziedzinie rozwiązań w zakresie monitoringu, doceniamy możliwość udziału w procesie konsultacji proponowanego projektu nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa z dnia 23 kwietnia 2024. 1 https://www.hikvision.com/pl/ 2 https://www.hikvision.com/content/dam/hikvision/eu/support/cybersecurity/Guide-to-the-NIS2-Directive- Hikvision.pdf Jesteśmy obecni w Polsce od 2014 roku. Od tego czasu nawiązaliśmy wiele długotrwałych i udanych partnerstw w całym kraju, w ramach których wspieramy naszych klientów dostarczając produkty i rozwiązania, które mają pozytywny wpływ na społeczeństwo - pomagają chronić ludzi, mienie, aktywa i zwalczać przestępczość. Naszą wizją jest dostarczanie klientom bezpiecznej i zaufanej technologii. Stale aktualizujemy nasze własne praktyki w zakresie cyberbezpieczeństwa, uwzględniając wymagania wprowadzone przez dyrektywę NIS2, jak również zachęcamy do szerszej komunikacji między interesariuszami, koncentrując się na przeciwdziałaniu zagrożeniom i zwiększaniu zdolności do obrony sieci. Regularnie udzielamy również użytkownikom porad i najlepszych praktyk w zakresie ochrony sprzętu przed naruszeniami bezpieczeństwa. Ostatnio udostępniliśmy naszym partnerom Przewodnik po dyrektywie NIS2.2 Hikvision bardzo poważnie traktuje cyberbezpieczeństwo i przestrzega jednych z najbardziej rygorystycznych światowych standardów i certyfikatów, w tym ISO 27001, ISO 27701, CMMI Level 5 i CSA STAR. Hikvision jest również liderem w zabezpieczaniu danych klientów i jako jedna z pierwszych firm w branży usunęliśmy domyślne hasła oraz wymagamy od użytkowników tworzenia haseł przy pierwszym użyciu dowolnego produktu. Uwagi Hikvision do proponowanego projektu nowelizacji ustawy Cyberbezpieczeństwo jest problemem globalnym, który dotyczy każdego kraju i branży. Każde urządzenie podłączone do internetu, niezależnie od jego producenta czy pochodzenia, jest narażone na potencjalne zagrożenia. Bezpieczeństwo urządzenia zależy od tego, jak często aktualizowane jest jego oprogramowanie.	Uwaga nieuwzględniona Wszystkie podmioty kluczowe i podmioty ważne są obowiązane do zapewnienia bezpieczeństwa łańcuchów dostaw. Stąd też postępowanie ws. uznania za dostawcę wysokiego ryzyka powinno dotyczyć także ich.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			Przestarzałe oprogramowanie często ma znane luki w zabezpieczeniach, które mogą zostać wykorzystane przez hakerów. Nie jest to problem charakterystyczny jedynie dla jednego producenta, ale jest powszechnym wyzwaniem w branży technologicznej. Proponowany projekt ustawy wprowadza procedurę przewidzianą w art. 67a-67k, która pozwala Ministrowi właściwemu do spraw informatyzacji na wszczęcie postępowania w sprawie uznania dostawcy sprzętu lub oprogramowania wykorzystywanego przez podmioty kluczowe i ważne za dostawcę wysokiego ryzyka. W ramach tej procedury minister miałby obowiązek zasięgnąć opinii Kolegium do Spraw Cyberbezpieczeństwa, które przedstawiłaby swoją opinię w terminie 3 miesięcy od daty złożenia wniosku. Jednym z elementów opinii, o którym mowa w art. 67b ust. 11 pkt 2, jest analiza <i>"prawdopodobieństwa z jakim dostawca sprzętu lub oprogramowania znajduje się pod kontrolą państwa spoza terytorium Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego"</i>. Naszym zdaniem ocena i potencjalne wyznaczenie podmiotu jako dostawcy wysokiego ryzyka powinny opierać się wyłącznie na kryteriach technicznych, o których mowa w art. 64b ust. 11 pkt 4-6, a nie koncentrować się na kraju pochodzenia producenta. Proponujemy, aby prawodawstwo uwzględniało proponowane przez UE rozwiązania zawarte w akcie o cyberodporności³, w którym określono wymogi w zakresie cyberbezpieczeństwa dla "produktów z elementami cyfrowymi" wprowadzanych na rynek UE. 23 stycznia 2023 roku firma Hikvision przekazała swoje stanowisko na temat proponowanego aktu o cyberodporności.⁴ Aby zapewnić wysoki poziom cyberbezpieczeństwa produktów, proponowane rozporządzenie nakłada na producentów obowiązki m.in. projektowania, opracowywania i wytwarzania produktów gwarantujących odpowiedni poziom cyberbezpieczeństwa, przeprowadzania obowiązkowej oceny bezpieczeństwa oraz wdrażania procedur postępowania w przypadku wykrycia podatności. 3 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/... w sprawie horyzontalnych wymogów cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi oraz zmieniające rozporządzenia (UE) nr 168/2013 i (UE) 2019/1020 oraz dyrektywę (UE) 2020/1828 (akt o cyberodporności) 4 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13410-Cyber-resilience-act-new-cybersecurity-rules-for-digital-products-and-ancillary-services/F3376610_en Wierzimy, że producenci, którzy uzyskają odpowiednią certyfikację i/lub wywiążą się z obowiązków związanych z oznakowaniem CE, wykazują swoje zaangażowanie w najwyższe standardy cyberbezpieczeństwa. W związku z tym nie stanowią oni zagrożenia i nie powinni być uznawani za dostawców wysokiego ryzyka. Ponadto, o ile rozumiemy zasadność proponowanego wprowadzania ograniczeń i przeprowadzania ocen, o których mowa w art. 67b ust. 11 pkt 2, dostawców sprzętu wykorzystywanego w sieciach telekomunikacyjnych, zgodnie z unijnym zestawem środków dot. minimalnej harmonizacji i standaryzacji na poziomie UE rozwiązań cyberbezpieczeństwa sieci 5G, tzw. 5G Toolbox, lub w odniesieniu do produktów zamawianych lub wykorzystywanych w celu zapewnienia bezpieczeństwa narodowego lub obronności, rozszerzenie takich ocen na wszystkie produkty, usługi i procesy ICT, z których korzystają podmioty kluczowe i ważne, jest naszym zdaniem nieproporcjonalne.	

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			Uprzejmie prosimy o rozważenie powyżej przedstawionych uwag. Hikvision pozostaje zaangażowane we współpracę z interesariuszami w celu zapewnienia bezpiecznego i odpornego ekosystemu technologicznego w Polsce i pozostajemy do dyspozycji na wypadek jakichkolwiek pytań.	
34.	Huawei	Art. 67b	W nawiązaniu do prowadzonych konsultacji publicznych projektu nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa (dalej jako „Projekt KSC”), pragniemy w imieniu Huawei Polska sp. z o.o. (dalej: "Huawei" lub "Spółka") zgłosić następujące uwagi. Przede wszystkim chcielibyśmy podkreślić, że w pełni rozumiemy i popieramy cel, do którego zmierza transpozycja dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii („Dyrektywa NIS2”), jakim jest zwiększenie bezpieczeństwa kluczowych i ważnych sektorów. Priorytetem naszej firmy jest zapewnianie jak najwyższego bezpieczeństwa i odporności produkowanej i dostarczanej infrastruktury. Ważne jest jednak, aby środki służące temu celowi były przejrzyste, proporcjonalne i traktowały wszystkich zainteresowanych jednakowo. Z tej perspektywy nie można nie zauważyć, że niektóre z istotnych rozwiązań zaproponowanych w Projekcie KSC zawierają polityczne, nietransparentne postanowienia i mogą skutkować dyskryminacją podmiotową w oparciu o kryteria niezwiązane z cyberbezpieczeństwem. Powyższe jest nie tylko naszą opinią, ale też podzielaną przez innych przedsiębiorców z branży ICT, a także ekspertów w tej dziedzinie. W rezultacie proponowane ustawowe mechanizmy definiowania dostawcy wysokiego ryzyka mogą wykluczyć z polskiego rynku część dostawców ICT, nie zwiększając jednocześnie bezpieczeństwa kluczowych i ważnych sektorów, a w niektórych sytuacjach mogą nawet skutkować jego pogorszeniem. Taki ruch natomiast z całą pewnością wpłynie na konkurencyjność rynku oraz na wzrost cen. Projekt KSC, który z założenia ma na celu implementację unijnej Dyrektywy NIS2, poważnie odbiega od unijnych wymogów skoordynowanego bezpieczeństwa cybernetycznego. Polska jest jedynym krajem członkowskim UE, który uwzględnił klauzule wyłączające dostawców wysokiego ryzyka („DWR”) na podstawie politycznych i niemierzalnych kryteriów w projekcie wdrożenia Dyrektywy NIS2. Jest również jedynym państwem członkowskim UE, które stosuje wyłączenie DWR do 18 sektorów. Trudno zrozumieć cel, dla którego Polska wprowadza dodatkowe dyskryminujące standardy, które to podważają przewidywalność jednolitego rynku UE i Dyrektywy NIS2, jakim jest ustanowienie zharmonizowanych ram cyberbezpieczeństwa w UE. Jednocześnie Projekt KSC nakłada na przedsiębiorstwa wyższe obowiązki niż implementacja unijnej Dyrektywy NIS2 w porównaniu z innymi państwami UE, co osłabi konkurencyjność polskich przedsiębiorstw. Co więcej, w przypadku wdrożenia takiej wersji Projektu KSC, w ekstremalnym przypadku, Polska wykluczy potencjalnie rozwiązania, które z powodzeniem będą funkcjonowały w innych państwach UE. Huawei zdecydowanie nie zgadza się z proponowanym mechanizmem oceny dostawców ICT (w tym produktów/usług/procesów), opartym na przesłance państwa pochodzenia spoza UE i spoza NATO, jako potencjalnych dostawców wysokiego ryzyka na podstawie dyskryminujących, politycznych kryteriów i niemierzalnych czynników. W tym kontekście wszelkie potencjalne ograniczenia lub wykluczenie dostawców, bez dowodów i należytego procesu, mogłyby naruszać krajowe, unijne i międzynarodowe zasady prawa, takie jak równe traktowanie, niedyskryminacja, swobodny przepływ towarów i usług, zasada	Uwaga wyjaśniona Postępowanie w sprawie uznania za dostawcę wysokiego ryzyka ma na celu zabezpieczenie polskiej gospodarki i polskiego społeczeństwa przed dostawcą sprzętu lub oprogramowania, który stwarza poważne zagrożenie dla bezpieczeństwa państwa, obronności, bezpieczeństwa i porządku publicznego lub zdrowia i życia ludzi. W ramach postępowania administracyjnego będą brane pod uwagę zarówno aspekty techniczne związane z dostarczaniem przez dostawcę sprzętem i oprogramowaniem jak również aspekty nietechniczne związane z dostawcą. Dzięki temu zostanie zidentyfikowany pełen obraz zagrożeń jakie stwarza dostawca sprzętu lub oprogramowania. Postępowanie umożliwia badanie dostawcy sprzętu lub oprogramowania dla wszystkich sektorów gospodarki wskazanych w ustawie. Jest to wskazane z uwagi na to, że każdy podmiot kluczowy i podmiot ważny musi dbać o bezpieczeństwo łańcuchów dostaw. Podmioty kluczowe i podmioty ważne mają istotny charakter dla funkcjonowania współczesnej gospodarki i społeczeństwa informacyjnego. Zakłócenie funkcjonowania tych podmiotów poprzez atak przez łańcuch dostaw może spowodować niepowetowane straty. Z uwagi na charakter tego postępowania wyłączono część przepisów Kodeksu postępowania administracyjnego. Przede wszystkim nie jest możliwe

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

		proporcjonalności i pewności prawa określone w Traktacie o Funkcjonowaniu Unii Europejskiej, Europejskiej Konwencji Praw Człowieka Układzie ogólnym w sprawie taryf celnych i handlu (GATT), a także w dwustronnych umowach inwestycyjnych zawartych między Chinami a Polską. Ponadto, w naszym rozumieniu wszelkie ograniczenia polityczne na rynku ICT są nie do pogodzenia z potrzebą stymulowania inwestycji w infrastrukturę cyfrową, ponieważ nieuchronnie doprowadzą do ograniczenia konkurencji, a tym samym do wyższych cen, co negatywnie wpłynie na nakłady inwestycyjne w infrastrukturę. Zaufanie musi opierać się na faktach, fakty muszą być weryfikowalne, a weryfikacja musi opierać się na międzynarodowych, uznanych na całym świecie standardach. Wszelkie środki bezpieczeństwa cybernetycznego muszą być adekwatne i odnosić się do rzeczywistych, a nie abstrakcyjnych ryzyk. W kontekście proponowanych przepisów zwracamy uwagę, że na podstawie art. 21 ust. 1 Dyrektywy NIS2 wprowadzane przez państwa członkowskie środki zarządzania ryzykiem w cyberbezpieczeństwie powinny być odpowiednie i proporcjonalne. Oceniając proporcjonalność tych środków, uwzględnia się należy stopień narażenia danego podmiotu na ryzyko, jego wielkość i prawdopodobieństwo wystąpienia incydentów oraz ich dotkliwość, w tym ich skutki społeczne i gospodarcze. W naszej opinii te aspekty wynikające z Dyrektywy NIS2 zostały całkowicie pominięte w Projekcie KSC, o czym świadczy chociażby brak oszacowania kosztów w Ocenie Skutków Regulacji załączonej do Projektu KSC. Mając to na uwadze, zwracamy się o: • wycofanie z Projektu KSC dyskryminacyjnych postanowień odnoszących się do państwa pochodzenia doświadczeń produktów, oprogramowania i usług ICT; • w zakresie wdrażania środków dotyczących analizy bezpieczeństwa łańcuchów dostaw możliwie jak najwierniejsze wdrożenie rozwiązań wynikających z Dyrektywy NIS2, poprzedzonych należytą oceną ich proporcjonalności i stopnia narażenia danych podmiotów na ryzyko; • dokonanie pełnej analizy skutków oraz kosztów społecznych i gospodarczych w Ocenie Skutków Regulacji; • dokonanie notyfikacji Projektu do Komisji Europejskiej w ramach procedury TRIS, albowiem w naszym przekonaniu zawiera on przepisy o charakterze technicznym i jako taki powinien podlegać obowiązkowi notyfikacji. Wyrażamy nadzieję, że powyższe uwagi okażą się pomocne w procesie tworzenia dobrego rynku i środowiska dla inwestycji w obszarze cyberbezpieczeństwa. Będziemy wdzięczni za możliwość osobistego spotkania z Panem Ministrem, w trakcie którego chętnie podejmiemy dialog w wyżej przez nas przedstawionym zakresie. Tym samym jesteśmy otwarci na wszelkie rozmowy, konsultacje, a także wsparcie. Jako firma działająca w 170 państwach na świecie oraz dostarczająca sprzęt do ponad 1500 sieci telekomunikacyjnych mamy dostateczną wiedzę i zasoby, żeby wspierać Ministerstwo Cyfryzacji oraz inne zainteresowane tym agendy publiczne w poprawie poziomu cyberbezpieczeństwa w Polsce.	przeprowadzenie postępowania administracyjnego przy udziale wszystkich podmiotów, które wykorzystują sprzęt lub oprogramowanie pochodzące od danego dostawcy. Rygor natychmiastowej wykonalności jest konieczny z uwagi na to, że kwestia dotyczy poważnego zagrożenia dla bezpieczeństwa państwa. Nie przewiduje się rekompensat za wycofanie sprzętu lub oprogramowania, ponieważ ten sprzęt i tak z czasem podlegałby wymianie z uwagi na naturalne zużycie. Termin 7 lat na wycofanie sprzętu wydaje się terminem adekwatnym. Jednocześnie skrócono ten termin do 4 lat dla sprzętu i oprogramowania realizującego funkcje krytyczne w zakresie bezpieczeństwa sieci i usług. Wycofanie sprzętu pochodzącego od dostawcy wysokiego ryzyka w terminie 4 lat dla przedsiębiorców telekomunikacyjnych jest zasadne z uwagi na to, że chodzi o funkcje krytyczne dla sieci i usług. Zauważyć należy, że sprzęt i oprogramowanie i tak wymagałby okresowej wymiany z uwagi na naturalne zużycie sprzętu. Izby telekomunikacyjne będą mogły przedstawić swoje stanowisko Ministrowi Cyfryzacji W ramach opinii ale także i postępowania (co wynika z art. 7 KPA) należy wszechstronnie zbadać sprawę a więc także wziąć pod uwagę certyfikaty bezpieczeństwa, które posiada dostawca. W przypadku MŚP nie jest możliwe zastosowanie proporcjonalnych obowiązków. Jeśli np. duży telekom musi wycofać sprzęt, a jego podwykonawca,

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

				mały telekom świadczący usługi telekomunikacyjne w gminie, nie musiałby wycofać, to użytkownicy końcowi nie będą równomiernie zabezpieczeni przed wykorzystanie niebezpiecznego sprzętu pochodzącego od dostawcy wysokiego ryzyka.
35.	KIKE	Art. 67b	Dostawca wysokiego ryzyka (art. 67b projektowanego uKSC) Projekt wprowadza konstrukcję dostawcy sprzętu i oprogramowania ICT za dostawcę wysokiego ryzyka. Wiąże się to następnie z obowiązkami wszystkich przedsiębiorców telekomunikacyjnych (z wyjątkiem mikroprzedsiębiorców) zakazu nabywania określonych sprzętów i oprogramowani takiego dostawcy, a także usunięcia ze swoich systemów takich produktów. Jest to konstrukcja całkowicie nieznana dyrektywie NIS 2 i stanowi jaskrawe jej przekroczenie. Co więcej, bez względu na zakres prowadzonej działalności ma ona objąć małych i średnich przedsiębiorców, mimo iż KSC powinno zajmować się zagrożeniami poziomu krajowego, a nie lokalnego. mDodatkowo zwracamy uwagę na samą procedurę uznania dostawcy produktów za dostawcę wysokiego ryzyka, która jest nieprzejrzysta, pozbawiona faktycznej kontroli zarówno społecznej jak i sądowej. Przede wszystkim zwracam uwagę, że decyzja w sprawie uznania za dostawcę wysokiego ryzyka ma mieć rygor natychmiastowej wykonalności, co oznacza, że nawet złożenie od niej odwołania nie zwalnia całego niemal rynku telekomunikacyjnego od jej wykonania. Z kolei uchylenie czy zmiana tej decyzji w toku postępowań sądowych nie będzie miała już żadnego realnego wpływu, gdyż do tego czasu dostawcy telekomunikacyjni (pod groźbą kar finansowych lub zakazu działalności gospodarczej) usuną nieodwołalnie produkty tego dostawcy ze swoich systemów. Przywrócenie starych urządzeń po uchyleniu decyzji będzie już nieopłacalne ekonomicznie, stąd kontrola sądowa będzie iluzoryczna. ePrawdziwe obawy Izby wywołuje przede wszystkim procedura uznania dostawcy produktów ICT za dostawcę wysokiego ryzyka. Przedsiębiorcy telekomunikacyjni MŚP w ogóle nie będą mogli brać udziału w tym postępowaniu, nawet w formie wyrażania opinii, mimo że postępowanie to będzie skutkowało nałożeniem na nich ważnych i kosztownych obowiązków. Projekt nie przewiduje nawet udziału izb branżowych na prawach strony (jedynie możliwość wyrażenia stanowiska). óWątpliwości Izby wywołują przesłanki uznania za dostawcę wysokiego ryzyka, gdzie mają być brane pod uwagę m.in. rekomendacje Pełnomocnika z art. 33 uKSC (z definicji niewiążące). Same przesłanki z kolei nie dotyczą bezpośrednio produktów tego dostawcy, ale samego dostawcy: „<i>dostawca ten stanowi poważne zagrożenie dla obronności, bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego, lub życia i zdrowia ludzi.</i>” Przesłanki są więc bardzo ogólne i umożliwiają Ministrowi ds. informatyzacji niedopuszczalną uznaniowość, zwłaszcza w obliczu licznych włączeń z procedury przepisów kodeksu postępowania administracyjnego. Całość postępowania może więc doprowadzić do zakazu stosowania w Polsce produktów, które będą legalne na terenie reszty Unii Europejskiej. Uderzy to z kolei w konkurencyjność naszych przedsiębiorców zmuszając ich do zwiększenia kosztów działalności. Instytucja dostawcy wysokiego ryzyka jest najbardziej jaskrawym przykładem w Projekcie naruszania wspomnianych na początku stanowiska zasad z Prawa przedsiębiorców. Prawdziwe obawy Izby wywołuje przede wszystkim	Uwaga wyjaśniona Postępowanie w sprawie uznania za dostawcę wysokiego ryzyka ma na celu zabezpieczenie polskiej gospodarki i polskiego społeczeństwa przed dostawcą sprzętu lub oprogramowania, który stwarza poważne zagrożenie dla bezpieczeństwa państwa, obronności, bezpieczeństwa i porządku publicznego lub zdrowia i życia ludzi. W ramach postępowania administracyjnego będą brane pod uwagę zarówno aspekty techniczne związane z dostarczaniem przez dostawcę sprzętem i oprogramowaniem jak również aspekty nietechniczne związane z dostawcą. Dzięki temu zostanie zidentyfikowany pełen obraz zagrożeń jakie stwarza dostawca sprzętu lub oprogramowania. Postępowanie umożliwia badanie dostawcy sprzętu lub oprogramowania dla wszystkich sektorów gospodarki wskazanych w ustawie. Jest to wskazane z uwagi na to, że każdy podmiot kluczowy i podmiot ważny musi dbać o bezpieczeństwo łańcuchów dostaw. Podmioty kluczowe i podmioty ważne mają istotny charakter dla funkcjonowania współczesnej gospodarki i społeczeństwa informacyjnego. Zakłócenie funkcjonowania tych podmiotów poprzez atak przez łańcuch dostaw może spowodować niepowetowane straty.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

		procedura uznania dostawcy produktów ICT za dostawcę wysokiego ryzyka. Przedsiębiorcy telekomunikacyjni MŚP w ogółu Wątpliwości Izby wywołują przesłanki uznania za dostawcę wysokiego ryzyka, gdzie mają być brane pod uwagę m.in. rekomendacje Pełnomocnika z art. 33 uKSC (z definicji niewiążące). Same przesłanki z kolei nie dotyczą bezpośrednio produktów tego dostawcy, ale samego dostawcy: „dostawca ten stanowi poważne zagrożenie dla obronności, bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego, lub życia i zdrowia ludzi.” Przesłanki są więc bardzo ogólne i umożliwiają Ministrowi ds. informatyzacji niedopuszczalną uznaniowość, zwłaszcza w obliczu licznych włączeń z procedury przepisów kodeksu postępowania administracyjnego. Całość postępowania może więc doprowadzić do zakazu stosowania w Polsce produktów, które będą legalne na terenie reszty Unii Europejskiej. Uderzy to z kolei ogółem nie bierze pod uwagę zasady proporcjonalności i adekwatności nakazanej zarówno w art. 67 Prawa przedsiębiorców jak i dyrektywie NIS 2. Zasady te w ogółem nie występują w procedurze, co oznacza, że w ogółem nie będą brane pod uwagę. Prawdziwym problemem dla członków Izby jest jednak fakt, że procedura ta rażąco narusza art. 68 Prawa przedsiębiorców. Poza wąskim gronem mikroprzedsiębiorców (o zasięgu najczęściej osiedlowym, rzadziej jednej gminy), reszta MŚP będzie bezwzględnie zmuszona do przebudowy swoich sieci telekomunikacyjnych, bez względu na to czy ich działalność ma wymiar „krajowy” czy też działania te w ogółem są ekonomicznie wykonalne dla nich. W Projekcie zaniechano proporcjonalnego ograniczenia tego obowiązku wobec MŚP. Tymczasem wobec MŚP obowiązki wynikające z decyzji o uznaniu za dostawcę wysokiego ryzyka powinny zostać proporcjonalnie ograniczone zarówno co do samych zakazów używania sprzętów i oprogramowania jak też czasu na ich usunięcie z systemów. oW przypadku nieprzychylenia się do postulatu Izby usunięcia całej konstrukcji prawnej dostawcy wysokiego ryzyka, Izba postuluje o: - uprawnienie Izb telekomunikacyjnych do udziału w postępowaniu na prawach strony; - uszczegółowienia przesłanek uznania za dostawcę wysokiego ryzyka w kontekście jego produktów; - wprowadzenia obowiązku określenia w decyzji proporcjonalnego zmniejszenia obowiązków wobec MŚP przedsiębiorców telekomunikacyjnych; - usunięcia rygoru natychmiastowej wykonalności decyzji o dostawcy wysokiego ryzyka; - wskazania dodatkowych przesłanek związanych z uznaniem za dostawcę wysokiego ryzyka wobec dostawcy produktów posiadających certyfikaty wydane lub uznane na terenie większości krajów UE/ członkowskich NATO.	Z uwagi na charakter tego postępowania wyłączono część przepisów Kodeksu postępowania administracyjnego. Przede wszystkim nie jest możliwe przeprowadzenie postępowania administracyjnego przy udziale wszystkich podmiotów, które wykorzystują sprzęt lub oprogramowanie pochodzące od danego dostawcy. Rygor natychmiastowej wykonalności jest konieczny z uwagi na to, że kwestia dotyczy poważnego zagrożenia dla bezpieczeństwa państwa. Nie przewiduje się rekompensat za wycofanie sprzętu lub oprogramowania, ponieważ ten sprzęt i tak z czasem podlegałby wymianie z uwagi na naturalne zużycie. Termin 7 lat na wycofanie sprzętu wydaje się terminem adekwatnym. Jednocześnie skrócono ten termin do 4 lat dla sprzętu i oprogramowania realizującego funkcje krytyczne w zakresie bezpieczeństwa sieci i usług. Wycofanie sprzętu pochodzącego od dostawcy wysokiego ryzyka w terminie 4 lat dla przedsiębiorców telekomunikacyjnych jest zasadne z uwagi na to, że chodzi o funkcje krytyczne dla sieci i usług. Zauważyć należy, że sprzęt i oprogramowanie i tak wymagałby okresowej wymiany z uwagi na naturalne zużycie sprzętu. Izby telekomunikacyjne będą mogły przedstawić swoje stanowisko Ministrowi Cyfryzacji. W ramach opinii ale także i postępowania (co wynika z art. 7 KPA) należy wszechstronnie zbadać sprawę a więc także wziąć pod uwagę certyfikaty bezpieczeństwa, które posiada dostawca.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

				W przypadku MSP nie jest możliwe zastosowanie proporcjonalnych obowiązków. Jeśli np. duży telekom musi wycofać sprzęt, a jego podwykonawca, mały telekom świadczący usługi telekomunikacyjne w gminie, nie musi wycofać, to użytkownicy końcowi nie są równomiernie zabezpieczeni przed wykorzystanie niebezpiecznego sprzętu pochodzącego od dostawcy wysokiego ryzyka.
36.	KIGEIT	Art. 67b – art. 67f	Dostawca wysokiego ryzyka [DWR] (procedura wskazana w art. 67b-67f Projektu KSC). Wprowadzenie nadregulacji poprzez zaadresowanie względem wszystkich podmiotów kluczowych i ważnych. Izba wskazała, że zastosowanie przewidzianej w art. 67b-67f Projektu KSC Procedury DWR w sposób nieuzasadniony zostało rozszerzone z sieci 5G (zgodnie z założeniami 5G Toolbox), a więc części sektora telekomunikacyjnego obejmującej de facto kilku operatorów mobilnych, na wszystkie podmioty kluczowe oraz ważne (zgodnie z OSR co najmniej 38 tys. podmiotów). Tak duże powiększenie zakresu podmiotowego przepisów dotyczących dostawców wysokiego ryzyka, które wpływają na swobodę prowadzenia działalności gospodarczej (art. 22 Konstytucji RP), nie znajduje uzasadnienia ani w Dyrektywie NIS2, ani w cytowanym w uzasadnieniu oraz OSR dokumencie 5G Toolbox. Projekt KSC w zakresie Procedury DWR stanowi przykład wprowadzania przez państwo członkowskie nieuzasadnionych restrykcji w ramach dokonywania implementacji regulacji unijnych (gold-platingu), biorąc pod uwagę brak szczegółowych analiz i wpływu regulacji na poszczególne sektory negatywne skutki takiego działania mogą być daleko idące, ponieważ w wyniku wydania decyzji i konieczności wycofania i zakazu zakupu produktów, usług ICT od danego dostawcy, nie tylko nastąpić może wzrost kosztów po stronie przedsiębiorców, ale w najgorszym przypadku może dojść wręcz do czasowego ograniczenia albo zakończenia prowadzenia działalności przez przedsiębiorcę, który zmuszony będzie do dostosowania się do wydanej decyzji zgodnie z art. 67c. IDodatkowo w zakresie wprowadzanego Projektem KSC przeregulowania w zakresie wykorzystania Procedury DWR, Izba zwraca uwagę, że zgodnie z informacjami wskazanymi w OSR i uzasadnieniu - projektowane przepisy nie są oparte na faktycznych analizach ich możliwego oddziaływania na przedsiębiorców uznawanych za podmioty kluczowe i ważne ze wszystkich sektorów i podsektorów. Projekt KSC obejmuje 17 zróżnicowanych sektorów, dlatego konieczna jest co najmniej ocena wpływu i możliwych konsekwencji wydania w Procedurze DWR decyzji obejmującej którykolwiek z nich. Istotne jest w szczególności odpowiednie ocenienie czasu amortyzacji produktów, usług i procesów ICT wykorzystywanych w poszczególnych podsektorach i sektorach, ponieważ Izba stoi na stanowisku, że wbrew wskazaniom w uzasadnieniu i OSR, przewidziany czas na wycofanie wykorzystywanych produktów, usług i procesów ICT nie bierze pod uwagę szczegółowych analiz czasu amortyzacji jaki następuje w przypadku poszczególnych sektorów. aWymiana produktów, usług i procesów ICT, która ma	Uwaga wyjaśniona Postępowanie umożliwia badanie dostawcy sprzętu lub oprogramowania dla wszystkich sektorów gospodarki wskazanych w ustawie. Jest to wskazane z uwagi na to, że każdy podmiot kluczowy i podmiot ważny musi dbać o bezpieczeństwo łańcuchów dostaw. Podmioty kluczowe i podmioty ważne mają istotny charakter dla funkcjonowania współczesnej gospodarki i społeczeństwa informacyjnego. Zakłócenie funkcjonowania tych podmiotów poprzez atak przez łańcuch dostaw może spowodować niepowetowane straty.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			przebiegać w czasie standardowego, niezakłóconego świadczenia usług przez przedsiębiorców identyfikowanych jako podmioty kluczowe i ważne, to proces długotrwały, wymagający organizacyjnie i kosztowny dla podmiotów zobowiązanych do uwzględnienia skutków decyzji i rezygnacji z określonego sprzętu. W przypadku wydania decyzji przez ministra właściwego do spraw informatyzacji, konsekwencje dla podmiotów zobowiązanych do dostosowania swojej działalności sprowadzać się będą do analiz z zakresu architektury sieci/infrastruktury, zmian polityki zakupowej i trwających procesów zakupowych, analizy i wyboru nowego dostawcy, wdrożenia zmian. Zwracamy uwagę, że przy tak szerokim katalogu podmiotów, do których zastosowanie ma mieć decyzja wydana w Procedurze DWR, konieczne jest uwzględnienie, że podmioty te to przedsiębiorcy, dysponujący różnymi możliwościami finansowymi i kompetencjami umożliwiającymi sprawne przeprowadzenie procesów - z tego względu w przypadku utrzymania obecnego szerokiego zakresu Procedury DWR, Projekt KSC powinien zakładać okres wycofania rozwiązań w odniesieniu do amortyzacji oraz okresu użytkowania danego sprzętu.	
37.	KIGEIT	Art. 67b	Ograniczenie możliwości udziału w Procedurze DWR (możliwość przystąpienia na prawach strony) tylko do największych przedsiębiorców telekomunikacyjnych, pomimo że wydawana decyzja może oddziaływać również na inne podmioty kluczowe i ważne. Jak wskazane zostało powyżej w punkcie III podpunkt 1, wprowadzane w art. 67b-67d postępowanie w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka i konsekwencje wydania decyzji Ministra Cyfryzacji, oddziaływać mają na: 1) podmioty kluczowe lub podmioty ważne, z wyłączeniem podsektora komunikacji elektronicznej, 2) przedsiębiorców telekomunikacyjnych, których roczne przychody z tytułu wykonywania działalności telekomunikacyjnej w poprzednim roku obrotowym były wyższe niż 10 milionów złotych, a zgodnie z art. 67b ust. 2 możliwość udziału tych podmiotów w postępowaniu na prawach strony (art. 28 KPA) jest wyłączana. Jednak w projektowanym art. 67b ust. 4 Projektodawca wprowadza wyjątek od wyłączenia i dopuszcza udział w postępowaniu na prawach strony jedynie wybranych przedsiębiorców komunikacji elektronicznej (którzy w poprzednim roku obrotowym uzyskali przychód z tytułu prowadzenia działalności telekomunikacyjnej w wysokości co najmniej dwudziestotysięcznej krotności przeciętnego wynagrodzenia w gospodarce narodowej, a więc ok. 143 mln zł). oZgodnie z uzasadnieniem do Projektu KSC „Zmiana odpowiada na postulaty strony społecznej, jednocześnie zapewniając sprawny przebieg postępowania.”, jednak zdaniem Izby takie wyróżnienie tylko części jednego z podsektorów objętych przepisami Projektu KSC jest niezrozumiałe i niedopuszczalne. W przypadku utrzymania w Projekcie KSC objęcia Procedurą DWR podmiotów kluczowych i ważnych (główną uwagą Izby, wskazaną w punkcie III podpunkt 1, jest konieczność ograniczenia Procedury DWR tylko do sektora telekomunikacyjnego), wszystkie podmioty do których może mieć zastosowanie wydana w Procedurze DWR decyzja ingerująca w prowadzoną działalność gospodarczą, powinny mieć możliwość uczestnictwa w postępowaniu. h	Uwaga wyjaśniona Postępowanie umożliwia badanie dostawcy sprzętu lub oprogramowania dla wszystkich sektorów gospodarki wskazanych w ustawie. Jest to wskazane z uwagi na to, że każdy podmiot kluczowy i podmiot ważny musi dbać o bezpieczeństwo łańcuchów dostaw. Podmioty kluczowe i podmioty ważne mają istotny charakter dla funkcjonowania współczesnej gospodarki i społeczeństwa informacyjnego. Zakłócenie funkcjonowania tych podmiotów poprzez atak przez łańcuch dostaw może spowodować niepowetowane straty. Z uwagi na charakter tego postępowania wyłączono część przepisów Kodeksu postępowania administracyjnego. Przede wszystkim nie jest możliwe przeprowadzenie postępowania administracyjnego przy udziale wszystkich podmiotów, które wykorzystują sprzęt lub oprogramowanie pochodzące od danego dostawcy.
38.	KIGEIT	Art. 67b ust. 11	W ramach oceny dokonywanej w procedurze DWR poza oceną faktyczną danego produktu, usługi, procesu ICT w zakresie podatności występują odwołania do oceny na podstawie kryteriów	Uwaga nieuwzględniona

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

		politycznych, niemierzalnych (np. przepisów prawa dot. kraju pochodzenia danego dostawcy), w przypadku wydawania decyzji opartej na ocenie politycznej - zakaz i wycofanie dot. produktu, usługi, procesu ICT może doprowadzić do zaburzenia konkurencyjności na rynkach obejmujących podmioty kluczowe i ważne, w tym – powstania duopoli czy monopoli. Zgodnie z projektowanym art. 67b ust. 11 opinia przygotowywana w ramach procedury oceny dostawcy wysokiego ryzyka bazuje na elementach niejasnych i ocennych, które nie zawierają rzeczywistych elementów analizy technicznej działalności prowadzonej przez dostawcę sprzętu lub oprogramowania w zakresie produktów, usług, procesów ICT. Z uwagi na brak precyzji sformułowań, zakres swobody pozostawiony Kolegium do Spraw Cyberbezpieczeństwa - w przypadku przygotowywania opinii dla Ministra Cyfryzacji w ramach wszczętego postępowania, nie daje też wystarczających gwarancji ograniczenia ryzyka dyskryminacji, co będzie wpływało negatywnie na poziom zaufania adresatów regulacji do organów państwa i może powodować konsekwencje dla Skarbu Państwa w postaci postępowań odnoszących się do obowiązujących Polskę międzynarodowych umów handlowych. mW ramach przygotowanego Projektu KSC, Projektodawca odwołuje się do dokumentu 5G Toolbox, ale wbrew komunikacji Komisji Europejskiej, odnoszące się do wdrażania rozwiązań tzw. 5G Toolbox jednoznacznie przewidują, że ocena ryzyka dostawców powinna być niedyskryminująca, a „ocena profili ryzyka dostawców była prowadzona wyłącznie ze względów bezpieczeństwa i na podstawie obiektywnych kryteriów”¹⁾. Przykładowo, zarówno czeskie, jak i niemieckie regulacje nie przewidują dokonywania oceny politycznej dostawcy, skupiając się na kwestiach technicznych. Dodatkowo, w wyroku TSUE C 390/99 z dnia 22 stycznia 2002 r. w sprawie Canal Satélite Digital²⁾, wskazuje się, że w ramach wprowadzania towarów do obrotu (a de facto do tego też odnosić się będzie wydawana w ramach postępowania decyzja) konieczne jest uwzględnienie „obiektywnych, niedyskryminacyjnych kryteriów, które są znane z góry, w taki sposób, aby ograniczyć wykonywanie uprawnień dyskrecyjnych przez organy krajowe, tak aby nie były one stosowane arbitralnie”. Wprowadzenie możliwości oparcia opinii w Procedurze DWR na przesłankach politycznych budzi wątpliwości Izby w zakresie międzynarodowych umów handlowych oraz konkurencji na rynku dostawców sprzętu lub oprogramowania w poszczególnych sektorach i podsektorach, które ma obejmować decyzja wydana w Procedurze DWR. Zakaz i wycofanie dot. produktu, usługi, procesu ICT może doprowadzić do zaburzenia konkurencyjności na rynkach obejmujących podmioty kluczowe i ważne, w tym, doprowadzić do powstania duopoli czy monopoli, biorąc pod uwagę to, że podmioty kluczowe i ważne działają w zakresie usług specjalistycznych, z niewielką ilością dostawców. Kryteria oceny przeprowadzanej zgodnie z art. 67b ust. 11 w ramach opinii Kolegium do Spraw Cyberbezpieczeństwa powinny umożliwiać ocenę nie pod względem politycznym, ale technicznym, czyli weryfikację za pomocą mierzalnych kryteriów bezpieczeństwa ocenianych produktów, usług czy procesów ICT i zapewnić zgodność wprowadzanych	Trudno mówić o prawidłowo rozwijającej się gospodarce gdy jednocześnie w obrocie gospodarczym uczestniczyłby dostawca niebezpiecznego sprzętu lub oprogramowania, który stwarza poważne zagrożenie dla bezpieczeństwa państwa. Zaproponowane rozwiązanie nie odwołuje się do kryteriów politycznych.

¹⁾ <https://digital-strategy.ec.europa.eu/en/library/secure-5g-deployment-eu-implementing-eu-toolbox-communication-commission>

²⁾ <https://curia.europa.eu/juris/liste.jsf?language=en&num=C-390/99>

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			rozwiązań z międzynarodowymi umowami handlowymi, z tego też względu z katalogu powinny zostać usunięte kryteria nieobiektywne, polityczne na rzecz weryfikacji i oceny produktów, usług czy procesów ICT z perspektywy m.in. zapewniania przez ich dostawcę weryfikacji integralności nabytych produktów/usług.	
39.	KIGEIT	Art. 67b	Brak ograniczenia czasowego dla decyzji wydanej w Procedurze DWR oraz brak możliwości poprawy w zakresie oferowanych produktów, usług i procesów ICT - konieczność wprowadzenia możliwości rewizji oceny dostawcy sprzętu lub oprogramowania oraz jego produktów i usług ICT. W związku wydaną w Procedurze DWR decyzją, która ma daleko idące konsekwencje dla dostawcy oprogramowania i sprzętu, mogące prowadzić nawet do wyłączenia możliwości prowadzenia działalności danego rodzaju, regulacje odnoszące się do Procedury DWR i wykluczenia dostawcy powinny przewidywać możliwość dokonania tzw. rewizji decyzji. Projekt KSC powinien przewidywać by dostawca względem którego produktów, usług ICT wydana została decyzja w Procedurze DWR, miał możliwość zawnioskowania do ministra właściwego o spraw informatyzacji o dokonanie ponownej oceny. Procesy technologiczne nieustannie się zmieniają, z tego względu decyzja w zakresie danego dostawcy i jego produktów ICT nie powinna być wydawana bezterminowo, bez możliwości jej usunięcia. W czasie obowiązywania decyzji dany dostawca może mieć możliwość ulepszenia, dostosowania danego produktu do wymogów bezpieczeństwa, z tego względu proponowane przepisy powinny zakładać możliwość zawnioskowania, np. nie wcześniej niż po roku od wydania decyzji, o ponowne dokonanie oceny przez Kolegium do Spraw Cyberbezpieczeństwa. Wprowadzenie tego rodzaju zmiany pozwoliłoby na uwzględnienie dynamicznych zmian w zakresie zagrożeń związanych z cyberbezpieczeństwem i szybkiego rozwoju technologicznego umożliwiającego radzenie sobie z nimi.i	Uwaga wyjaśniona Zdaniem projektodawcy z ogólnych przepisów KPA wynika, że minister może uchylić decyzję ostateczną. Stąd nie ma potrzeby wprowadzenia ograniczeń czasowych dla decyzji. To samo narzędzie można zastosować także do sytuacji, gdy dostawca wysokiego ryzyka przestanie stwarzać poważne zagrożenie dla bezpieczeństwa państwa.
40.	KIGEIT	Art. 67b	Ograniczenie uprawnień strony dostępnych w procedurze administracyjnej oraz natychmiastowe wykonanie decyzji wydawanej w Procedurze DWR i brak możliwości wnioskowania o ponowne rozpatrzenie sprawy. W ramach Procedury DWR, co do zasady zastosowanie mają mieć przepisy Kodeksu postępowania administracyjnego (dalej: „KPA”)³, jednak Projekt KSC w art. 67b ust. 2 i ust. 10 przewiduje ograniczenie istotnych z perspektywy kontroli postępowania uprawnień podmiotów kluczowych albo ważnych oraz dostawcy sprzętu i oprogramowania: a) ograniczenie udziału jako strony postępowania podmiotów innych niż podmiot, wobec którego zostanie wszczęte postępowanie, nawet jeśli postępowanie dot. bezpośredniego interesu innego podmiotu (art. 28 KPA); b) uniemożliwienie udziału zainteresowanych organizacji społecznych w postępowaniu (art. 31 KPA);	Uwaga wyjaśniona Ograniczenie udziału stron ma na celu zapewnienie sprawności przeprowadzenia postępowania administracyjnego. Jednocześnie zapewniono izbom gospodarczym możliwość wypowiedzenia się co do dostawcy wobec którego wszczęto postępowanie. Wyłączenie metryki sprawy ma na celu zapewnienie bezpieczeństwa dla urzędników wykonujących czynności w sprawie.

³⁾ Ustawa z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (Dz. U. z 2024 r. poz. 572).

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

		c) wyłączenie prowadzenie metryki sprawy wskazującej wszystkie osoby, które uczestniczyły w podejmowaniu czynności w postępowaniu administracyjnym oraz określającej wszystkie podejmowane przez te osoby czynności wraz z odpowiednim odesłaniem do dokumentów określających te czynności (art. 66a); d) wyłączenie zawiadomienia strony o miejscu i terminie przeprowadzenia dowodu ze świadków, biegłych lub oględzin przynajmniej na siedem dni przed terminem (art. 79 KPA); e) wyłączenie, w przypadku wydawania decyzji wraz z zajęciem stanowiska przez inny organ, obowiązku zajęcia tego stanowiska w drodze postanowienia, na które służy stronie zażalenie. (art. 106 § 5 KPA). Taki katalog wyłączeń uprawnień co do zasady dostępnych w procedurze administracyjnej jest nieuzasadnionym ograniczeniem praw podmiotów, względem których wydawana decyzja kształtować będzie prawa i obowiązki. Szczególnie uwagę Izby zwraca propozycja usunięcia obowiązku stosowania metryki sprawy, która do KPA zgodnie z uzasadnieniem wprowadzona została jako obowiązkowa część akt administracyjnych jako rozwiązanie zapewniające „zwiększenie transparentności udziału poszczególnych urzędników w procesie wydania rozstrzygnięć w sprawach obywateli [...] oraz transparentności uzasadnienia podjęcia takiego a nie innego rozstrzygnięcia w sprawie”. Natomiast wyłączenie art. 106 § 5 KPA spowodować by mogło, że w przypadku wydania opinii Kolegium do Spraw Cyberbezpieczeństwa nie będzie stosowana forma postanowienia, a więc opinia będzie mogła zostać wydana nawet w formie ustnej - wyłączenie stosowania art. 106 § 5 k.p.a. oznacza brak określenia formy prawnej wydawanej opinii, a w konsekwencji brak możliwości jasnego określenia jej statusu. Co więcej, zgodnie z tym przepisem zajęcie stanowiska przez organ następuje w drodze postanowienia, na które służy stronie zażalenie, stąd efektem wyłączenia art. 106 § 5 KPA będzie także brak możliwości wniesienia zażalenia na opinię. W przypadku opinii, która w procesie oceny dostawcy jest elementem kluczowym, nie można dopuścić do zastosowania wyłączeń, które będą powodowały wątpliwości i ograniczenie praw strony co do skutków wydania opinii czy też np. braku jej wydania w terminie. Ponadto w art. 67b ust. 19 Projekt KSC zakłada poważne ograniczenie prawa strony postępowania poprzez odebranie możliwości złożenia wniosku o ponowne rozpatrzenie sprawy przez ten sam organ, które to rozwiązanie w polskim systemie prawnym ma na celu zapewnienie dodatkowej formy kontroli prawidłowości decyzji, co jest szczególnie istotne w przypadku Postępowania DWR, w wyniku którego dochodzi do ograniczenia konstytucyjnej swobody prowadzenia działalności gospodarczej. W art. 67b ust. 18 Projekt KSC zakłada natychmiastowe wykonanie decyzji uznającej dostawcę sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, przy czym zgodnie z przepisami KPA - rygor natychmiastowej wykonalności może zostać nadany decyzji w przypadku, gdy jest to niezbędne ze względu na ochronę zdrowia lub życia ludzkiego albo dla zabezpieczenia gospodarstwa narodowego przed ciężkimi stratami bądź też ze względu na inny interes społeczny lub wyjątkowo ważny interes strony, jednak w każdym wypadku to na organie wydającym decyzję leży obowiązek wskazania przesłanek uzasadniających zastosowanie tego mechanizmu. yWskazane powyżej wykluczenie w ramach Procedury DWR, powodującej daleko idące konsekwencje dla przedsiębiorców (zarówno organizacyjne, jak i	Wyłączono przepis art. 106 § 5 KPA z uwagi na to, że Kolegium do Spraw Cyberbezpieczeństwa nie ma charakteru organu administracji publicznej i nie może wydawać postanowień.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			finansowe), elementów procedury administracyjnej kreujących uprawnienia stron, jak i tych, które mają na celu zapewnienie transparentności prowadzonego postępowania jest niedopuszczalne, z tego względu Izba postuluje o usunięcie wskazanych wyłączeń stosowania KPA. Brak jest określenia momentu początkowego biegu terminu z art. 67c, rozsądnym byłoby liczenie tego terminu od dnia uprawomocnienia się decyzji wydanej w Procedurze DWR, po rozpatrzeniu odwołań. Nie wiadomo czy rygor dotyczy uznania z HRV czy obowiązku wymiany z Projektu KSC. Projektując tak daleko idące konsekwencje organizacyjne i finansowe powinno się wskazać początek biegu 4 letniego terminu (7letniego też) z uwzględnieniem w takim wskazaniu możliwość prawnego kwestionowania decyzji.	
41.	OPOR	Art. 67b	Odnosząc się natomiast również do samej instytucji dostawcy wysokiego ryzyka, postulujemy, żeby decyzję administracyjną w tym zakresie oprzeć na przesłankach technicznych, odnoszących się w szczególności do certyfikacji⁴, co pozwoli zarówno podmiotom kluczowym i ważnym jak również dostawcom spoza UE i NATO na skupienie się w swej działalności gospodarczej na zapewnieniu zgodności oferowanych produktów z wymogami cyberbezpieczeństwa (a przecież zakładamy, że o to chodzi w Projekcie). „Postawienie” w Projekcie na przesłanki nietechniczne spowoduje niepewność funkcjonowania wielu podmiotów na rynku w Polsce i zahamuje wiele procesów inwestycyjnych w nowe technologie, bowiem przedsiębiorcy będą obawiać się, że ich decyzje biznesowe będą wiązać się z niekontrolowanym i niezarządzalnym ryzykiem, gdyż nawet gdy zapewnią najwyższe standardy techniczne i zadbają o należytą certyfikację to i tak nie będą mogli mieć pewności czy dany dostawca ze względów nietechnicznych zostanie uznany za HRV, co spowoduje obowiązek wycofania sprzętu, oprogramowania, procesów ICT takiego dostawcy. Mając to na względzie wymaga podnieść w stosunku do Projektu również ogólny postulat usunięcia z Projektu wszelkich nieproporcjonalnych i nietechnicznych kryteriów.	Uwaga wyjaśniona Projekt zawiera zarówno przesłanki techniczne jak i nietechniczne uznania za dostawcę wysokiego ryzyka. Pozostawienie wyłącznie przesłanek nietechnicznych byłoby niezgodne z wdrażanym tą instytucją Toolboxem 5G, który wprost wskazuje, że państwa członkowskie UE muszą brać pod uwagę również przesłanki o naturze strategicznej.
42.	Konfederacja Lewiatan	Art. 67b-67f	Niezgodność procedury uznania dostawcy za dostawcę wysokiego ryzyka („Procedura DWR”) z Dyrektywą NIS2 Jednostka redakcyjna: art. 67b – 67f projektu KSC Jednostka redakcyjna NIS2: 20 ust.1; art. 21 ust 1 w zw. z ust.2 w zw. z ust. 3 Uwaga: Sama Procedura DWR nie została przewidziana w dyrektywie NIS2. <u>W szczególności, nie zakłada się, by ryzyko związane z danym dostawcą było badane ogólnie przez organy wyłącznie ze względu na okoliczności dotyczące samego dostawcy, bez związku z cechami konkretnego podmiotu kluczowego lub ważnego (podmiotu krajowego systemu cyberbezpieczeństwa).</u> Dodatkowo, w art. 22 ust. 3 Dyrektywy NIS2 wspomina się jedynie o krytycznych usługach ICT, systemach ICT lub produktach ICT. Tymczasem decyzja o uznaniu dostawcy za dostawcę wysokiego ryzyka w odniesieniu do podmiotów krajowego systemu cyberbezpieczeństwa może dotyczyć niemal dowolnego sprzętu lub oprogramowania. W odniesieniu do przedsiębiorców telekomunikacyjnych może objąć sprzęt i oprogramowanie określone „w wykazie kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług” w załączniku nr 3 do ustawy. Wykaz ten obejmuje jednak m.in. „5G Radio Base Station Baseband Unit oraz inne funkcje”, które zgodnie	Uwaga wyjaśniona Postępowanie umożliwia badanie dostawcy sprzętu lub oprogramowania dla wszystkich sektorów gospodarki wskazanych w ustawie. Jest to wskazane z uwagi na to, że każdy podmiot kluczowy i podmiot ważny musi dbać o bezpieczeństwo łańcuchów dostaw. Podmioty kluczowe i podmioty ważne mają istotny charakter dla funkcjonowania współczesnej gospodarki i społeczeństwa informacyjnego. Zakłócenie funkcjonowania tych podmiotów poprzez atak przez łańcuch dostaw może spowodować niepowetowane straty.

⁴ wzorem projektu ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa <https://legislacja.rcl.gov.pl/projekt/12385350>).

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

		z 5G Toolbox nie są funkcjami krytycznymi („critical”). Co prawda, dyrektywa NIS2 uprawnia państwa członkowskie do przyjęcia lub utrzymania przepisów zapewniających wyższy poziom cyberbezpieczeństwa, ale tylko pod warunkiem, że takie przepisy będą spójne z obowiązками państw członkowskich ustanowionymi w prawie Unii. Poniżej przedstawiono podstawowe zastrzeżenia do proponowanej Procedury DWR, która nie tylko jest w zasadzie powtórzeniem poprzednio forsowanego rozwiązania, ale również rozszerza zakres jej oddziaływania z sektora telekomunikacyjnego na 18 sektorów objętych NIS2: Dyskryminacyjne kryteria Procedury DWR - przesłanki oceny dostawcy usług, produktów i procesów ICT za dostawcę wysokiego ryzyka mają charakter wysoce ocenny, a kluczowe znaczenie przypisane zostało kryteriom politycznym i organizacyjnym (bliżej niezdefiniowane związki dostawcy z państwem trzecim, praktyka stosowania prawa w państwie trzecim itd.). Z kolei kryteria techniczne oceny zostały uwzględnione jedynie w ograniczonym zakresie. Projekt w obecnym kształcie może zostać uznany za dyskryminujący, co może być uznane za naruszające TFUE (zasada niedyskryminacji – art. 18 TFUE, zasady swobodnego przepływu towarów i usług – art. 34 i 35 TFUE, zakaz nadużywania pozycji dominującej art. 102 TFUE), Karty Praw podstawowych (art. 20 i 21 ust. 2 Karty praw podstawowych), a także innych zobowiązań międzynarodowych Rzeczypospolitej Polskiej. Ograniczenie prawa stron w Procedurze DWR oraz zasady jawności - projekt wprowadza Procedurę DWR, zgodnie z którą podmioty wykorzystujące sprzęt lub oprogramowanie lub procesy takiego dostawcy, muszą wymienić sprzęt lub oprogramowanie w ciągu 7 lat lub w przypadku przedsiębiorców telekomunikacyjnych 4 lat, a także natychmiast zaprzestać wykorzystania nowych urządzeń lub oprogramowania. Jednocześnie projekt ustawy ogranicza w sposób bezprecedensowy możliwość udziału na prawach strony podmiotów objętych skutkami decyzji o uznaniu dostawcy za dostawcę wysokiego ryzyka („Decyzja DWR”), art. 28 k.p.a.), wyklucza możliwość dopuszczenia do udziału w postępowaniu zainteresowanych organizacji społecznych (art. 31 k.p.a.), czy wreszcie ogranicza uprawnienia strony w zakresie przeprowadzenia czynności dowodowych (art. 79 k.p.a.). Projektodawca zachował rozwiązaniu zgodnie z którym tylko przedsiębiorcy telekomunikacyjni z przychodami rocznymi wynoszącymi co najmniej ok. 160 mln zł mogą wziąć udział w postępowaniu. Ograniczenie prawa do udziału w postępowaniu dla przedsiębiorców, pomimo że będą objęci skutkami Decyzji DWR, może stanowić podstawę do stwierdzenia niezgodności przepisów z art. 45 Konstytucji RP oraz art. 47 Karty praw podstawowych Unii Europejskiej. Brak jawności postępowania - dostawcy objęci Procedurą DWR, nie otrzymują treści całego wyroku w sprawie odwołania od Decyzji DWR, co więcej także elementy uzasadnienia Decyzji DWR mogą być niejawnie (nawet jeśli byłyby reprezentowane przez osoby, posiadające dostęp do informacji objętych klauzulami tajności). Kwestię tę podniosła także Rada Legislacyjna w opinii do poprzedniego przedłożenia projektu z dnia 23 lutego 2021 r., która zwróciła uwagę na brak dostatecznej precyzji w przepisach o doręczaniu odpisów wyroków sądu administracyjnego w sprawach skarg na decyzję o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Rada Legislacyjna podnosiła także wątpliwość o charakterze konstytucyjnym, a mianowicie, czy w ogóle jest zgodne z Konstytucją RP odstępowanie od doręczania stronie pełnego uzasadnienia wyroku sądu administracyjnego (według Rady, nie ulega	Państwo jest też odpowiedzialne za zapewnienie swojego bezpieczeństwa, stąd też może podejmować działania mające na celu mitygację zagrożeń dla państwa. Dyrektywa NIS 2 wskazuje minimalne wymagania dotyczące Cyberbezpieczeństwa na poziomie unijnym. Nie zakazuje przyjmowania przepisów mających na celu zapewnienie bezpieczeństwa państwa. Dostawca wysokiego ryzyka to dostawca, który stwarza poważne zagrożenie dla bezpieczeństwa państwa, obronności, bezpieczeństwa i porządku publicznego lub zdrowia i życia ludzi. To są przesłanki do uznania za takiego dostawcy. Nie w tych przesłankach kryterium narodowościowych czy politycznych. Za dostawcę wysokiego ryzyka może być także uznany podmiot w całości mający kapitał polski – o ile stwarza poważne zagrożenie dla państwa. Z uwagi na charakter tego postępowania wyłączono część przepisów KPA. Przede wszystkim nie jest możliwe przeprowadzenie postępowania administracyjnego przy udziale wszystkich podmiotów, które wykorzystują sprzęt lub oprogramowanie pochodzące od danego dostawcy. Rygor natychmiastowej wykonalności jest konieczny z uwagi na to, że kwestia dotyczy poważnego zagrożenia dla bezpieczeństwa państwa. Wniosek o ponowne rozpoznanie sprawy został wyłączony, aby pozwolić na szybsze rozpatrzenie ewentualnej skargi przez sąd administracyjny. Wyłączenia z zakresu jawności postępowania sądowoadministracyjnego mają na celu ochronę informacji niejawnych.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

		wątpliwości, że w świetle konstytucyjnego prawa do sądu (art. 45 Konstytucji RP) zasadą musi być dostarczanie stronie pełnego uzasadnienia faktycznego decyzji administracyjnej, tak aby strona (będąca adresatem decyzji) mogła w sposób skuteczny, zaskarżyć tę decyzję do sądu administracyjnego. Ograniczenie prawa do obrony dla dostawcy, a także dla podmiotów objętych skutkami Decyzji DWR, może stanowić podstawę do stwierdzenia niezgodności przepisów z art. 45 Konstytucji RP oraz art. 47 Karty praw podstawowych Unii Europejskiej. Natychmiastowa wykonalność Decyzji DWR i brak dwuinstancyjności - Decyzja DWR jest natychmiast wykonalna, pomimo istotnych skutków gospodarczych (konieczność natychmiastowego zaprzestania nabywania nowego sprzętu lub oprogramowania i rozpoczęcie procedury wycofania). Dodatkowo projekt ustawy nie przewiduje możliwości złożenia wniosku o ponowne rozpatrzenie sprawy przez ministra właściwego do spraw informatyzacji ograniczając zasadę dwuinstancyjności. Oznacza to, że dopiero w postępowaniu odwoławczym, dostawca lub inna strona ma prawo wstrzymać natychmiastową wykonalność (przy czym może otrzymać niepełną treść Decyzji DWR, co naturalnie ogranicza prawo do zaskarżenia takiej decyzji). Ograniczenie prawa do obrony dla dostawcy, a także dla podmiotów objętych skutkami Decyzji DWR, może stanowić podstawę do stwierdzenia niezgodności przepisów z art. 45 Konstytucji RP oraz art. 47 Karty praw podstawowych Unii Europejskiej. Nieprecyzyjny zakres decyzji ministra o uznaniu dostawcy za dostawcę wysokiego ryzyka – w pkt 3 załącznika nr 3 związanego z zarządzaniem łącznością z urządzeniami użytkowników mowa o „innych funkcjach” oprócz 5G Radio Base Station Baseband Unit, co powoduje, że w pkt 3 mieszczą się wszystkie urządzenia zarządzające łącznością z urządzeniami użytkowników i przydzielanie zasobów radiowych, a nie tylko związane z RAN. Taka redakcja prowadzi do niepewności co do ostatecznego zakresu decyzji, a także umożliwia szerokie i nieproporcjonalne wykluczenie urządzeń danego dostawcy, nawet jeśli urządzenia te nijak odpowiadają za krytyczne funkcje w komunikacji. Ponadto istnieją poważne konstytucyjne wątpliwości co do możliwości wprowadzenia normy technicznej (standardu) jako obowiązującego aktu prawa, tj. choć załącznik nr 3 stanowi niewątpliwie część ustawy, to odwołanie się do funkcji 3GPP powoduje, że normy lub standardy tej organizacji stają się źródłem obowiązującego prawa w Polsce. Innymi słowy, 3GPP poprzez zmianę (np. aktualizację) standardu wpływać będzie na prawa i obowiązku adresatów załącznika nr 3 w Polsce, a tym samym moc prawna zostanie zrównana z ustawą. Szeroki zakres załącznika nr 3 do ustawy, wraz z odwołaniem się do zmieniających się norm 3GPP może stanowić podstawę do uchylenia tych przepisów przez Trybunał Konstytucyjny ze względu na naruszenie zasady praworządności (art. 2 Konstytucji RP) oraz powszechnie obowiązujących źródeł prawa (art. 87 Konstytucji RP). Negatywny wpływ na rynek i wzrost cen w efekcie zastosowania Procedury DWR - uchwalenie projektu ustawy w jego obecnej treści może mieć liczne negatywne skutki dla konkurencji i konsumentów, w szczególności dlatego, że realizacja jego założeń może w wielu branżach doprowadzić do powstania duopolu lub oligopolu z nieuniknionym negatywnym skutkiem w postaci wzrostu cen dla konsumentów i przedsiębiorców. Z uwagi na strukturę rynku, wyeliminowanie dostawców spoza UE i NATO czyli w praktyce tych z chińskim kapitałem – doprowadzi do faktycznego zakłócenia konkurencji. Jeśli chińscy dostawcy utracą możliwość prowadzenia działalności, ich udział zostanie przejęty przez konkurencję.	Odnosnie załącznika 3 to wskazać należy, że w poprzednich wersjach projektu domagano się doprecyzowania tych funkcji właśnie przez odniesienie się do standardów 3GPP. Publikacja informacji o wszczęciu postępowania na BIP ma na celu skuteczne doręczenie tego zawiadomienia oraz umożliwienie np. izmom gospodarczym przekazanie stanowiska dot. dostawcy. Projekt nie przewiduje ani jawnej ani tym bardziej ukrytej dyskryminacji inwestorów spoza Polski. Podkreślić należy, że w postępowaniu o uznanie za dostawcę wysokiego ryzyka należy zachować zasadę prawdy materialnej a minister będzie musiał należycie uzasadnić tą decyzję, która będzie mogła być kontrolowana przez sąd administracyjny. Minister właściwy do spraw informatyzacji jest członkiem Kolegium do Spraw Cyberbezpieczeństwa ale nie jest jedynym członkiem. Opinia Kolegium będzie przygotowywana przy udziale wszystkich członków Kolegium, a nie tylko przez ministra właściwego do spraw informatyzacji.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

		Wskutek wysokich barier wejścia związanych z kosztem badań i rozwoju i prawami własności intelektualnej, wejście na rynek innych, poważnych konkurentów nie wydaje się być możliwe. W dobie rosnącej inflacji już taki przypadek wystąpił w Wielkiej Brytanii, gdzie brytyjski operator – British Telecom – wprost odwołał się do konieczności podwyżki cen dla konsumentów m.in. z uwagi na konieczność kompensacji kosztów związanych z wymogiem usunięcia z sieci sprzętu wysokiego ryzyka⁵⁾. Zastosowanie Procedury DWR spowoduje wzrost cen usług dla konsumentów. Nie można wykluczyć również obniżenia jakości, szczególnie w okresie zastępowania urządzeń. Ograniczenie swobody przepływu towarów i zgodności z przepisami UE - projekt ustawy wprowadza Procedurę DWR, w ramach którego przewiduje się mechanizm powiadamiania o wszczęciu postępowania na stronie BIP oraz dopuszczeniem do postępowania jedynie największych przedsiębiorców telekomunikacyjnych. Jak zwrócił uwagę w poprzednim przedłożeniu tego projektu Minister ds. Unii Europejskiej – w opinii nr DPUE.920.1030.2021.AR(27) - komunikowanie (publiczne z art. 66a ust. 8), jak i ograniczone (do największych nabywców produktów ICT z art. 66a ust. 5), może stanowić środek o skutku równoważnym do ograniczeń ilościowych w przywozie i wywozie, o których mowa w art. 34 i 35 TFUE. Zgodnie z orzecznictwem Trybunału Sprawiedliwości UE środkami o skutku równoważnym do ograniczeń ilościowych są bowiem wszelkie przepisy państw członkowskich dotyczące obrotu handlowego mogące bezpośrednio lub pośrednio, rzeczywiście lub potencjalnie utrudnić wewnątrzunijną wymianę handlową (zob. wyrok Trybunału Sprawiedliwości Dassonville, 8/74, pkt 5). Nierówne traktowanie podmiotów może skutkować naruszeniem art. 21 Karty praw podstawowych Unii Europejskiej, art. 32 Konstytucji RP oraz I:1 i III.4 Układu Ogólnego w Sprawie Taryf Celnych i Handlu Światowej Organizacji Handlu („GATT”) o art. 3 ust. 1 -2 umowy między Rządem Polskiej Rzeczypospolitej Ludowej a Rządem Chińskiej Republiki Ludowej w sprawie wzajemnego popierania i ochrony inwestycji z dnia 10 marca 1989 r. Ograniczenia związane z ograniczeniem stron i ograniczonym powiadamianiem może wpływać na handel wewnątrz Unii Europejskiej, w tym na swobodny przepływ produktów legalnie wprowadzonych już do obrotu w Polsce, jak i w innych państwach członkowskich. Narażenie Skarbu Państwa na odpowiedzialność odszkodowawczą w wyniku wdrożenia Procedury DWR - projekt ustawy zawiera rozwiązania jawnie dyskryminujące inwestorów z krajów trzecich, w stosunku do inwestorów krajowych – co przede wszystkim dotyczy kryteriów wydania opinii Kolegium, na której opierać się będzie decyzja ministra o wykluczeniu. Kryteria te opierają się na przesłankach narodowościowych, uznaniowych i politycznych. Ponadto, w projekcie istotnie ograniczono podstawowe gwarancje ustawowe jak prawo do rzetelnego procesu, z możliwością udziału czynnika społecznego. Działania takie są wprost sprzeczne z art. I:1 i III.4 GATT, które wykluczają dyskryminację produktów importowanych względem produktów lokalnych, a także produktów importowanych z jednego członków tej organizacji względem tych z innego państwa. Członek Światowej Organizacji Handlu („WTO”) nie może traktować towarów innego członka WTO w sposób mniej uprzywilejowany niż traktuje towary pochodzące	

⁵⁾ [BT misses deadline for removing Huawei from network core • The Register](#)

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			z własnego terytorium lub z terytorium innego członka WTO. Co więcej, Procedura DWR zakłada wymianę produktów, usług lub procesów w terminie 4 lat lub 7 lat. W przypadku wymiany sprzętu telekomunikacyjnego azjatyckich producentów, koszt takiej decyzji wyniósłby kilkanaście miliardów złotych. W efekcie Skarb Państwa będzie musiał się zmierzyć z groźbą postępowań odszkodowawczych, w tym powództw wnoszonych do międzynarodowych trybunałów arbitrażowych przez podmioty poszkodowane przez rozwiązania zawarte w projekcie KSC: co może skutkować ekspozycją finansową budżetu państwa. Jak wskazano w raporcie pn. „Prawne i ekonomiczne skutki ograniczenia konkurencji wśród dostawców sprzętu sieciowego 5G w Polsce”⁶⁾ w wyniku wejścia w życie Projektu szkody polskiej gospodarki wyniosłyby łącznie niemal -44 mld zł (w tym 21,5 mld zł obniżenia PKB, 1,2 mld zł utraconej korzyści konsumentów, 0,6 mld zł bezpośredniej straty dla Skarbu Państwa oraz 14,1 mld zł bezpośredniej straty dla operatorów telekomunikacyjnych), co przełoży się bezpośrednio na ryzyko sporu ze Skarbem Państwa. Jednocześnie kryteria oceny jedynie w szacunkowym stopniu odnoszą się do kryteriów technicznych – dających się jednoznacznie i obiektywnie ustalić oraz powiązanych z podatnością danych systemów lub urządzeń. Zamiast tego ocena opiera się przede wszystkim na niezwykle pojemnej przesłance <u>prawdopodobieństwie pozostawania dostawcy pod wpływem obcego państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego</u>. Takie ukształtowanie przesłanek stoi w sprzeczności z podstawowymi zasadami postępowania administracyjnego. W ramach postępowania administracyjnego organ wydający decyzję administracyjną obowiązany jest ustalić <u>stan faktyczny na podstawie którego dokona subsumcji stanu prawnego, w wyniku którego wyda decyzję administracyjną</u>. Ocena w ramach prowadzonego postępowania nie uwzględnia w żaden sposób takich okoliczności jak: – sposób wykorzystania produktów ICT, usług ICT lub procesów ICT przez podmioty ważne i kluczowe, w tym możliwość objęcie zakresem decyzji nie tylko sieci 5G, ale także jakichkolwiek innych technologii lub zastosowań (brak ograniczenia zakresu regulacji do krytycznych aktywów, o których mowa w SM03 Toolbox 5G), – możliwość dodatkowej konfiguracji urządzeń, pozbawiającej produktów ICT, usług ICT lub procesów ICT cech związanych z wysokim ryzykiem, – możliwość stopniowania skutków decyzji administracyjnej (brak jakiejkolwiek proporcjonalności), – brak wdrożenia jakiegokolwiek postępowania naprawczego. Procedura DWR obniży poziom inwestycji, w tym w sektorze innowacyjnym, wpływając bezpośrednio na obniżenie wpływów do budżetu państwa. Wprowadzony model wykluczenia dostawcy wysokiego ryzyka, polegający na jego całkowitym wykluczeniu także w odniesieniu do 18 sektorów spowoduje, że w wyniku jednej, arbitralnej decyzji ministra właściwego do spraw informatyzacji, wydanej na podstawie opinii Kolegium ds. Cyberbezpieczeństwa taki dostawca, w sposób natychmiastowy, nie będzie mógł prowadzić działalności gospodarczej w Polsce, bez względu na jego związki ekonomiczne z Polską i dokonane inwestycje, w tym w produkty, procesy i usługi cechujące się wysokim poziomem	

⁶⁾ Wykluczenie Huawei z 5G to 44 mld zł strat dla Polski do 2030 - Forsal.pl

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			innowacji. Stanie się tak bez poszanowania podstawowych gwarancji procesowych wynikających z Kodeksu postępowania administracyjnego i norm prawa międzynarodowego, co może wywołać efekt odstraszący dla innych zagranicznych podmiotów. Poważne wady związane z przyjętym modelem postępowania administracyjnego. Do tych negatywnych elementów projektowanego postępowania należą: - brak gwarancji bezstronności - brak ustawowego wyłączenia właściwego ministra z procedury wydania opinii poprzedzającej wszczęcie postępowania administracyjnego, powoduje naruszenie zasady niezależności i bezstronności. Jest to szczególnie istotne w przypadku opinii <u>poprzedzającej</u> wszczęcie postępowania administracyjnego z uwagi na brak zastosowania ogólnych reguł włączeń osób i organów na gruncie przepisów kodeksu postępowania administracyjnego (art. 24 i nast. ustawy z dnia 14 czerwca 1960 Kodeks postępowania administracyjnego („KPA")), - brak doręczania informacji o wszczęciu Procedury DWR wobec dostawców spoza UE/EFTA/Konfederacji Szwajcarskiej - W ramach Procedury DWR przewiduje się brak indywidualnego informowania dostawcy, którego dotyczy postępowanie, o jego wszczęciu, jeśli jego siedziba znajduje się poza Unią Europejską/EFTA/Konfederacją Szwajcarską (w to miejsce przewidziano informację na stronie podmiotowej BIP właściwego organu), co skutkuje dyskryminacją podmiotów spoza tego obszaru – wobec takich podmiotów postępowanie jest jawne, w sytuacji gdy sam fakt wszczęcia postępowania może skutkować znacznym ograniczeniem zamówień przez podmioty objęte regulacją, ze względu na przyszłe ryzyko wykluczenia takiego dostawcy. Różne traktowanie przedsiębiorców ze względu na kraj pochodzenia może skutkować naruszeniem art. 21 Karty praw podstawowych Unii Europejskiej, art. 32 Konstytucji RP oraz I:1 i III.4 GATT, art. 3 ust. 1 -2 umowy między Rządem Polskiej Rzeczypospolitej Ludowej a Rządem Chińskiej Republiki Ludowej w sprawie wzajemnego popierania i ochrony inwestycji z dnia 10 marca 1989 r., - brak gwarancji czynnego udziału strony w postępowaniu - identyfikujemy duże ryzyko wyłączenia uprawnień strony ww. zakresie w postaci możliwości wyłączenia dostępu do akt administracyjnych na podstawie art. 74 § 4 KPA (brak dostępu do akt sprawy zawierających informacje niejawne o klauzuli tajności „tajne” lub „ściśle tajne”, a także do innych akt, które organ administracji publicznej wyłączy ze względu na ważny interes państwowy). Istnieje uzasadnione ryzyko, iż na etapie postępowania akta będą wyłączone na podstawie klauzuli “ściśle tajne” lub “tajne” albo na podstawie przesłanki “ważnego interesu państwowego”. Takie ograniczenie dostępu do akt w połączeniu z powołanym wyżej możliwym brakiem sporządzenia uzasadnienia faktycznego może de facto uniemożliwić stronie postępowania realizacji jej uprawnień procesowych i przedstawienie swoich argumentów i dowodów tak na etapie postępowania administracyjnego jak i sądowno-administracyjnego, - brak transparentności postępowania sądowego - nie ma również podstaw do wyłączenia podstawowego trybu działania sądów administracyjnych ww. sprawie jakim jest rozprawa sądownoadministracyjna i wskazanie ww. zakresie na obowiązek rozpatrzenia jej na posiedzeniu niejawnym. Posiedzenie niejawne stanowi istotne ograniczenie, gdyż ogranicza w poważnym stopniu kontrolę społeczną nad postępowaniem sądowym. Tymczasem charakter decyzji wydanej wskazuje, iż jest to decyzja o ogromnych skutkach	

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

		społeczno-gospodarczych i przebieg postępowania sądowo administracyjnego ww. zakresie winien mieć charakter jawny, - brak przesłanek do wydania decyzji administracyjnej - proponowane przepisy nie zawierają żadnych przesłanek dotyczących podstaw prawnych do wydania decyzji administracyjnej przez ministra właściwego do spraw informatyzacji. Jediną przesłanką jest uznanie, że z przeprowadzonego postępowania wynika, że dostawca ten stanowi poważne zagrożenie dla bezpieczeństwa narodowego. W konsekwencji, minister właściwy do spraw informatyzacji, jest związany opinią Przewodniczącego Kolegium, nie mając żadnej możliwości zmiany decyzji administracyjnej wynikającej z tej opinii. W efekcie instancyjność postępowania ma charakter iluzoryczny, albowiem właściwy minister jedynie „broni” niejawnej opinii Kolegium, - brak określenia charakteru prawnego opinii Kolegium - choć projektodawca wskazuje, że opinia Kolegium ma charakter opinii uzgadnianej podczas posiedzeń Kolegium, to w istocie, jak wskazano wyżej, opinia ta ma charakter wiążący a minister właściwy do spraw informatyzacji potwierdza ją jedynie w drodze decyzji administracyjnej. To opinia Kolegium ma charakter przesądzający o wykluczeniu danego dostawcy, a nie decyzja administracyjna ministra właściwego ds. informatyzacji. Oznacza to zatem, że nie ma podmiotu, któremu można przypisać odpowiedzialność za opinię, ponieważ od opinii Kolegium nie przysługuje żadne odwołanie, a właściwy minister wydając decyzję odwołując się do niezaskarżalnej opinii, o niejasnym charakterze prawnym, - dyskryminacyjne kryteria Procedury DWR: Przesłanki oceny dostawcy usług, produktów i procesów ICT za dostawcę wysokiego ryzyka mają charakter wysoce ocenny, a kluczowe znaczenie przypisane zostało kryteriom politycznym i organizacyjnym (bliżej niezdefiniowane związki dostawcy z państwem trzecim, praktyka stosowania prawa w państwie trzecim itd.). Z kolei kryteria techniczne oceny zostały uwzględnione jedynie w ograniczonym zakresie. Takie podejście jest sprzeczne z wytycznymi określonymi w dokumencie Komisji Europejskiej 5G Toolbox, który podkreśla konieczność odniesienia oceny do kluczowych aktywów (key assets), a zatem skoncentrowanie się na aspektach przedmiotowych, nie zaś podmiotowych. W obecnym kształcie przepisy projektu ustawy w tym zakresie mogą naruszać zasadę równego traktowania (niedyskryminacji) ze względu na przynależność państwową, która została określona nie tylko w art. 18 TFUE, ale także w art. 20 i art. 21 ust. 2 Karty praw podstawowych. Zasada niedyskryminacji może zostać naruszona nie tylko jawną dyskryminacją ze względu na przynależność państwową, ale także wszelką ukrytą dyskryminacją, która poprzez zastosowanie innych kryteriów zróżnicowania prowadzi w rzeczywistości do tego samego rezultatu. Przepisy regulujące Procedurę DWR mogą naruszać również art. 34 i art. 35 TFUE, które chronią swobodny przepływ towarów. Zauważyć należy, że dany dostawca może wytwarzać produkty i usługi w jednym kraju członkowskim i dostarczać do innych krajów, co jest powszechną praktyką w UE. Przepis art. 34 TFUE zakazuje natomiast państwom członkowskim przyjmowania „ograniczeń ilościowych w przywozie” i „wszelkich środków o skutku równoważnym”. Wprawdzie zgodnie z art. 36 TFUE, postanowienia artykułów 34 i 35 nie stanowią przeszkody w stosowaniu wskazanych zakazów lub ograniczeń, gdy jest to uzasadnione m.in. względami bezpieczeństwa publicznego. Ochrona bezpieczeństwa publicznego zakłada jednak „istnienie rzeczywistego	

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

		i dostatecznie poważnego zagrożenia, które narusza jeden z podstawowych interesów społeczeństwa, a w kontekście wspólnotowym należy je interpretować w sposób ścisły”. Zwrócić należy także uwagę, że ciężar dowodu spoczywa na państwie członkowskim, które powinno „wykazać w każdym przypadku, że ich przepisy są niezbędne do zapewnienia skutecznej ochrony interesów, o których mowa w art. 36 TFUE”. Zastosowanie odstępstwa przewidzianego w art. 36 TFUE wymaga zastosowania tzw. testu proporcjonalności, czyli sprawdzenia czy przewidziane rozwiązania są proporcjonalne do zamierzonych celów, w więc w tym przypadku, do ochrony bezpieczeństwa publicznego. TSUE w swoim orzecznictwie także wskazywał, że przepis krajowy zakazujący przywozu produktu jest nieproporcjonalny, jeżeli istnieją mniej restrykcyjne środki, które pozwalają na osiągnięcie zamierzonego celu. Ograniczenie swobodnego przepływu towarów oraz swobody przedsiębiorczości można uzasadnić na podstawie art. 36 TFUE, tylko wtedy, gdy środek jest konieczny, <u>a więc w szczególności, gdy nie istnieją inne mniej restrykcyjne środki, które mogłyby osiągnąć ten sam cel.</u> Zauważyć wreszcie należy, że wykluczenie z polskiego rynku określonych dostawców oznacza automatyczne polepszenie sytuacji innych dostawców działających na polskim rynku. Stanowiąc to może z kolei naruszenie art. 106 ust. 1 TFUE, który zakazuje państwom członkowskim przyjmowania lub utrzymywania w mocy, w odniesieniu do przedsiębiorstw, którym przyznano prawa wyłączne lub specjalne, wszelkich środków, które prowadziłyby do naruszenia innej zasady w traktatach UE. Przepisy te obejmują w szczególności art. 18 TFUE (zasada niedyskryminacji), art. 34 TFUE (swobodny przepływ towarów) i art. 102 TFUE (zakaz nadużywania pozycji dominującej). Projekt w obecnym kształcie może zostać uznany za dyskryminujący, co może być uznane za naruszające TFUE (zasada niedyskryminacji – art. 18 TFUE, zasady swobodnego przepływu towarów i usług – art. 34 i 35 TFUE, zakaz nadużywania pozycji dominującej art. 102 TFUE), Karty Praw podstawowych (art. 20 i 21 ust. 2 Karty praw podstawowych), a także potencjalnie naruszeniami innych zobowiązań międzynarodowych Rzeczypospolitej Polskiej. Arbitralność Procedury DWR: projekt ustawy KSC przewiduje silnie dyskrejonalną i arbitralną, a przede wszystkim jednoosobową, procedurę oceny ryzyka dostawcy sprzętu lub oprogramowania z punktu widzenia cyberbezpieczeństwa, i w szerszym ujęciu, bezpieczeństwa państwa. W ramach postępowania oddziałującego arbitralnie i szeroko na przedsiębiorców decyzja nie powinna być podejmowana wyłącznie jednoosobowo przez ministra właściwego do spraw informatyzacji. Zakres oceny bezpieczeństwa oraz wykluczenia produktów przedsiębiorcy z rynku ma skomplikowany charakter wymagający wiedzy eksperckiej, która w ramach administracji państwowej skumulowana jest w różnych ministerstwach czy urzędach, jak np. Urzędzie Ochrony Konkurencji i Konsumentów, czy Urzędzie Komunikacji Elektronicznej. Z tego względu ważne byłoby uczestnictwo w podejmowaniu decyzji przez ministrów odpowiedzialnych za obszary istotne z perspektywy chronionych wartości (obronność, bezpieczeństwo i porządek publiczny) lub za obszary właściwe merytorycznie z perspektywy sektora, którego dotyczy decyzja (rozwój i technologia)– uczestnictwo w procesie decyzyjnym mogłoby sprowadzać się do możliwości wyrażenia sprzeciwu w zakresie wydania decyzji: <u>Za błędne rozwiązanie uznać należy również brak zapewnienia udziału czynnika eksperckiego w procesie wydania opinii przez Kolegium, co stanowi przecież istotny element całego postępowania w sprawie uznania za dostawcę wysokiego ryzyka, poprzedzającego decyzję ministra.</u> Przedmiotowa opinia z założenia powinna brać pod uwagę wyniki	

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			analizy szeregu uwarunkowań – politycznych, ekonomicznych, technologicznych i organizacyjnych oraz stanowić kluczowy element merytorycznego uzasadnienia podejmowanej decyzji. Tym samym właściwy dobór osób biorących udział w jej wydaniu wydaje się być kluczowy dla zapewnienia jej kompletności i rzetelności, a w konsekwencji prawidłowości całego postępowania. Z tego względu nie ulega wątpliwości, że do prac nad jej treścią powinni zostać włączeni np. przedstawiciele izb zrzeszających podmioty z sektora ICT czy przedsiębiorców korzystających z rozwiązań ICT. Powyższa uwaga ma tym większe znaczenie, że Kolegium jest z definicji organem politycznym, złożonym przede wszystkim z ministrów (art. 66 ustawy o krajowym systemie cyberbezpieczeństwa), a zaangażowanie CSIRT'ów nie spełnia wystarczającej gwarancji udziału czynnika eksperckiego, czy też następczo izb gospodarczych.	
43.	Konfederacja Lewiatan	67b- 67f	Nadmierne rozszerzenie zakresu wykluczenia dostawcy na wszystkie podmioty ważne i kluczowe Jednostka redakcyjna: art. 67b – 67f projektu KSC Jednostka redakcyjna NIS2: 20 ust.1; art. 21 ust 1 w zw. z ust.2 w zw. z ust. 3 Uwaga: W odróżnieniu od wcześniejszych propozycji, obecna wersja projektu ustawy zakłada rozszerzenie Procedury DWR na cały sektor cyberbezpieczeństwa (18 sektorów). Taki krok może prowadzić do znacznego rozszerzenia zakresu regulacji, potencjalnie obejmując szeroki wachlarz produktów i usług ICT. Wprowadzenie tej procedury objęłoby około 38 532 podmioty (dane OSR), co jest istotnym rozszerzeniem w stosunku do wcześniejszych propozycji legislacyjnych. Wśród tych produktów znajdują się na przykład panele fotowoltaiczne, falowniki, chipsety czy procesory przemysłowe, które są powszechnie stosowane we wszystkich sektorach. Może to zagrażać ciągłości funkcjonowania sektorów i generować znaczne koszty, co jest skutkiem trudnym do przewidzenia na etapie wprowadzania regulacji. Warto podkreślić, że: 1) zgodnie z NIS2 środki zarządzania ryzykiem w cyberbezpieczeństwie powinny być adekwatne do rzeczywistego poziomu ryzyka, na które są narażone sieci i systemy informatyczne poszczególnych podmiotów kluczowych i ważnych. Stosowane środki powinny być oparte na najnowszej wiedzy oraz, gdzie to możliwe, na europejskich i międzynarodowych normach. Powinny również uwzględniać koszty ich wdrożenia, aby unikać nakładania na podmioty nieproporcjonalnie dużych obciążeń finansowych i administracyjnych. Istotne jest również dostosowanie tych środków do specyfiki każdego podmiotu, biorąc pod uwagę takie czynniki jak krytyczność działalności, wielkość podmiotu, prawdopodobieństwo wystąpienia incydentów oraz potencjalne skutki społeczne i gospodarcze związane z takimi incydentami (por. motyw. 81 i 82, art. 21 ust. 1 NIS2). 2) wdrożone przez NIS2 skoordynowane oszacowania ryzyka dla bezpieczeństwa krytycznych łańcuchów dostaw koncentrują się na konkretnych sektorach, mając na uwadze konieczność dostosowania oszacowania do jego specyfiki (por. motyw 91, art. 22 NIS2). Te oszacowania prowadzone są przez Grupę Współpracy we współpracy z Komisją Europejską i ENISA, a nie przez ministra właściwego do spraw informatyzacji. 3) 5G Toolbox, nakazuje analizę i weryfikację łańcucha dostaw w sieciach mobilnych (telekomunikacji), a nie w każdym sektorze, w którym wykorzystywane są systemy informatyczne, a w szczególności zaleca: - oceniać profil ryzyka dostawców w odniesieniu do kluczowych zasobów uznanych za krytyczne i wrażliwe w unijnej skoordynowanej ocenie ryzyka, - utrzymywania zróżnicowanego i zrównoważonego łańcucha dostaw 5G w celu	Uwaga wyjaśniona Postępowanie umożliwia badanie dostawcy sprzętu lub oprogramowania dla wszystkich sektorów gospodarki wskazanych w ustawie. Jest to wskazane z uwagi na to, że każdy podmiot kluczowy i podmiot ważny musi dbać o bezpieczeństwo łańcuchów dostaw. Podmioty kluczowe i podmioty ważne mają istotny charakter dla funkcjonowania współczesnej gospodarki i społeczeństwa informacyjnego. Zakłócenie funkcjonowania tych podmiotów poprzez atak przez łańcuch dostaw może spowodować niepowetowane straty.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			uniknięcia długotrwałej zależności, - koordynację między państwami członkowskimi. Wprowadzenie w projekcie ustawy KSC procedury wykluczenia dostawcy obejmującej wszystkie podmioty kluczowe i ważne. Proponowany zakres wprowadza rygorystyczne regulacje osiemnastu sektorów, co jest rozwiązaniem niespotykanym w Unii Europejskiej i mogącym prowadzić do poważnych konsekwencji operacyjnych i finansowych dla szerokiego spektrum przedsiębiorstw. Sektory takie jak administracja publiczna, zdrowie, bankowość, energetyka, a także nauka i produkcja (w tym żywności i chemikaliów), znajdują się wśród tych, które będą musiały zastosować się do Procedury DWR, co oznacza całkowite wyeliminowanie i zastąpienie urzędów oraz oprogramowania wykluczonego dostawcy w ciągu zaledwie 7 lat. To nie tylko stwarza ryzyko znaczących przerw w działalności, ale także narzuca ogromne koszty związane z wymianą sprzętu i oprogramowania, bez przewidzianego odszkodowania dla dotkniętych tym podmiotów. Tak szerokie zastosowanie Procedury DWR bez proporcjonalnej oceny ryzyka i specyfiki każdego sektora jest nieadekwatne i może prowadzić do nadmiernego obciążenia podmiotów, które niekoniecznie są wrażliwe na zagrożenia związane z wykorzystaniem technologii od określonych dostawców. Co więcej, brak rekompensaty za wymianę sprzętu może spowodować poważne obciążenia finansowe dla wielu przedsiębiorstw, co z kolei może wpłynąć negatywnie na całą gospodarkę. W obliczu potencjalnych niezgodności z NIS2 oraz nieproporcjonalnego charakteru proponowanych środków zarządzania cyberbezpieczeństwem, postulujemy: – ujednolicenie terminu na usuwanie sprzętu dla wszystkich sektorów do 7 lat, – w kontekście brzmienia 5G toolbox, który przewiduje ewentualne ograniczenia w zakresie korzystania ze sprzętu lub usług do funkcji krytycznych, postulujemy by ewentualne wykluczenia dotyczyły infrastruktury krytycznej;szczegółowe wytyczne w zakresie infrastruktury krytycznej były formułowane dla każdego sektora w akcie prawnym niższego rzędu, tj. w rozporządzeniu wydawanym przez organu ds. cyberbezpieczeństwa właściwy dla danego sektora. Takie podejście umożliwi dynamiczne reagowanie na zmiany na rynku i w technologii, umożliwiając dostosowanie zakresu do faktycznych potrzeb i konkretnej specyfiki danego sektora. Wprowadzenie przepisów na poziomie aktów niższego rzędu pozwoli na bardziej elastyczne i precyzyjne zarządzanie infrastrukturą krytyczną, co jest niezbędne w obliczu szybko zmieniających się technologii i rosnących zagrożeń w obszarze cyberbezpieczeństwa. Pozwoli to na lepsze zrozumienie specyficznych potrzeb poszczególnych sektorów i na zastosowanie środków adekwatnych do rzeczywistych zagrożeń, bez konieczności stałych zmian ustawowych. Takie rozwiązanie sprzyja również transparentności i przejrzystości procesu legislacyjnego, umożliwiając konsultacje i współpracę z zainteresowanymi stronami, co jest kluczowe dla skutecznego wdrożenia regulacji i zapewnienia wysokiego poziomu ochrony infrastruktury krytycznej, – przywrócenie konstytucyjnych gwarancji procesowych w postępowaniu dotyczącym wykluczenia dostawcy.	
44.	Przedsiębiorcy RP	Art. 67b i nast.	Przepisy dotyczące postępowania w sprawie uznania za DWR są nieprzejrzyste i nieproporcjonalne. Wykluczenie dostawcy ze względu na państwo pochodzenia możliwe jest we wszystkich 18 obszarach	Uwaga wyjaśniona

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			określonych w dyrektywie NIS2. Członkowie Pracodawców RP wskazują, że wprowadzone zostały niemierzalne kryteria wyraźnie adresowane do chińskich dostawców, co dotknie również wszystkie podmioty korzystające z ich usług. Ograniczona została jawność postępowania oraz nie uwzględniona została możliwość dostępu do treści uzasadnienia. Dodatkowo procedura uznania dostawcy za DWR przewiduje natychmiastową wykonalność decyzji Ministra Cyfryzacji, niezależnie od losów procesu odwoławczego, a jednocześnie nie wprowadza zasad zastępowania.	Wprowadzone przepisy zawierają niedyskryminacyjną procedurę uznania dostawcy za dostawcę wysokiego ryzyka. Przepisy nie odnoszą się do podmiotów z żadnego wprost określonego kraju.
45.	Przedsiębiorcy RP	Art. 67b i nast.	Procedura uznania dostawcy za DWR Zbyt szeroki katalog podmiotów objętych procedurą uznania za DWR Nowelizacja rozszerzy zakres stosowania przepisów o dostawcy wysokiego ryzyka (wątpliwych pod kątem zgodności z TFUE już na gruncie 5G Toolboxa) na podmioty ze wszystkich sektorów objętych w NIS 2, zapewniające technologie i usługi ICT niemalże wszystkim istotnym sektorom rynkowym. Ustalone zasady będą stosowane jednolicie do każdego dostawcy, niezależnie od charakteru jego usług i sektora, dla którego te usługi świadczy — jak również niezależnie od rozmiaru konsekwencji, jakie wywoła decyzja dla podmiotów z konkretnego sektora. ICo więcej dostawca sprzętu lub oprogramowania, który może być objęty tą procedurą jest zdefiniowany szeroko. Definicja obejmuje nie tylko producenta, ale również upoważnionego przedstawiciela, importera oraz dystrybutora. Ponadto szeroki zakres ustawy umożliwi arbitralne uznanie dowolnych dostawców ICT za dostawców „wysokiego ryzyka” na podstawie niejasno określonych kryteriów (np. kryterium państwa pochodzenia). Takie rozszerzenie stosowania uznaniowego DWR dla różnych technologii ICT, które charakteryzują odmienny poziom ryzyka i wymagają różnych podejść, będzie skutkować nieadekwatnymi regulacjami, nieodpowiadającymi specyfice poszczególnych technologii i rynków. Dodatkowo, doprowadzi do obciążeń z perspektywy obowiązków regulacyjnych i nadzoru nad wdrażaniem i stosowaniem sprzętu lub oprogramowania ICT, niekoniecznie związanym bezpośrednio z ryzykiem prezentowanym przez technologię 5G. Brak zróżnicowanego podejścia do różnych sektorów gospodarki w ramach procesu decyzyjnego prowadzi do nieadekwatnych i niewspółmiernych ograniczeń dla niektórych branż, potencjalnie szkodząc konkurencyjności i innowacyjności polskiej gospodarki. Nadmierny ciężar podwójnej oceny dostawcy Polski model przyjmuje założenie, zgodnie z którym kwestia DWR jest rozpatrywana równolegle na dwóch poziomach: (i) na poziomie decyzji administracyjnej z art. 67b Nowelizacji, oraz (ii) na poziomie oceny wdrożenia środków w zakresie cyberbezpieczeństwa dot. łańcucha dostaw (art. 8 ust. 1 pkt. 2 lit. d w zw. z art. 8 ust. 4 pkt. 3 Nowelizacji). Rozwiązanie to jest słusznie odosobnione w UE. Wynika to z kilku względów: Docelowy model proponowany przez UE zakładał przyjęcie przez państwa członkowskie takich regulacji, które będą dostosowywały się do kolejnych Toolboxów wydawanych dla poszczególnych sektorów na szczeblu europejskim, co miało zapewnić jednolite podejście do cyberbezpieczeństwa na poziomie unijnym. W związku z przepisami zawartymi w Nowelizacji, możliwe będzie wydanie decyzji wykluczającej przez	Uwaga wyjaśniona Postępowanie w sprawie uznania za dostawcę wysokiego ryzyka ma na celu zabezpieczenie polskiej gospodarki i polskiego społeczeństwa przed dostawcą sprzętu lub oprogramowania, który stwarza poważne zagrożenie dla bezpieczeństwa państwa, obronności, bezpieczeństwa i porządku publicznego lub zdrowia i życia ludzi. W ramach postępowania administracyjnego będą brane pod uwagę zarówno aspekty techniczne związane z dostarczaniem przez dostawcę sprzętem i oprogramowaniem jak również aspekty nietechniczne związane z dostawcą. Dzięki temu zostanie zidentyfikowany pełen obraz zagrożeń jakie stwarza dostawca sprzętu lub oprogramowania. Postępowanie umożliwia badanie dostawcy sprzętu lub oprogramowania dla wszystkich sektorów gospodarki wskazanych w ustawie. Jest to uzasadnione z uwagi na fakt, że każdy podmiot kluczowy i podmiot ważny musi dbać o bezpieczeństwo łańcuchów dostaw. Podmioty kluczowe i podmioty ważne mają istotny charakter dla funkcjonowania współczesnej gospodarki i społeczeństwa informacyjnego. Zakłócenie funkcjonowania tych podmiotów poprzez atak przez łańcuch dostaw może spowodować niepowetowane straty.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

		Ministra w stosunku do dowolnego dostawcy sprzętu, usługi czy programu ICT w dowolnym sektorze. Jest to niezgodne zarówno z założeniami NIS 2, jak i sensem wydawania Toolboxów, szczególnie z perspektywy zasady proporcjonalności. Celem art. 21 ust. 3 dyrektywy NIS 2 jest wymuszenie przez państwo na podmiotach kluczowych i ważnych uwzględnienia wyników skoordynowanych oszacowań ryzyka przeprowadzonej na poziomie UE. Jest to ocena nie z perspektywy pojedynczego państwa członkowskiego, ale z perspektywy łańcucha dostaw na poziomie europejskim. W związku z przepisami zawartymi w Nowelizacji, możliwe będzie wydanie decyzji wykluczającej przez Ministra w stosunku do dowolnego dostawcy sprzętu, usługi czy programu ICT w dowolnym sektorze. Jest to niezgodne zarówno z założeniami NIS 2, jak i sensem wydawania Toolboxów, szczególnie z perspektywy polskiej regulacja jest zatem całkowicie oderwana od tego modelu i stanowi autorskie rozwiązanie bez oparcia w prawie UE. t Znacząco ograniczona rola dostawcy w postępowaniu i brak możliwości odwołania Sposób prowadzenia postępowania w sprawie uznania dostawcy za dostawcę wysokiego ryzyka przewidziane w Nowelizacji znacząco narusza naczelne zasady stosowane w relacji organu z przedsiębiorcą. Znikoma przejrzystość i niejawność procesów decyzyjnych Procedura określona w art. 67b ustawy umożliwia Ministerstwu Cyfryzacji ograniczenie dostępu do informacji podczas decydowania o statusie dostawcy wysokiego ryzyka (np. w czasie postępowania wyłączone są przepisy KPA pozwalające na szeroki dostęp stron do dowodów zgromadzonych w postępowaniu, w szczególności art. 28 i 31 KPA). Wprowadzenie takich ograniczeń jest uzasadniane ochroną bezpieczeństwa państwa. W rezultacie mamy do czynienia wyłącznie z pozorną przejrzystością procesu orzekania w sprawie uznania podmiotu za DWR. Takie działanie z perspektywy biznesu i użytkowników końcowych zmniejsza zaufanie do władzy i sprawia znaczące trudności w sprawowaniu obywatelskiej kontroli nad procesem decyzyjnym w ramach administracji państwowej. Decyzje o tak daleko idących skutkach powinny móc być szeroko komentowane w przestrzeni publicznej, tak aby uczynić cały proces bardziej transparentnym i uwzględnić głos podmiotów zainteresowanych rozwojem postępowania. o Ograniczenie przekazywanej treści uzasadnienia Zgodnie z procedurą, minister może również ograniczać informacje zawarte w uzasadnieniach decyzji. Podobnie na dalszym etapie, w procedurze sądowej, stronom doręczane jest uzasadnienie wyroku w takim zakresie w jakim nie zawiera informacji niejawnych w rozumieniu przepisów o ochronie informacji niejawnych, zakres uzasadnienia zależeć będzie w praktyce od decyzji ministra. To ograniczenie uniemożliwi zrozumienie przez zainteresowane strony, dlaczego dany dostawca został zaklasyfikowany jako DWR, a tym samym faktyczną możliwość rzetelnego zaskarżenia wyroku. Kwestią sporną i budzącą wątpliwości jest również samo odniesienie do ustawy o ochronie informacji niejawnych ze względu na różnicę w regulowanej materii. Jest to o tyle nietrafione odwołanie, że ustawa o ochronie informacji niejawnych reguluje zasady ochrony informacji, których nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo byłoby z punktu widzenia jej interesów niekorzystne, także w trakcie ich opacowywania oraz niezależnie od formy i sposobu ich wyrażania.	Z uwagi na charakter tego postępowania wyłączono część przepisów KPA. Przede wszystkim nie jest możliwe przeprowadzenie postępowania administracyjnego przy udziale wszystkich podmiotów, które wykorzystują sprzęt lub oprogramowanie pochodzące od danego dostawcy.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

		Zdecydowanie nie można uznać, że zapoznanie się z wyrokiem strony mogłoby być uznane o informację na równi z informacją niekorzystną czy szkodliwą dla Rzeczypospolitej Polskiej. Taka konstrukcja przepisów dalej bezpodstawnie umacnia obawy dotyczące braku przejrzystości i znacząco ogranicza możliwość odpowiedniej obrony. Prawa procesowe i możliwości odwoławcze Art. 67b ust. 19 Nowelizacji zakłada wykluczenie możliwości wnioskowania o ponowne rozpatrzenie sprawy, co jest szczególnie problematyczne. Ogranicza to drogi odwoławcze dostępne dla podmiotów, które będą negatywnie dotknięte decyzją (zarówno dostawców ICT, jak i podmiotów korzystających z ich usług). Taki skrócony proces odwoławczy doprowadzi do błędów i nietrafionych decyzji bez możliwości ich korekty w kolejnych instancjach. Właściwie jedyną możliwością podważenia decyzji będzie wejście na drogę sądową. Tymczasem, postępowanie to jest niejawne, a strona otrzymuje jedynie fragment uzasadnienia, co ogranicza jej możliwość skutecznej ochrony swoich praw. Pożądanym rozwiązaniem byłoby zapewnienie potencjalnemu DWR możliwości dialogu z wykwalifikowanym urzędem nadzorującym dany sektor aby rozważyć możliwości osiągnięcia kompromisu, przed wszczęciem oficjalnego postępowania wobec dostawcy. Natychmiastowa wykonalność decyzji Procedura przewiduje natychmiastową wykonalność decyzji ministra, co oznacza, że należy się do niej stosować od chwili jej wydania — niezależnie od losów procesu odwoławczego. Ta cecha procedury uznania za DWR stawia podmioty gospodarcze w trudnej sytuacji. Z uwagi na krótki czas na wycofanie sprzętu lub oprogramowania (przyp. 4 lata dla przedsiębiorców telekomunikacyjnych o których mowa w art. 67b ust. 1 pkt 2), podmioty korzystające z objętych decyzją rozwiązań poniosą duże straty operacyjne i nakłady finansowe (np. z uwagi na niejednokrotnie dłuższe okresy amortyzacyjne nabytych sprzętów), nawet jeśli ostatecznie decyzja zostanie uchylona przez sąd. Jednocześnie, w rezultacie dostawca, wobec którego wydano pierwotnie decyzję, zostanie w praktyce bezprawnie wykluczony z rynku. Ograniczenia w dostępie do pełnych informacji, brak szerszych możliwości odwoławczych i natychmiastowa wykonalność decyzji sprawia, że cały proces będzie postrzegany jako dominowany przez arbitralnie działające organy państwowe, z minimalnymi gwarancjami dla podmiotów gospodarczych, które są podmiotem decyzji o uznaniu za DWR. W takiej sytuacji organ decyzyjny będzie działać praktycznie samodzielnie. To podważa fundamentalną zasadę działania w sposób zmierzający do wzbudzenia zaufania do systemu prawnego i rządów prawa. Wnioski z analizy projektów NIS2 w powyższych obszarach w państwach członkowskich (jak wskazano w sekcji 5 analizy) wskazują, że polskie podejście do regulacji DWR jest odosobnione. Biorąc pod uwagę zasadę proporcjonalności i kwestie związane ze wspólnym rynkiem unijnym takie podejście uznać należy za błędne. Brak miarkowania ryzyka dostawców oraz procedury naprawczej W pierwotnym projekcie przewidziano podział dostawców na kategorie wysokiego, umiarkowanego i niskiego ryzyka, bazując na kryteriach analogicznych do tych zastosowanych w obecnym projekcie. Jednakże, taki podział został wyeliminowany w nowelizacji obecnie rozpatrywanej. Wcześniejsza wersja	

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

		artykułu 66a umożliwia dostawcom poddanym procedurze uznania za dostawcę o wysokim ryzyku (DWR - High Risk Vendor) przedstawienie argumentów przeciwko procedurze, sugerując na przykład implementację dodatkowych zabezpieczeń. Obecna wersja projektu nie przewiduje takiej możliwości. W poprzednim projekcie, wpływ oceny ryzyka na dostawcę był następujący: r Decyzja o umiarkowanym lub niskim ryzyku pozwalała dostawcy na przedstawienie środków zaradczych i planu naprawczego, co mogło skutkować zmianą oceny. Decyzja o wysokim ryzyku dawała dostawcy prawo do odwołania się, które musiało być rozpatrzone przez odpowiednie Kolegium. Dodatkowo, w przypadku pojawienia się nowych okoliczności, istniała możliwość złożenia wniosku o zmianę oceny ryzyka. Regulacje dotyczące procedury uznania dostawcy za DWR powinny uwzględniać specyfikę działania poszczególnych sektorów, w tym zróżnicowany czas na przeprowadzenie procedur, aby uniknąć destabilizacji całego sektora. W obecnym projekcie, decyzje Ministra nie biorą pod uwagę środków bezpieczeństwa, które dostawca wdrożył lub planuje wdrożyć w celu zmniejszenia ryzyka. Taka sytuacja jest nieakceptowalna i stoi w sprzeczności z celem dyrektywy NIS2, którym jest podnoszenie poziomu cyberbezpieczeństwa, między innymi poprzez wymogi dotyczące środków cyberbezpieczeństwa i certyfikacji. Ignorowanie możliwości zmniejszenia ryzyka przez dostawcę poprzez wysoki standard bezpieczeństwa produktów prowadzi do arbitralności decyzji. W skrajnych przypadkach, taka decyzja może być wykorzystywana jako narzędzie politycznego nacisku.e Rozszerzenie zakresu procedury poza UE Warto również przypomnieć, że w 5G Toolbox mowa jest jedynie o państwie spoza UE, natomiast w Nowelizacji dodano również kryterium państwa spoza NATO, co jest zdecydowanie nadregulacją w stosunku do 5G Toolboxa (art. 67a ust. 11 Nowelizacji). Model zaprojektowany na poziomie UE obejmuje analizę ryzyka dostawcy z perspektywy łańcucha dostaw na poziomie UE. Polski model jest w tym zakresie znacznie bardziej restrykcyjny z dwóch powodów. Po pierwsze model polski wymusza analizę na poziomie krajowym co odbiega od metodologii przewidzianej w treści NIS2 i w projektach innych państw członkowskich. Po drugie, dodanie wzmianki o NATO rozszerza zakres tej oceny na globalny łańcuch dostaw. Jest to całkowite zaprzeczenie sensu procedury skoordynowanej oceny ryzyka na poziomie UE i może prowadzić do nadregulacji przez konieczność uwzględniania interesów państw spoza UE w krajowej procedurze administracyjnej. Koncentracja uprawnień po stronie Ministra Cyfryzacji W obecnym modelu decyzja Ministra Cyfryzacji w sprawie uznania dostawcy za DWR może być orzeczona w ramach każdego sektora. Oznacza to, że o krytyczności sprzętu w danym sektorze będzie orzekał jeden minister, często niezwiązany z tym sektorem. Przeanalizowanie rzeczywistego nakładu pracy nałożonej na Ministra Cyfryzacji poprzez art. 67b Nowelizacji dobrze obrazuje zestawienie przedstawiające katalog i	

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

		wolumen podmiotów objętych nowymi przepisami. Na tym tle rysuje się szereg obaw, które wiążą się z tak daleko idącą centralizacją uprawnień.mProblem centralizacji procesu podejmowania decyzji Obecny model centralizuje decyzję o uznaniu danego podmiotu za DWR w rękach jednego ministra. Ministerstwo Cyfryzacji nie posiada wystarczających zasobów lub specjalistycznej wiedzy na temat każdego sektora. W rezultacie wydane prowadzona ocena ryzyka może być chybiona, a wydawane decyzje - nietrafne. Przepisy wprowadzie przewidują wsparcie Kolegium ds. cyberbezpieczeństwa w procesie decyzyjnym, w którym mają sprawować funkcje przedstawiciele organów sektorowych, lecz będzie to organ doradczy, którego zalecePrzepisy wprowadzie przewidują wsparcie Kolegium ds. cyberbezpieczeństwa w procesie decyzyjnym, w którym mają sprawować funkcje przedstawiciele organów sektorowych, lecz będzie to organ doradczy, którego zalecenia nie będą wiążące. Brak obowiązku stosowania się do rekomendacji Kolegium ogranicza skuteczność tego mechanizmu w zapewnianiu, że decyzje są gruntownie analizowane i oparte na solidnych danych sektorowych.e Brak gwarancji reprezentacji organów sektorowych w składzie wydającym opinięZgodnie z projektowanymi rozwiązaniami, skład zespołu opracowującego projekt opinii jest determinowany przez przewodniczącego Kolegium, bez gwarancji, że w jego składzie znajdą się przedstawiciele organów właściwych dla sektorów, które zostaną szczególnie dotknięte skutkami wydanej decyzji. W rezultacie opinia wydawana przez Kolegium nie musi uwzględniać wiedzy specjalistycznej dotyczącej specyficznych aspektów sektorowych. Ponadto fakt wyboru członków Kolegium przez przewodniczącego niesie za sobą ryzyko potencjalnego wpływu na ich bezstronność przy wydawaniu opinii.e Niespójność w uprawnieniach organów w ramach różnych procesów decyzyjnych. Zgodnie z projektowanymi rozwiązaniami, skład zespołu opracowującego projekt opinii jest determinowany przez przewodniczącego Kolegium, bez gwarancji, że w jego składzie znajdą się przedstawiciele organów właściwych dla sektorów, które zostaną szczególnie dotknięte skutkami wydanej decyzji. W rezultacie opinia wydawana przez Kolegium nie musi uwzględniać wiedzy specjalistycznej dotyczącej specyficznych aspektów sektorowych. Ponadto fakt wyboru członków Kolegium przez przewodniczącego niesie za sobą ryzyko pNowelizacja rezerwuje dla Ministra Cyfryzacji możliwość wydania decyzji o uznaniu dostawcy za dostawcę wysokiego ryzykav podczas gdy pozostawia władztwo właściwym dla danego sektora (nie zawsze organem właściwym będzie Minister Cyfryzacji) w innych aspektach (np. przy wydaniu decyzji o nałożeniu kary). Takie podejście jest pozbawione uzasadnienia i rodzi ryzyko podejmowania działań organów wobec tego samego podmiotu, bez ich wcześniejszej koordynacji. Ograniczenie możliwości włączenia podmiotów trzecich w postępowanie. W obecnym kształcie proces uznawania danego podmiotu za DWR nie pozwala na uczestnictwo w procesie interesariuszy spoza sektora telekomunikacyjnego. Takie ograniczenie jest niezasadne w świetle rozszerzenia skutków tej procedury na pozostałe sektory. W sytuacji, w której procedura uznania za DWR będzie prowadzona wobec dostawcy świadczącego usługi w innym sektorze np. energetyki, powinna istnieć możliwość przyłączenia się do postępowania podmiotu reprezentującego interesy sektora, w celu	

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			uwzględnienia jego specyfiki. Centralizacja procesu decyzyjnego w rękach Ministra Cyfryzacji dla całej gospodarki zwiększa ryzyko opóźnień i braku elastyczności, ograniczając zdolność do szybkiego reagowania na zmieniające się zagrożenia. Decydowanie przez pojedyncze ministerstwo, bez wsparcia zróżnicowanych perspektyw ekspertów z różnych dziedzin, może nie adekwatnie odzwierciedlać złożone i dynamiczne zagrożenia związane z różnorodnymi technologiami. Takie podejście może również prowadzić do braku przejrzystości i obiektywizmu w decyzjach krytycznych dla bezpieczeństwa narodowego. Ustawa, poprzez swoją nieprecyzyjność i ogólność, może otwierać drogę do arbitralnych lub błędnych decyzji administracyjnych, negatywnie wpływając na zaufanie do rynku ICT w Polsce i wprowadzając brak pewności prawa wśród przedsiębiorców.	
46.	Sobiesław Zasada Spółka Akcyjna S.K.A.	Art. 67b	Projekt nie uwzględnia szczegółowych kryteriów, jakie musiałby spełnić podmiot, aby został zakwalifikowany jako Dostawca Wysokiego Ryzyka. Zwrócić należy uwagę, iż bez katalogu enumeratywnie wskazanych przesłanek podmioty gospodarcze będą zmuszone do prowadzenia działalności w warunkach niepewności prawa i działalności gospodarczej w kraju. Podmioty gospodarcze nie będą miały świadomości z jakim podmiotem nawiązać współpracę, a z jakim zerwać. Brak ustawowych kryteriów kwalifikacji podmiotu jako dostawcy wysokiego ryzyka spowoduje szereg zagrożeń dla krajowego obrotu gospodarczego. Dokonywanie oceny czy dany podmiot jest dostawcą wysokiego ryzyka, powinno odbywać się na podstawie ustawowych, jasnych kryteriów uwzględniających ochronę własności prywatnej, jak i bezpieczeństwo państwa i obywateli. Wykluczenie konkretnego podmiotu z obrotu gospodarczego kwalifikując go jako dostawcę wysokiego ryzyka, spowoduje, że wiele podmiotów będzie zmuszonych do zakończenia projektów, bądź też do zmiany dostawcy kluczowych komponentów, co będzie generowało konieczność zmiany projektów, rozwiązań technologicznych, licencji, a w konsekwencji poniesienie ogromnych nakładów finansowych.	Uwaga wyjaśniona Zgodnie propozycją dostawcą wysokiego ryzyka jest dostawca sprzętu i oprogramowania, który stwarza poważne zagrożenie dla bezpieczeństwa państwa, obronności, bezpieczeństwa i porządku publicznego lub zdrowia i życia ludzi. Przesłanki są wskazane w przepisie.
47.	Konfederacja Lewiatan	Art. 67b	Przegląd decyzji HRV Jednostka redakcyjna: Art. 67b Postulujemy, aby wprowadzić zasadę cyklicznego przeglądu wydanych decyzji dot. dostawcy wysokiego ryzyka. Przykłady takiego podejścia podano w samym załączniku nr do OSR, gdzie przywołano taką instytucję funkcjonującą w Słowenii (przegląd co 2 lata). Także w przypadku Wielkiej Brytanii wskazano, że <i>Designated vendor directions mają być przeglądane, co jakiś czas</i> . Kwestia ta wydaje się bardzo ważna, z uwagi na bardzo doniosłe skutki wydania decyzji HRV, a także dynamikę zmian technicznych i poza-technicznych mogących skutkować zmianą okoliczności będących podstawą do wydania pierwotnej decyzji.	Uwaga wyjaśniona Zgodnie z art. 161 KPA minister może uchylić lub zmienić w niezbędnym zakresie każdą decyzję ostateczną, jeżeli w inny sposób nie można usunąć stanu zagrażającego życiu lub zdrowiu ludzkiemu albo zapobiec poważnym szkodom dla gospodarki narodowej lub dla ważnych interesów Państwa. W ocenie projektodawcy ten przepis spełnia rolę, o której mowa w uwadze – minister będzie mógł zawsze uchylić decyzję HRV, jeżeli zostaną spełnione przesłanki z art. 161 KPA. Innymi słowy minister będzie aktywnie monitorował, czy zachodzą przesłanki do uruchomienia art. 161 KPA i

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

				wobec tego dodawanie odrębnego przepisu nie jest konieczne ani celowe.
48.	Konfederacja Lewiatan	Art. 67b	Notyfikacja techniczna Jednostka redakcyjna: Art. 67b Wyjaśnienia wymaga wyrażone w uzasadnieniu utrzymanie założenia dot. braku uzasadnienia dla dokonania notyfikacji technicznej w zakresie przepisów wprowadzających możliwość uznania danego dostawcy za dostawcę wysokiego ryzyka. Zauważamy, że w biegu prac nad poprzednią nowelizacją uznawano taką potrzebę, a dopiero na finalnym etapie podejście to zostało zmodyfikowane bez przedstawienia szerszego uzasadnienia. Z uwagi na doniosłość projektowanych przepisów uważamy, że kwestia ta powinna zostać w pełni wyjaśniona, szczególnie, że odnotowaliśmy, że część krajów UE takich notyfikacji dokonywała, w tym: Belgia, Estonia, Finlandia, Francja, Hiszpania, Słowenia. Wnosimy więc uzupełnienie uzasadnienia o wskazanie przyczyn uznania braku zasadności notyfikacji.	Uwaga uwzględniona Uzasadnienie zostanie uzupełnione w tym zakresie.
49.	Konfederacja Lewiatan	Art. 67b	Podmioty, do których może być kierowana decyzja HRV Jednostka redakcyjna: Art. 67b ust. 1 Według projektu skutki decyzji dot. dostawcy wysokiego ryzyka mogą zostać skierowane do podmiotów kluczowych lub ważnych, z wyłączeniem podsektora komunikacji elektronicznej lub do przedsiębiorców telekomunikacyjnych. W ten sposób precyzyjnie wyłączone zostały <i>podmioty świadczące usługę komunikacji interpersonalnej niewykorzystującej numerów</i>, które należą do podsektora komunikacji elektronicznej, ale mogą nie być przedsiębiorcami telekomunikacyjnymi. Uzasadnienie nie odnosi się do tego czy jest to zabieg celowy i z jakich wynika przesłanek. Należy więc wprost przesądzić o objęciu wszystkich podmiotów podsektora komunikacji elektronicznej potencjalnymi skutkami wydania decyzji dot. dostawcy wysokiego ryzyka.	Uwaga uwzględniona Podmioty świadczące usługę komunikacji interpersonalnej niewykorzystującej numerów także będą musiały wycofać sprzęt od dostawcy wysokiego ryzyka.
50.	Związek Pracodawców Technologii Cyfrowych Lewiatan	Art. 67b	Stanowisko co do dostawcy wysokiego ryzyka (art. 67b ust. 9) Wskazana została Izba Gospodarcza jako strona, która przedstawia stanowisko co do dostawcy. Członkostwo w samorządzie gospodarczym nie jest w Polsce obowiązkowe, choć oczywiście jest odpłatne, stąd potrzeba rozszerzenia katalogu podmiotów, które mogą przedstawiać takie stanowiska. Postulujemy, aby podmiot składający takie stanowisko powinien ujawnić ministrowie właściwemu ds. informatyzacji wszelkie przychody jakie otrzymał od dostawcy w ciągu ostatnich trzech lat. Informacja ta stanowi tajemnicę handlową. Postulujemy by warunek ujawnienia relacji pomiędzy dostawcą a podmiotem powinien pojawić się w zapisach ustawy.	Uwaga częściowo uwzględniona Stanowisko w ramach postępowania będą mogły wnieść organizacje społeczne, nie tylko izby gospodarcze.
51.	Polskie Stowarzyszenie Fotowoltaiki	Art. 67b-67f	Uznanie dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Projekt zakłada wprowadzenie procedury uznania dostawcy sprzętu lub oprogramowania wykorzystywanego przez PK, PW (z wyłączeniem podsektora komunikacji elektronicznej) oraz niektórych przedsiębiorców telekomunikacyjnych jako dostawcy wysokiego ryzyka. W przypadku dostawców spoza UE, Szwajcarii, EOG, zawiadomienie o wszczęciu postępowania dokonywane jest poprzez publikację w BIP. Po wszczęciu postępowania, izba gospodarcza ma 14 dni od publikacji informacji o wszczęciu postępowania w BIP na wydanie opinii o danym dostawcy oraz dostarczanych przez niego produktów ICT,	Uwaga wyjaśniona Postępowanie w sprawie uznania za dostawcę wysokiego ryzyka ma na celu zabezpieczenie polskiej gospodarki i polskiego społeczeństwa przed dostawcą sprzętu lub oprogramowania, który stwarza poważne zagrożenie dla bezpieczeństwa

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

		usług ICT oraz procesów ICT. Przed wydaniem decyzji o uznaniu za dostawcę wysokiego ryzyka, minister właściwy ds. informatyzacji zasięga opinii Kolegium w rozumieniu Projektu zawierającą analizę dostawcy oraz dostarczanych przez niego produktów ICT, usług ICT oraz procesów ICT. Postanowienia Projektu dot. ww. opinii nie przewidują udziału dostawcy. W oparciu o ww. opinię, minister właściwy ds. Informatyzacji wydaje decyzję o uznaniu za dostawcę wysokiego ryzyka, jeżeli dostawca ten stanowi poważne zagrożenie dla obronności, bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego, lub życia i zdrowia ludzi. Decyzja zawiera wskazanie typów produktów ICT, rodzajów usług ICT lub konkretnych procesów ICT pochodzących od dostawcy wysokiego ryzyka oraz podlega natychmiastowemu wykonaniu. Od decyzji nie przysługuje wniosek o ponowne rozpatrzenie sprawy. Skutki decyzji o uznaniu za dostawcę wysokiego ryzyka - zakaz wprowadzania do użytkowania; - obowiązek wycofania z użytkowania w terminie 7 lat od dnia ogłoszenia decyzji (lub 4 lat w odniesieniu do krytycznych ICT określonych w załączniku nr 3 do Projektu); przez PK, PW (z wyłączeniem podsektora komunikacji elektronicznej) oraz niektórych przedsiębiorców telekomunikacyjnych typów produktów ICT, rodzajów usług ICT lub konkretnych procesów ICT objętych decyzją. Do czasu wycofania możliwe będzie korzystanie z objętego decyzją produktu ICT, usługi ICT lub procesu ICT jedynie w niezbędnym zakresie dla zapewnienia odpowiedniej jakości i ciągłości świadczonych usług (ust. 3) Zakaz nabywania produktu ICT, usługi ICT lub procesu ICT objętego decyzją o uznaniu za dostawcę wysokiego ryzyka w ramach publicznych zamówień (ust. 4). Produkt ICT, usługa ICT lub proces ICT nabyte w ramach publicznych zamówień przed wydaniem decyzji mogą być wykorzystywane przez okres 7 lat (lub 5 lat w odniesieniu do ICT wykorzystywanych do wykonywania funkcji krytycznych określonych w załączniku nr 3 do KSC wg Projektu (ust. 5)). Obowiązek informowania przez PK i PW o wycofaniu produktu ICT, usługi ICT lub procesu ICT objętych decyzją na wniosek organów właściwych ds. cyberbezpieczeństwa (art. 67d ust. 1 KSC wg Projektu). Ogólny wpływ regulacji: Jednym z najważniejszych wyzwań nowego Projektu będzie dla PW i PK obowiązek wymiany sprzętu i rezygnacja z usług dostawców wysokiego ryzyka. O tym, jaki podmiot spełnia kryteria uznania za dostawcę wysokiego ryzyka będzie decydował minister właściwy do spraw informatyzacji, zgodnie z projektowanym art. 67b ust. 1 KSC wg Projektu, w drodze decyzji administracyjnej. Wskazane w decyzji zakresy produktów ICT, rodzaje usług ICT lub konkretne procesy ICT pochodzące od dostawcy wysokiego ryzyka, będą musiały być wycofane z tych podmiotów. Termin wycofania sprzętu lub oprogramowania ICT objętego decyzją o uznaniu za dostawcę wysokiego ryzyka jest niewspółmierny względem nakładów finansowych ponoszonych na ich nabycie i wynosi zgodnie z Projektem 7 lub 4 lata. Wpływ na sektor energetyczny:	państwa, obronności, bezpieczeństwa i porządku publicznego lub zdrowia i życia ludzi. W ramach postępowania administracyjnego będą brane pod uwagę zarówno aspekty techniczne związane z dostarczaniem przez dostawcę sprzętem i oprogramowaniem jak również aspekty nietechniczne związane z dostawcą. Dzięki temu zostanie zidentyfikowany pełen obraz zagrożeń jakie stwarza dostawca sprzętu lub oprogramowania. Postępowanie umożliwia badanie dostawcy sprzętu lub oprogramowania dla wszystkich sektorów gospodarki wskazanych w ustawie. Jest to wskazane z uwagi na to, że każdy podmiot kluczowy i podmiot ważny musi dbać o bezpieczeństwo łańcuchów dostaw. Podmioty kluczowe i podmioty ważne mają istotny charakter dla funkcjonowania współczesnej gospodarki i społeczeństwa informacyjnego. Zakłócenie funkcjonowania tych podmiotów poprzez atak przez łańcuch dostaw może spowodować niepowetowane straty. Z uwagi na charakter tego postępowania wyłączono część przepisów KPA. Przede wszystkim nie jest możliwe przeprowadzenie postępowania administracyjnego przy udziale wszystkich podmiotów, które wykorzystują sprzęt lub oprogramowanie pochodzące od danego dostawcy. Rygor natychmiastowej wykonalności jest konieczny z uwagi na to, że kwestia dotyczy poważnego zagrożenia dla bezpieczeństwa państwa. Nie przewiduje się rekompensat za wycofanie sprzętu lub oprogramowania, ponieważ ten sprzęt i tak z czasem podlegałby wymianie z uwagi na naturalne

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

		W nawiązaniu do uwag ogólnych wskazanych powyżej, w pierwszej kolejności należy wskazać, że produkty ICT oraz usługi ICT odgrywają kluczową rolę w sektorze energetycznym. Jako jeden z podstawowych przykładów można wskazać chociażby Smart Metering – rozwiązania wykorzystywane w ramach inteligentnych systemów opomiarowania pozwalają na dokonywanie dokładnych wyliczeń związanych chociażby z krajowym zapotrzebowaniem na energię, a w konsekwencji umożliwiają ograniczenie strat w tym zakresie. Cały system elektroenergetyczny opiera się na wykorzystywaniu inteligentnych rozwiązań, począwszy od paneli fotowoltaicznych, a na sieci elektroenergetycznej kończąc, dlatego przyznanie ministrowi ds. informatyzacji wyłącznej kompetencji do uznania poszczególnych producentów oraz usługodawców produktów ICT, usług ICT oraz procesów ICT za dostawców wysokiego ryzyka będzie miało negatywny wpływ na prowadzenie działalności gospodarczej przez podmioty z sektora energetycznego. Po pierwsze, przedsiębiorstwa energetyczne będą musiały znaleźć nowych dostawców w stosunkowo krótkim terminie (co zostało szerzej opisane poniżej). Po drugie, spowoduje to znaczące straty finansowe po stronie sektora w związku z koniecznością wymiany całego sprzętu zakupionego od dostawców wysokiego ryzyka i poniesienia kosztów wymiany, co zwiększy koszty działalności gospodarczej. Po trzecie, uznanie poszczególnych podmiotów za dostawców wysokiego ryzyka będzie pośrednio oddziaływać także na obciążenie dostawców, którzy nie zostali zaliczeni do grupy dostawców wysokiego ryzyka, co również wpłynie na szybkość i płynność dokonywania zmiany dostawcy. Zwracamy również uwagę, że z uwagi na nieprecyzyjne kryteria uznania określonych podmiotów za dostawców wysokiego ryzyka, na dzień dzisiejszy trudno jednoznacznie określić, jakie podmioty mogłyby zostać za takich dostawców uznane, i w konsekwencji brak jest możliwości zabezpieczenia się przed konsekwencjami projektowanej regulacji. Terminy wycofania sprzętu lub oprogramowania ICT objętego decyzją o uznaniu za dostawcę wysokiego ryzyka są nie niewspółmierne do okresu użytkowania oraz standardów sektora energetycznego. W przypadku wielu środków trwałych wykorzystywanych w sektorze energetyki, okres ich amortyzacji może wynosić do 15 lat (przykładowo środki trwałe wskazane w pozycji 3 w Wykazie rocznych stawek amortyzacyjnych na gruncie Ustawy z dnia 15 lutego 1992 r. o podatku dochodowym od osób prawnych. W efekcie, podmioty zobowiązanie będą zobowiązane dowycofania produktów przy jednoczesnym poniesieniu dodatkowych kosztów związanych z ich nabyciem. Nadregulacja względem Dyrektywy NIS2 Proponowana regulacja nie znajduje jakiegokolwiek podstawy w Dyrektywie NIS2 i stanowi nadregulację względem wymogów jakie państwa członkowskie powinny spełnić w celu jej wdrożenia. Niezależnie, proponowane przepisy dotyczące uznawania dostawców dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka opierają się na postulatach wypracowanych na poziomie unijnym w ramach Toolbox 5G. Niemniej, celem oraz zakresem zastosowania Toolbox 5G jest zapewnienie bezpiecznego rozwoju sieci 5G oraz wykorzystywanych w tym celu produktów i usług ICT. Tymczasem, proponowane w Projekcie regulacje dotyczą nie tylko oprogramowania i sprzętu wykorzystywanego w tym celu, ale również wszelkich innych systemów informacyjnych wykorzystywanych przez m.in. PK i PW. Proponowana regulacja wykracza zatem znacząco poza zakres przedmiotowy wynikający z Toolbox 5G. W	zużycie. Termin 7 lat na wycofanie sprzętu wydaje się terminem adekwatnym. Jednocześnie skrócono ten termin do 4 lat dla sprzętu i oprogramowania realizującego funkcje krytyczne w zakresie bezpieczeństwa sieci i usług. Wycofanie sprzętu/oprogramowania pochodzącego od dostawcy wysokiego ryzyka w terminie 4 lat dla przedsiębiorców telekomunikacyjnych jest zasadne z uwagi na to, że chodzi o funkcje krytyczne dla sieci i usług. Zauważyć należy, że sprzęt i oprogramowanie i tak wymagałby okresowej wymianie z uwagi na naturalne zużycie sprzętu. Sieć 4g też będzie z czasem wycofywana.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			efekcie, konieczne jest właściwe wypracowanie listy funkcji krytycznych infrastruktury z uwzględnieniem specyfiki każdej branży i stopnia ryzyka dla poszczególnych podmiotów. Co istotne, już sama publikacja informacji o samym wszczęciu postępowania w sprawie uznania za dostawcę wysokiego ryzyka może skutkować negatywnym odbiorem przez kontrahentów. Wobec tego rekomendowane jest usunięcie obowiązku publikacji tej informacji w BIP. Dodatkowo, przepis przewiduje możliwość przedstawienia stanowiska co do dostawcy sprzętu lub oprogramowania, wobec którego wszczęto postępowanie w sprawie uznania za dostawcę wysokiego ryzyka przez izbę gospodarczą. Brak jednak w Projekcie definicji tego pojęcia. Na marginesie wskazujemy, że treść proponowanych w Projekcie art. 67b – 67f w nieznacznym sposób różni się od treści odpowiednich postanowień Projektu z 3 lipca 2023 r., które spotkały się z szeroką krytyką przedstawicieli rynku. Rekomendacje: - wycofanie w całości przepisów dot. uznania za dostawcę wysokiego ryzyka z Projektu i pozostawienie możliwości uznania produktu ICT, usługi ICT lub procesu ICT za generujące istotne ryzyko podmiotom podlegającym pod KSC, tj. PW i PK, na gruncie szacowania ryzyka wykonywanego przez same PW i PK, opartego na konkretnych kryteriach o charakterze technicznym. Alternatywnie: - wydłużenie okresu na wycofanie z użytkowania ICT objętych decyzją; - ograniczenie możliwości publikacji informacji o wszczęciu postępowania w sprawie uznania za dostawcę wysokiego ryzyka; - zwiększenie udziału zainteresowanych podmiotów (PK, PW, dostawców) w postępowaniu w sprawie uznania za dostawcę wysokiego ryzyka przed wydaniem decyzji; - określenie precyzyjnych i niedyskryminujących kryteriów oceny uznania za dostawcę wysokiego ryzyka.	
52.	Polska Izba Informatyki i Telekomunikacji	Art. 67c	Art. 67c ust. 2 – termin na wycofanie produktów ICT, rodzajów usług ICT, konkretnych procesów ICT wskazanych w decyzji HRV Zasadniczym terminem na wycofanie zasobów wskazanych w decyzji jest 7 lat. Obowiązywał będzie on wszystkie podmioty z najbardziej krytycznych sektorów krajowej gospodarki, w tym z sektorów energetyki czy transportu. Termin ten został uznany za adekwatny i właściwy, także w świetle ich podstawowego wręcz znaczenia dla bezpieczeństwa państwa i usług niezbędnych do funkcjonowania firm i obywateli. Jednocześnie warto zauważyć, że dotyczył on będzie podmiotów w dużej mierze będących własnością lub współwłasnością Skarbu Państwa. Jednocześnie wyłącznie wobec przedsiębiorców telekomunikacyjnych – i to tylko tych wdrażających sieć 5G – zdecydowano o wprowadzeniu terminu istotnie krótszego, tj. 4-letniego. Skrócono więc nawet dotychczas projektowany termin mający wynieść 5 lat. W uzasadnieniu wskazano jedynie, że „<i>Takie skrócenie okresu na wycofanie jest spowodowane szczególnym znaczeniem dla bezpieczeństwa państwa usług telekomunikacyjnych, szczególnie sprzętu lub oprogramowania wykorzystywanych do realizowania funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku nr 3 do ustawy.</i>”. Z drugiej	Uwaga wyjaśniona i częściowo uwzględniona Wycofanie sprzętu/oprogramowania pochodzącego od dostawcy wysokiego ryzyka w terminie 4 lat dla przedsiębiorców telekomunikacyjnych jest zasadne z uwagi na to, że chodzi o funkcje krytyczne dla sieci i usług. Zauważyć należy, że sprzęt i oprogramowanie i tak wymagałyby okresowej wymiany z uwagi na naturalne zużycie sprzętu. Sieć 4g też będzie z czasem wycofywana.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

		jednak strony (na str. 71 uzasadnienia) dokonano już bardziej racjonalnej (niż wynika to z samego projektu) oceny wskazując następująco: <i>W proponowanych przepisach jest mowa o 5–7 latach – termin ten jest często uznawany za średni okres użytkowania sprzętu lub oprogramowania, czyli tzw. cykl życia urządzenia. Raport BEREC wskazuje, że w przypadku sprzętu 5G wykorzystywanego w radiowej sieci dostępowej (RAN) cykl życia urządzenia wynosi w większości przypadku od 5 do 10 lat.</i> Wobec pozostałych podmiotów – których usługi są w naszej ocenie są co najmniej tak samo istotne jak sieć 5G – wskazano: <i>Będzie więc musiał wycofać go w terminie 7 lat. Jest to związane z tym, że natychmiastowe wycofanie produktów ICT, usług ICT lub procesów ICT mogłoby być niemożliwe w praktyce, gdyż mogłoby spowodować zaprzestanie świadczenia usług.</i> Nie jest dla nas zrozumiałe tak daleko idące zróżnicowanie oceny dot. możliwości dokonania wymiany oraz ryzyka zaprzestania świadczenia usług. Już z samego tego względu - w pierwszej kolejności - wnosimy o równe traktowanie różnych podmiotów w takich samych sytuacjach faktycznych - poprzez określenie identycznych terminów wycofania zasobów wskazanych w decyzji. Dalej – odnosząc się już wprost do terminu 4-letniego wskazujemy, że będzie to czas zbyt krótki na dokonanie wymiany. Wynika to ze względów technicznych, organizacyjnych, a także samego rynku usług i dostaw. Wskazujemy, że w przypadku dużych przedsiębiorców telekomunikacyjnych, skutki wydania decyzji HRV wpłyną bardzo istotnie na strategiczne i kluczowe procesy funkcjonowania tych podmiotów, włączając w to wygenerowanie ryzyka dotyczącego ciągłości świadczenia usług telekomunikacyjnych. Wskazujemy dodatkowo, że okres amortyzacji, jaki jest przyjmowany dla urządzeń sieciowych wynosi przeważnie 10 lat. W zakres zasobów objętych potencjalnymi decyzjami może wejść zarówno obszar sieci radiowej oraz sieci rdzeniowej. Nie mając wiedzy o tym, którzy dostawcy mogliby zostać objęci decyzjami, musimy wskazać, że potencjalnie decyzje mogłoby obejmować tysiące obiektów w całym kraju. Niezbędne do wykonania prace obejmowałyby m.in. prace instalacyjne wymagające wyspecjalizowanych podwykonawców robót telekomunikacyjnych. Szacujemy, że sama ta kwestia będzie problematyczna, szczególnie uwzględniając, że w najbliższych latach spodziewamy się ogromnego obciążenia podwykonawców realizacją projektów inwestycyjnych z udziałem środków Krajowego Planu Odbudowy i programu Fundusze Europejskie na Rozwój Cyfrowy o łącznej wartości ponad 10 mld zł. Istotne w tym zakresie jest, że w tak krótkim czasie łańcuch dostaw może okazać się niewydolny do zrealizowania tego wymogu na racjonalnych warunkach – szczególnie jeśli zakres decyzji obejmowałby istotną część takich zasobów. Jakikolwiek ograniczenia występujące w tym względzie – niezależnie od ich uzasadnienia – będą negatywnie oddziaływały przede wszystkim na przedsiębiorców telekomunikacyjnych oraz ich ryzyko poniesienia wysokich kar finansowych z tytułu naruszenia ustawowego terminu wymiany. Z perspektywy przedsiębiorców telekomunikacyjnych zobowiązanych do dokonania wymiany w nieprzekraczalnym terminie 4 lat będzie to miało ogromny wpływ na faktyczne warunki prowadzenia procedur zakupowych i potencjalne zaburzenia możliwości negocjacyjnych wobec wykonawców i dostawców. Będzie to miało szczególne znaczenie w warunkach już teraz istniejącego ograniczonego poziomu konkurencji. Liczymy, że przewidziany w nowym projekcie ustawy udział Prezesa UOKiK w procesie wydawania opinii Kolegium będzie zapewniał dogłębne zbadane także tego obszaru, jeszcze przed	Odesłanie w art. 67c ust. 3 zostanie poprawione.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

		wydaniem decyzji. Powyższe okoliczności będą z kolei miały niebagatelny wpływ na koszty przeprowadzenia ewentualnej wymiany, które będą musiały zostać potencjalnie poniesione przez przedsiębiorców telekomunikacyjnych. Warto w tym miejscu odnotować, że już teraz trwają kosztowne inwestycje związane z realizacją zobowiązań inwestycyjnych w ramach rezerwacji pasma C, a także szerokie inwestycje w sieci VHCN, w tym wspierane ze środków unijnych. W tych okolicznościach, uważamy, że ustalane teraz warunki dokonywania ew. wymiany powinny szeroko uwzględniać niemożliwe do uniknięcia skutki dla kondycji sektora telekomunikacyjnego, świadczącego przecież usługi dla szerokiego grona odbiorców. Podsumowując, przeprowadzenie (po wydaniu decyzji) na dużą skalę szeregu procesów w ramach międzynarodowego łańcucha dostaw obejmujących m.in. procedury przetargowe, zakupowe, produkcję, demontaż, instalację, integrację i uruchomienie wielu tysięcy specjalistycznych urządzeń rozproszonych w całym kraju może nie być możliwe do zrealizowania w okresie zaledwie 4 lat, szczególnie biorąc pod uwagę niewielką dostawców alternatywnych, którzy w tym okresie zapewne spotkają się ze zwiększonym popytem ze strony rynku i wydłużonymi terminami dostaw. Wreszcie musimy również wskazać na - zapewne znane Ministerstwu Cyfryzacji - doświadczenia z innych krajów gdzie wprowadzone zostały nakazy wymiany określonych zasobów sieciowych. W Wielkiej Brytanii termin na wymianę urządzeń w sieci rdzeniowej został przesunięty o niemal rok, a i tak okazał się nierealizowalny dla największego operatora³. W Stanach Zjednoczonych, istotnych opóźnień doznaje także program wymiany zasobów „lokalnych operatorów”, w którym zabrakło publicznych środków finansujących zmiany w sieciach⁴. Może to – wg FCC – grozić upadkiem niektórych firm telekomunikacyjnych oraz niewystarczającym zasięgiem sieci na części obszarów. W naszej ocenie pokazuje to jak ważne jest, aby warunki wykonywania ewentualnych decyzji były proporcjonalne i szeroko uwzględniające warunki rynkowe. Szczególnie, że projekt ustawy nie przewiduje żadnych form rekompensaty w tym zakresie. Podsumowując, wnosimy o: W pierwszej kolejności o wprowadzenie dla wszystkich podmiotów jednolitego terminu wycofania wynoszącego 7 lat. W drugiej kolejności o przywrócenie brzmienia poprzednich wersji projektu, tj. wprowadzenie terminu 5-letniego dla zasobów z załącznika nr 3. W obu powyższych wypadkach o wprowadzenie wyraźnej procedury umożliwiającej podmiotowi obowiązkanemu do wymiany złożenie wniosku o wyrażenie przez Ministra zgody na przedłużenie terminu określonego w decyzji. Art. 67c ust. 3 – użytkowanie w czasie na wycofanie <i>3. Do czasu wycofania sprzętu lub oprogramowania, o którym mowa w ust. 1 pkt 2, dopuszcza się użytkowanie dotychczas posiadanych typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT (...)</i>	

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			W art. 67c ust. 3 zawarto błędne odwołanie do art. 67b ust. 1 pkt 2, który wskazuje: „2) wycofują z użytkowania typy produktów ICT, rodzaje usług ICT i konkretne procesy ICT w zakresie objętym decyzją dostarczanych przez dostawcę wysokiego ryzyka nie później niż 7 lat”. Może to sugerować, że jedynie zasoby podlegające wymianie w 7 lat mogą być użytkowane w okresie na wycofanie. Uzasadnienie projektu nie wskazuje na takie rozróżnienie, które byłoby jednocześnie skrajnie nieadekwatne i mogłoby skutkować koniecznością natychmiastowego przerwania działania usług. Dlatego niezbędne jest wprowadzenie poprawki w projekcie, która będzie zawierała odwołanie do wszystkich typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT niezależnie od okresu na ich wymianę. W przypadku utrzymania konstrukcji zawierającej odwołanie, powinno ono odnosić się zarówno do ust. 1 pkt 2, jak i do ust. 2.	
53.	Konfederacja Lewiatan	Art. 67c	Termin na wycofanie Jednostka redakcyjna: Art. 67c ust. 2 Zasadniczym terminem na wycofanie zasobów wskazanych w decyzji jest 7 lat. Obowiązywał będzie on wszystkie podmioty z najbardziej krytycznych sektorów krajowej gospodarki, w tym z sektorów energetyki czy transportu. Termin ten został uznany za adekwatny i właściwy, także w świetle ich podstawowego wręcz znaczenia dla bezpieczeństwa państwa i usług niezbędnych do funkcjonowania firm i obywateli. Jednocześnie warto zauważyć, że dotyczył on będzie podmiotów w dużej mierze będących własnością lub współwłasnością Skarbu Państwa. Jednocześnie, wyłącznie wobec przedsiębiorców telekomunikacyjnych – i to tylko tych wdrażających sieć 5G – zdecydowano o wprowadzeniu terminu istotnie krótszego, tj. 4letniego. Skrócono więc nawet dotychczas projektowany termin mający wynieść 5 lat. W uzasadnieniu wskazano jedynie, że <i>„Takie skrócenie okresu na wycofanie jest spowodowane szczególnym znaczeniem dla bezpieczeństwa państwa usług telekomunikacyjnych, szczególnie sprzętu lub oprogramowania wykorzystywanych do realizowania funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku nr 3 do ustawy.”</i>. Z drugiej jednak strony (na str. 71 uzasadnienia) dokonano już bardziej racjonalnej (niż wynika to z samego projektu) oceny wskazując następująco: <i>W proponowanych przepisach jest mowa o 5–7 latach – termin ten jest często uznawany za średni okres użytkowania sprzętu lub oprogramowania, czyli tzw. cykl życia urządzenia. Raport BEREC wskazuje, że w przypadku sprzętu 5G wykorzystywanego w radiowej sieci dostępowej (RAN) cykl życia urządzenia wynosi w większości przypadku od 5 do 10 lat.</i> Wobec pozostałych podmiotów – których usługi są w naszej ocenie są co najmniej tak samo istotne jak sieć 5G – wskazano: <i>Będzie więc musiał wycofać go w terminie 7 lat. Jest to związane z tym, że natychmiastowe wycofanie produktów ICT, usług ICT lub procesów ICT mogłoby być niemożliwe w praktyce, gdyż mogłoby spowodować zaprzestanie świadczenia usług.</i> Nie jest dla nas zrozumiałe tak daleko idące zróżnicowanie oceny dot. możliwości dokonania wymiany oraz ryzyka zaprzestania świadczenia usług. Już z samego tego względu - w pierwszej kolejności - wnosimy o równe traktowanie różnych podmiotów w takich samych sytuacjach faktycznych - poprzez określenie identycznych terminów wycofania zasobów wskazanych w decyzji. Dalej – odnosząc się już wprost do terminu 4-letniego wskazujemy, że będzie to czas zbyt krótki na dokonanie wymiany. Wynika to ze względów technicznych, organizacyjnych, a także samego rynku usług i dostaw.	Uwaga wyjaśniona Wycofanie sprzętu/oprogramowania pochodzącego od dostawcy wysokiego ryzyka w terminie 4 lat dla przedsiębiorców telekomunikacyjnych jest zasadne z uwagi na to, że chodzi o funkcje krytyczne dla sieci i usług. Zauważyć należy, że sprzęt i oprogramowanie i tak wymagały okresowej wymianie z uwagi na naturalne zużycie sprzętu. Sieć 4g też będzie z czasem wycofywana.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

		Wskazujemy, że w przypadku dużych przedsiębiorców telekomunikacyjnych, skutki wydania decyzji HRV wpłyną bardzo istotnie na strategiczne i kluczowe procesy funkcjonowania tych podmiotów, włączając w to wygenerowanie ryzyka dotyczącego ciągłości świadczenia usług telekomunikacyjnych. Wskazujemy dodatkowo, że okres amortyzacji, jaki jest przyjmowany dla urządzeń sieciowych wynosi przeważnie 10 lat. W zakres zasobów objętych potencjalnymi decyzjami może wejść zarówno obszar sieci radiowej oraz sieci rdzeniowej. Nie mając wiedzy o tym, którzy dostawcy mogliby zostać objęci decyzjami, musimy wskazać, że potencjalnie decyzje mogłyby obejmować tysiące obiektów w całym kraju. Niezbędne do wykonania prace obejmowałyby m.in. prace instalacyjne wymagające wyspecjalizowanych podwykonawców robót telekomunikacyjnych. Szacujemy, że sama ta kwestia będzie problematyczna, szczególnie uwzględniając, że w najbliższych latach spodziewamy się ogromnego obciążenia podwykonawców realizacją projektów inwestycyjnych z udziałem środków Krajowego Planu Odbudowy i programu Fundusze Europejskie na Rozwój Cyfrowy o łącznej wartości ponad 10 mld zł. Istotne w tym zakresie jest, że w tak krótkim czasie łańcuch dostaw może okazać się niewydolny do zrealizowania tego wymogu na racjonalnych warunkach – szczególnie jeśli zakres decyzji obejmowałby istotną część takich zasobów. Jakikolwiek ograniczenia występujące w tym względzie – niezależnie od ich uzasadniania – będą negatywnie oddziaływały przede wszystkim na przedsiębiorców telekomunikacyjnych oraz ich ryzyko poniesienia wysokich kar finansowych z tytułu naruszenia ustawowego terminu wymiany. Z perspektywy przedsiębiorców telekomunikacyjnych zobowiązanych do dokonania wymiany w nieprzekraczalnym terminie 4 lat będzie to miało ogromny wpływ na faktyczne warunki prowadzenia procedur zakupowych i potencjalne zaburzenia możliwości negocjacyjnych wobec wykonawców i dostawców. Będzie to miało szczególne znaczenie w warunkach już teraz istniejącego ograniczonego poziomu konkurencji. Liczymy, że przewidziany w nowym projekcie ustawy udział Prezesa UOKiK w procesie wydawania opinii Kolegium będzie zapewniał dogłębne zbadanie także tego obszaru, jeszcze przed wydaniem decyzji. Powyższe okoliczności będą z kolei miały niebagatelny wpływ na koszty przeprowadzenia ewentualnej wymiany, które będą musiały zostać potencjalnie poniesione przez przedsiębiorców telekomunikacyjnych. Warto w tym miejscu odnotować, że już teraz trwają kosztowne inwestycje związane z realizacją zobowiązań inwestycyjnych w ramach rezerwacji pasma C, a także szerokie inwestycje w sieci VHCN, w tym wspierane ze środków unijnych. W tych okolicznościach, uważamy, że ustalane teraz warunki dokonywania ew. wymiany powinny szeroko uwzględniać niemożliwe do uniknięcia skutki dla kondycji sektora telekomunikacyjnego, świadczącego przecież usługi dla szerokiego grona odbiorców. Podsumowując, przeprowadzenie (po wydaniu decyzji) na dużą skalę szeregu procesów w ramach międzynarodowego łańcucha dostaw obejmujących m.in. procedury przetargowe, zakupowe, produkcję, demontaż, instalację, integrację i uruchomienie wielu tysięcy specjalistycznych urządzeń rozproszonych w całym kraju może nie być możliwe do zrealizowania w okresie zaledwie 4 lat, szczególnie biorąc pod uwagę niewielką dostawców alternatywnych, którzy w tym okresie zapewne spotkają się ze zwiększonym popytem ze strony rynku i wydłużonymi terminami dostaw. Kwestią, która również zasługuje na uwzględnienie jest fakt, że projektowany w ustawie 4letni termin jest istotnie krótszy niż przewidziany w wydanych już decyzjach rezerwacyjnych dla pasma C, a rozpoczęcie	

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			jego biegu również jest różne na poziomie projektu ustawy oraz decyzji rezerwacyjnych. Wprowadzenie tak istotnego zaostreżenia na etapie po wydaniu decyzji rezerwacyjnych jest w naszej ocenie nieproporcjonalne i rodzi znaczące obiekcje wobec braku stabilności otoczenia prawno-regulacyjnego działalności telekomunikacyjnej. Wreszcie musimy również wskazać na - zapewne znane Ministerstwu Cyfryzacji - doświadczenia z innych krajów, gdzie wprowadzone zostały nakazy wymiany określonych zasobów sieciowych. W Wielkiej Brytanii termin na wymianę urządzeń w sieci rdzeniowej został przesunięty o niemal rok, a i tak okazał się nierealizowalny dla największego operatora⁷. W Stanach Zjednoczonych, istotnych opóźnień doznaje także program wymiany zasobów „lokalnych operatorów”, w którym zabrakło publicznych środków finansujących zmiany w sieciach⁷. Może to – wg FCC – grozić upadkiem niektórych firm telekomunikacyjnych oraz niewystarczającym zasięgiem sieci na części obszarów. W naszej ocenie pokazuje to jak ważne jest, aby warunki wykonywania ewentualnych decyzji były proporcjonalne i szeroko uwzględniające warunki rynkowe. Szczególnie, że projekt ustawy nie przewiduje żadnych form rekompensaty w tym zakresie. Podsumowując, wnosimy o: wprowadzenie dla wszystkich podmiotów jednolitego terminu wycofania wynoszącego 7 lat. Zarówno uzasadnienie do Projektu KSC jak i OSR nie wskazuje na podstawowy problem związany z Procedurą DWR dla podmiotów, których dotyczy Załącznik nr 3 do projektu, mianowicie nie zwrócono uwagi, że wymiana sprzętu dla sieci 5G wymaga wymiany sprzętu również dla 4G (wykorzystywana obecnie konfiguracja 5G non-standalone), nie tylko na tych samym lokalizacjach ale de facto w całej sieci. W konsekwencji jest to dużo bardziej złożony projekt niż budowa sieci 5G obejmujący wielokrotnie więcej lokalizacji fizycznych. Skala inżynierska projektu jest tak duża, że próba jego realizacji w ciągu 4 lat będzie ograniczona ze względu na brak dostępności wyspecjalizowanych ekip instalacyjnych (podkreślenia wymaga, że wymiany będą dokonywane przez kilku przedsiębiorców telko równolegle). Wymiana sprzętu zaś to uruchomienie bardzo dużego programu obejmującego nie jeden, ale co najmniej kilka projektów, dotyczących równolegle zmiany kilku systemów w tym samym czasie oraz dostosowanie pozostałych systemów do współpracy z nowym rozwiązaniem. Podkreślić, należy że ryzyko nie dotrzymania wskazanego w Projekcie KSC terminu z art. 67c może być całkowicie niezależne od przedsiębiorcy telekomunikacyjnego w sytuacji gdy, pozostali dostawcy oferujący dany typ rozwiązania (ilość ich jest również ograniczona), nie będą w stanie wywiązać się z zamówień od nowych klientów w określonym czasie.	
54.	Osoba fizyczna	Art. 67c	Art. 67c ust. 3 – Zastosowano zapisy warunkujące dopuszczenie użytkowania produktów ICT, usług ICT i procesów ICT dostawcy wysokiego ryzyka. Dopuszczenie użytkowania takiego rodzaju produktów ICT, usług ICT i procesów ICT przez 4 i 7 lat jest wyrażeniem zgody na wieloletnie narażenie systemów informacyjnych i usług oraz państwa naruszenie i utratę bezpieczeństwa o dużych skutkach, co jest niezrozumiałe w projektowaniu transsektorowego systemu bezpieczeństwa – cyberbezpieczeństwa.	Uwaga wyjaśniona Zgodnie z art. 8 podmioty kluczowe i podmioty ważne mają obowiązek dbać o bezpieczeństwo łańcuchów dostaw. W ramach tego obowiązku powinny podjąć

⁷⁾ <https://www.ft.com/content/54d46cf2-5e24-49d4-9939-63a564c27ca6> ⁶ [DOC-402312A1.pdf \(fcc.gov\)](#)

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			Proponuję wprowadzić zapisy obligujące podmioty użytkujące produkty ICT, usługi ICT lub procesy ICT dostawcy wysokiego ryzyka do wdrożenia rozwiązań organizacyjnych i technicznych podwyższonego nadzoru tych produktów ICT, usług ICT i procesów ICT oraz systemów informacyjnych z nich zbudowanych i usług zależnych od tych systemów. Proponuję wprowadzić zapisy obligujące organy właściwe, CSIRTy krajowe i CSIRTy sektorowe do podwyższonego nadzoru tych produktów ICT, usług ICT i procesów ICT oraz systemów informacyjnych z nich zbudowanych i usług zależnych od tych systemów. Proponuję wprowadzić zapisy warunkujące dalsze użytkowanie produktów ICT, usług ICT i procesów ICT dostawcy wysokiego ryzyka.	działania mitygujące ryzyka związane ze sprzętem pochodzącym od dostawcy wysokiego ryzyka. Np. monitorować kto ma dostęp do tego sprzętu, monitorować informacje przepływające przez ten sprzęt. Wprowadzono okresy na wycofanie sprzętu/oprogramowania ponieważ istotne jest także zapewnienie ciągłości świadczenia usług przez dany podmiot. Nie jest możliwe natychmiastowe wycofanie sprzętu, ponieważ zakłócona zostanie przez to ciągłość świadczenia usług.
55.	Federacja Przedsiębiorców Polskich	Art. 67c ust. 19	Proponuje się następujące brzmienie art. 67c ust. 19: <i>19. Od decyzji, o której mowa w ust. 15, przysługuje wniosek o ponowne rozpatrzenie sprawy.</i> Przepis art. 67b ust. 19 przewiduje możliwość złożenia wniosku o ponowne rozpatrzenie sprawy. Oznacza to, że podmioty, których dotyczy decyzja o uznaniu za dostawcę wysokiego ryzyka, mają prawo do ponownego rozpatrzenia sprawy w ramach postępowania administracyjnego. Możliwość zaskarżenia decyzji administracyjnej w ramach postępowania administracyjnego jest zgodna z art. 78 Konstytucji RP, który stanowi, że każda decyzja administracyjna wydana w pierwszej instancji może być zaskarżona. Artykuł ten zalicza możliwość zaskarżenia decyzji administracyjnej do podstawowych praw podmiotowych obywateli, co obejmuje również prawo do ponownego rozpatrzenia sprawy. Wprowadzenie możliwości ponownego rozpatrzenia sprawy zapewnia dodatkową ochronę prawną dla podmiotów gospodarczych, które mogą być dotknięte decyzją o uznaniu za dostawcę wysokiego ryzyka. Jest to istotne, ponieważ decyzje te mogą mieć dalekosiężne skutki ekonomiczne i operacyjne dla przedsiębiorstw. Dzięki przepisowi art. 67b ust. 19, przedsiębiorstwa te mają zapewnioną możliwość odwołania się od decyzji i przedstawienia dodatkowych argumentów oraz dowodów na swoją obronę. Możliwość ponownego rozpatrzenia sprawy wpisuje się w zasady sprawiedliwości proceduralnej, które są kluczowe dla zapewnienia, że wszystkie decyzje administracyjne są podejmowane na podstawie pełnej i rzetelnej analizy wszystkich dostępnych informacji. Procedura ponownego rozpatrzenia sprawy pozwala również na korektę ewentualnych błędów popełnionych w toku pierwszego postępowania, co zwiększa ogólną jakość i wiarygodność procesu decyzyjnego. Dodatkowo, wniosek o ponowne rozpatrzenie sprawy stanowi ważny element systemu kontroli administracyjnej, który zapewnia, że decyzje podejmowane przez organy administracyjne są zgodne z prawem i sprawiedliwe. Umożliwienie podmiotom dotkniętym decyzją korzystania z tego środka prawnego wzmacnia zaufanie do administracji publicznej i systemu prawnego jako całości.	Uwaga nieuwzględniona Zrezygnowano z wniosku o ponowne rozpatrzenie sprawy, aby umożliwić szybsze rozpatrzenie ewentualnej skargi przez sąd administracyjny. Konstytucja RP nie wyklucza takiego modelu postępowania.
56.	Federacja Przedsiębiorców Polskich	Art. 67c ust. 1 - 2	Proponuje się następujące brzmienie art. 67c ust. 1-2:	Uwaga nieuwzględniona

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

		1. W przypadku wydania decyzji, o której mowa w art. 67b ust. 15, podmioty, o których mowa w art. 67b ust. 1: 1) nie wprowadzają do użytkowania typów produktów ICT, usług ICT i procesów ICT o funkcjach krytycznych w zakresie objętym decyzją, dostarczanych przez dostawcę wysokiego ryzyka, po upływie 18 miesięcy od dnia ogłoszenia lub udostępnienia informacji o decyzji, o której mowa w art. 67b ust. 15; 2) wycofują z użytkowania produkty ICT, usługi ICT i procesy ICT o funkcjach krytycznych w zakresie objętym decyzją, dostarczane przez dostawcę wysokiego ryzyka nie później niż 7 lat od dnia opublikowania informacji o decyzji, o której mowa w art. 67b ust. 15 z zastrzeżeniem ust. 2. 2. Przedsiębiorcy telekomunikacyjni obowiązani posiadać aktualne i uzgodnione plany działań oraz wprowadzone do stosowania w sytuacji szczególnego zagrożenia, wycofują w ciągu 7 lat produkty ICT, usługi ICT, procesy ICT o funkcjach krytycznych wskazane w decyzji. Przepis art. 67b ust. 1 pkt 1 dotyczy niewprowadzania do użytkowania nie wszystkich typów produktów i usług ICT, ale tylko tych o funkcjach krytycznych. Koncentracja na funkcjach krytycznych pozwala na precyzyjne określenie zakresu produktów i usług, które mogą stanowić zagrożenie dla bezpieczeństwa narodowego i infrastruktury krytycznej. Dzięki temu, inne produkty i usługi ICT, które nie mają bezpośredniego wpływu na bezpieczeństwo, mogą być nadal używane bez dodatkowych restrykcji. Przewiduje się okres 18 miesięcy, po upływie którego wskazane produkty i usługi nie będą mogły być wprowadzane do użytkowania. Okres ten jest wystarczający, aby zapewnić płynne przejście oraz umożliwić podmiotom dostosowanie się do nowych wymogów bez powodowania problemów technicznych i organizacyjnych. Daje to również czas na dokładne przetestowanie i wdrożenie alternatywnych rozwiązań, które będą zgodne z nowymi wymaganiami bezpieczeństwa.⁸Dodatkowo, przepis wymaga, aby produkty ICT, usługi ICT i procesy ICT o funkcjach krytycznych były wycofywane z użytkowania nie później niż 7 lat od dnia opublikowania informacji o decyzji. Ten okres zapewnia wystarczający czas na przeprowadzenie wymaganych zmian bez nagłych zakłóceń w działaniu infrastruktury krytycznej. Długoterminowe planowanie wycofania tych produktów i usług umożliwia podmiotom gospodarczym przygotowanie się na zmiany, zarówno pod względem finansowym, jak i operacyjnym.⁸Siedmioletni okres wycofania produktów, usług i procesów ICT o funkcjach krytycznych jest kluczowy dla zapewnienia stabilności i bezpieczeństwa infrastruktury krytycznej. Wymaga on, aby przedsiębiorstwa miały odpowiednio długi czas na analizę, zaplanowanie i wdrożenie alternatywnych rozwiązań, co minimalizuje ryzyko przerw w świadczeniu usług i zapewnia ciągłość operacyjną. Taki okres jest również zgodny z cyklami inwestycyjnymi i technologicznymi w sektorze ICT, umożliwiając amortyzację istniejącego sprzętu i oprogramowania oraz racjonalne planowanie budżetu na przyszłe inwestycje.⁸Przedsiębiorcy telekomunikacyjni, którzy są obowiązani posiadać aktualne i uzgodnione plany działań na wypadek szczególnego zagrożenia, również powinni mieć taki sam okres, tj. 7 lat, na wycofanie produktów ICT, usług ICT i procesów ICT o funkcjach krytycznych wskazanych w decyzji. W innym przypadku byłiby dyskryminowani w stosunku do innych branż. Równe traktowanie wszystkich sektorów, które korzystają z krytycznych funkcji ICT, jest niezbędne do zapewnienia sprawiedliwości i unikania zakłóceń w poszczególnych branżach. Proponowany przez ustawodawcę okres 4-letni, a nawet 5-letni, jest zdecydowanie zbyt krótki, ponieważ nie zapewnia ciągłości	Postępowanie identyfikuje niebezpiecznego dostawcę sprzętu i oprogramowania. W związku z tym należy niezwłocznie podjąć działania mitygujące ryzyka związane ze sprzętem. Wprowadzanie do użytkowania sprzętu pochodzącego od dostawcy wysokiego ryzyka nie jest rozwiązaniem ani zasadnym ani celowym. Wobec tego nie można wprowadzać swoistej karencji 18 miesięcy i w tym okresie wprowadzać nowy sprzęt od dostawcy wysokiego ryzyka. Skrócenie terminu na wycofanie sprzętu/oprogramowania do 4 lat w funkcjach krytycznych jest związane właśnie z tym, że są to funkcje krytyczne.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			działania urządzeń lub oprogramowania oraz ich amortyzacji. Tak krótki okres wycofania może prowadzić do znacznych kosztów i zakłóceń, które mogą negatywnie wpływać na stabilność i bezpieczeństwo infrastruktury telekomunikacyjnej oraz innych sektorów zależnych od ICT. Amortyzacja sprzętu i oprogramowania w sektorze ICT jest procesem, który często trwa kilka lat, dlatego skrócenie okresu wycofania może prowadzić do niepełnego zwrotu z inwestycji, co obciąża przedsiębiorstwa finansowo. Ponadto, nagłe zmiany mogą prowadzić do konieczności szybkiego zakupu nowych rozwiązań, które mogą być droższe i mniej dostosowane do specyficznych potrzeb danego przedsiębiorstwa. Ewentualne skrócenie terminu powinno być uzależnione od tego, czy zgodnie z pozostałymi uwagami, minister do spraw informatyzacji określał będzie funkcje krytyczne. Określenie funkcji krytycznych przez ministra zapewnia, że tylko najbardziej istotne elementy infrastruktury ICT będą podlegały szybszemu wycofaniu, co może być bardziej zarządzalne dla przedsiębiorstw. Takie podejście pozwala na elastyczność i dostosowanie harmonogramu wycofywania do specyficznych potrzeb i zagrożeń związanych z konkretnymi funkcjami krytycznymi. Ewentualne skrócenie terminu powinno być uzależnione od tego, czy zgodnie z pozostałymi uwagami, minister do spraw informatyzacji określał będzie funkcje krytyczne. Określenie funkcji krytycznych przez ministra zapewnia, że tylko Podsumowując, zapewnienie siedmioletniego okresu na wycofanie produktów, usług i procesów ICT o funkcjach krytycznych jest niezbędne dla zachowania stabilności operacyjnej i finansowej przedsiębiorstw oraz dla zapewnienia równych warunków dla wszystkich sektorów. Skrócenie tego okresu bez odpowiednich mechanizmów zarządzania ryzykiem i amortyzacji może prowadzić do poważnych zakłóceń i niesprawiedliwości w traktowaniu różnych branż. Wprowadzenie tych przepisów jest konieczne, aby zapewnić odpowiedni poziom bezpieczeństwa narodowego, jednocześnie umożliwiając podmiotom gospodarczym dostosowanie się do nowych wymogów w sposób uporządkowany i przewidywalny. Przepisy te pomagają w zrównoważeniu potrzeb bezpieczeństwa z potrzebami operacyjnymi i ekonomicznymi podmiotów działających w sektorze ICT.	
57.	Federacja Konsumentów	Art. 67c	Uzasadnienie dla modyfikacji terminu Art. 67c ust. 2 projektu ustawy przewiduje że „Przedsiębiorcy telekomunikacyjni, o których mowa w art. 67b ust. 1 pkt 2, wycofują w ciągu 4 lat typy produktów ICT, rodzaje usług ICT, konkretne procesy ICT wskazane w decyzji i określone w wykazie kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług w załączniku nr 3 do ustawy.”. Określony w tym przepisie termin na wycofanie z sieci przedsiębiorców telekomunikacyjnych produktów ICT, rodzajów usług ICT oraz konkretnych procesów ICT dostawcy uznanego za dostawcę wysokiego ryzyka jest odmienny od generalnego 7-letniego terminu (art. 67c ust. 1 pkt 2) na przeprowadzenie takiego procesu przez inne podmioty niż przedsiębiorcy telekomunikacyjni. W ocenie Federacji Konsumentów projektowane rozwiązanie może mieć pośredni wpływ na interes wszystkich konsumentów. Biorąc pod uwagę fakt, że przeprowadzenie procesu wycofania ze swoich sieci sprzętu dostawcy uznanego za dostawcę wysokiego ryzyka niewątpliwie wygeneruje określone koszty po stronie przedsiębiorców telekomunikacyjnych, może się to finalnie przełożyć na wzrost kosztów usług detalicznych świadczonych użytkownikom końcowym. Przy czym, jak wynika z ogólnie dostępnych raportów Prezesa UKE, ceny usług telekomunikacyjnych w Polsce do tej pory należały do tej pory do	Uwaga wyjaśniona Wycofanie sprzętu/oprogramowania pochodzącego od dostawcy wysokiego ryzyka w terminie 4 lat dla przedsiębiorców telekomunikacyjnych jest zasadne z uwagi na to, że chodzi o funkcje krytyczne dla sieci i usług. Zauważyć należy, że sprzęt i oprogramowanie i tak wymagałyby okresowej wymianie z uwagi na naturalne zużycie sprzętu. Sieć 4g też będzie z czasem wycofywana.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			jednych z najniższych w Europie. Federacja Konsumentów działa na rzecz utrzymania tego poziomu cen, biorąc chociażby pod uwagę element ubóstwa cyfrowego, a jest na nie narażone około 25% Polek i Polaków. sW ocenie Federacji Konsumentów przyjęcie projektowanego rozwiązania może mieć zatem niekorzystny wpływ na interes konsumentów. Tym samym, w naszej ocenie zasadnym byłoby ustalenie w projekcie ustawy dla przedsiębiorców telekomunikacyjnych analogicznego terminu na przeprowadzenie procesu wycofania z ich sieci sprzętów dostawcy uznanego za dostawcę wysokiego ryzyka jak w przypadku wszystkich innych podmiotów, które mogą być objęte takim obowiązkiem, aby nie generować ryzyka wzrostu cen detalicznych usług telekomunikacyjnych.	
58.	Fundacja Rozwoju Obrotu Bezgotówkowego	Art. 67c	Zgodnie z art. 67c noweli k.s.c. podmioty z tego sektora bankowego i infrastruktura rynków finansowych będą mogły zostać zobowiązane do usunięcia sprzętu i usług pochodzących od podmiotu uznanego za dostawcę wysokiego ryzyka na zasadach i w terminach określonych w tym przepisie. Natomiast w OSR nie dokonano żadnej oceny finansowej konsekwencji usunięcia z tego sektora sprzętu i usług dla 547 podmiotów, które działają w tym sektorze.	Uwaga wyjaśniona Wskazanie kosztów wycofania sprzętu/oprogramowania stanowiłoby niedopuszczalny przedśąd – pośrednio już w OSR, przed przeprowadzeniem szczególnego postępowania, wskazany zostałby dostawca wysokiego ryzyka.
59.	Fundacja Open Allies	Art. 67c	[Art. 67c ust. 1 i 2 termin wycofania z użytkowania typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT dla przedsiębiorców telekomunikacyjnych] Rozumiemy, że skrócony termin (4 lata) do wycofania niektórych typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT może dotyczyć wyłącznie typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT określonych w wykazie kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług w załączniku nr 3 do ustawy. Jest to kluczowe dla faktycznych możliwości wdrożenia projektowanej ustawy. Open Allies postuluje również wprowadzenie zmiany w odniesieniu do liczenia tego terminu. Termin ten powinien być liczony od daty, w której decyzja dot. wycofania produktów stanie się prawomocna, tj. nie zostanie od niej wniesiony środek odwoławczy, lub w razie wniesienia takiego środka, zapadnie prawomocne orzeczenie sądu. Zwracamy się o przedłużenie ogólnego terminu wycofania urządzeń – z 7 do 9 lat. Taka zmiana, w związku z naturalnymi zmianami technologicznymi, pozwoli zmniejszyć koszty transformacji. Zwracamy się również o wydłużenie skróconego terminu 4 lata, określonego wobec niektórych typów produktów ICT, rodzajów usług ICT i procesów ICT, do 5 lat.	Uwaga wyjaśniona Krytyczny charakter funkcji wskazanych w załączniku nr 3 do projektu ustawy przemawia za tym, aby skrócić okres wycofania sprzętu/oprogramowania do 4 lat.
60.	Fundacja Open Allies	Art. 67c	[Art. 67c ust. 3 możliwość korzystania z sprzętu lub oprogramowania hrv] Zwracamy się o doprecyzowanie ust. 3 w ten sposób, aby z przepisu wprost wynikało, że oprócz „użytkowania (...) w zakresie naprawy, modernizacji, wymiany elementu lub aktualizacji” sprzętu lub	Uwaga wyjaśniona W ocenie projektodawcy przepis nie wymaga doprecyzowania, można to wywnioskować z obecnego brzmienia przepisu.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			oprogramowania hrv, możliwe było również świadczenie usług użytkownikom. Można to pośrednio wnioskować z brzmienia przepisu. Zasadne wydaje się doprecyzowanie.	
61.	KIKE	Art. 67c	Izba wskazuje, że termin na usunięcie z sieci telekomunikacyjnej urządzeń i oprogramowania dostawcy wysokiego ryzyka jest rażąco za krótki (4 lata). W przypadku przedsiębiorców MŚP z uwagi na długie terminy amortyzacji sprzętu i oprogramowania koszty wykonania takiego obowiązku mogą zagrozić opłacalności dalszej działalności gospodarczej. Co więcej, jak podkreślałem wcześniej, taka regulacja w stosunku do MŚP nie odpowiada zasadzie proporcjonalności i adekwatności. Z tego powodu postuluję (w wypadku utrzymania tego mechanizmu) niewyznaczanie terminu dla przedsiębiorców telekomunikacyjnych do usuwania produktów dostawcy wysokiego ryzyka. Te elementy systemów sieci telekomunikacyjnych powinny zostać usuwane w toku normalnego ich zużycia lub usuwania awarii, co jest okresem znacząco dłuższym niż 4 lata. Elementy sieci telekomunikacyjnej podlegają procesowi wymiany w okresie od 10 do 20 lat (niektóre nawet 30 lat). Wystarczającą sankcją powinien być zakaz nabywania nowych produktów ICT dostawcy wysokiego ryzyka. Zwracam uwagę na potencjalne skutki nie tylko ekonomiczne, ale też dla rozwoju społeczeństwa informatycznego w Polsce. Konieczność w krótkim czasie usuwania całych odcinków sieci telekomunikacyjnej może cofnąć wskaźniki dostępu do Internetu szerokopasmowego o całe lata, a jednocześnie spowodować wzrost cen i spadek konkurencji. Jednocześnie Izba wskazuje, że komplikacje z usuwaniem sprawnych urządzeń ICT z sieci budowanych ze środków publicznych w ramach KPO czy FERC. Żaden z beneficjentów tych programów nie dostanie dodatkowych środków na ich modernizację pod kątem usuwania produktów ICT dostawcy wysokiego ryzyka, co spowoduje zagrożenie realizacji tych programów. i	Uwaga wyjaśniona Krytyczny charakter funkcji wskazanych w załączniku nr 3 do projektu ustawy przemawia za tym, aby skrócić okres wycofania sprzętu/oprogramowania do 4 lat.
62.	Skandynawska Izba Gospodarcza	Art.67c	Uruchomienie sieci 5G oznacza istotne korzyści zarówno dla konsumentów jak i dla przemysłu. Sieć piątej generacji, jako podstawa cyfryzacji wszystkich sektorów przemysłu, stanie się swoistym katalizatorem rozwoju przemysłu, umożliwiając wykorzystanie sztucznej inteligencji, automatyzacji i robotyki. W rezultacie implementacja technologii 5G doprowadzi do ożywienia polskiej gospodarki przy jednoczesnym zwiększeniu konkurencyjności Polski i całej Europy. Jednocześnie ryzyko związane z cyberzagrożeniami nigdy nie było większe niż obecnie. Regulacje prawne na poziomie krajowym z zakresu cyberbezpieczeństwa, są niezbędne, by zminimalizować ryzyko ataków, które mogą dotknąć także przedsiębiorców, w tym naszych członków. Projekt nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa w zakresie dotyczącym dostawców wysokiego ryzyka ma kluczowe znaczenie dla zminimalizowania tych zagrożeń. Zachodzi jednak obawa, że czas wyznaczony na wycofanie sprzętu dostarczonego przez podmioty uznane za dostawców wysokiego ryzyka jest zbyt długi. W związku z powyższym rekomendujemy dodanie klauzuli określającej minimalną, proporcjonalną ilość sprzętu, która będzie wycofywana każdego roku z sieci, aż do całkowitego wycofania sprzętu. Przykładowo, jeżeli sprzęt od dostawcy wysokiego ryzyka ma być wycofany w ciągu siedmiu lat, co roku należy wycofać co najmniej 1/7 całkowitej ilości sprzętu. Jeżeli natomiast sprzęt ma zostać wycofany w ciągu czterech lat co roku należy wycofać co najmniej % całkowitej ilości sprzętu. Zalecenie to zagwarantowałoby systematyczną, coroczną poprawę bezpieczeństwa cyfrowego, aż do momentu całkowitego wycofania z sieci sprzętu od dostawców wysokiego ryzyka.	Uwaga wyjaśniona Projektodawca pozytywnie przyjmuje stanowisko poparcia dla wprowadzonych regulacji. W ocenie projektodawcy podmioty zobowiązane do wycofania sprzętu/oprogramowania pochodzącego od dostawcy wysokiego ryzyka powinny same podjąć decyzję ile sprzętu/oprogramowania rocznie powinno być wycofywane.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			Uwzględniając powyższe rekomendacje Skandynawsko-Polska Izba Gospodarcza wspiera nowelizację przepisów regulujących cyberbezpieczeństwo.	
63.	ZPP	Art. 67c	Termin na wycofanie sprzętu wysokiego ryzyka przedsiębiorców ICT Zachęcamy, żeby podmioty infrastruktury krytycznej w Polsce otrzymały obowiązek do wycofania sprzętu w ciągu 1 roku. Natomiast przewidziany w art. 67c ust. 2 projektu KSC dla przedsiębiorców telekomunikacyjnych termin 4-letni na wycofanie typów produktów ICT, rodzajów usług ICT oraz konkretnych procesów ICT, wskazanych w decyzji uznającej dostawcę sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, w naszej opinii jest zbyt krótki i nie uwzględnia praktycznych możliwości realizacji takiego procesu. Zarówno uzasadnienie do Projektu KSC, jak i OSR, nie wskazują na podstawowy problem związany z Procedurą DWR dla podmiotów objętych Załącznikiem nr 3 do projektu. Niezauważono, że wymiana sprzętu dla sieci 5G wymaga również wymiany sprzętu dla sieci 4G (ze względu na obecnie wykorzystywaną konfigurację 5G non-standalone), i to nie tylko w tych samych lokalizacjach, ale w całej sieci. W konsekwencji jest to znacznie bardziej złożony projekt niż budowa sieci 5G, obejmujący wielokrotnie więcej lokalizacji fizycznych. Skala inżynierska projektu jest tak duża, że próba jego realizacji w ciągu 4 lat będzie ograniczona z powodu braku dostępności wyspecjalizowanych ekip instalacyjnych, które będą dokonywały wymian, równoległe dla kilku przedsiębiorców telekomunikacyjnych. Wymiana sprzętu oznacza uruchomienie dużego programu obejmującego wiele projektów, dotyczących równoczesnej zmiany kilku systemów oraz dostosowania pozostałych systemów do współpracy z nowym rozwiązaniem. Ryzyko niedotrzymania terminu z art. 67c może być całkowicie niezależne od przedsiębiorcy telekomunikacyjnego, ponieważ pozostali dostawcy oferujący dany typ rozwiązania (ich liczba również jest ograniczona) mogą nie być w stanie wywiązać się z zamówień od nowych klientów w określonym czasie.	Uwaga wyjaśniona Krytyczny charakter funkcji wskazanych w załączniku nr 3 do projektu ustawy przemawia za tym, aby skrócić okres wycofania sprzętu/oprogramowania do 4 lat.
64.	Związek Cyfrowa Polska	Art. 67c	W zakresie Dostawców Wysokiego Ryzyka: w Art. 67c ust 1 pkt 1) – chcielibyśmy wnioskować o wprowadzenie zasady proporcjonalnego wycofania z użytkowania typy produktów ICT, rodzaje usług ICT i konkretne procesy ICT w zakresie objętym decyzją dostarczanych przez dostawcę wysokiego ryzyka nie później niż 7 lat od dnia ogłoszenia lub udostępnienia informacji o decyzji, o której mowa w art. 67b ust. 15. w Art. 67c ust 2 – chcielibyśmy wnioskować o skrócenie terminu i rozróżnienie warunków dla infrastruktury krytycznej. Wnoskujemy o wycofanie sprzętu HRV w ciągu: (i) 1 roku dla infrastruktury krytycznej w geograficznie wrażliwych obszarach (np. bazy wojskowe, instalacja militarne/ NATO, budynki administracji publicznej) i (ii) w ciągu 3 lat dla pozostałej infrastruktury krytycznej proporcjonalnie w każdym roku, z uwzględnieniem pierwszeństwa obszarów o największej gęstości zaludnienia Uzasadnienie:	Uwaga wyjaśniona Wycofanie sprzętu/oprogramowania znajdującego się wokół baz wojskowych czy infrastruktury krytycznej może być problematyczne, ponieważ podmiot obowiązany do wycofania sprzętu może po prostu nie wiedzieć gdzie są te nieruchomości.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			Aby zapewnić stopniowe wycofywanie w celu ograniczenia zidentyfikowanych ryzyk z wyznaczonymi dostawcami wysokiego ryzyka, a tym samym stale wzmacniać cyberbezpieczeństwo kraju, zaleca się stopniową, ale proporcjonalną fazę wycofania sprzętu HRV.	
65.	Związek Pracodawców Technologii Cyfrowych Lewiatan	Art. 67c	Czas korzystania produktów, usług i procesów ICT od dostawców wysokiego ryzyka (art. 67c ust. 1 oraz ust. 5) Postulujemy skrócenie czasu zapisanego w punkcie 2) do 5 lat. Zapis taki realizuje potrzebę utrzymania tych produktów, usług lub procesów, które podlegają wymaganiom okresu trwałości wynikających z zasad postępowania przy zamówieniach publicznych. Utrzymywanie w systemach mających znaczenie dla cyberbezpieczeństwa sprzętu lub oprogramowania przez 7 lat samo w sobie nosi znamiona podnoszenia ryzyka.	
66.	Związek Telewizji Kablowych Izba Gospodarcza	Art. 67b-67c	Instytucja prawna decyzji uznania za dostawcę wysokiego ryzyka oraz procedura prowadząca do wydania decyzji o uznaniu za dostawcę wysokiego ryzyka Projektodawca do ustawy o KSC dodaje art. 67 b- art. 67 f poświęcone procedurze dotyczącej uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka (art. 1 pkt. 70 projektu ustaw zmieniającej ustawę o KSC). Przed wszystkim wdrożenia przedmiotowej procedury i środków prawnych będących efektem jej uruchomienia do polskiego systemu nie można uznać za dążenie do zadośćuczynienia obowiązowi implementacji dyrektywy NIS 2 do wewnętrznego porządku prawnego naszego kraju. Dyrektywa bowiem NIS 2 milczy na temat tego rodzaju środka prawnego, ani nie przewiduje jego wdrażania, ani tym bardziej w tym zakresie na państwa członkowskie nie nakłada obowiązku jego wdrożenia. Oznacza to, iż wprowadzenie do wewnętrznego porządku prawnego przedmiotowej instytucji nie stanowi implementacji dyrektywy NIS 2, a zatem w omawianym przypadku nie mamy do czynienia z realizacją obowiązku prawnego wynikającego z normy art. 288 zd. 4 Traktatu o funkcjonowaniu Unii Europejskiej. Natomiast prawodawca europejski przewiduje dla państw członkowskich uprawnienie, a nie obowiązek, wprowadzenia wobec podmiotów ważnych i podmiotów kluczowych wymogu stosowania konkretnych produktów ICT, usług ICT i procesów ICT opracowanych przez dany podmiot kluczowy lub ważny lub nabytych od osób trzecich certyfikowanych zgodnie z europejskimi programami certyfikacji cyberbezpieczeństwa (art. 24 ust. 1 zd. 1 dyrektywy NIS 2). Ponadto prawodawca europejski dopuszcza opcję, iż państwa członkowskie będą zachęcały podmioty kluczowe i ważne do korzystania z kwalifikowanych usług zaufania (art. 24 ust. 1 zd. 2 dyrektywy NIS 2). Niewątpliwie jednak regulacja art. 24 ust. 1 dyrektywy NIS 2 nie nakłada na państwa członkowskie obowiązku wdrożenia regulacji wewnętrznych obligujących podmioty kluczowe i ważne do nabywania od osób trzecich certyfikowanych produktów ICT, usług ICT i procesów ICT, a także certyfikowania opracowanych przez te podmioty (kluczowe i ważne) własnych produktów ICT, usług ICT i procesów ICT, a jedynie dopuszcza opcję, iż państwa członkowskie takie regulacje będą mogły w wewnętrznym porządku prawnym wdrażać. Odnosnie z kolei kwalifikowanych usług zaufania regulacja art. 24 ust. 1 zd. 2 dyrektywy NIS 2 dopuszcza jedynie uprawnienie państw członkowskich do zachęcania podmiotów ważnych i kluczowych do korzystania z kwalifikowanych usług zaufania.	Uwaga wyjaśniona Postępowanie w sprawie uznania za dostawcę wysokiego ryzyka ma na celu zabezpieczenie polskiej gospodarki i polskiego społeczeństwa przed dostawcą sprzętu lub oprogramowania, który stwarza poważne zagrożenie dla bezpieczeństwa państwa, obronności, bezpieczeństwa i porządku publicznego lub zdrowia i życia ludzi. W ramach postępowania administracyjnego będą brane pod uwagę zarówno aspekty techniczne związane z dostarczaniem przez dostawcę sprzętem i oprogramowaniem jak również aspekty nietechniczne związane z dostawcą. Dzięki temu zostanie zidentyfikowany pełen obraz zagrożeń jakie stwarza dostawca sprzętu lub oprogramowania. Postępowanie umożliwia badanie dostawcy sprzętu lub oprogramowania dla wszystkich sektorów gospodarki wskazanych w ustawie. Jest to wskazane z uwagi na to, że każdy podmiot kluczowy i podmiot ważny musi dbać o bezpieczeństwo łańcuchów dostaw. Podmioty kluczowe i podmioty ważne mają istotny charakter dla funkcjonowania współczesnej gospodarki i społeczeństwa informacyjnego. Zakłócenie funkcjonowania tych podmiotów poprzez

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

		Natomiast w sytuacji stwierdzenia przez Komisję Europejską niewystarczających poziomów cyberbezpieczeństwa Komisja Europejska została wyposażona w możliwość przyjmowania aktów delegowanych w celu uzupełnienia dyrektywy NIS 2 poprzez określenie, od których kategorii podmiotów kluczowych i ważnych należy wymagać stosowania nabytych od osób trzecich certyfikowanych produktów ICT, usług ICT i procesów ICT lub uzyskania certyfikacji dla swoich własnych produktów ICT, usług ICT i procesów ICT na podstawie europejskiego programu certyfikacji cyberbezpieczeństwa (art. 24 ust. 2 dyrektywy NIS 2). Jedynie zatem w takim wyjątkowym przypadku występowania niewystarczających poziomów cyberbezpieczeństwa w oparciu o aktywność normatywną Komisji Europejskiej (jeśli z niej skorzysta) zaistnieje obowiązek certyfikacji własnych produktów ICT, usług ICT i procesów ICT opracowanych przez podmioty ważne i kluczowe oraz powstanie obowiązek nabywania od osób trzecich przez podmioty kluczowe i ważne wyłącznie certyfikowanych na podstawie europejskiego programu certyfikacji cyberbezpieczeństwa produktów ICT, usług ICT i procesów ICT. Ponadto państwa członkowskie w celu wspierania spójnego wdrażania dążenia do tego, aby podmioty kluczowe i ważne wprowadzały odpowiednie i proporcjonalne środki techniczne, operacyjne i organizacyjne w celu zarządzania ryzykiem dla bezpieczeństwa sieci i systemów informatycznych wykorzystywanych przez te podmioty do prowadzenia działalności lub świadczenia usług oraz w celu zapobiegania wpływowi incydentów na odbiorców ich usług lub na inne usługi bądź minimalizowania takiego wpływu nie narzucając, ani też nie faworyzując stosowania określonego rodzaju technologii zostały uprawnione do zachęcania podmiotów kluczowych i ważnych do stosowania europejskich i międzynarodowych norm i specyfikacji technicznych istotnych z punktu widzenia bezpieczeństwa sieci i systemów informatycznych (art. 25 ust. 1 dyrektywy NIS 2). Także w tym przypadku państwa członkowskie nie zostały ani zobowiązane, ani też uprawnione do wdrożenia w wewnętrznym systemie prawnym regulacji przewidujących obowiązek stosowania europejskich i międzynarodowych norm i specyfikacji technicznych istotnych z punktu widzenia bezpieczeństwa sieci i systemów informatycznych, a jedynie prawodawca europejski upoważnił je do stosowania systemów zachęt zmierzających do przekonania podmiotów kluczowych i ważnych do stosowania europejskich i międzynarodowych norm i specyfikacji technicznych istotnych z punktu widzenia bezpieczeństwa sieci i systemów informatycznych. Powyższa analiza świadczy o tym, iż normalizacja dotycząca stosowania określonych rodzajów sieci i systemów informatycznych nie jest obowiązkowa w państwach członkowskich i państwa członkowskie nie zostały nawet uprawnione do narzucania w tym zakresie podmiotom kluczowym i ważnym normalizacji w tym zakresie (art. 25 ust. 1 dyrektywy NIS 2), natomiast certyfikacja nabywanych od osób trzecich przez podmioty kluczowe i ważne, jak i wytwarzanych przez podmioty kluczowe i ważne produktów ICT, usług ICT i procesów ICT co do zasady nie jest obligatoryjna w państwach członkowskich, zaś państwa członkowskie mogą, ale wcale nie muszą, w tym zakresie nałożyć stosowne obowiązki na podmioty ważne i kluczowe (art. 24 ust. 1 dyrektywy NIS 2), natomiast zupełnie wyjątkowo w razie stwierdzenia niewystarczających poziomów cyberbezpieczeństwa Komisja Europejska została wyposażona w uprawnienie do wydawania aktów delegowanych, mocą których zostanie określone od których kategorii podmiotów kluczowych i ważnych należy wymagać stosowania nabytych od osób trzecich certyfikowanych	atak przez łańcuch dostaw może spowodować niepowetowane straty. Z uwagi na charakter tego postępowania wyłączono część przepisów KPA. Przede wszystkim nie jest możliwe przeprowadzenie postępowania administracyjnego przy udziale wszystkich podmiotów, które wykorzystują sprzęt lub oprogramowanie pochodzące od danego dostawcy. Rygor natychmiastowej wykonalności jest konieczny z uwagi na to, że kwestia dotyczy poważnego zagrożenia dla bezpieczeństwa państwa. Nie przewiduje się rekompensat za wycofanie sprzętu lub oprogramowania, ponieważ ten sprzęt i tak z czasem podlegałby wymianie z uwagi na naturalne zużycie. Termin 7 lat na wycofanie sprzętu/oprogramowania wydaje się terminem adekwatnym. Jednocześnie skrócono ten termin do 4 lat dla sprzętu i oprogramowania realizującego funkcje krytyczne w zakresie bezpieczeństwa sieci i usług.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			produktów ICT, usług ICT i procesów ICT lub uzyskania certyfikacji dla swoich własnych produktów ICT, usług ICT i procesów ICT opracowanych przez podmioty ważne i kluczowe na podstawie europejskiego programu certyfikacji cyberbezpieczeństwa (art. 24 ust. 2 dyrektywy NIS 2). W przypadku jednakże wydawania decyzji o uznaniu dostawcy za dostawcę wysokiego ryzyka nie mamy do czynienia ani z kwestią certyfikacji, ani też z kwestią normalizacji za nabywane od osób trzecich przez podmioty ważne i kluczowe produktów ICT, usług ICT i procesów ICT. Tego rodzaju instytucji (decyzja i procedura prowadząca do jej wydania) dyrektywa NIS 2, ani też jakiegokolwiek inne dyrektywy unijne lub decyzje unijne kierowane do konkretnych państw, w tym i do państwa polskiego, nie przewidują, a zatem nie zachodzi prawny obowiązek jej implementacji do wewnętrznego porządku prawnego naszego kraju (art. 288 zd. 4, zd., zd. 5, zd. 6 Traktatu o funkcjonowaniu Unii Europejskiej). Analizując uzasadnienie projektu ustawy zmieniającej ustawę o KSC dochodzimy do wniosku, że projektodawca wywodzi potrzebę wprowadzenia instytucji uznania dostawcy za dostawcę wysokiego ryzyka z: a/ zalecenia Komisji (UE) 2019/534 z dnia 26.03.2019 r. Cyberbezpieczeństwo sieci 5G (Dz.U. UE.L. 2019.88.42), zwanego dalej zaleceniem w sprawie Cyberbezpieczeństwa sieci 5G(str. 59-60 uzasadnienia projektu ustawy zmieniającej ustawę o KSC), b/ Unijnej skoordynowanej oceny ryzyka cyberbezpieczeństwa sieci 5G, zwanej dalej Unijną oceną Cyberbezpieczeństwa sieci 5G(str. 61 uzasadnienia projektu ustawy zmieniającej ustawę o KSC), c/ Unijnego zestawu środków dla sieci 5 G tzw. Toolbox 5G, zwanego dalej Toolbox 5G (str. 61 uzasadnienia projektu ustawy zmieniającej ustawę o KSC), d/ Komunikatu Komisji Europejskiej z dnia 29.01.2020 r., zwanego dalej Komunikatem Komisji z 29.01.2020 r. (str. 62 uzasadnienia projektu ustawy zmieniającej ustawę o KSC). Projektodawca zatem wprowadzenie instytucji decyzji uznania dostawcy za dostawcę wysokiego ryzyka, której wydanie stanowić będzie niewątpliwie ograniczenie konstytucyjnej wolności gospodarczej uzasadnia ważnym interesem publicznym (art. 22 Konstytucji RP), który jednakże zostaje wywiedziony z zalecenia w sprawie Cyberbezpieczeństwa sieci 5G, które woła prawodawcy unijnego nie posiada jakiegokolwiek mocy obowiązującej (art. 288 zd. 7 Traktatu o funkcjonowaniu Unii Europejskiej) oraz z Unijnej oceny Cyberbezpieczeństwa sieci 5G, Toolbox 5G i Komunikatu Komisji z 29.01.2020 r., które to z kolei dokumenty(opracowania) nie stanowią ani źródła prawa Unii Europejskiej wskazanego w art. 288 zd. 1 Traktatu o funkcjonowaniu Unii Europejskiej, ani też źródła prawa powszechnie obowiązującego w ujęciu art. 87 Konstytucji RP, co automatycznie przesądza o braku mocy wiążącej także tych trzech ostatnio wzmiankowanych dokumentów o charakterze nienormatywnym. Wywiedzenie zatem ważnego interesu publicznego, który miałby przemawiać za ograniczaniem konstytucyjnej wolności gospodarczej poprzez wprowadzenie nowej instytucji do prawa polskiego (decyzja o uznaniu dostawcy za dostawcę wysokiego ryzyka) z trzech dokumentów o charakterze nienormatywnym nie posiadających dla państwa polskiego jakiegokolwiek mocy wiążącej i z jednego dokumentu normatywnego także pozbawionego mocy wiążącej dla państw członkowskich Unii Europejskiej niezwykle negatywnie świadczy o postawie polskiego projektodawcy, który zamiast chronić konstytucyjną wolność działalności gospodarczej nade wszystko polskich przedsiębiorców, ale i wolność działalności gospodarczej	

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			przypisaną mocą art. 20 Konstytucji RP także przedsiębiorcy zagranicznemu, który mógłby być uznany za dostawcę wysokiego ryzyka, wyżej stawia racje wynikające z dokumentów unijnych pozbawionych jakiegokolwiek mocy wiążącej na terenie tejże Unii Europejskiej. Wbrew bowiem wywodom zawartym w uzasadnieniu projektu ustawy zmieniającej ustawę o KSC wprowadzenie rzeczonoj instytucji stanowić będzie ograniczenie konstytucyjnej wolności działalności gospodarczej (art. 22 Konstytucji RP) albowiem w przypadku uznania dostawcy za dostawcę wysokiego ryzyka podmioty kluczowe i podmioty ważne, z wyłączeniem pochodzących z podsektora komunikacji elektronicznej, oraz przedsiębiorcy telekomunikacyjni, których roczne przychody z tytułu wykonywania działalności telekomunikacyjnej w poprzednim roku obrotowym były wyższe niż 10 milionów złotych: a/ nie będą już mogły wprowadzać do użytkowania typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT w zakresie objętym decyzją dostarczanych przez dostawcę wysokiego ryzyka(projektowany art. 67 c ust. 1 pkt. 1 ustawy o KSC), b/ będą zobowiązani do wycofania z użytkowania typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT objętych decyzją, a dostarczanych przez dostawcę wysokiego ryzyka w terminie 7 lat od dnia ogłoszenia lub udostępnienia informacji o przedmiotowej decyzji (projektowany art. 67 c ust. 1 pkt. 2 ustawy o KSC), także wówczas, gdy nabyły produkty ICT, procesy ICT lub usługi ICT w drodze zamówienia publicznego przed dniem ogłoszenia lub udostępnienia informacji o decyzji o uznaniu danego podmiotu za dostawcę wysokiego ryzyka (projektowany art. 67 c ust. 5 ustawy o KSC), c/ będą zobowiązani do wycofania z użytkowania typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT objętych decyzją, a dostarczanych przez dostawcę wysokiego ryzyka w terminie 5 lat od dnia ogłoszenia lub udostępnienia informacji o przedmiotowej decyzji jeżeli nabyli je w trybie zamówienia publicznego przed udostępnieniem lub ogłoszeniem informacji o decyzji o uznaniu za dostawcę wysokiego ryzyka (projektowany art. 67 c ust. 5 in fine ustawy o KSC). Co równie ważne przedsiębiorcy telekomunikacyjni których roczne przychody z tytułu wykonywania działalności telekomunikacyjnej w poprzednim roku obrotowym były wyższe niż 10 milionów złotych będą zobowiązani do wycofania typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT objętych decyzją i określonych w wykazie kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług w załączniku nr 3 do ustawy o KSC w ciągu 4 lat od dnia ogłoszenia lub udostępnienia informacji o przedmiotowej decyzji (projektowany art. 67 c ust. 2 ustawy o KSC). Niewątpliwie bowiem pozbawienie podmiotów kluczowych i podmiotów ważnych oraz przedsiębiorców telekomunikacyjnych, których roczne przychody z tytułu wykonywania działalności telekomunikacyjnej w poprzednim roku obrotowym były wyższe niż 10 milionów złotych możliwości nabywania od konkretnych dostawców uznanych za dostawców wysokiego ryzyka typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT objętych decyzją oraz wycofania z eksploatacji typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT objętych decyzją, a pochodzących od dostawcy wysokiego ryzyka w ciągu 7 lub 4 lat od ogłoszenia lub udostępnienia informacji o decyzji o uznaniu dostawcy za dostawcę wysokiego stanowi klasyczny wręcz przykład ograniczenia konstytucyjnej wolności działalności gospodarczej (art. 22 Konstytucji RP). Rozważania czynione w uzasadnieniu projektu ustawy zmieniającej ustawę o KSC (str. 71 i str. 72) wedle których średni okres użytkowania sprzętu lub oprogramowania wynosi od 5- 7 lat, a w przypadku sprzętu	

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

		wykorzystywanego w radiowej sieci dostępowej wynosi od 5 do 10 lat, co miałoby przemawiać za brakiem ograniczenia wolności działalności gospodarczej, skoro przedsiębiorca i tak w tym okresie czasu wymieniałby ten sprzęt lub oprogramowanie nie uwzględnia tego, iż: a/ do ogłoszenia informacji o decyzji może dojść niewiele czasu po nabyciu sprzętu lub oprogramowania przez przedsiębiorcę, co znacząco skróciłoby możliwość jego użytkowania przez tegoż przedsiębiorcę, w stosunku do wskazanych powyżej terminów ich użytkowania, b/ sprzęt nabyty wiele lat temu, w tym zwłaszcza wyprodukowany przez podmiot Huawei z Chińskiej Republiki Ludowej użytkowany jest przez znaczącą część przedsiębiorców telekomunikacyjnych, a także inne podmioty kluczowe lub ważne, jest sprzętem użytkowanym od bardzo wielu lat i praktycznie jest sprzętem niezawodnym działającym bezawaryjnie lub przy niezwykle niskiej awaryjności w zestawieniu z innymi tęgo rodzaju sprzętami i oprogramowaniem produkowanym w Unii Europejskiej lub w państwach Organizacji Paktu Północnoatlantyckiego, których to sprzęt, produkty, usługi i oprogramowanie pragnie chronić polski projektodawca. Przymusowa zatem wymiana w pełni sprawnego, wysokiej jakości, niemalże bezawaryjnego sprzętu i oprogramowania i zastąpienie go o wiele niższej jakości, mocno awaryjnym sprzętem i oprogramowaniem pochodzącym od producentów zlokalizowanych w Unii Europejskiej lub na terenie państw Paktu Północnoatlantyckiego lub nawet w naszym kraju z jednej strony narazi przedsiębiorców na konieczność poniesienia zupełnie zbędnych, nieplanowanych do poniesienia dodatkowych kosztów, a zarazem pozostaje w pełnej sprzeczności z zasadą racjonalnego gospodarowania środkami finansowymi przez przedsiębiorców. Należy także zważyć, że w projekcie ustawy zmieniającej ustawę o KSC nie przewidziano jakichkolwiek rekompensat dla podmiotów kluczowych, ważnych oraz przedsiębiorców telekomunikacyjnych, których przychody z działalności telekomunikacyjnej w poprzednim roku obrotowym przekroczyły 10.000.000 złotych z tytułu obowiązku wymiany produktów ICT, procesów ICT oraz usług ICT nabytych od dostawcy uznanego za dostawcę wysokiego ryzyka, co sprawi, że koszty tej wymiany w pierwszej kolejności poniosą podmioty zobowiązane do ich wymiany, a w dalszej kolejności konsumenci korzystający z ich usług (str. 30 OSR stanowiącą część składową uzasadnienia projektu ustawy zmieniającej ustawę o KSC). Jeżeli zważywszy natomiast, że przez dostawcę sprzętu lub oprogramowania projektodawca uznaje klasycznego dostawcę (importera, dystrybutora), jak i producenta oraz upoważnionego przedstawiciela (projektowany art. 2 pkt. 4 c ustawy o KSC), to wówczas zobaczymy jak dużej liczby podmiotów dotknie decyzja o uznaniu dostawcy za dostawcę wysokiego ryzyka, który to importer, dystrybutor, ale i producent sprzętu lub oprogramowania (produktów ICT oraz procesów ICT), jak i podmiot świadczący usługi ICT zostaną pozbawieni możliwości wprowadzania na terytorium Rzeczypospolitej Polskiej produktów ICT, procesów ICT oraz usług ICT i ich sprzedawania zarówno swoim stałym odbiorcom, jak i potencjalnym nowym odbiorcom. Taka decyzja doprowadzi do znaczącego ograniczenia rynku zbytu dla swoich usług, oprogramowania oraz sprzętu.	

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			Niewątpliwie zatem tego rodzaju decyzja sprawi, że dojdzie do znaczącego ograniczenia konstytucyjnie gwarantowanej wolności gospodarczej także rzeczzonego przedsiębiorcy zagranicznego (art. 22 Konstytucji RP). Nie sposób także zgodzić się z poglądem projektodawcy jakoby konstytucyjna wolność działalności gospodarczej miała ustąpić przed potrzebami bezpieczeństwa państwa(str. 72 uzasadnienia projektu ustawy zmieniającej ustawę o KSC) albowiem w omawianym przypadku nie mamy do czynienia z prawem przyznanym z mocy zapisów konstytucyjnych jak np. prawo własności (art. 21 w zw. z art. 20 Konstytucji RP) lecz z wolnością działalności gospodarczej (art. 22 w zw. z art. 20 Konstytucji RP), co oznacza, że normy konstytucyjne jedynie potwierdzają ochronę wolności działalności gospodarczej, która istnieje niezależnie od zapisów konstytucyjnych, powstała niezależnie od zapisów konstytucyjnych, odmiennie niż w przypadku praw, które tworzone i przyznawane są mocą zapisów konstytucyjnych. Konstytucja RP zatem jedynie potwierdza istnienie konstytucyjnej wolności działalności gospodarczej oraz potwierdza zapewnienie jej ochrony. Wzmiankowane w uzasadnieniu projektu bezpieczeństwo państwa ma zatem rangę niewątpliwie niższą od wolności działalności gospodarczej, która istnieje niezależnie od istnienia państwa i niezależnie od zapisów prawnych w danym państwie obowiązujących, wynika bowiem ona niejako z prawa natury, czy też z prawa boskiego, a jej istnienie nie jest zależne od woli człowieka, odmiennie niż bezpieczeństwo państwa, które przede wszystkim wymaga stworzenia państwa wolą człowieka, a następnie stworzenie ram prawnych jego funkcjonowania, w tym i ram zakreślonych wolą człowieka dla jego bezpieczeństwa, a idąc dalej także jego cyberbezpieczeństwa. Niewątpliwie zatem mając na uwadze powyżej zakreślony wywód natury prawnokonstytucyjnej przesądza on o tym, iż w hierarchii wartości chronionych przez Konstytucję RP wyżej stoi każda wolność, w tym i wolność działalności gospodarczej, której ochronę jedynie potwierdza Konstytucja RP w art. 22, od każdej formy bezpieczeństwa państwa. Tym bardziej nie można zgodzić się z wywodami projektodawcy albowiem powołuje się on na niezwykle rzadko występujące, iluzoryczne wręcz postaci zagrożeń przejawiające się w atakach hakerskich oraz aktach sabotażu, czy wręcz atakach terrorystycznych organizowanych zdaniem projektodawcy przez służby wywiadowcze państw obcych oraz przez grupy przestępcze podlegane do działania na szkodę państwa polskiego przez władze lub służby wywiadowcze państw obcych(str. 72-73 uzasadnienia projektu ustawy zmieniającej ustawę o KSC).. Iluzoryczność, a nawet wręcz marginalność zagrożeń dla bezpieczeństwa państwa polskiego, na jakie wskazuje projektodawca niewątpliwie przemawia za zapewnieniem ochrony wolności działalności gospodarczej w zestawieniu z interesem państwa polskiego wyrażającym się w ochronie jego bezpieczeństwa. Minister właściwy do spraw informatyzacji wydaje decyzję o uznaniu dostawcy za dostawcę wysokiego ryzyka po zasięgnięciu opinii Kolegium do spraw Cyberbezpieczeństwa (projektowany art. 67 b ust. 10 ustawy o KSC). Treść przedmiotowej opinii jest niezwykle ważna albowiem w sposób jednoznaczny ukierunkowuje nas w zamiarach polskiego projektodawcy, który wychodzi z niczym nieuzasadnionego założenia, iż dostawca wysokiego ryzyka rekrutować się będzie spośród dostawców sprzętu lub oprogramowania znajdujących się	

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

		pod kontrolą państwa spoza terytorium Unii Europejskiej lub Organizacji Paktu Północnoatlantyckiego (projektowany art. 67 b ust. 11 pkt. 2 in principio ustawy o KSC). Nie sposób zrozumieć dlaczego to ataki hakerskie lub akty sabotażowe, a nawet ataki terrorystyczne kierowane pod adresem podmiotów działających w naszym kraju mogą pochodzić wyłącznie od dostawców sprzętu lub oprogramowania znajdujących się pod kontrolą państw spoza terytorium Unii Europejskiej lub Organizacji Paktu Północnoatlantyckiego. Przecież jest kwestią dowiedzioną, sojusznicy z NATO także się wzajemnie szpiegują (przykłady podsłuchów założonych przez CIA Kanclerz RFN Angeli Merkel, czy też szpiegowanie władz Wielkiej Brytanii przez służby wywiadowcze Stanów Zjednoczonych Ameryki), a zatem działania służb wywiadowczych, akty terrorystyczne i sabotażowe, czy też ataki hakerskie mogą być efektem działania władz lub służb także państw Unii Europejskiej lub Państw zrzeszonych w Organizacji NATO. Mając z kolei na uwadze, iż dostawca sprzętu lub oprogramowania może znajdować się pod kontrolą władz państwa spoza terytorium Unii lub NATO nie można wykluczyć, że rzeczony dostawca niekoniecznie musi posiadać swoją siedzibą poza terytorium Unii lub NATO, bo przecież kontrolowanie dostawców może odnosić się także do podmiotów mających siedzibę na terytorium Unii Europejskiej lub państw zrzeszonych w NATO, w tym mających swoją siedzibę w Polsce, ale kontrolowanych przez władze państw znajdujących się poza terytorium NATO lub Unii Europejskiej. Niezrozumiałe natomiast jest pominięcie zakresem opinii Kolegium do spraw Cyberbezpieczeństwa, a co za tym idzie i zakresem podmiotowym decyzji o uznaniu dostawcy za dostawcę wysokiego ryzyka, analizowania znajdowania się konkretnych dostawców pod kontrolą władz państwa zlokalizowanego na terytorium NATO lub Unii Europejskiej. Przecież władze państwa zrzeszonych w NATO w lub wchodzących w skład Unii Europejskiej także mogą w poważnym i szerokim zakresie kontrolować dostawców sprzętu lub oprogramowania mających siedzibę na terytorium NATO lub Unii Europejskiej lub poza tym terytorium. Dlaczego zatem projektodawca nie widzi problemu w nabywaniu przez podmioty kluczowe i ważne oraz przez pewną grupę większych przedsiębiorców telekomunikacyjnych usług ICT, produktów ICT oraz procesów ICT od dostawców znajdujących się pod kontrolą państwa z terytorium NATO lub Unii Europejskiej i tym samym wyklucza uznanie takiego dostawcy za dostawcę wysokiego ryzyka. Przecież dla naszego kraju równie poważnym problemem może być nabywanie produktów ICT, usług ICT lub procesów ICT od dostawców znajdujących się pod kontrolą władz państw zlokalizowanych na terytorium NATO lub Unii, żeby tylko wskazać na autorytarne reżimy rządzące w państwach NATO takich jak Turcja, Korea Południowa, Tajwan, Izrael, czy też pod kontrolą władz państw Unii Europejskiej lub NATO wielce nieprzyjaznych dla naszego państwa takich jak Niemcy, Holandia, Belgia, czy też Malta. Te państwa mimo swojej siedziby na terytorium Unii lub NATO także mogą w wyniku kontroli dostawców sprzętu lub oprogramowania doprowadzić na terytorium naszego kraju do aktów sabotażu gospodarczego (najbardziej takimi aktami niewątpliwie mogą być zainteresowani Niemcy czujący się mocno zagrożeni wzrostem gospodarczym naszego kraju, których władze na przestrzeni dziejów zawsze były wrogo nastawione do naszego kraju i nic w tej materii zmianie nie uległo), ataków hakerskich, ataków terrorystycznych, czy też innych czynów przestępczych.	

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			Takie zróżnicowane traktowanie dostawców oprogramowania i sprzętu zależnie od tego czy znajdują się pod kontrolą władz lub służb państw zlokalizowanych na terytorium Unii Europejskiej lub NATO, czy też poza tym terytorium wyrażające się w możliwości uznania za dostawcę wysokiego ryzyka jedynie tych dostawców produktów ICT, usług ICT lub procesów ICT, którzy znajdują się pod kontrolą władz lub służb państw zlokalizowanych poza terytorium Unii Europejskiej lub NATO, przy jednoczesnym wyłączeniu możliwości uznania za dostawcę wysokiego ryzyka dostawcy znajdującego się pod kontrolą władz lub służb państw zlokalizowanych na terytorium Unii Europejskiej lub NATO świadczy o naruszeniu wolności wykonywania działalności gospodarczej oraz równości przedsiębiorców (art. 2 prawa przedsiębiorców), a także o naruszeniu prawa do równego traktowania wszystkich przez władze publiczne (art. 32 ust. 1 zd. 2 Konstytucji RP) oraz konstytucyjnej zasady równości wszystkich wobec prawa (art. 32 ust. 1 zd. 1 Konstytucji RP). Co więcej, w omawianym przypadku możemy wręcz mówić o dyskryminacji jednych przedsiębiorców, a zarazem nieuprawnionym uprzywilejowaniu drugich przedsiębiorców, zależnie od terytorialnej lokalizacji państwa, którego władze lub służby danego dostawcę oprogramowania lub sprzętu kontrolują (art. 32 ust. 2 Konstytucji RP). Takie zróżnicowanie możliwości uznania danego dostawcy za dostawcę wysokiego ryzyka zależnie od lokalizacji państwa, którego władze go kontrolują, czy znajduje się to państwo na terytorium NATO lub Unii Europejskiej, czy też poza tym terytorium nie jest możliwe także do pogodzenia z konstytucyjną zasadą sprawiedliwości społecznej i demokratycznego państwa prawnego (art. 2 Konstytucji RP). Projektodawca zdecydował się na prowadzenie postępowania administracyjnego dotyczącego wydania decyzji o uznaniu danego dostawcy za dostawcę wysokiego ryzyka w oparciu o przepisy k.p.a. z wyłączeniem jednakże pewnych przepisów k.p.a.(projektowany art. 67 b ust. 2 ustawy o KSC). Biorąc pod uwagę materię przedmiotowego postępowania możemy zaakceptować wyłączenie stosowania art. 66 a k.p.a. poświęconego metryce sprawy administracyjnej, a także regulacji art. 51 k.p.a. przewidującej obowiązek osobistego stawiennictwa się wezwanego przed organem prowadzącym postępowanie administracyjne. Nie budzi także cienia wątpliwości uznanie za stronę postępowania administracyjnego w sprawie uznania za dostawcę wysokiego ryzyka każdego wobec kogo zostało wszczęte przedmiotowe postępowanie (projektowany art. 67 b ust. 3 ustawy o KSC). Niestety dalsze regulacje projektu ustawy zmieniającej ustawę o KSC dotyczące uczestników postępowania administracyjnego, a także ich praw nie mogą spotkać się z naszą aprobatą. Projektodawca jest niekonsekwentny albowiem z jednej strony wyłącza stosowanie art. 28 k.p.a. definiującego pojęcie strony postępowania administracyjnego z uwagi na to, że „w celu usprawnienia przebiegu postępowania i wzmocnienia trwałości rozstrzygnięć konieczne jest zawężenie przymiotu strony oraz udziału organizacji społecznej, mając na względzie, że do każdego takiego postępowania, według zasad ogólnych mogłoby przystąpić na prawach strony nawet setki podmiotów korzystających z konkretnych produktów pochodzących od konkretnego dostawcy sprzętu lub oprogramowania” (str. 64 uzasadnienia projektu ustawy zmieniającej ustawę o KSC). Argumentacja ta zasługuje na akceptację jedynie w zakresie, w którym odnosi się do ograniczenia udziału w takim akurat postępowaniu administracyjnym stron, którymi mógłby być każdy użytkownik sprzętu lub	

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			oprogramowania, a zatem tego rodzaju stron w takim postępowaniu byłyby zapewne nawet nie setki, jak pisze projektodawca, ale nawet tysiące. Niekonsekwencja jednakże projektodawcy przejawia się w tym, iż tworzy jakąś dziwną hybrydę przyjmując, że na wniosek tegoż podmiotu na prawach strony, a więc nie w charakterze strony postępowania, do postępowania administracyjnego w sprawie o uznanie za dostawcę wysokiego ryzyka może jednakże przystąpić przedsiębiorca komunikacji elektronicznej, który w poprzednim roku obrotowym uzyskał przychód z tytułu prowadzenia działalności telekomunikacyjnej w wysokości co najmniej dwudziestotysięcznej krotności przeciętnego wynagrodzenia w gospodarce narodowej wskazanego w ostatnim komunikacie Prezesa Głównego urzędu Statystycznego, o którym mowa w art. 20 pkt. 1 lit. a ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych, a którego do udziału w tymże postępowaniu dopuszcza organ postępowanie prowadzący (art. 31 § 2 k.p.a. w zw. z art. 31 § 3 k.p.a. w zw. z projektowanym art. 67 b ust. 4 ustawy o KSC). Wykluczając bowiem z udziału w przedmiotowym postępowaniu administracyjnym prawie wszystkich użytkowników sprzętu i oprogramowania pochodzącego od osoby, wobec której wszczęto postępowanie o uznanie za dostawcę wysokiego ryzyka, które byłyby stronami tegoż postępowania w świetle regulacji art. 28 k.p.a. „gdyby nie wyłączono stosowania tegoż przepisu mocą regulacji projektowanego art. 67 b ust. 2 ustawy o KSC, przy jednoczesnym dopuszczeniu do udziału w tymże postępowaniu dużego przedsiębiorcy komunikacji elektronicznej, co prawda jedynie na prawach strony (art. 31 § 2 k.p.a. w zw. z art. 31 § 3 k.p.a. w zw. z projektowanym art. 67 b ust. 4 ustawy o KSC), a nie jako stronę postępowania administracyjnego (art. 28 k.p.a.), jest rozwiązaniem kompletnie nieakceptowalnym, a zarazem całkowicie niekonsekwentnym i kontrowersyjnym w swym wyrazie. Przede wszystkim rozwiązanie to narusza wynikająca z konstytucji biznesu zasadę równości wszystkich przedsiębiorców (art. 2 prawa przedsiębiorców), a zarazem narusza konstytucyjną zasadę równości wszystkich wobec prawa (art. 32 ust. 1 zd. 1 Konstytucji RP) oraz konstytucyjny obowiązek równego traktowania wszystkich przez organy władzy (art. 32 ust. 1 zd. 2 Konstytucji RP). Co więcej omawiana regulacja stanowi jaskrawy wręcz przykład dyskryminacji mniejszych przedsiębiorców wobec większych przedsiębiorców ze względu na wysokość przychodu osiąganego przez nich z realizowanej działalności gospodarczej, co jest nie do pogodzenia z normą art. 32 ust. 2 Konstytucji RP). Trudno bowiem zrozumieć dlaczego to duży przedsiębiorca komunikacji elektronicznej mógłby jednak aktywnie uczestniczyć w postępowaniu administracyjnym nakierowanym na uznanie dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka korzystając z pełni praw przysługujących podmiotowi na prawach strony, gdy tymczasem mniejsi przedsiębiorcy komunikacji elektronicznej, a także pozostałe podmioty korzystające ze sprzętu lub oprogramowania pozyskanego od tegoż dostawcy mieliby być tej możliwości w majestacie prawa pozbawieni. Wyjaśnienie bowiem dopuszczenia do udziału w tym postępowaniu na prawach strony grupy największych przedsiębiorców komunikacji elektronicznej jest niejasne, enigmatyczne, a zarazem kompletnie niezrozumiałe oraz sprzeczne z zasadami racjonalnego wnioskowania, a zapewne także po prostu nieprawdziwe, skoro projektodawcy twierdzi, że w ten sposób uwzględnił postulaty strony społecznej	

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

		zapewniając zarazem sprawny przebieg postępowania (str. 64-65 uzasadnienia projektu ustawy zmieniającej ustawę o KSC). Trudno bowiem wyobrazić sobie sytuację, w której mniejsi użytkownicy sprzętu i oprogramowania postulowaliby, aby do postępowania dopuścić nieliczną grupę największych przedsiębiorców komunikacji elektronicznej z pominięciem zarazem mniejszych użytkowników sprzętu i oprogramowania pochodzącego od strony tegoż postępowania. Jeżeli zaś za stronę społeczną uznano tę grupę nielicznych największych przedsiębiorców komunikacji elektronicznej, to mamy do czynienia z oczywistym zakłamaniem przez projektodawcę rzeczywistości, gdyż tak niewielką grupę przedsiębiorców trudno uznać za stronę społeczną występującą o wprowadzenie tego rodzaju regulacji co zawarta w projektowanym art. 67 b ust. 4 ustawy o KSC. W sytuacji natomiast, gdy projektodawca mógłby prowadzić postępowanie administracyjne z udziałem jednej tylko strony, do czego przyczyniło się wyłączenie stosowania art. 28 k.p.a. i art. 31 k.p.a., to trudno zgodzić się z poglądem zaprezentowanym w uzasadnieniu projektu ustawy, wedle którego zwiększenie liczby uczestników tegoż postępowania o grupę kilkunastu największych przedsiębiorców komunikacji elektronicznej zapewni sprawny przebieg postępowania. Oczywistym wręcz jest, że prowadzenie postępowania z udziałem jednej raptem strony niewątpliwie zapewni sprawniejsze prowadzenie postępowania administracyjnego niż prowadzenie tej samej sprawy z udziałem jednakże jednej strony i dodatkowo kilkunastu podmiotów uczestniczących w postępowaniu na prawach strony. Projektodawca zatem albo powinien dopuścić do udziału w przedmiotowym postępowaniu, i to w charakterze stron, wszystkich użytkowników sprzętu i oprogramowania pochodzących od podmiotu, wobec którego toczy się postępowanie o uznanie za dostawcę wysokiego ryzyka, niezależnie od ich wielkości i osiąganych przez nich przychodów z działalności gospodarczej albo też nie dopuścić do udziału w tymże postępowaniu ani jako stron, ani jako podmiotów na prawach strony żadnego z użytkowników sprzętu i oprogramowania pochodzących od podmiotu, którego postępowanie o uznanie za dostawcę wysokiego ryzyka dotyczy. Takie rozwiązanie narusza także konstytucyjne zasady sprawiedliwości społecznej i demokratycznego państwa prawnego (art. 2 w zw. z art. 8 Konstytucji RP). Nie sposób także zaakceptować przekonania wyrażonego przez projektodawcę przemawiającego za wyłączeniem w przedmiotowym postępowaniu stosowania art. 31 k.p.a. „w celu usprawnienia przebiegu postępowania i wzmocnienia trwałości rozstrzygnięć konieczne jest zawężenie przymiotu strony oraz udziału organizacji społecznej, mając na względzie, że do każdego takiego postępowania, według zasad ogólnych mogłoby przystąpić na prawach strony nawet setki podmiotów korzystających z konkretnych produktów pochodzących od konkretnego dostawcy sprzętu lub oprogramowania” (str. 64 uzasadnienia projektu ustawy zmieniającej ustawę o KSC).. a także z powołaniem się na szczególny związek tego postępowania z kwestiami bezpieczeństwa narodowego (str. 64 uzasadnienia projektu ustawy zmieniającej ustawę o KSC). Trudno bowiem zrozumieć w jakiż to sposób powiązanie postępowania o uznanie za dostawcę wysokiego ryzyka z kwestiami bezpieczeństwa narodowego miałoby przesądzać o potrzebie wyłączenia czynnego udziału w postępowaniu administracyjnym przez organizacje społeczne na prawach strony.	

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			Nie przekonuje także argumentacja przemawiająca za wyeliminowaniem z udziału w postępowaniu organizacji społecznych na prawach strony, za którym to udziałem przemawia interes społeczny oraz jej cele statutowe (art. 31 § 1 in fine k.p.a.) z uwagi na potrzebę usprawnienia przebiegu postępowania oraz wzmocnienia trwałości rozstrzygnięć. W sytuacji bowiem, gdy z postępowania przedmiotowego eliminujemy tysiące podmiotów posiadających status strony (art. 28 k.p.a.) będących użytkownikami sprzętu i oprogramowania pochodzącego od podmiotu, którego postępowanie o uznanie za dostawcę wysokiego ryzyka dotyczy, jedyną możliwość reprezentowania ich praw w tym postępowaniu zapewnia udział organizacji społecznych na prawach strony. Pozbawienie zatem udziału w tym postępowaniu także organizacji na prawach strony jest w omawianej sytuacji kompletnie niezrozumiałe albowiem właśnie z tego powodu udział tych organizacji w postępowaniu winien być zapewniony w sposób bezdyskusyjny. Argumentacja wskazująca na wyeliminowanie z udziału w tymże postępowaniu także organizacji społecznych na prawach strony z uwagi na potrzebę usprawnienia przebiegu postępowania upada z uwagi na jednoczesne dopuszczenie do udziału w tymże postępowaniu na prawach strony największych przedsiębiorców komunikacji elektronicznej (projektowany art. 67 b ust. 4 ustawy o KSC). Co więcej wyeliminowanie z udziału w przedmiotowym postępowaniu organizacji społecznych na prawach strony, przy jednoczesnym zapewnieniu udziału na prawach strony kilkunastu największych przedsiębiorców komunikacji elektronicznej przesadza o naruszeniu konstytucyjnej zasady równości wszystkich wobec prawa (art. 32 ust. 1 zd. 1 Konstytucji RP), narusza konstytucyjny obowiązek równego traktowania wszystkich przez władze publiczne (art. 32 ust. 1 zd. 2 Konstytucji RP), a zarazem stanowi jaskrawy przykład dyskryminacji organizacji społecznych wobec pozycji przyznanej w projekcie największym przedsiębiorcom komunikacji elektronicznej (art. 32 ust. 2 Konstytucji RP). Zaproponowanie przez projektodawcę tego rodzaju regulacji nie może się także ostać w świetle wymogu przestrzegania konstytucyjnej zasady sprawiedliwości społecznej i demokratycznego państwa prawnego (art. 2 Konstytucji RP). Niczego w sprawie nie zmienia zagwarantowanie wąskiej grupie organizacji społecznych (art. 5 § 2 pkt. 5 k.p.a.), a mianowicie jedynie izbom gospodarczym, prawa do przedstawienia stanowiska co do dostawcy sprzętu lub oprogramowania, wobec którego wszczęto postępowanie o uznanie za dostawcę wysokiego ryzyka (projektowany art. 67 b ust. 9 ustawy o KSC) albowiem gdyby nie wyłączono stosowania w tymże postępowaniu regulacji art. 31 k.p.a. (projektowany art. 67 b ust. 2 ustawy o KSC), to izby gospodarcze, podobnie jak i pozostałe organizacje społeczne, mogłyby uczestniczyć w przedmiotowym postępowaniu administracyjnym na prawach strony korzystając z prawie wszystkich praw stronie postępowania administracyjnego przysługujących (art. 31 § 3 k.p.a.), a nie jedynie z prawa do wyrażenia opinii w sprawie zagwarantowanego organizacji społecznej w postępowaniu administracyjnym na prawach strony nie uczestniczącej (art. 31 § 5 k.p.a.), które projektodawca przyznał jedynie izbom gospodarczym w tymże postępowaniu administracyjnym (projektowany art. 67 b ust. 9 ustawy o KSC). Wyłączenie stosowania w postępowaniu administracyjnym o uznanie za dostawcę wysokiego ryzyka przepisu art. 79 k.p.a. zapewniającego czynny udział strony w postępowaniu dowodowym z powołaniem się na szczególny charakter tego postępowania mającego na celu zapewnienie bezpieczeństwa narodowego (str. 64 uzasadnienia projektu ustawy zmieniającej ustawę o KSC) jest nieprzekonujące, a projektodawca	

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			nie wyjaśnił w przedmiotowym uzasadnieniu w jakiż to sposób zapewnienie czynnego udziału strony w postępowaniu dowodowym prowadzonym w ramach niniejszego postępowania administracyjnego miałyby stanowić jakąkolwiek formę zagrożenia dla bezpieczeństwa narodowego. I. W odniesieniu zatem do nowej instytucji prawnej wydania decyzji o uznaniu danego podmiotu za dostawcę wysokiego ryzyka jako główny postulat Związek Telewizji Kablowych w Polsce Izba Gospodarcza zgłasza wprowadzenie zmiany art. 1 pkt. 70 projektu ustawy zmieniającej ustawę o KSC zasadzającej się na wykreśleniu proponowanej do dodania regulacji art. 67 b- art. 67 f ustawy o KSC regulującej instytucję decyzji uznania za dostawcę wysokiego ryzyka oraz procedurę prowadzącą do wydania tej decyzji. II. Gdyby jednakże ten najpełniejszy postulat nie został uwzględniony, to na taką okoliczność wnioskujemy o wprowadzenie zmiany art. 1 pkt. 70 ustawy zmieniającej ustawę o KSC co najmniej poprzez: a/ wykreślenie z proponowanego art. 67 b ust. 2 ustawy o KSC zapisu wskazującego na wyłączenie stosowania w postępowaniu o uznanie za dostawcę wysokiego ryzyka art. 31 k.p.a. i art. 79 k.p.a., b/ wykreślenie proponowanej regulacji art. 67 b ust. 4 ustawy o KSC, c/ wykreślenie proponowanej regulacji art. 67 b ust. 9 ustawy o KSC, d/ wykreślenie w proponowanej regulacji art. 67 b ust. 11 pkt. 1 in fine ustawy o KSC treści w brzmieniu „uzyskanych od państw członkowskich lub organów Unii Europejskiej lub Organizacji Paktu Północnoatlantyckiego”, e/ wykreślenie z proponowanej regulacji art. 67 b ust. 11 ustawy o KSC pkt. 2 i pkt. 3.	
67.	Federacja przedsiębiorców Polskich	art. 67e ust. 2	Przepis art. 67e ust. 2 otrzymuje brzmienie: <i>2. Odpis sentencji wyroku z uzasadnieniem doręcza się ministrowi właściwemu do spraw informatyzacji oraz skarżącemu.</i> Zarówno minister właściwy do spraw informatyzacji, jak i skarżący powinni otrzymywać wyrok z całym uzasadnieniem. Uregulowanie zgodnie z którym skarżącemu doręczałoby się odpis wyroku z tą częścią uzasadnienia, która nie zawiera informacji niejawnych w rozumieniu przepisów o ochronie informacji niejawnych, naruszałoby postanowienia art. 45 Konstytucji RP, gwarantujące każdemu prawo do sądu. Naruszałoby także art. 47 Karty Praw Podstawowych i art. 6 ust. 1 Europejskiej Konwencji Praw Człowieka, które także gwarantują każdemu prawo do sprawiedliwego rozpoznania sprawy przez sąd. W punkcie 7 opinii Rady Legislacyjnej z dnia 23 lutego 2021 r. do noweli ustawy o Krajowym systemie cyberbezpieczeństwa, Rada Legislacyjna także zgłosiła zastrzeżenia o charakterze konstytucyjnym do art. 66d ust. 2 (w poprzedniej wersji noweli ustawy o krajowym systemie cyberbezpieczeństwa, a w obecnej art. 67e ust. 2), co do zgodności z Konstytucją RP odstąpienia od doręczania stronie pełnego uzasadniania wyroku sądu administracyjnego. Według Rady Legislacyjnej, nie ulega wątpliwości, że w świetle konstytucyjnego prawa do sądu (art. 45 Konstytucji RP) zasadą musi być dostarczanie stronie pełnego uzasadnienia wyroku sądu administracyjnego, tak aby strona postępowania sądowo-administracyjnego mogła w sposób skuteczny wykorzystać swoje uprawnienia do zaskarżenia tego wyroku na drodze sądowej (zwłaszcza skargą kasacyjną do Naczelnego Sądu Administracyjnego).	Uwaga wyjaśniona Zasadne jest zapewnienie ochrony informacji niejawnych w ramach postępowania sądowo-administracyjnego. Stronie nie będzie doręczane uzasadnienie w zakresie, w jakim zawiera ono informacje niejawne.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

68.	ISSA Polska	Art. 67g	Nadmierny zakres poleceń zabezpieczających i ograniczone prawa odwoławcze (art. 53 ust. 8 ustawy KSC) Ustawa KSC przywraca, już uprzednio wykreśloną w poprzednich projektach ustawy, instytucję poleceń zabezpieczających, które mają obowiązywać wszystkie podmioty kluczowe i ważne. Mechanizm ten umożliwia ministrowi właściwemu do spraw informatyzacji wydawanie szeroko zakrojonych poleceń mających na celu minimalizowanie skutków incydentu krytycznego lub zapobieganie jego rozprzestrzenianiu. Te polecenia mogą obejmować szeroki zakres działań, od nakazu przeprowadzenia szacowania ryzyka po zakaz korzystania z określonych produktów ICT. Niepokojące jest, że w procesie wydawania tych poleceń nie stosuje się wielu przepisów Kodeksu postępowania administracyjnego, co ogranicza prawa podmiotów objętych takim poleceniem odwołań oraz procedur administracyjnych, które zwykle chronią interesy stron. W praktyce oznacza to, że polecenia są obligatoryjne i mają natychmiastową wykonalność, ogłaszane są jedynie na stronie internetowej bez konieczności ich doręczenia, co stawia podmioty w szczególnie trudnej sytuacji, jeśli chcą się odwołać. Dodatkowo, ograniczenie możliwości odwołania do jedynie skargi do sądu administracyjnego, która musi być złożona w ciągu dwóch miesięcy od ogłoszenia polecenia, jest znaczącym ograniczeniem prawa do obrony. Takie podejście stwarza ryzyko nadużyć i może prowadzić do nieproporcjonalnych działań, które mogą negatywnie wpłynąć na operacje i stabilność działania podmiotów gospodarczych, szczególnie w sytuacji, gdy nałożone wymagania są nieadekwatne do rzeczywistego ryzyka czy skali problemu.	Uwaga wyjaśniona Polecenie zabezpieczające dotyczy niebezpiecznej sytuacji incydentu krytycznego, który w istotny sposób zagraża bezpieczeństwu państwa. Jest to rozwiązanie które ma uchronić gospodarkę i społeczeństwo od dalszych następstw takiego incydentu. Polecenie musi być adekwatne – proporcjonalne do ryzyk związanych z incydentem krytycznym. Korzystanie z urzędów, które nie zapewniają bezpieczeństwa może zaszkodzić podmiotom kluczowym i podmiotom ważnym. Wyłączenie wniosku o ponowne rozpatrzenie sprawy ma uprościć możliwość odwołania do sądu administracyjnego. Z racji tego że polecenie zabezpieczające ma charakter decyzji generalnej to należy wyłączyć szereg przepisów Kodeksu postępowania administracyjnego które odnoszą się do udziału strony w postępowaniu. Bezpośredni udział strony w postępowaniu przy decyzji generalnej nie jest możliwy.
69.	Fundacja Bezpieczna Cyberprzestrzeń	Art. 67g	Art. 1 pkt 70, treść art. 67g – procedura wydania polecenia zabezpieczającego stoi w sprzeczności z potrzebą szybkiej reakcji na incydent krytyczny np. działań wskazanych w ust. 10 pkt 4, pkt 7 czy pkt 8. Stoi również w sprzeczności z korelacją czasową przedstawioną w tym artykule. Skoro bowiem polecenie ma być wydane na czas koordynacji obsługi incydentu krytycznego (zgodnie z ust. 12), to znaczy, że analizy, o których mowa w ust. 5 powinny być przeprowadzone przed klasyfikacją incydentu jako krytyczny, a zawiadomienie jednocześnie w klasyfikacją takiego incydentu. Proponuje się ponowna analizę przepisów tego dotyczących wprowadzania polecenia zabezpieczającego, pod kątem celu jaką jest szybka reakcja na incydent krytyczny, który zgodnie z definicją „skutkuje znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi.	Uwaga wyjaśniona Polecenie zabezpieczające dotyczy incydentu krytycznego – który uprzednio został już sklasyfikowany przez jeden z CSIRT poziomu krajowego. Kolejnym etapem może być wydanie polecenia zabezpieczającego. Jego wydanie poprzedza analiza. Analiza ta ma potwierdzić lub zaprzeczyć konieczności wydania polecenia zabezpieczającego.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

70.	PGE SA	Art. 67g ust. 10 pkt 6	W kontekście Art. 67g ust. 14, w przypadku, gdy zakaz korzystania z określonego produktu ICT, usługi ICT lub procesu ICT uniemożliwia świadczenie usługi powinna być określona ścieżka uzgadniania postępowania podmiotu kluczowego, w szczególności zawieszenie wykonania polecenia zabezpieczającego. Wskazane jest uzupełnienie przepisów o określenie trybu odwoławczego.	Uwaga wyjaśniona Przedstawiciele podmiotów kluczowych i ważnych będą mogli być zapraszani na posiedzenie Zespołu do spraw Incydentów krytycznych celem przedstawienia niezbędnych informacji.
71.	PTI	Art. 67g	Pkt 70, art. 67g, ust. 1 „ <i>Minister właściwy do spraw informatyzacji w przypadku wystąpienia incydentu krytycznego może, w drodze decyzji, wydać polecenie zabezpieczające</i> ” – uczestnictwo Ministra w obsłudze incydentu krytycznego jest wątpliwe – jedyną przyczyną takiego stanu rzeczy byłaby procedura eskalacji, kiedy CSIRT-y nie dają rady obsłużyć incydentu z uwagi na skalę lub powagę konsekwencji, to powinno być opisane jako czynnik uruchamiający działania ekstraordynaryjne Ministra; całość tego przepisu jest niedopracowana i powinna powrócić na ścieżkę uzgodnień technicznych z ekspertami. Poniżej przedstawiamy dalsze zastrzeżenia do konkretnych punktów trybu wprowadzenia oraz zakresu „polecenia zabezpieczającego”	Uwaga wyjaśniona Minister właściwy do spraw informatyzacji nie dokonuje obsługi incydentu krytycznego. Jako organ administracji rządowej odpowiedzialny za zapewnienie bezpieczeństwa w cyberprzestrzeni w wymiarze cywilnym będzie mógł wydać polecenie zabezpieczające.
72.	Konfederacja Lewiatan	Art. 67g	Polecenia zabezpieczające naruszające standardy demokratycznego państwa prawa Jednostka redakcyjna: art. 67g projektu KSC Jednostka redakcyjna NIS2: art. 9 ust. 1 Uwaga: Przepis art. 67g projektu ustawy w nowym brzmieniu daje szerokie kompetencje ministrowi właściwemu do spraw informatyzacji w zakresie wydawania poleceń zabezpieczających w przypadku wystąpienia incydentu krytycznego. Zasadniczym celem tej regulacji jest ochrona cyberbezpieczeństwa. Niemniej jednak, wiele argumentów prawnych można przytoczyć przeciwko aktualnemu kształtowi tego przepisu, bazując zarówno na analizie samego przepisu. Art. 67g ust. 14 stanowi, że polecenie zabezpieczające podlega natychmiastowej wykonalności. Taka regulacja znacząco ogranicza możliwość obrony podmiotów, na które nałożono takie polecenia. Co więcej, przepisy KPA przewidują w tym zakresie odpowiednie narzędzia umożliwiające ochronę interesów stron postępowania administracyjnego. Rygor natychmiastowej wykonalności może prowadzić do sytuacji, w której podmiot, w tym zarówno jednostka samorządu terytorialnego, jak i inne podmioty kluczowe i ważne, nie będzie miał możliwości wypełnienia swoich zadań ustawowych ze względu na brak środków finansowych na realizację polecenia zabezpieczającego. Przepis nie przewiduje żadnego okresu na wycofanie sprzętu lub oprogramowania, co może prowadzić do natychmiastowego paraliżu działalności jednostek, które muszą stosować się do polecenia zabezpieczającego. Sytuacja ta jest szczególnie trudna dla jednostek samorządu terytorialnego, które muszą przestrzegać przepisów o zamówieniach publicznych, co de facto uniemożliwia im szybkie przeprowadzenie zamówienia na nowy sprzęt lub oprogramowanie. Jednakże, dotyczy to również innych podmiotów objętych poleceniem, które mogą mieć ograniczone możliwości finansowe i organizacyjne do szybkiej adaptacji do nowych wymogów. Art. 67g ust. 17 stanowi, że od polecenia zabezpieczającego nie przysługuje wniosek o ponowne rozpatrzenie sprawy. To istotne ograniczenie prawa do sądu i środka odwoławczego, co jest sprzeczne z	Uwaga wyjaśniona Polecenie zabezpieczające dotyczy niebezpiecznej sytuacji incydentu krytycznego, który w istotny sposób zagraża bezpieczeństwu państwa. Jest to rozwiązanie które ma uchronić gospodarkę i społeczeństwo od dalszych następstw takiego incydentu. Polecenie musi być adekwatne – proporcjonalne do ryzyk związanych z incydentem krytycznym. Korzystanie z urządzeń, które nie zapewniają bezpieczeństwa może zaszkodzić podmiotom kluczowym i podmiotom ważnym. Natomiast z pewnością wycofanie sprzętu jest jednym ze środków ostatecznych. Wyłączenie wniosku o ponowne rozpatrzenie sprawy ma uprościć możliwość odwołania do sądu administracyjnego. Odpowiedzialność odszkodowawcza Skarbu Państwa została unormowana w Kodeksie cywilnym, stąd nie ma potrzeby dublowania regulacji.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

		podstawowymi zasadami państwa prawa. Zgodnie z art. 78 Konstytucji RP, każda decyzja administracyjna powinna być poddana kontroli sądu administracyjnego, co w przypadku poleceń zabezpieczających jest znacząco ograniczone. Ograniczenie możliwości odwołania się od decyzji stawia podmioty, na które nakładane są polecenia, w sytuacji bezsilności wobec decyzji administracyjnych, które mogą mieć istotny wpływ na ich funkcjonowanie. Proces wydawania polecenia zabezpieczającego jest arbitralny i może prowadzić do nadmiernej uznaniowości organów administracyjnych. Wydawanie takich poleceń bez szczegółowego uzasadnienia oraz brak możliwości skutecznego odwołania się od decyzji podważają zaufanie do administracji publicznej oraz mogą prowadzić do nieprzewidywalności w funkcjonowaniu podmiotów kluczowych i ważnych. Taka arbitralność może prowadzić do sytuacji, w której decyzje są podejmowane bez pełnego zrozumienia kontekstu i skutków dla poszczególnych podmiotów. Nałożenie polecenia zabezpieczającego na podmioty prywatne może prowadzić do znacznych kosztów finansowych, które nie są rekompensowane przez Skarb Państwa. W kontekście przedsiębiorstw, które zainwestowały znaczne środki w swoją infrastrukturę, wymóg natychmiastowego zaprzestania używania określonych produktów lub oprogramowania może prowadzić do ich bankructwa. Brak odpowiedzialności odszkodowawczej po stronie Państwa za szkody wynikłe z wykonania polecenia zabezpieczającego stawia podmioty prywatne w bardzo trudnej sytuacji ekonomicznej. Przepisy dotyczące poleceń zabezpieczających nie uwzględniają zasady proporcjonalności, która jest kluczowa w prawie administracyjnym. Nakładane środki powinny być adekwatne do zagrożenia oraz powinny być stosowane tylko w ostateczności, po wyczerpaniu innych mniej drastycznych środków. Brak proporcjonalności może prowadzić do nieuzasadnionych ograniczeń działalności gospodarczej i nadmiernych kosztów po stronie podmiotów, które są objęte poleceniem. Przepis art. 67g projektu KSC nie przewiduje obowiązku konsultacji z podmiotami, na które ma być nałożone polecenie zabezpieczające, co narusza zasadę partycypacji społecznej w procesie stanowienia prawa. Brak konsultacji może prowadzić do wydania decyzji bez pełnego zrozumienia skutków jej wykonania, co w konsekwencji może skutkować niewłaściwym zastosowaniem środków zabezpieczających i dodatkowymi problemami dla podmiotów, na które te środki są nakładane. Możliwość nakazania zablokowania dostępu do określonych serwerów, stron internetowych czy usług stwarza ryzyko nadużyć i wprowadzenia cenzury, co jest sprzeczne z art. 54 Konstytucji RP, gwarantującym wolność słowa i prawo do informacji. Takie środki mogą być wykorzystywane w sposób nieproporcjonalny, co zagraża wolnościom obywatelskim i transparentności działania administracji publicznej. Brak bezpośredniego doręczenia polecenia zabezpieczającego, które jest uznawane za doręczone z chwilą ogłoszenia w dzienniku urzędowym, narusza podstawowe zasady postępowania administracyjnego dotyczące komunikacji z zainteresowanymi stronami. Podmioty objęte takim poleceniem mogą nie być świadome nałożonych na nie obowiązków w odpowiednim czasie, co ogranicza ich możliwość reakcji i przygotowania się do wykonania polecenia. Bezpośrednie doręczenie decyzji jest kluczowe dla zapewnienia, że wszystkie strony są w pełni poinformowane i mogą odpowiednio dostosować swoje działania. Jest to o tyle istotne, że przy podobnej konstrukcji prawnej (wyłączenia doręczenia) Trybunał Konstytucyjny w orzeczeniu z 26.11.2019 r. sygn. akt P 9/18 z orzekł, że art. 49 ustawy zmieniającej w zakresie, w jakim w sprawach dotyczących wpisów, o których mowa w art. 55 pkt 4 i 5 KRSU, wyłącza	Nie można zgodzić się z tym, że zablokowanie adresów IP stanowi cenzurę – jest przeciwdziałanie np. atakom typu DDOS, które mogłyby utrudnić świadczenie usług. Polecenie zabezpieczające ma charakter decyzji generalnej, stąd też przewidziano możliwość doręczenia poprzez udostępnienie w dzienniku urzędowym Ministra Cyfryzacji. Z racji tego, że polecenie zabezpieczające ma charakter decyzji generalnej to należy wyłączyć szereg przepisów KPA, które odnoszą się do udziału strony w postępowaniu. Bezpośredni udział strony w postępowaniu przy decyzji generalnej nie jest możliwy.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			obowiązek doręczenia przez sąd uczestnikowi postępowania rejestrowego postanowienia o wpisie do rejestru dłużników niewypłacalnych wraz z uzasadnieniem, a także pozbawia uczestnika tego postępowania prawa do wniesienia skargi na postanowienie re-renderarza sądowego zarządzające wpis do takiego rejestru, jest niezgodny z art. 45 ust. 1 w związku z art. 31 ust. 3 Konstytucji. z perspektywy wymogów wynikających z art. 45 ust. 1 Konstytucji osoba wpisana do rejestru dłużników na mocy postanowienia re-renderarza sądowego powinna mieć zapewnione nie tylko prawo do otrzymania informacji o wydaniu takiego postanowienia i jego treści, ale także prawo do przedstawienia sprawy or-ganowi będącemu sądem w konstytucyjnym rozumieniu (por. także wyrok z 23.05.2018 r. sygn. SK 8/14). Polecenie zabezpieczające w obecnym kształcie przepisu art. 67g projektu KSC budzi zatem poważne wątpliwości prawne i konstytucyjne. W celu ochrony interesów podmiotów objętych takim poleceniem oraz zapewnienia zgodności z zasadami państwa prawa, zaleca się zniesienie rygoru natychmiastowej wykonalności lub wprowadzenie możliwości zawieszenia wykonania polecenia do czasu rozpatrzenia odwołania, wprowadzenie okresu „<i>vacatio legis</i>” na wycofanie sprzętu lub oprogramowania, zapewnienie możliwości odwołania się od polecenia zabezpieczającego, ograniczenie uznaniowości poprzez precyzyjne określenie przesłanek wydania polecenia zabezpieczającego, zapewnienie rekompensat finansowych dla podmiotów, na które nakładane są polecenia zabezpieczające, obowiązkowe konsultacje z podmiotami objętymi poleceniem przed jego wydaniem, wprowadzenie zasady proporcjonalności w stosowaniu poleceń zabezpieczających oraz ograniczenie możliwości blokowania stron internetowych i usług tylko do wyjątkowych sytuacji, z pełnym uzasadnieniem. Powyższe zmiany są niezbędne, aby przepisy dotyczące poleceń zabezpieczających były zgodne z zasadami demokratycznego państwa prawa oraz chroniły zarówno interesy publiczne, jak i prywatne. W demokratycznym państwie prawnym konieczne jest zapewnienie realnej kontroli instancyjnej decyzji dotyczących zgromadzenia przed jego terminem⁸⁾. Warto także zwrócić uwagę na wyłączenie stosowania art. 10, art. 34, art. 79, art. 81, art. 81a, art. 107 § 1 pkt 3, art. 145 § 1 pkt 4 i art. 156 § 1 pkt 4 oraz rozdziału 8 działu I KPA w procedurze wydawania polecenia zabezpieczającego ma poważne konsekwencje dla stron postępowania, a także dla praworządności. Poniżej znajduje się analiza poszczególnych przepisów KPA, których wyłączenie wpływa na przebieg postępowania: – art. 10 KPA - Zasada czynnego udziału stron w postępowaniu: Wyłączenie tego przepisu oznacza, że strony nie mają zapewnionego prawa do czynnego udziału w postępowaniu, co ogranicza ich możliwość przedstawienia swojego stanowiska, dowodów i argumentów. To może prowadzić do wydania decyzji bez uwzględnienia wszystkich istotnych okoliczności, co wpływa na rzetelność i sprawiedliwość postępowania.	

⁸⁾ Jak stwierdził Trybunał Konstytucyjny w orzeczeniu z 18.09.2014 sygn. K 4412 procedura odwołania od decyzji o zakazie zgromadzenia publicznego nie spełnia - w obecnym kształcie - wymogu skuteczności środka odwoławczego. Biorąc pod uwagę sposób ujęcia terminów doręczenia decyzji zakazującej zgromadzenia, wniesienie odwołania od tej decyzji oraz rozpatrzenia tego odwołania, uzyskanie rozstrzygnięcia konkretnej sprawy przed planowanym terminem zgromadzenia staje się w praktyce niewykonalne. Świadczy to o nieefektywności obowiązującej procedury odwoławczej.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

		– art. 34 KPA - Udział organizacji społecznych: Wyłączenie tego artykułu pozbawia organizacje społeczne możliwości uczestniczenia w postępowaniu, co ogranicza społeczną kontrolę nad działaniami administracji i może prowadzić do pominięcia interesu publicznego i zbiorowych interesów społecznych. – art. 79 KPA - Prawo do zapoznania się z aktami sprawy i wypowiedzenia się co do zebranych dowodów: Bez tego przepisu, strony nie mają możliwości zapoznania się z aktami sprawy, co uniemożliwia im pełną obronę swoich praw. Brak dostępu do dowodów i informacji zebranych w sprawie prowadzi do nierówności stron i ogranicza transparentność postępowania. – art. 81 KPA - Obowiązek informowania stron o zebranych dowodach: Wyłączenie tego przepisu powoduje, że strony nie są informowane o zebranych dowodach, co może prowadzić do sytuacji, w której nie są świadome podstaw decyzji administracyjnej, a tym samym nie mogą skutecznie bronić swoich interesów. – art. 81a KPA - Prawo do uzupełnienia dowodów i materiałów w sprawie: Brak stosowania tego przepisu uniemożliwia stronom przedstawienie dodatkowych dowodów i wyjaśnień, co może skutkować wydaniem decyzji na podstawie niepełnych lub jednostronnych informacji. – art. 107 § 1 pkt 3 KPA - Obowiązek uzasadnienia decyzji: Wyłączenie tego obowiązku oznacza, że decyzje administracyjne mogą być wydawane bez szczegółowego uzasadnienia, co utrudnia stronom zrozumienie podstaw decyzji oraz ogranicza możliwość skutecznego zaskarżenia decyzji w sądzie. – art. 145 § 1 pkt 4 KPA - Wznowienie postępowania: Bez możliwości wznowienia postępowania na podstawie nowych okoliczności lub dowodów, strony są pozbawione ważnej drogi prawnej do korekty decyzji administracyjnej w przypadku pojawienia się nowych faktów, które mogłyby wpłynąć na wynik sprawy. – art. 156 § 1 pkt 4 KPA - Stwierdzenie nieważności decyzji: Wyłączenie tego przepisu uniemożliwia stwierdzenie nieważności decyzji administracyjnej z powodu rażącego naruszenia prawa. To pozbawia strony ważnej ochrony prawnej przed decyzjami, które są obarczone poważnymi wadami prawnymi. – Rozdział 8 działu I KPA - Przepisy dotyczące doręczeń: Wyłączenie tych przepisów oznacza, że procedura doręczenia decyzji administracyjnej nie musi być zgodna z KPA, co może prowadzić do sytuacji, w której strony nie są właściwie informowane o wydanych decyzjach i nie mają możliwości podjęcia odpowiednich działań prawnych w odpowiednim czasie. – Wyłączenie powyższych przepisów KPA w procedurze wydawania poleceń zabezpieczających znacząco ogranicza prawa stron i narusza zasady praworządności. Brak udziału stron w postępowaniu, brak dostępu do akt sprawy, brak możliwości wznowienia postępowania czy stwierdzenia nieważności decyzji oraz brak należytego doręczenia decyzji osłabiają kontrolę nad działaniami administracji i mogą prowadzić do decyzji, które są nieprzejrzyste, niesprawiedliwe i trudne do zaskarżenia. Taka regulacja podważa fundamenty sprawiedliwego postępowania administracyjnego i zaufanie obywateli do państwa prawa.	

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

73.	Konfederacja Lewiatan	Art. 67g	Polecenia zabezpieczające – brak notyfikacji technicznej TRIS podważa skuteczność nowego rozwiązania Jednostka redakcyjna: art. 67g projektu KSC Jednostka redakcyjna NIS2: nie dotyczy Uwaga: Projektodawca zdecydował się na wprowadzenie dodatkowych poleceń zabezpieczających, które nie zostały przewidziane w dyrektywie NIS2. Projektodawca w uzasadnieniu do projektu ustawy jednocześnie twierdzi, że nie ma konieczności notyfikacji technicznej TRIS tych przepisów, mimo, że polecenia zabezpieczające nie stanowią implementacji prawa UE. W poprzedniej wersji projektu ustawy z 2023 r. zrezygnowano z poleceń zabezpieczających, co było spowodowane właśnie wymogiem notyfikacji technicznej, jak wynika z pisma Ministra Cyfryzacji z dnia 23 czerwca 2023 r. (DRC.WL.0610.4.2021). Natomiast w obecna wersja na powrót wprowadza to rozwiązanie a projektodawca twierdzi, że taka notyfikacja techniczna nie jest wymagana. Konsekwencje zaniechania notyfikacji technicznej TRIS są następujące: – Podważenie skuteczności przepisów: Brak notyfikacji technicznej TRIS może skutkować podważeniem skuteczności nowych rozwiązań prawnych. Notyfikacja jest istotnym elementem zapewniającym, że nowe przepisy są zgodne z prawem unijnym i nie stwarzają barier w jednolitym rynku. – Ryzyko procedur naruszeniowych: Komisja Europejska może wszcząć procedurę naruszeniową przeciwko Polsce za niewłaściwą implementację prawa unijnego. To może prowadzić do nałożenia kar finansowych oraz konieczności modyfikacji wprowadzonych przepisów. – Niepewność prawna dla przedsiębiorców: Brak notyfikacji technicznej TRIS może powodować niepewność prawną dla przedsiębiorców działających w sektorach objętych nowymi przepisami. Przedsiębiorcy mogą być zmuszeni do stosowania się do przepisów, które mogą być później zmienione lub uchylone, co generuje dodatkowe koszty i ryzyko biznesowe. – Ograniczenia dla polskich przedsiębiorców: Nowe, nienotyfikowane przepisy mogą stanowić barierę dla działalności gospodarczej polskich firm na rynku unijnym. Przedsiębiorcy mogą napotkać trudności w uzyskaniu certyfikacji lub zgodności z unijnymi standardami, co ogranicza ich konkurencyjność. – Zahamowanie inwestycji: Inwestorzy mogą być niechętni do angażowania się w projekty w Polsce, obawiając się niestabilności prawnej i potencjalnych konfliktów z prawem unijnym. To może negatywnie wpłynąć na rozwój gospodarczy i innowacyjność kraju. Wobec powyższego, wprowadzenie dodatkowych poleceń zabezpieczających bez notyfikacji technicznej TRIS jest decyzją ryzykowną, która może przynieść więcej szkód niż korzyści. Zaleca się ponowne rozważenie konieczności notyfikacji tych przepisów, aby zapewnić zgodność z prawem unijnym i uniknąć potencjalnych negatywnych konsekwencji.	Uwaga wyjaśniona W przypadku polecenia zabezpieczającego w ocenie projektodawcy może zająć wyjątek z art. 6 ust. 7 lit. a dyrektywy 2015/1535.
74.	Konfederacja Lewiatan	Art. 67g	Polecenie zabezpieczające Jednostka redakcyjna: Art. 67g Zgodnie z projektowanym ust. 8 wprowadzono słuszne uprawnienie dyrektora RCB do dopraszania podmiotów kluczowych lub ważnych do prac zespołu prowadzącego analizę przed wydaniem polecenia	Uwaga wyjaśniona W ocenie projektodawcy wystarczające jest dotychczasowe uprawnienie zawarte w przepisie.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			zabezpieczającego. Udział w pracach podmiotu wydaje się wręcz niezbędny, aby polecenie było proporcjonalne do zagrożenia oraz realne do wdrożenia bez tworzenia dodatkowych zagrożeń w ramach obsługi incydentu krytycznego. Wnosimy o uzupełnienie przepisów o wprowadzenie zasady informowania podmiotu kluczowego lub ważnego o rozpoczęciu prac nad ewentualnym wydaniem polecenia zabezpieczającego.	
75.	Konfederacja Lewiatan	Art. 67g	Przesłanki do uwzględniania w toku analizy Jednostka redakcyjna: Art. 67g ust. 5 w zw. z ust. 11 Wnosimy o uzupełnienie katalogu przesłanek analizowanych przed wydanie polecenia zabezpieczającego, o określenie spodziewanych skutków zastosowania się do polecenia w zakresie kosztów jego wdrożenia, czasu niezbędnego na realizację, a także ciągłość świadczenia usług przez podmiot kluczowy lub ważny oraz odtworzenie ich działania. Rozumiejąc nadzwyczajną instytucję polecenia, zwracamy jednak uwagę na bardzo poważne skutki, które jego zastosowanie może wywołać, także w zakresie odpowiedzialności podmiotu kluczowego lub ważnego wobec podmiotów trzecich, w tym dostawców, usługodawców lub usługobiorców. Tym bardziej jego wydanie musi odbywać się w sposób szeroko uwzględniający skutki wydania decyzji. Przewidziana w ust. 11 „adekwatność” wydaje się w tym zakresie istotnie niewystarczająca	Uwaga częściowo uwzględniona Przepis zostanie zmodyfikowany zgodnie z uwagą RCL.
76.	PTI	Art. 67g	Pkt 70, art. 67g, ust. 5 „ <i>Przed wydaniem polecenia zabezpieczającego minister właściwy do spraw informatyzacji przeprowadza we współpracy z Zespołem, o którym mowa w art. 35 ust. 3, analizę obejmującą (...)</i> ” – to powinna być określona procedura eskalacji, a czynnik uruchomienia procedury powinien wynikać z prac CSIRT-ów przy obsłudze incydentu krytycznego	Uwaga wyjaśniona Tak to właśnie widzimy, polecenie zabezpieczające współgra właśnie z procedurami w ramach Zespołu do spraw Incydentów Krytycznych.
77.	PTI	Art. 67g	Pkt 70, art. 67g, ust 10 ppkt 3) dot. „określonego zachowania”: „ <i>nakaz zastosowania określonej poprawki bezpieczeństwa w produkcie ICT, procesie ICT lub usłudze ICT posiadającym daną podatność;</i> ” – z analizy wykonanej przez dany podmiot może wynikać, że w danej konfiguracji, w danym systemie poprawki NIE DA się wprowadzić; z tego względu proponuje się wprowadzić uzupełnienie: „w wypadku, gdy z przyczyn technicznych, organizacyjnych lub biznesowych tej poprawki bezpieczeństwa nie można wprowadzić, podmiot będący stroną postępowania zabezpieczającego przedstawia swoje stanowisko, wraz z uzasadnieniem, które jest brane pod uwagę przez ministra właściwego do spraw informatyzacji.”	Uwaga wyjaśniona Polecenie zabezpieczające dotyczy reakcji na incydent krytyczny – jest to najgorszy rodzaj incydentu. Jeżeli więc produkt/usługa ICT posiadają podatność, która spowodowała incydent krytyczny to może zaistnieć sytuacja, w której proporcjonalnym działaniem będzie wprowadzenie odpowiedniej aktualizacji. Ponadto uwaga nie wskazuje, w jaki sposób minister miałby wziąć pod uwagę stanowisko podmiotu. W skrajnej sytuacji, gdyby niewykonanie polecenia zabezpieczającego wynikało z obiektywnej siły wyższej, to podmiot nie będzie ukarany za niewykonanie na podstawie art. 189e KPA.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

78.	PTI	Art. 67g	Pkt 70, art. 67g, ust 10 ppkt 4) dot. „określonego zachowania”: „<i>nakaz szczególnej konfiguracji produktu ICT, usługi ICT lub procesu ICT, zabezpieczającej przed wykorzystaniem określonej podatności;</i>” - z analizy wykonanej przez dany podmiot może wynikać, że wskazanej konfiguracji w danym konkretnym systemie NIE DA się wprowadzić; z tego względu proponuje się wprowadzić uzupełnienie: „w wypadku, gdy z przyczyn technicznych, organizacyjnych lub biznesowych nakazywanej konfiguracji nie można zastosować, podmiot będący stroną postępowania zabezpieczającego przedstawia swoje stanowisko, wraz z uzasadnieniem, które jest brane pod uwagę przez ministra właściwego do spraw informatyzacji.”	Uwaga wyjaśniona Polecenie zabezpieczające dotyczy reakcji na incydent krytyczny – jest to najgorszy rodzaj incydentu. Jeżeli więc produkt/usługa ICT posiadają podatność, która spowodowała incydent krytyczny to może zaistnieć sytuacja w której proporcjonalnym działaniem będzie wprowadzenie odpowiedniej konfiguracji sprzętu. Ponadto uwaga nie wskazuje, w jaki sposób minister miałby wziąć pod uwagę stanowisko podmiotu. W skrajnej sytuacji, gdyby niewykonanie polecenia zabezpieczającego wynikało z obiektywnej siły wyższej, to podmiot nie będzie ukarany za niewykonanie na podstawie art. 189e KPA.
79.	PTI	Art. 67g	Pkt 70, art. 67g, ust 10 ppkt 5) dot. „określonego zachowania”: „<i>nakaz wzmożonego monitorowania zachowania systemu</i>” – jest to sformułowanie nieprecyzyjne; co Autor ma na myśli, nakazując „wzmożone monitorowanie”? Zważyć należy, że działające obecnie systemy monitorowania bezpieczeństwa klasy SIEM lub SOAR działają w oparciu o rozwiązania sprzętowo-programowe których zachowanie (wyświetlanie alertów personelowi monitorującemu – SOC) bazuje na predefiniowanych regułach korelujących określone zdarzenia w monitorowanym systemie. Wzmożone monitorowanie wymagałoby zmiany tych reguł polegające na wykrywanie szerszej klasy zdarzeń, niekoniecznie z pozytywnym skutkiem dla faktycznego bezpieczeństwa, na skutek wywoływania fałszywych alertów tzw. False Positive. Prowadzi to najczęściej do przemęczenia personelu i może spowodować skutek odwrotny do zamierzonego. Potrzebne jest wyjaśnienie, o jakie działanie tu chodzi. Jeśli nie można tego wyjaśnić, to proponuje się skreślić ten podpunkt.	Uwaga wyjaśniona Wzmożone monitorowanie oznacza konieczność szczególnego zwrócenia uwagi na zdarzenia, które mogą informować o pojawieniu się incydentu krytycznego.
80.	PTI	Art. 67g	Pkt 70, art. 67g, ust 10 ppkt 6) dot. „określonego zachowania”: <i>zakaz korzystania z określonego produktu ICT, usługi ICT lub procesu ICT, które posiada podatność, która przyczyniła się do zaistnienia incydentu krytycznego;</i>” - z analizy wykonanej przez dany podmiot może wynikać, że danego elementu systemu NIE DA się usunąć; z tego względu proponuje się wprowadzić uzupełnienie: „w wypadku, gdy z przyczyn technicznych, organizacyjnych lub biznesowych zakazu nie można zastosować, podmiot będący stroną postępowania zabezpieczającego przedstawia swoje stanowisko, wraz z uzasadnieniem, które jest brane pod uwagę przez ministra właściwego do spraw informatyzacji.”	Uwaga wyjaśniona Polecenie zabezpieczające dotyczy reakcji na incydent krytyczny – jest to najgorszy rodzaj incydentu. Jeżeli więc produkt/usługa ICT posiadają podatność, która spowodowała incydent krytyczny to może zaistnieć sytuacja w której jedynym proporcjonalnym działaniem będzie zaprzestanie korzystania z nich. Rozumiemy przez to sytuację, w której np.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

				aktualizacja jest niemożliwa lub nie przyniesie skutków. Ponadto uwaga nie wskazuje, w jaki sposób minister miałby wziąć pod uwagę stanowisko podmiotu. W skrajnej sytuacji, gdyby niewykonanie polecenia zabezpieczającego wynikało z obiektywnej siły wyższej, to podmiot nie będzie ukarany za niewykonanie na podstawie art. 189e KPA.
81.	PTI	Art. 67g	Pkt 70, art. 67g, ust 10 ppkt 9) i 10) dot. „9) <i>nakaz zabezpieczenia określonych informacji, w tym dzienników systemowych; 10) nakaz wytworzenia obrazów stanu określonych urządzeń zainfekowanych złośliwym oprogramowaniem.</i> ” – takie informacje zbiera się w trakcie trwania incydentu od samego początku, stąd mechanizm polecenia zabezpieczającego może być mało skuteczny – często już jest za późno na pozyskanie takich informacji; sugeruje się dodać na końcu ppkt 9 oraz 10) odpowiednio: „o ile takie informacje są możliwe do pozyskania”.	Uwaga wyjaśniona Polecenie zabezpieczające może także dotyczyć podmiotów, które jeszcze nie wiedzą, że mają do czynienia z incydemem u siebie.
82.	PTI	Art. 67g	Pkt 70, art. 67g, ust 11 „11. <i>Wskazanie obowiązku określonego zachowania, o którym mowa w ust. 9 pkt 2, następuje z uwzględnieniem środków adekwatnych, w szczególności w świetle analizy, o której mowa w ust. 5.</i> ” – co oznacza „środki adekwatne”? Adekwatne do czego? Wskazanie powinno być dość precyzyjne, ponieważ polecenie zabezpieczające zawiera same zakazy i nakazy, a środki adekwatne mogą sugerować ominięcie tych zakazów lub nakazów. Proponuje się zmianę tego zapisu na: <i>Wskazanie obowiązku określonego zachowania, o którym mowa w ust. 9 pkt 2, następuje z uwzględnieniem dobrych praktyk, w szczególności w świetle analizy, o której mowa w ust. 5</i> ” lub skreślenie tego ustępu.	Uwaga wyjaśniona Adekwatne czyli proporcjonalne do stwierdzonych ryzyk. Jest to zabezpieczenie przed nadmierną arbitralnością władzy.
83.	ZBP	Art. 67g	Art. 67g. 1. Minister właściwy do spraw informatyzacji w przypadku wystąpienia incydentu krytycznego może, w drodze decyzji, wydać polecenie zabezpieczające. 2. Polecenie zabezpieczające dotyczy nieokreślonej liczby podmiotów kluczowych i podmiotów ważnych. 3. Do postępowania w sprawie o wydanie polecenia zabezpieczającego nie stosuje się art. 10, art. 34, art. 79, art. 81, art. 81a, art. 107 § 1 pkt 3, art. 145 § 1 pkt 4 i art. 156 § 1 pkt 4 oraz rozdziału 8 działu I ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego, pozostałe przepisy tej ustawy stosuje się odpowiednio. 4. Stronę zawiadamia się o czynnościach w sprawie przez publiczne udostępnienie informacji w Biuletynie Informacji Publicznej na stronie podmiotowej ministra właściwego do spraw informatyzacji. 5. Przed wydaniem polecenia zabezpieczającego minister właściwy do spraw informatyzacji przeprowadza we współpracy z Zespołem, o którym mowa w art. 35 ust. 3, analizę obejmującą: 1) istotność cyberzagrożenia; 2) rodzaje ryzyk; 3) przewidywane lub zaistniałe skutki incydentu krytycznego;	Uwaga nieuwzględniona Sektor bankowy z uwagi na swoją krytyczność również powinien podlegać wymogom polecenia zabezpieczającego. Pamiętać należy, że jest to instytucja wyjątkowa, stosowana w szczególnej sytuacji wystąpienia incydentu krytycznego.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			4) skuteczność obowiązku określonego zachowania zmniejszającego skutki incydentu krytycznego lub zapobiegającego jego rozprzestrzenianiu się. 6. Do analizy, o której mowa w ust. 5, nie stosuje się art. 106 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego. 7. Dyrektor Rządowego Centrum Bezpieczeństwa, Szef Agencji Bezpieczeństwa Wewnętrznego oraz minister właściwy do spraw informatyzacji, może wzywać podmioty, o których mowa w ust. 2, lub organy administracji publicznej do udzielenia informacji niezbędnych do przeprowadzenia analizy. 8. Przedstawiciele podmiotów, o których mowa w ust. 2, lub organów administracji publicznej mogą być zapraszani przez dyrektora Rządowego Centrum Bezpieczeństwa do udziału w pracach Zespołu lub posiedzeniach Zespołu w związku z przygotowywaniem analizy, o której mowa w ust. 5. 9. Polecenie zabezpieczające zawiera: 1) wskazanie rodzaju lub rodzajów podmiotów, których dotyczy; 2) obowiązek określonego zachowania zmniejszającego skutki incydentu krytycznego lub zapobiegającego jego rozprzestrzenianiu się; 3) termin jego wdrożenia. 10. Obowiązkiem określonego zachowania, o którym mowa w ust. 9 pkt 2, jest: 1) nakaz przeprowadzenia szacowania ryzyka związanego ze stosowaniem określonego produktu ICT, usługi ICT lub procesu ICT i wprowadzenie środków ochrony proporcjonalnych do zidentyfikowanych ryzyk; 2) nakaz przeglądu planów ciągłości działania i planów odtworzenia działalności pod kątem ryzyka wystąpienia incydentu krytycznego związanego z daną podatnością; 3) nakaz zastosowania określonej poprawki bezpieczeństwa w produkcie ICT, procesie ICT lub usłudze ICT posiadającym daną podatność; 4) nakaz szczególnej konfiguracji produktu ICT, usługi ICT lub procesu ICT, zabezpieczającej przed wykorzystaniem określonej podatności; 5) nakaz wzmożonego monitorowania zachowania systemu; 6) zakaz korzystania z określonego produktu ICT, usługi ICT lub procesu ICT, które posiada podatność, która przyczyniła się do zaistnienia incydentu krytycznego; 7) nakaz wprowadzenia ograniczenia ruchu sieciowego z adresów IP lub adresów URL wchodzącego do infrastruktury podmiotu kluczowego lub podmiotu ważnego, który skutkując zakłóceniem usług świadczonych przez ten podmiot został sklasyfikowany przez CSIRT MON, CSIRT NASK lub CSIRT GOV jako przyczyna trwającego incydentu krytycznego; 8) nakaz wstrzymania dystrybucji lub zakaz instalacji określonej wersji oprogramowania; 9) nakaz zabezpieczenia określonych informacji, w tym dzienników systemowych; 10) nakaz wytworzenia obrazów stanu określonych urządzeń zainfekowanych złośliwym oprogramowaniem. 11. Wskazanie obowiązku określonego zachowania, o którym mowa w ust. 9 pkt 2, następuje z uwzględnieniem środków adekwatnych, w szczególności w świetle analizy, o której mowa w ust. 5. 12. Polecenie zabezpieczające wydaje się na czas koordynacji obsługi incydentu krytycznego lub na czas oznaczony, nie dłużej niż na dwa lata.	

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

		13. Polecenie zabezpieczające wygasa: 1) z dniem wskazanym w ogłoszeniu o zakończeniu koordynacji obsługi incydentu w dzienniku urzędowym ministra właściwego do spraw informatyzacji, lub 2) po upływie czasu, na który zostało wydane. 14. Polecenie zabezpieczające podlega natychmiastowej wykonalności. 15. Minister właściwy do spraw informatyzacji ogłasza polecenie zabezpieczające w dzienniku urzędowym ministra właściwego do spraw informatyzacji. Informacje o poleceniu zabezpieczającym udostępnia się również na stronie internetowej urzędu obsługującego ministra. 16. Polecenie zabezpieczające uznaje się za doręczone z chwilą ogłoszenia polecenia zabezpieczającego w dzienniku urzędowym ministra właściwego do spraw informatyzacji. 17. Od polecenia zabezpieczającego nie przysługuje wniosek o ponowne rozpatrzenie sprawy. Uwaga ogólna Podmioty kluczowe będą zobowiązane do wykonania polecenia zabezpieczającego wydawanego przez ministra właściwego do spraw informatyzacji, w sytuacji wystąpienia incydentu krytycznego. Wskazany instrument budzi wątpliwości, ponieważ może naruszać swobodę działalności gospodarczej podmiotów kluczowych, które – w przypadku wejścia w życie projektowanej regulacji - nie będą mogły same podjąć decyzji o zastosowaniu adekwatnego środka, a ich działania będą ograniczone do natychmiastowego wykonania nakazu określonego zachowania. Jakie będzie podejście do wskazanego zagadnienia w przypadku, gdy podmiot kluczowy zareaguje szybciej niż organ administracyjny, a przedsięwzięte przez niego środki będą inne od tych, które zostały określone w decyzji administracyjnej i ich zastosowanie będzie niemożliwe z uwagi na podjęcie innych środków przeciwdziałających incydentowi krytycznemu? Mając jednak na uwadze przewidziane w projekcie ustawy wysokie kary pieniężne, może to doprowadzić do sytuacji, w której podmioty kluczowe nie będą mogły szybko i efektywnie reagować na pojawiające się incydenty o charakterze krytycznym. Banki w swojej bieżącej działalności stosują bowiem rozwiązania w zakresie bezpieczeństwa na bardzo wysokim poziomie, wdrażając najlepsze praktyki rynkowe i rozwiązania dostosowane do charakteru prowadzonej działalności oraz adekwatne do przeprowadzonego szacowania ryzyka. Wprowadzenie polecenia zabezpieczającego może spowodować znaczne zmniejszenie efektywności w reagowaniu na incydenty o charakterze krytycznym oraz wpłynąć istotnie na kwestię zarządzania ryzykiem z uwagi na fakt, że to organy administracji rządowej będą decydowały o sposobie rozwiązania incydentu o charakterze krytycznym, a nie same podmioty kluczowe. Samodzielne zarządzanie bezpieczeństwem umożliwia bankom wdrażanie zaawansowanych i kosztownych systemów zabezpieczeń dostosowanych do specyfiki działalności, natomiast proponowane rozwiązanie legislacyjne może spowodować niepełne wykorzystanie ich możliwości. Należy zauważyć, że koszty zastosowania wskazanych poleceń organów poniosą podmioty kluczowe, które i tak stosują adekwatne, kosztowne zabezpieczenia w wykorzystywanych systemach informacyjnych. M.in. z uwagi na wskazane wyżej argumenty, uzasadnione jest wyłączenie stosowania wskazanych przepisów w odniesieniu do sektora bankowego – vide uwaga nr 1. Stosowne działania dotyczące banków, w przypadku incydentów krytycznych podejmowane są już obecnie przez CSIRT KNF. Dublowanie	

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			uprawnień i obowiązków w tym zakresie będzie powodować szereg trudności praktycznych oraz interpretacyjnych oraz dodatkowo doprowadzi do zaangażowania znacznych zasobów, które powinny być w takich przypadkach przeznaczone na obsłużenie incydentu.	
84.	Polska Izba Informatyki i Telekomunikacji	Art. 67g	Art. 67g – polecenie zabezpieczające Zgodnie z projektowanym ust. 8 wprowadzono słuszne uprawnienie dyrektora RCB do dopraszania podmiotów kluczowych lub ważnych do prac zespołu prowadzącego analizę przed wydaniem polecenia zabezpieczającego. Udział w pracach podmiotu wydaje się wręcz niezbędny, aby polecenie było proporcjonalne do zagrożenia oraz realne do wdrożenia bez tworzenia dodatkowych zagrożeń w ramach obsługi incydentu krytycznego. Wnosimy o uzupełnienie przepisów o wprowadzenie zasady informowania podmiotu kluczowego lub ważnego o rozpoczęciu prac nad ewentualnym wydaniem polecenia zabezpieczającego.	Uwaga nieuwzględniona Należy tutaj jednak zostawić fakultet zapraszania – incydent krytyczny może dotyczyć różnego zakresu podmiotowego.
85.	Polska Izba Informatyki i Telekomunikacji	Art. 67g	Art. 67g ust. 5 w zw. z ust. 11 – przesłanki do uwzględniania w toku analizy Wnosimy o uzupełnienie katalogu przesłanek analizowanych przed wydanie polecenia zabezpieczającego, o określenie spodziewanych skutków zastosowania się do polecenia w zakresie kosztów jego wdrożenia, czasu niezbędnego na realizację, a także ciągłość świadczenia usług przez podmiot kluczowy lub ważny oraz odtworzenie ich działania. Rozumiejac nadzwyczajną instytucję polecenia, zwracamy jednak uwagę na bardzo poważne skutki, które jego zastosowanie może wywołać, także w zakresie odpowiedzialności podmiotu kluczowego lub ważnego wobec podmiotów trzecich, w tym dostawców, usługodawców lub usługobiorców. Tym bardziej jego wydanie musi odbywać się w sposób szeroko uwzględniający skutki wydania decyzji. Przewidziana w ust. 11 „adekwatność” wydaje się w tym zakresie istotnie niewystarczająca.	Uwaga uwzględniona W związku z uwzględnieniem uwagi RCL.
86.	Polska Izba Informatyki i Telekomunikacji	Art. 67g	Art. 67g ust. 12 – czas obowiązywania polecenia zabezpieczającego Przewidziany maksymalny czas (2 lata) stosowania polecenia zabezpieczającego wydaje się zdecydowanie zbyt długi. W naszej ocenie polecenie powinno być wydawane na okres obsługi incydentu, nie dłuższy niż 30 dni, z możliwością jego przedłużenia, jeśli incydent nie został zamknięty.	Uwaga wyjaśniona Może się wydarzyć incydent który będzie trwał długo – i nikt nie jest w stanie tego przewidzieć.
87.	Polska Organizacja Handlu i Dystrybucji	Art. 67g.12.	Wydawanie Poleceń zabezpieczających podlegających natychmiastowej wykonalności i obowiązujące na okres do dwóch lat może sparaliżować działanie podmiotu kluczowego i ważnego. Polecenie zabezpieczające co do zasady powinno być krótkookresowe i służyć ograniczeniu strat w sytuacji incydentu poważnego - max 2 tygodnie.	Uwaga wyjaśniona Trudno przewidzieć czas trwania incydentu krytycznego – incydent może trwać nawet kilka miesięcy, stąd też wskazano okres dwuletni.
88.	Konfederacja Lewiatan	Art. 67g 12.	Czas obowiązywania polecenia zabezpieczającego Jednostka redakcyjna: Art. 67g ust. 12 Przewidziany maksymalny czas (2 lata) stosowania polecenia zabezpieczającego wydaje się zdecydowanie zbyt długi. W naszej ocenie polecenie powinno być wydawane na okres obsługi incydentu, nie dłuższy niż 30 dni, z możliwością jego przedłużenia, jeśli incydent nie został zamknięty.	Uwaga wyjaśniona Trudno przewidzieć czas trwania incydentu krytycznego, stąd też wskazano okres dwuletni.
89.	Polskie Stowarzyszenie Fotowoltaiki	Art. 67g-67k	[Polecenie zabezpieczające] W razie wystąpienia incydentu krytycznego minister właściwy ds. informatyzacji może wydać tzw. polecenie zabezpieczające. Zgodnie z KSC, incydent krytyczny oznacza incydent skutkujący znaczną	Uwaga wyjaśniona Co do przesłanek wydana polecenia zabezpieczającego to będzie ono

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

		szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi, klasyfikowany przez właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV. Pojęcie incydentu krytycznego nie jest obecne zarówno w Dyrektywie NIS jak i Dyrektywie NIS2. Polecenie zabezpieczające w formie tzw. decyzji generalnej ma zastosowanie do nieokreślonej liczby PK i PW. Wydanie polecenia zabezpieczającego poprzedzone ma być analizą cyberzagrożenia, ryzykami, skutkami incydentu oraz skutecznością obowiązku określonego zachowania na zmniejszenie skutków incydentu przeprowadzanej wraz z Zespołem do spraw incydentów krytycznych. PW i PK zobowiązane będą do udzielenia odpowiednim organom informacji niezbędnych do przeprowadzenia ww. analizy. Polecenie zabezpieczające określa (1) rodzaje podmiotów, których dotyczy, (2) obowiązek określonego zachowania przewidzianego skutkiem incydentu krytycznego; (3) termin jego wdrożenia. Polecenie zabezpieczające może obejmować zobowiązanie m.in. do: - przeprowadzenia szacowania ryzyka związanego ze stosowaniem określonego produktu ICT, usługi ICT lub procesu ICT - przeglądu planów ciągłości działania i planów odtworzenia działalności; - zastosowania określonej poprawki bezpieczeństwa w produkcie ICT, procesie ICT lub usłudze ICT; - szczególnej konfiguracji produktu ICT, usługi ICT lub procesu ICT; - niekorzystania z określonego produktu ICT, usługi ICT lub procesu ICT; - wprowadzenia ograniczenia ruchu sieciowego z adresów IP lub adresów URL; - wstrzymania dystrybucji lub zakaz instalacji określonej wersji oprogramowania. Polecenie zabezpieczające wydaje się na czas koordynacji obsługi incydentu krytycznego lub na czas oznaczony, nie dłużej niż na dwa lata. Informacja o wydaniu polecenia zabezpieczającego podlega publikacji również na stronie internetowej urzędu ministra. Podmioty objęte poleceniem zabezpieczającym zobowiązane są do poinformowania o jego wykonaniu. Na polecenie zabezpieczające przysługuje skarga do sądu administracyjnego, niemniej nie jest dopuszczalny wniosek o przywrócenie terminu do jej złożenia. Ogólny wpływ regulacji: Przepisy dotyczące możliwości wydawania poleceń zabezpieczających w proponowanym kształcie mogą powodować daleko idące skutki w postaci wykluczenia wskazanych w poleceniu dostawców. Zgodnie z projektowanym art. 67g ust. 14 KSC wg Projektu, polecenie zabezpieczające podlega natychmiastowemu wykonaniu, co może oddziaływać na zakłócenie działalności przedsiębiorcy i powodować nadmierne koszty prowadzenia działalności. Co istotne, z poleceń wynikają restrykcyjne obowiązki nałożone na PK i PW, których wydaniu towarzyszy rygor natychmiastowej wykonalności, a dodatkowo polecenia zabezpieczające wydawane są w oparciu o nieokreślone przesłanki. Zwracamy uwagę, że Projekt nie przewiduje katalogu przesłanek, które muszą zostać spełnione, aby minister właściwy do spraw informatyzacji wydał polecenie zabezpieczające.	wydawane w sytuacji zaistnienia incydentu krytycznego, czyli tego najgorszego w skutkach incydentu. Polecenie zabezpieczające ma być adekwatne do zidentyfikowanych ryzyk, co będzie też mogło być zbadane potem przez sąd administracyjny. Nie jest intencją projektodawcy aby polecenie doprowadziło do kolejnego incydentu albo do cenzury internetu.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			Wpływ na sektor energetyczny: Jednym z obowiązków nałożonych na PK i PW wynikających z polecenia zabezpieczającego jest zakaz korzystania określonego produktu ICT, usługi ICT lub procesu ICT, które posiada podatność, która przyczyniła się do zaistnienia incydentu krytycznego. Wykorzystanie bowiem usług ICT w energetyce jest elementem kluczowym z punktu widzenia źródeł energii oraz zasadami sterowania pracą sieci elektroenergetycznych. W tym kontekście, widzimy potencjalne ryzyko, że wprowadzenie możliwości wydawania poleceń zabezpieczających posiadających rygor natychmiastowej wykonalności, oprócz zaburzenia prowadzenia działalności gospodarczej przez określone podmioty, obciążania tych podmiotów dodatkowymi kosztami, może także pośrednio wpływać na ciągłość dostaw energii elektrycznej. [Nadregulacja względem Dyrektywy NIS2] Regulacje dot. incydentu krytycznego na gruncie obecnie obowiązującej KSC nie znajdują oparcia w przepisach Dyrektywy NIS. Podobnie, Dyrektywa NIS2 nie rozróżnia tego rodzaju incydentu. Również proponowane w Projekcie postanowienia dot. wydawania poleceń zabezpieczających w razie zaistnienia incydentu krytycznego nie znajduje oparcia w Dyrektywie NIS2. W rezultacie, wprowadzenie postanowień dotyczących polecenia zabezpieczającego znacząco wykracza poza zakres przedmiotowy Dyrektywy NIS2. Ponadto, Projekt zakłada kompetencję ministra ds. informatyzacji m.in. do zakazania stosowania przez PK i PW określonych produktów ICT, usług ICT lub procesów ICT lub ich zmian, niezależnie od innych środków prawnych przewidzianych w ustawie. Stosowanie polecenia zabezpieczającego może umożliwiać arbitralne blokowanie dostępu do treści w Internecie lub wykorzystanie dostępnych na rynku produktów, w tym produktów ICT. Instytucja polecenia zabezpieczającego była przedmiotem poprzednich projektów ustaw zmieniających KSC, w szczególności projektu z 8 września 2020 r. Pomimo jej wycofania z Projektu z 3 lipca 2023 r. na skutek szerokiej krytyki środowisk branżowych, instytucja ta ponownie została wprowadzona do Projektu. Rekomendacja: - usunięcie z Projektu propozycji nowych przepisów art. 67g-67k KSC wg Projektu; - alternatywnie, usunięcie rygoru natychmiastowej wykonalności decyzji - polecenia zabezpieczającego.	
90.	Związek Pracodawców Technologii Cyfrowych Lewiatan	Art. 67g	Polecenie zabezpieczające a stopnie alarmowe CRP Wydaje się zasadne by w sytuacji wystąpienia incydentu krytycznego była również możliwość zmiany stopnia alarmowego CRP (ustawa o działaniach antyterrorystycznych, art. 15 ust. 2, art. 16 ust. 2 Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (sejm.gov.pl)) Patrz także uwagę dotyczącą niezbędnej nowelizacji ustawy o działaniach antyterrorystycznych.	Uwaga wyjaśniona W praktyce to może się okazać zasadne, natomiast aktualnie nie wydaje się konieczna zmiana wskazanych przepisów.
91.	Związek Pracodawców Technologii	Art. 67g	Sposób powiadamiania w przypadku incydentu krytycznego skutkującego poleceniem zabezpieczającym (art. 67g ust. 4) Jeśli wystąpi incydent krytyczny to proponowane w projekcie rozwiązanie polegające na publikowaniu informacji na stronie Biuletynu Informacji Publicznej należy uznać za dalece niewystarczające. W tym przypadku jednak należy użyć zarówno metody push (np. wysłanie wiadomości	Uwaga wyjaśniona Polecenie zabezpieczające będzie mogło być przekazane także za pomocą systemu S46.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

	Cyfrowych Lewiatana		przez system S46, wysłanie SMSem wiadomości do właściwych osób o pojawieniu się polecenia zabezpieczającego, itd.), jak i metody pull (wprowadzenie polecenia na BIP).	
92.	Związek Pracodawców Technologii Cyfrowych Lewiatan	Art. 67g	Podział kompetencji (art. 67g ust. 7 i ust. 8 oraz art. 35) Zgodnie z art. 35 ust. 1 Dyrektor Rządowego Centrum Bezpieczeństwa jest tylko informowany o incydencie krytycznym. O jego obecności w Zespole do spraw Incydentów Krytycznych nic nie mówi ust. 3. W zasadzie działanie od Dyrektora jest oczekiwane jeśli pojawi się wniosek o zwołanie Rządowego Zespołu Zarządzania Kryzysowego, co jest tylko opcjonalne (patrz art. 35 ust. 2 punkt 2). Zapisy art. 67g ust. 7 i ust. 8 powinny być zatem zrewidowane pod kątem zapisu kompetencji właściwych organów.	Uwaga wyjaśniona Przedstawiciel RCB jest członkiem Zespołu do Spraw Incydentów Krytycznych.
93.	Związek Pracodawców Technologii Cyfrowych Lewiatan	Art. 67g	Obowiązek określonego zachowania (art. 67g ust. 10) Proponujemy zmianę w zapisie ust. 10 Jest: „Obowiązkiem określonego zachowania, o którym mowa w ust. 9 pkt 2, jest:” Propozycja: „Obowiązkiem określonego zachowania, o którym mowa w ust. 9 pkt 2, może być m.in.:” Uzasadnienie: dla różnych poleceń zabezpieczających mogą być różne zakresy działań. Proponowany zapis pozwala na kształtowanie wymaganych zachowań wskazując jednocześnie na podstawową listę oczekiwanych zachowań. Jednocześnie: Postulujemy dodanie do listy nakazów obowiązku przygotowania odpowiednich kopii bezpieczeństwa (backupów) dla wszystkich podmiotów kluczowych i ważnych. Postulujemy dodanie do listy nakazów dla podmiotów krytycznych przygotowanie do ewakuacji do chmury obliczeniowej, zgodnie z przygotowanym planem ochrony. Por. Narodowy Program Ochrony Infrastruktury Krytycznej, załącznik Nr 1.	Uwaga wyjaśniona Minister właściwy do spraw informatyzacji jest obowiązany wybrać adekwatne rozwiązanie do polecenia zabezpieczającego – może to być wskazanie kilku nakazów. I wynika to już z obecnego brzmienia. W poleceniu mamy już obowiązek zabezpieczenia informacji, co uznajemy za równoważne z backupem. Kwestie obowiązków podmiotów krytycznych wolimy pozostawić w dyrektywie CER.
94.	Związek Pracodawców Technologii Cyfrowych Lewiatan	Art. 67g	Sposób doręczenia polecenia zabezpieczającego (art. 67g ust. 16) Postulujemy zrewidowanie tego zapisu tak aby wszystkie podmioty kluczowe i ważne były odpowiednio szybko powiadomione, zwłaszcza że ust. 14 mówi o natychmiastowej wykonalności. Por. uwagę dot. art. 67g ust. 4 powyżej.	Uwaga wyjaśniona Informacja o poleceniu będzie mogła być przekazywana także za pomocą S46.
95.	Związek Telewizji Kablowych Izba Gospodarcza	Art. 67h	Polecenie zabezpieczające Dyrektywa NIS 2 mimo regulowania problematyki incydentów ¹ związanych z cyberbezpieczeństwem, to jednakże nie przewiduje na okoliczność wystąpienia incydentu krytycznego wydawania w formie decyzji poleceń zabezpieczających, ani też nie zobowiązuje państw członkowskich do wprowadzania regulacji poświęconych instytucji poleceń zabezpieczających. Wprowadzenie zatem do projektu ustawy zmieniającej ustawę o KSC regulacji poświęconych poleceniu zabezpieczającemu nie stanowi implementacji dyrektywy NIS 2, a zatem państwo polskie nie jest zobowiązane do wprowadzenia tego rodzaju regulacji do wewnętrznego porządku prawnego, co przesądza o tym, iż wprowadzenie tego rodzaju regulacji nie jest obowiązkowe dla państwa polskiego w świetle normy art. 288 zd. 4 Traktatu o funkcjonowaniu Unii Europejskiej. Propozycja zatem wprowadzenia niezwykle dolegliwej dla podmiotów ważnych i kluczowych regulacji polecenia zabezpieczającego stanowi kolejny przykład złej woli projektodawcy, który zamiast dążyć do jak najmniejszego obciążania polskich przedsiębiorców dolegliwymi regulacjami postępuje dokładnie	Uwaga wyjaśniona Zgodnie z dyrektywą NIS 2 (art. 32 ust. 4 lit. b): „Państwa członkowskie zapewniają, aby wykonując uprawnienia w zakresie egzekwowania przepisów wobec podmiotów kluczowych, ich właściwe organy były uprawnione co najmniej do: b) wydawania wiążących poleceń – w tym dotyczących podjęcia środków niezbędnych do zapobieżenia incydentowi lub usunięcia jego skutków oraz określenia terminów wdrożenia takich środków i

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			odwrotnie dążąc ze wszystkich sił do jak najpoważniejszego ich dociążenia (projektowany art. 67 g ust. 9 ustawy o KSC). W sytuacji zatem, gdy dyrektywa NIS 2 nie obliguje polskiego prawodawcy do wdrażania do polskiego systemu prawnego instytucji polecenia zabezpieczającego, a zatem odnośnie tej instytucji obowiązek przewidziany w art. 288 zd. 4 Traktatu o funkcjonowaniu Unii Europejskiej nie zachodzi postulujemy wprowadzenie zmiany art. 1 pkt. 70 projektu ustawy zmieniającej ustawę o KSC poprzez wykreślenie proponowanej regulacji art. 67 g, art. 67 h, art. 67 i ustawy o KSC poświęconej problematyce polecenia zabezpieczającego.	<i>zgłoszenia ich wdrożenia – lub nakazów zobowiązujących dane podmioty do naprawienia stwierdzonych uchybień lub usunięcia naruszeń niniejszej dyrektywy;”</i> Wobec powyższego, w ocenie projektodawcy, polecenie zabezpieczające mieści się w ramach dyrektywy NIS 2.
96.	Fundacja Bezpieczna Cyberprzestrzeń	Art. 67j	Art. 1 pkt 70, treść art. 67j – przepisy tego artykułu są niezrozumiałe. Dlaczego i w jakim zakresie publikacja listy produktów ICT, usług ICT i konkretnych procesów ICT objętych decyzjami, o których mowa w art. 67b ust. 15 nie stosuje się do NBP? Może ustawodawca miał na myśli art. 67g? To tym bardziej prawdopodobne, że w ust. 2 powołuje się na nieistniejącą jednostkę redakcyjną czyli art. 67f ust. 1 – art. 67f nie ma ustępu 1. Ponadto, wyłączenie NBP ze stosowania przepisów dotyczących wycofania produktów ICT, usług ICT lub procesów ICT pochodzących od dostawcy wysokiego ryzyka należy uznać za nieuzasadnioną lukę w krajowym systemie cyberbezpieczeństwa i niebezpieczny precedens. Wskazana w uzasadnieniu niezależność NBP nie może być w tym przypadku usprawiedliwieniem tworzenia takiej luki. Właśnie w tym celu tworzy się przepisy ustawowe, które mogą regulować, w określonym celu, niezależność instytucji typu NBP. W kontekście bezpieczeństwa państwa objęcie przepisami art. 67b i art. 67g wszystkich podmiotów KSC wydaje się niezbędne. Dodatkowo, cele ustawy o KSC i NBP w kontekście jego zadań i funkcji (NBP) w zakresie bezpieczeństwa są tożsame i ograniczenia w tym zakresie byłyby w sprzeczności lub utrudniałyby wręcz NBP realizację tych zadań i funkcji.	Uwaga wyjaśniona Odesłanie w przepisie art. 67j zostanie poprawione. Ponownie należy podkreślić, że wyłączenie NBP spod polecenia zabezpieczającego i decyzji HRV wynika z jego konstytucyjnej niezależności.
97.	Związek Telewizji Kablowych Izba Gospodarcza	Art. 67j	Uprzywilejowana pozycja Narodowego Banku Polskiego Z sobie tylko znanych powodów projektodawca przewiduje szczególnie uprzywilejowaną pozycję Narodowego banku Polskiego przejawiająca się w tym, że wobec przedmiotowego Banku nie znajdują zastosowania regulacje poświęcone wydaniu decyzji o uznaniu za dostawcę wysokiego ryzyka oraz skutkom płynącym z faktu wydania tego rodzaju decyzji (art. 67 b i art. 67 f ustawy o KSC), co przesądza o tym, iż nawet jeżeli konkretny podmiot zostanie uznany za dostawcę wysokiego ryzyka, to i tak Narodowy Bank Polski ani nie będzie zobowiązany do wycofania produktów ICT, usług ICT, procesów ICT w jakimkolwiek terminie, ani też nie zostanie pozbawiony możliwości na przyszłość zakupywania i stosowania od takiego dostawcy oferowanych przez niego produktów ICT, procesów ICT, czy też usług ICT. Nie trzeba chyba nikogo przekonywać, że taka regulacja projektowanego art. 67 j ustawy o KSC narusza konstytucyjną zasadę równości wszystkich wobec prawa (art. 32 ust. 1 zd. 1 Konstytucji RP), oraz obowiązku traktowania przez władze publiczne wszystkich z poszanowaniem zasady równości (art. 32 ust. 1 zd. 2 Konstytucji RP). Również przedmiotową regulację trudno by było uznać za zgodną z konstytucyjnymi zasadami sprawiedliwości społecznej i demokratycznego państwa prawnego (art. 2 w zw. z art. 8 Konstytucji RP).	Uwaga wyjaśniona Ponownie należy podkreślić, że wyłączenie NBP spod polecenia zabezpieczającego i decyzji HRV wynika z jego konstytucyjnej niezależności.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			Kierując się zasadami racjonalnego myślenia doprawdy trudno zrozumieć tego rodzaju decyzję projektodawcy, który z jednej strony przejawia olbrzymie obawy z powodu różnorodnych zagrożeń dla bezpieczeństwa państwa polskiego, czemu daje wyraz także proponowaniem wprowadzenia regulacji nie będących skutkiem implementacji dyrektywy NIS 2, z drugiej zaś strony nie przejawia żadnej obawy o środki finansowe i rezerwy złota zgromadzone w polskim Banku Centralnym, skoro dopuszcza do sytuacji, w której Narodowy Bank Polski przez nieograniczony okres czasu będzie korzystał z produktów ICT, usług ICT oraz procesów ICT pochodzących od dostawcy wysokiego ryzyka. Kierując się zasadami racjonalnego myślenia, względami słuszności oraz naruszeniem przytoczonych powyżej norm konstytucyjnych zdecydowanie optujemy za usunięciem z ustawy o KSC uprzywilejowanej pozycji Narodowego banku Polskiego i z tego właśnie powodu wnosimy o wprowadzenie zmiany art. 1 pkt. 70 projektu ustawy zmieniającej ustawę o KSC poprzez wykreślenie projektowanego przepisu art. 67 j ustawy o KSC.	
98.	Konfederacja Lewiatan	Art. 67k	Niedopuszczalne zmieszanie kompetencji wojskowych z cywilnymi oraz brak transparentności w formie komunikatu w tej sprawie Jednostka redakcyjna: art. 67k projektu KSC Jednostka redakcyjna NIS2: nie dotyczy Uwaga: Na podstawie art. 67k ust. 1 projektu KSC, Prezes Rady Ministrów, działając na podstawie rekomendacji Kolegium, w uzgodnieniu z Ministrem Obrony Narodowej, może czasowo powierzyć temu ministrowi realizację wybranych zadań, o których mowa w art. 26 ustawy. Jednakże, niniejsze przepisy budzą poważne zastrzeżenia z kilku kluczowych powodów: Po pierwsze przepisy art. 67k projektu KSC pozwalają Ministrowi Obrony Narodowej przejąć koordynację działań związanych z obsługą incydentów cyberbezpieczeństwa, bez względu na stan wojny lub stan wojenny. Oznacza to, że w drodze arbitralnego komunikatu, MON może uzyskać kompetencje, o których mowa w art. 26 projektu KSC, rozciągające się na całą cyberprzestrzeń w Polsce, nawet w czasie pokoju. Takie rozwiązanie jest niedopuszczalne, ponieważ prowadzi do zmieszania kompetencji wojskowych z cywilnymi. Wprowadzenie tego typu kompetencji dla MON w czasie pokoju narusza zasadę rozdziału władzy cywilnej i wojskowej, co jest fundamentalną zasadą demokratycznego państwa prawa. Po drugie powierzenie realizacji zadań odbywa się na podstawie komunikatu ogłaszanego w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski”. Komunikat ten nie ma charakteru decyzji administracyjnej, co uniemożliwia podmiotom dotkniętym tym komunikatem odwołanie się od niego i skutecznie kwestionowanie jego zasadności. Taka forma jest nieakceptowalna, gdyż łamie podstawowe zasady praworządności i transparentności, przewidziane w Konstytucji RP. Po trzecie przepisy nie określają maksymalnego okresu, na jaki mogą zostać powierzone zadania Ministrowi Obrony Narodowej. Aby zapewnić tymczasowy charakter tego powierzenia, powinno być ono ograniczone do konkretnego okresu, np. nie dłużej niż 3 miesiące. Brak takiego ograniczenia stwarza ryzyko, że tymczasowe powierzenie zadań może de facto stać się permanentne, co dodatkowo narusza zasadę rozdziału kompetencji wojskowych i cywilnych	Uwaga częściowo uwzględniona Zostanie wprowadzony maksymalny termin na powierzenie zadań MON.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			Wreszcie powierzenie Ministrowi Obrony Narodowej realizacji zadań w zakresie cyberbezpieczeństwa, nawet w czasie pokoju, może prowadzić do erozji cywilnej kontroli nad wojskiem. Jest to szczególnie niebezpieczne w kontekście utrzymania równowagi między siłami cywilnymi a wojskowymi, co jest kluczowym elementem stabilności i bezpieczeństwa demokratycznego państwa.	
99.	Osoba fizyczna	Art. 69	Art. 69 ust. 1 – Zastosowano zapis określający zakres strategii, gdzie w pkt 2 jest mowa o szacowaniu ryzyka – proponuję rozwiniecie zapisu do postaci „szacowania ryzyka w cyberbezpieczeństwie” lub „ryzyka cyberbezpieczeństwa”.	Uwaga uwzględniona Brzmienie przepisu zostanie zmienione.
100.	Osoba fizyczna	Art. 69	Art. 69 ust. 2 – Zastosowano zapisy określające zagadnienia uwzględniane w opracowywaniu strategii. Proponuję wprowadzić zapisy rozszerzające o zagadnienia: 1) współzależności i integracji strategii cyberbezpieczeństwa ze strategią bezpieczeństwa narodowego, 2) współzależności i integracji zarządzania i operowania w zakresie cyberbezpieczeństwa na poziomie krajowym, zarządzania sytuacjami kryzysowymi w cyberbezpieczeństwie i zarządzania kryzysowego w cyberbezpieczeństwie z zarządzaniem kryzysowym i zarządzaniem sytuacjami kryzysowymi, realizowanymi w ramach zarządzania kryzysowego ustawy o zarządzaniu kryzysowym i CER.	Uwaga nieuwzględniona W ramach przygotowywania strategii następuje współdziałanie z organami odpowiedzialnymi za strategię bezpieczeństwa narodowego. Nie ma potrzeby większego powiązania tych dokumentów. W zakresie punktu 2 należy zauważyć, że te kwestie będą rozstrzygnięte w ramach Krajowego Planu reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę.
101.	Osoba fizyczna	Art. 69	Art. 69 ust. 2 pkt 1 i 2 – Proponuję rozszerzyć zakres zapisu do pełnej stosowanej formuły „produkty ICT, usługi ICT i procesy ICT”	Uwaga uwzględniona
102.	Konfederacja Lewiatan	Art. 69	Brak odpowiedniej formy Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskie Jednostka redakcyjna: art. 69 projektu KSC Jednostka redakcyjna NIS2: art. 7 Uwaga: Implementacja przepisów nie powinna polegać na automatycznym przenoszeniu postanowień Dyrektywy NIS2 do krajowego porządku prawnego. Konieczna jest adaptacja i implementacja do realiów prawnych, co obejmuje obowiązujący w Polsce katalog źródeł prawa. Dyrektywa NIS2 nakłada określone obowiązki na państwa członkowskie UE w zakresie cyberbezpieczeństwa, ale każda implementacja musi uwzględniać specyficzne warunki i wymagania prawne danego kraju. Zasady określone w art. 69 ust. 1 pkt 3 projektu KSC dotyczące współpracy między sektorem publicznym i prywatnym powinny być sformalizowane jako ustawa, aby zapewnić ich przestrzeganie. Taka regulacja zapewniłaby, że obie strony będą zobowiązane do współpracy w określonych warunkach i na określonych zasadach, co zwiększy efektywność działań w zakresie cyberbezpieczeństwa. Mechanizmy wymiany informacji między organami właściwymi w art. 69 ust. 1 pkt 5 i ust. 2 pkt 8 projektu KSC powinny stanowić materię ustawową. To zapewniłoby, że wszystkie istotne informacje dotyczące cyberzagrożeń, incydentów oraz ryzyka będą systematycznie i skutecznie wymieniane między odpowiednimi podmiotami, co przyczyni się do zwiększenia bezpieczeństwa narodowego w obszarze cybernetycznym.	Uwaga wyjaśniona Postanowienia Strategii będą odnosić się do organów administracji rządowej podlegających Radzie Ministrów i nie będą zawierać postanowień prawa powszechnie obowiązującego. Jej postanowienia nie będą podstawą rozstrzygnięć wobec podmiotów spoza administracji rządowej. Postanowienia tego dokumentu nie naruszają kompetencji organów określonych w przepisach prawa. W związku z tym nie ma konieczności zmiany jego formy prawnej.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			Wymogi związane z cyberbezpieczeństwem w zamówieniach publicznych (art. 69 ust. 2 pkt 2 projektu KSC) powinny być również wprowadzone jako przepisy rangi ustawowej. Ustawowe wprowadzenie tych wymogów zapewni, że wszystkie zamówienia publiczne będą uwzględniać kwestie bezpieczeństwa cyfrowego, co jest kluczowe dla ochrony infrastruktury krytycznej. Wątpliwości budzi relacja strategii, o której mowa w art. 69 projektu KSC, w stosunku do strategii, o których mowa w art. 9 ustawy o zasadach prowadzenia polityki rozwoju. Analiza treści uzasadnienia nie przynosi w tym zakresie rozstrzygnięcia. Wprowadzenie strategii cyberbezpieczeństwa powinno być spójne z innymi strategiami rozwojowymi, aby zapewnić jednolitość i koherencję działań na poziomie krajowym. W tym celu niezbędne jest dokładne zbadanie i wyjaśnienie, jak nowa strategia będzie współgrać z istniejącymi planami i strategiami rozwoju, w szczególności w kontekście wykorzystania środków europejskich na realizację celów w zakresie osiągania wysokiego poziomu cyberbezpieczeństwa.	
103.	Fundacja Bezpieczna Cyberprzestrzeń	Rozdział 13a	Art. 1 pkt 73, treść rozdziału 13a (uwagę należy czytać w powiązaniu z uwagą ogólną nr 2 i pkt. 4 uwag szczegółowych) – przepisy tego rozdziału dublują rozwiązania przedstawione w dokumentach opracowanych na podstawie art. 5 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym. W opracowanym Krajowym Planie Zarządzania Kryzysowego, w siatce bezpieczeństwa, zidentyfikowano 19 zagrożeń, a w tym „zakłócenie funkcjonowania systemów i usług telekomunikacyjnych”. Natomiast w samym planie są moduły zadaniowe (zestawienie szczegółowych przedsięwzięć i sposobu ich realizacji), które dotyczą ministra właściwego do spraw informatyzacji. Postulowane w uzasadnieniu „zbliżenie reżimu krajowego systemu cyberbezpieczeństwa oraz zarządzania kryzysowego” da się zatem osiągnąć implementując wymagania dyrektywy NIS2 w istniejące mechanizmy zarządzania kryzysowego np. poprzez dodanie nowych modułów lub standardowych procedur operacyjnych. W związku z powyższym proponuje się usunięcie rozdziału 13a, a ewentualne przepisy w zakresie implementacji dyrektywy NIS2 umieścić w przepisach zmieniających ustawę o zarządzaniu kryzysowym, której nowelizacja jest aktualnie procedowana.	Uwaga nieuwzględniona Dyrektywa NIS 2 wymaga przyjęcia przez Polskę Krajowego planu reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę o określonej treści. Z tego względu należy zachować przedmiotowe przepisy w projekcie. Równocześnie projektodawca zdaje sobie sprawę z powiązań tego dokumentu z Krajowym Planem Zarządzania Kryzysowego co zostanie uwzględnione na etapie jego przygotowywania. Przedmiotowe przepisy były również przedmiotem konsultacji z Rządowym Centrum Bezpieczeństwa.
104.	Międzynarodowe Centrum Bezpieczeństwa Chemicznego	Rozdział 13	Promowanie kwalifikacji zawodowych w strategiach i planach krajowych Propozycja zapisu: W rozdziale 13 (STRATEGIA) proponujemy dodać punkt dotyczący kwalifikacji: „Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej oraz krajowy plan reagowania na incydenty i sytuacje kryzysowe uwzględniają rozwój i promocję kwalifikacji rynkowych w zakresie niezawodności i cyberbezpieczeństwa w przemyśle jako elementu zwiększania bezpieczeństwa narodowego.” Uzasadnienie: Uwzględnienie rozwoju kwalifikacji w strategiach i planach krajowych podkreśla ich znaczenie dla bezpieczeństwa narodowego. Dyrektywa NIS 2 wymaga oceny poziomu dojrzałości zdolności i zasobów w zakresie cyberbezpieczeństwa, co wymaga odpowiednich kompetencji.	Uwaga uwzględniona Przedmiotowa kwestia zostanie uwzględniona w ramach art. 69 ust. 2.
105.	Osoba fizyczna	Art. 72a	Art. 72a ust. 2 pkt 3 – Zastosowano zapis definiujący zakres Krajowego Planu w postaci „procedury zarządzania kryzysowego w cyberprzestrzeni, w tym ich włączenie do ogólnych krajowych ram zarządzania kryzysowego...”. Proponuję uszczegółowić poprzez dodanie „w rozumieniu ustawy o zarządzaniu	Uwaga uwzględniona

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			kryzysowym”. Proponuję uszczegółowić, że intencją jest współzależność i integracja Krajowego Planu z NPOIK w najszerszym możliwym zakresie.	
106.	Osoba fizyczna	Art. 72a	Art. 72a ust. 2 pkt 6 – Zastosowano zapis wprowadzający nowe pojęcie i nowy, jednorazowo wskazany byt: „krytyczna infrastruktura informatyczna”. Proponuję wprowadzić definicję tego pojęcia.	Uwaga wyjaśniona Określenie zostanie usunięte z projektu.
107.	Związek Pracodawców Technologii Cyfrowych Lewiatan	Art. 72b	Rodzaje krytycznej infrastruktury informatycznej (art. 72b ust. 2 punkt 6) Wydaje się, że zapisy dotyczące infrastruktury krytycznej (także: informatycznej) powinny znaleźć się w aktach prawnych dotyczących IK, natomiast w uksc powinien znaleźć się odpowiedni odnośnik.	Uwaga wyjaśniona Kwestia ta wykracza poza projekt.
108.	Osoba fizyczna	Art. 72a	Art. 72a ust. 2 pkt 7 – Zastosowano zapisy wprowadzające nowe pojęcia i nowe rodzaje działań: „skoordynowane zarządzanie incydentami”, „zarządzanie kryzysowe w cyberbezpieczeństwie na dużą skalę”. Proponuję wprowadzić definicje tych pojęć.	Uwaga nieuwzględniona Wskazane pojęcia opisują szerokie zestawy czynności jakie będą podejmowane. Niecelowe jest ograniczenie ich zakresu poprzez wskazanie konkretnych czynności, które miałyby się na nie składać.
109.	Konfederacja Lewiatan	Art. 72a	Nieprawidłowa forma prawna Krajowego planu reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę (uchwała Rady Ministrów to akt prawa wewnętrznego, a nie źródło prawa). Jednostka redakcyjna: art. 72a projektu KSC Jednostka redakcyjna NIS2: art. 9 Uwaga: Zgodnie z art. 72a projektu KSC Rada Ministrów przyjmuje Krajowy plan reagowania na incydenty i sytuacja kryzysowe w cyberbezpieczeństwie na dużą skalę w drodze uchwały. Taki plan określa cele i tryb zarządzania incydentami i zarządzania kryzysowego w cyberbezpieczeństwie na dużą skalę, a w szczególności zawiera: 1) zadania organów zaangażowanych w zarządzanie kryzysowe w cyberbezpieczeństwie; 2) zasady współpracy między sektorem publicznym i prywatnym w obszarze zarządzania kryzysowego; 3) rodzaje krytycznej infrastruktury informatycznej; 4) krajowe procedury i ustalenia między odpowiednimi organami i instytucjami krajowymi mające na celu zapewnienie efektywnego uczestnictwa danego państwa członkowskiego w skoordynowanym zarządzaniu incydentami i zarządzaniu kryzysowym w cyberbezpieczeństwie na dużą skalę na poziomie Unii oraz efektywnego wsparcia ze strony danego państwa członkowskiego dla tego rodzaju skoordynowanego zarządzania. Ww. materia nie powinna jednak stanowić przedmiot regulacji uchwały Rady Ministrów. Zgodnie z art. 93 Konstytucji RP uchwały Rady Ministrów oraz zarządzenia Prezesa Rady Ministrów i ministrów mają charakter wewnętrzny i obowiązują tylko jednostki organizacyjnie podległe organowi wydającemu te akty. Oznacza to zatem, że uchwała Rady Ministrów w postaci Krajowego planu reagowania na incydenty i	Uwaga nieuwzględniona Postanowienia planu będą odnosić się organów administracji rządowej podlegających Radzie Ministrów i nie będzie zawierał postanowień prawa powszechnie obowiązującego. Jego postanowienia nie będą podstawą rozstrzygnięć wobec podmiotów spoza administracji rządowej. W związku z tym nie ma konieczności zmiany jego formy prawnej.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			sytuacje kryzysowe w cyberbezpieczeństwie nie może obejmować materii dotyczących sektora prywatnego, sektora publicznego w zakresie jakim nie podlega Radzie Ministrów (np. jednostki samorządu terytorialnego). Proponowane zatem postanowienie wykracza poza kompetencje Rady Ministrów i wymagają one zmiany na formę odpowiedniego rozporządzenia lub ustawy.	
110.	Konfederacja Lewiatan	Art. 72b	Nieprecyzyjna zawartość Krajowego planu reagowania na incydenty i sytuacje kryzysowe w Cyberbezpieczeństwie na dużą skalę Jednostka redakcyjna: art. 72b projektu KSC Jednostka redakcyjna NIS2: art. 9 Uwaga: W art. 72b projektu KSC projektodawca posługuje się pojęciami, które nie są jednoznacznie zdefiniowane, co może negatywnie wpłynąć na wykonalność Krajowego planu. W szczególności: 1) W ust. 2 pkt 1) nie wiadomo, o jakiej gotowości mowa (<i>Krajowy Plan zawiera w szczególności: cele krajowych środków i działań służących w zakresie gotowości (?)</i>). Nie jest jasne, które podmioty zaliczają się do sektora publicznego, a które do prywatnego (czy np. spółki Skarbu Państwa należą do sektora prywatnego, czy publicznego – ust. 2 pkt 5). 2) Nie jest sprecyzowane, co rozumie się przez "krytyczną infrastrukturę informatyczną" (ust. 2 pkt 6), zwłaszcza w kontekście definicji infrastruktury krytycznej zawartej w ustawie o zarządzaniu kryzysowym, której wykazy stanowią załączniki do planów zarządzania kryzysowego (por. art. 5 ustawy o zarządzaniu kryzysowym). 3) Brak jest informacji na temat systemowej relacji ww. krajowego planu do planów zarządzania kryzysowego, a w szczególności niejasna jest relacja między Krajowym Planem Zarządzania Kryzysowego a Krajowym planem reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę.	Uwaga uwzględniona Doprecyzowano art. 72b i zmieniono brzmienie punktów budzących wątpliwości. Odnosząc się do uwagi w pkt 3 i wyjaśnienia relacji między dokumentami należy wskazać, że wymienione dokumenty będą się wzajemnie uzupełniać, a w przygotowaniu Krajowego Planu będą uczestniczyć też organy odpowiedzialne za kwestie zarządzania kryzysowego.
111.	PTI	Art. 72b	Pkt 73, art. 72b, ust. 2: ppkt 2) „<i>cele krajowych środków i działań służących w zakresie gotowości;</i>” – to zdanie nie ma żadnej treści; prośba o analizę, co Autor miał na myśli.	Uwaga uwzględniona Brzmienie przepisu zostanie zmienione.
112.	PTI	Art. 72b	Pkt 73, art. 72b, ust. 2 ppkt 3): „<i>procedury zarządzania kryzysowego w cyberprzestrzeni, w tym ich włączenie do ogólnych krajowych ram zarządzania kryzysowego, oraz kanały wymiany informacji;</i>” – do przemyślenia przez Autorów ustawy powiązanie mechanizmu „polecenia zabezpieczającego”, o którym mowa w art. 67g z procedurą eskalacji, która zwykle wpada w zarządzanie kryzysowe	Uwaga wyjaśniona Podniesione kwestie będą uregulowane w ramach zmian w ustawie o zarządzaniu kryzysowym związanych z wejściem w życie dyrektywy CER.
113.	Związek Pracodawców Technologii Cyfrowych Lewiatan	Art. 72b	Krajowy Plan (art. 72b, 72f) Czy Krajowy Plan, tak jak został zapisany w art. 72b jest dokumentem jawnym w całości? Mając na uwadze zapis art. 72f wydaje się, że tak, jednak czy wszystkie informacje opisane w ust. 2 powinny mieć taki charakter.	Uwaga wyjaśniona Ocena tego, które informacje zawarte w Krajowym Planie powinny być jawne zostanie podjęta w trakcie przygotowania tego planu.
114.	Osoba fizyczna	Art. 72c	Art. 72c. Zastosowano zapisy zobowiązujące podmioty realizujące zadania z zakresu zarządzania kryzysowego do przekazywania na żądanie ministra wł. ds. informatyzacji o realizacji zadań wynikających z Krajowego Planu. Należy zwrócić uwagę, że w ramach zarządzania kryzysowego podmioty raportują do	Uwaga wyjaśniona Przepis ten będzie dotyczył jedynie organów władzy publicznej, które będą

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			RCB i ministrów właściwych dla systemów IK. Proponuję zweryfikować intencję zapisu i odpowiednio skorygować. Zapewne możliwe jest, żeby podmioty zarządzania kryzysowego raportowały do ministra wł. ds. informatyzacji o realizacji zadań wynikających z Krajowego Planu, ale w ramach zarządzania kryzysowego w cyberbezpieczeństwie, co jest w zakresie ustawy uKSC.	wykonywać elementy Krajowego Planu. W związku z tym dotyczy jedynie wąskiej grupy podmiotów. Równocześnie jest on niezbędny dla zapewnienia Ministrowi Cyfryzacji możliwości badania na ile Krajowy Plan został wykonany.
115.	Konfederacja Lewiatan	Art. 72f	Przekazanie w całości Krajowego planu reagowania na incydenty i sytuacje kryzysowe w Cyberbezpieczeństwie na dużą skalę Komisji Europejskiej i europejskiej sieci organizacji łącznikowych do spraw kryzysów cyberbezpieczeństwa Jednostka redakcyjna: art. 72f projektu KSC Jednostka redakcyjna NIS2: art. 9 ust. 5 Uwaga: Zgodnie z art. 9 ust. 5 NIS2 Państwa członkowskie przedkładają Komisji i europejskiej sieci organizacji łącznikowych do spraw kryzysów cyberbezpieczeństwa (EU-CyCLONe) ważne informacje związane z wymogami określonymi w ust. 4, dotyczące krajowych planów reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę w terminie trzech miesięcy od daty przyjęcia tych planów. Państwa członkowskie mogą wyłączyć niektóre informacje, jeżeli i w zakresie w jakim jest to kluczowe z punktu widzenia ich bezpieczeństwa narodowego. Natomiast projekt ustawy w ogóle nie korzysta z tego zastrzeżenia, co może rodzić wątpliwości co do zakresu przekazywanych informacji mających istotne znaczenie z punktu widzenia bezpieczeństwa narodowego. Proponowane przepisy w tym zakresie nie przewidują objęcia informacji znajdujących się w tym planie tajemnicą państwową, a ponadto, mimo że NIS2 wymaga przekazania jedynie elementów takiego planu, projektodawca zamierza przekazywać plan w całości, bez względu na analizę co do przydatności takich informacji dla Komisji Europejskiej i europejskiej sieci organizacji łącznikowych, a także zasadę minimalizacji i ochrony informacji o krytycznym dla Polski znaczeniu (ujawnienie informacji może bowiem nastąpić na poziomie innego Państwa Członkowskiego).	Uwaga uwzględniona Zmieniono brzmienie art. 72f wskazując, że Krajowy Plan nie będzie przekazywany w całości.
116.	ISSA Polska	Art. 73	Sankcje w ustawie KSC – nieproporcjonalne i potencjalnie represyjne (art. 73, 74 ust. 2, 76b ustawy KSC) Ustawa KSC wprowadza system kar finansowych, które mogą osiągać wyjątkowo wysokie kwoty, znacznie przewyższające powszechne standardy. Według art. 73 tej ustawy, zgodnie z NIS2 maksymalna wysokość kary pieniężnej może wynieść do 10 milionów euro lub 2% rocznych przychodów podmiotu kluczowego, przy czym przyjęta jest zasada, że stosuje się wyższą z tych kwot. W przypadku nowo powstałych przedsiębiorstw lub takich, które nie osiągnęły przychodów, podstawa wymiaru kary wynosi równowartość 500 000 euro. Dla podmiotów ważnych maksymalna wysokość kary została określona na 7 milionów euro lub 1,4% rocznych przychodów, co również jest znaczącym obciążeniem finansowym. Dodatkowo, w przypadku szczególnie poważnych naruszeń zagrażających bezpieczeństwu publicznemu, życiu i zdrowiu ludzi lub powodujących poważne szkody majątkowe, możliwa jest kara do 100 milionów	Uwaga wyjaśniona Wskazać należy, że dyrektywa NIS 2 określa minimalną wysokość górnego limitu - oznacza to, że górne widełki kary nie mogą być niższe niż te wskazane w NIS 2. Tym samym państwa członkowskie mają dowolność w kształtowaniu kar ograniczoną wyłącznie koniecznością, proporcjonalnością i adekwatnością podejmowanych działań.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			złotych. Co jednak istotne, wprowadzono także mechanizm okresowych kar pieniężnych w wysokości od 500 zł do 100 000 zł za każdy dzień opóźnienia w wykonaniu nałożonych obowiązków, co może stanowić znaczące obciążenie dla podmiotów, które z różnych przyczyn nie są w stanie szybko dostosować się do wymagań ustawy. Standard dotyczący kar administracyjnych zaczyna się zwykle na poziomie 1000 zł (np. w przepisach dotyczących ochrony środowiska). Dotychczas ustawa o KSC przewidywała w art. 73 ust. 4 pałaty 1000, 5000 i 15000 zł. Dodatkowo brak jest mechanizmu odstąpienia od wymierzenia kary w uzasadnionych przypadkach, który jest znany przepisom dotyczącym zgodności wyrobów (np. sformułowany w przepisach dotyczących wyrobów budowlanych w formie obowiązku umorzenia postępowania). Tak wysokie sankcje, szczególnie w połączeniu z rygorem natychmiastowej wykonalności, mogą mieć represyjny charakter i stawiać przedsiębiorstwa w sytuacji, w której muszą podejmować pośpieszne decyzje, potencjalnie niekorzystne z długoterminowego punktu widzenia. W efekcie może to prowadzić nie tylko do finansowych trudności, ale również do ograniczenia innowacyjności i rozwoju technologicznego w kraju. W przepisie art. 73a ust. 4 ustawy o KSC pojawiła się również nieścisłość – jest tam mowa o karze w wysokości do 600% otrzymywanego przez ukaranego wynagrodzenia obliczanego według zasad obowiązujących przy ustalaniu ekwiwalentu pieniężnego za urlop. Nie określono okresu, którego ma dotyczyć wynagrodzenie przyjęte za podstawę wyliczenia kary.	Stopniowanie kary zostało wprowadzone w ramach art. 53 - określono tam szereg kryteriów, jakie organ właściwy musi brać pod uwagę określając wymiar kary. Są one na tyle rozbudowane, że zapewniają proporcjonalność kary do dokonanego naruszenia. Okresowe kary pieniężne również dopuszczalne są przez NIS 2 i mają na celu przymuszenie podmiotu do realizacji obowiązków nałożonych w ustawie. Pałap kar okresowych jest szeroki dzięki czemu można dostosować wysokość kary do rodzaju podmiotu i jego możliwości finansowych.
117.	Konfederacja Lewiatan	Art. 73	Zgodnie z art. 34 ust. 4 i 5 NIS2 państwa członkowskie zapewniają, by podmioty kluczowe i podmioty ważne dokonujące naruszeń art. 21 lub 23 NIS2 podlegały wysokim karom pieniężnym, których limit został określony w dyrektywie. Wysokość tych kar została wprowadzona w projekcie KSC, niemniej nie wszystkie naruszenia przepisów kwalifikujących się pod karę w wysokości określonej w projekcie ustawy to naruszenia art. 21 i 23 NIS2. Dodatkowo projektodawca nie wprowadził żadnego stopniowania kary – choć kary powinny być proporcjonalne (por. art. 36 NIS2). Innymi słowy polska implementacja zamiast dokonać stopniowania kar, tam gdzie to możliwe i zgodne z NIS2, to proponuje podejście zgodnie z którym wysokość kary została pozostawiona decyzji administracyjnej. W praktyce oznacza to, że podmiot ważny lub kluczowy może otrzymać kilkadziesiąt milionów EUR kary za czynności zakwalifikowane jako „utrudniania” wykonywania kontroli” (art. 73 ust. 1 pkt 15 projektu KSC), czy nie zapewnienia użytkownikowi usługi dostęp do wiedzy pozwalającej na zrozumienie cyberzagrożeń i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami w zakresie związanym ze świadczonymi usługami, w szczególności przez udostępnianie informacji na ten temat na swojej stronie internetowej (art. 73 ust. 1a projektu KSC). Ryzyko takie pewnie mogłoby być teoretyczne – jednak czy w kontekście zasady praworządności oraz zasady proporcjonalności kary, wynikającej z art. 36 NIS2, konieczne byłoby wprowadzenie stopniowania kar, tam gdzie to możliwe. W odróżnieniu od odpowiedzialności karnej, w przypadku administracyjnych kar pieniężnych często nie jest wymagane stwierdzenie winy. Istotne jest samo stwierdzenie faktu naruszenia przepisów	Uwaga wyjaśniona Wskazać należy, że dyrektywa NIS 2 określa minimalną wysokość górnego limitu - oznacza to, że górne widełki kary nie mogą być niższe niż te wskazane w NIS 2. Tym samym państwa członkowskie mają dowolność w kształtowaniu kar ograniczoną wyłącznie koniecznością, proporcjonalnością i adekwatnością podejmowanych działań. Stopniowanie kary zostało wprowadzone w ramach art. 53 - określono tam szereg kryteriów jakie organ właściwy musi brać pod uwagę określając wymiar kary. Są one na tyle rozbudowane, że zapewniają proporcjonalność kary do dokonanego naruszenia.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

118.	Konfederacja Lewiatan	Art. 73	Jednostka redakcyjna: Art. 73 ust. 1 Propozycja zmiany: „ust. 1 otrzymuje brzmienie: „1. Karze pieniężnej może podlegać podmiot kluczowy lub podmiot ważny, który: (...) – jeżeli przemawia za tym czas, zakres lub charakter naruszenia. W obecnym brzmieniu art. 73 ust. 1 każde naruszenie ww. obowiązków obliguje do nałożenia kary pieniężnej. W ocenie KL nieznaczne i nieintencjonalne naruszenie nie może skutkować automatyczną sankcją. Organ właściwy do spraw cyberbezpieczeństwa powinien za każdym razem uwzględniać czas, zakres oraz charakter naruszenia, podobnie jak w przypadku oceny naruszeń kierownika podmiotu kluczowego lub podmiotu ważnego (art. 73a). Powyższa zmiana ujednoliciłaby brzmienie art. 73 w zakresie ust. 1a projektu ustawy, przecinając wątpliwości interpretacyjne co do obligatoryjności administracyjnej kary pieniężnej, zwłaszcza w świetle możliwości odstąpienia od nałożenia kary przewidzianym w art. 76a ust	Uwaga nieuwzględniona W ocenie projektodawcy niezbędne jest zapewnienie nieuchronności kary – z pewnymi wyjątkami, kiedy to organ właściwy do spraw cyberbezpieczeństwa może od kary odstąpić. Ta nieuchronność realizuje założenie dyrektywy oraz ustawy, które mają na celu zwiększenie poziomu cyberbezpieczeństwa. Kara za naruszenia obowiązków wskazanych w ustawie powinna być środkiem domyślnym i powinna być różnicowana z uwzględnieniem kryteriów wskazanych w ustawie. Odstąpienie od niej powinno pozostać wyjątkiem.
119.	Konfederacja Lewiatan	Art. 73	Jednostka redakcyjna: Art. 73 ust. 2 „ust. 2 otrzymuje brzmienie: „2. Wysokość kary pieniężnej, o której mowa w: 1) ust. 1 pkt 1, wynosi do _____ 2) ust. 1 pkt 2, wynosi do 150 000 zł; 3) ust. 1 pkt 3, wynosi do _____ 4) ust. 1 pkt 4, wynosi do 100 000 zł; 5) ust. 1 pkt 5, wynosi do 50 000 zł; 6) ust. 1 pkt 6, wynosi do _____ 7) ust. 1 pkt 7, wynosi do 20 000 zł za każdy stwierdzony przypadek zaniechania obsługi incydentu; 8) ust. 1 pkt 8, wynosi do 20 000 zł za każdy stwierdzony przypadek niezgłoszenia incydentu poważnego 9) ust. 1 pkt 9, wynosi do _____ 10) ust. 1 pkt 10, wynosi do _____ 11) ust. 1 pkt 11, wynosi do _____ 12) ust. 1 pkt 12 i 13, wynosi do 20 000 zł; 13) ust. 1 pkt 14 i 17, wynosi do 200 000 zł; 14) ust. 1 pkt 15, wynosi do 50 000 zł 15) ust. 1 pkt 16, wynosi do _____ 16) ust. 1 pkt 18, wynosi do _____ 17) ust. 1 pkt 19, wynosi do _____ 18) ust. 1 pkt 20, wynosi do _____ 19) ust. 1 pkt 21, wynosi do _____ 20) ust. 1a pkt 2, wynosi do 20 000 zł; Postulujemy przywrócenie limitowania kar pieniężnych co do niektórych obowiązków, zwłaszcza tych, których naruszenie nie może prowadzić do wyrządzenia znacznej szkody. Nakładanie kary z uwzględnieniem sytuacji majątkowej podmiotu istniejącego w chwili wydania decyzji o nałożeniu kary nie może prowadzić do sytuacji, gdzie podmiot (np. wskutek niewyznaczenia osób odpowiedzialnych za utrzymywanie kontaktów z innymi podmiotami kluczowymi) może podlegać karze, której górna granica wynosi odpowiednio 7 milionów euro dla podmiotów ważnych, a 10 milionów euro w przypadku podmiotów kluczowych. Uwzględnienie specyfiki każdego z obowiązków oraz stopnia potencjalnego ich naruszenie pozwoli na ukształtowanie odpowiednich „limitów” kar pieniężnych, co ochroni podmioty kluczowe lub podmioty ważne przed nałożeniem nieproporcjonalnie wysokiej kary w stosunku do wagi naruszenia.	Uwaga nieuwzględniona Nie można zgodzić się ze stwierdzeniem, że przewidziane w projekcie kryteria wymiaru kary są nieproporcjonalne i nie pozwolą różnicować wysokości kary. W projekcie kryteria wymiaru kary zostały ukształtowane w ten sposób, żeby właśnie spełniały to założenie, tj. uwzględniały specyfikę każdego z obowiązków oraz stan faktyczny. Kary nie będą zatem arbitralne, a oparte na wielu przesłankach, które należy wziąć pod uwagę przy wydawaniu decyzji o jej nałożeniu.
120.	Konfederacja Lewiatan	Art. 73	Jednostka redakcyjna: art. 73 ust. 4 projektu KSC Jednostka redakcyjna NIS2: art. 34 ust. 5 Uwaga: Projektodawca proponuje określenie tej samej podstawy wymiaru kary dla podmiotów ważnych i kluczowych w sytuacji, gdy okres działalności takich podmiotów jest krótszy niż rok. Podstawą wymiaru kary jest kwota 500 000 EUR i kwota ta dotyczy zarówno podmiotu ważnego i kluczowego, podczas gdy	Uwaga uwzględniona Przeredagowano przepis w ten sposób, że w przypadku podmiotów ważnych za podstawę wymiaru kary w określonych

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			w art. 34 ust. 5 NIS2 dokonano obniżenia wysokości kary dla podmiotu ważnego. Zasada ta powinna zostać również odpowiednio odzwierciedlona w wymiarze kary dla podmiotu ważnego prowadzącego działalność gospodarczą krócej niż 12 miesięcy.	przypadkach będzie przyjmowana równowartość kwoty 250 000 euro, a nie 500 000 euro.
121.	Konfederacja Lewiatan	Art. 73	W pierwszej kolejności zauważamy, że określenie dodatkowych pułapów kar wykracza poza zakres wynikający wprost z NIS2. W naszej ocenie wystarczające są przewidziane już, bardzo wysokie kary za naruszenie poszczególnych przepisów ustawy, które mogą wynosić nawet do 10 mln EUR i będą wielokrotnie przekraczać dotychczasowy pułap maksymalny za naruszenia, który według art. 73 ust. 5 wynosi 10 mln zł. W drugiej kolejności zauważamy, że redakcja przepisu powoduje, że będzie istniała nadmiarowa dowolność w zakresie interpretacji danego naruszenia jako stanowiącego poważne zagrożenie, czy skutkującego powstaniem poważnych szkód majątkowych lub poważnych utrudnień w świadczeniu usług. W praktyce, zasadniczo niemal każde naruszenie będzie obarczone ryzykiem nałożenia kary w wysokości do 100 mln zł. Ponadto zauważamy usunięcie z przepisu istotnego słowa, które znajdowało się w jego dotychczasowym brzmieniu, tj. wskazania na „uporczywość” danego naruszenia. Miało ono kluczowe znaczenie dla nadania stosowaniu aktualnego przepisu większej proporcjonalności i ograniczenia do naruszeń, których w szczególności podmiot miał świadomość, a nie podejmował w ich zakresie działań naprawczych. Poza tym, w projektowanym stanie prawnym nie będzie jasne jaka jest relacja do uprawnienia nałożenia kary z ust. 1 do kary z ust. 5. W naszej ocenie istnieje ryzyko nakładania kar podwójnego karania za te same naruszenia. Z tego względu przepis ten powinien zostać usunięty z projektu. Kary maksymalne w wysokości do 10/7 mln EUR są zdecydowanie wystarczające i spełniają funkcję prewencyjną, represyjną i będzie adekwatnie dolegliwie odstraszać od naruszeń.	Uwaga nieuwzględniona Należy zauważyć, że pułap kar w NIS 2 to minimalna wysokość górnych widełek kary - kara maksymalna nie może być niższa niż 10 mln euro lub 7 mln euro w zależności od podmiotu. Tym samym kara 100 mln zł jest zgodna z dyrektywą. Ponadto należy pamiętać, że ustawa nie ma na celu wyłącznie wdrożenia dyrektywy, a jej zapisy są również efektem analizy funkcjonowania jej rozwiązań na przestrzeni lat. Z tego względu dokonano szeregu zmian w tym przepisie zaczynając od eliminacji uporczywości, a kończąc na wysokości kary. Sytuacja geopolityczna oraz wielość ataków w cyberprzestrzeni powoduje, że państwo polskie nie może pozwolić na naruszenia, które zagrożą bezpośrednio jego obronności, bezpieczeństwa czy życia i zdrowia ludzi. Są to wartości i dobra, które Rząd obowiązany jest chronić. Z tych samych powodów zdecydowano się na usunięcie przesłanki uporczywości. Już jednokrotne działanie o takich skutkach jest wysoce szkodliwe.
122.	PIKE i Mediakom	Art. 73	Przepis ten przewiduje karę 100 000 000 zł za bezpośrednie i poważne zagrożenie cyberbezpieczeństwa dla obronności, bezpieczeństwa państwa, bezpieczeństwa i porządku publicznego lub życia i zdrowia ludzi lub zagrożenie wywołania poważnej szkody majątkowej lub poważnych utrudnień w świadczeniu usług. Przepis ten budzi wyjątkowo duże zastrzeżenia i z pewnością jest sprzeczny z zasadą proporcjonalności: samo spowodowanie zagrożenia powoduje tak wysoką karę, jakiej nie ma w żadnym innym miejscu w ustawie i to bez możliwości miarkowania. Ponadto należy wyrazić poważne wątpliwości co do relacji tej kary do nowych przepisów karnych wynikających z wdrożenia dyrektywy NIS2, jak i podstawy prawnej stwierdzenia naruszenia, o którym mowa w tym przepisie. Art. 73 ust. 5 nie gwarantuje również zachowania zasady <i>ne bis in idem</i> .	Uwaga nieuwzględniona Należy zauważyć, że pułap kar w NIS 2 to minimalna wysokość górnych widełek kary - kara maksymalna nie może być niższa niż 10 mln euro lub 7 mln euro w zależności od podmiotu. Tym samym kara 100 mln zł jest zgodna z dyrektywą. Ponadto należy pamiętać, że ustawa nie ma na celu wyłącznie wdrożenia dyrektywy, a jej zapisy są również efektem analizy

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			Wykreślenie art. 73 ust. 5.	funkcjonowania jej rozwiązań na przestrzeni lat. Z tego względu dokonano szeregu zmian w tym przepisie zaczynając od eliminacji uporczywości, a kończąc na wysokości kary. Sytuacja geopolityczna oraz wielość ataków w cyberprzestrzeni powoduje, że państwo polskie nie może pozwolić na naruszenia, które zagrażą bezpośrednio jego obronności, bezpieczeństwa czy życia i zdrowia ludzi. Są to wartości i dobra, które Rząd obowiązany jest chronić. Z tych samych powodów zdecydowano się na usunięcie przesłanki uporczywości. Już jednokrotne działanie o takich skutkach jest wysoce szkodliwe. Przepis ten pozostaje w zgodności również z innymi przepisami sankcyjnymi bowiem aktualizuje się wyłącznie wtedy, gdy spełnione są przesłanki.
123.	Polska Izba Informatyki i Telekomunikacji	Art. 73	Art. 73 ust. 5 – kara do 100 mln zł W pierwszej kolejności zauważamy, że określenie dodatkowych pułapów kar wykracza poza zakres wynikający wprost z NIS2. W naszej ocenie wystarczające są przewidziane już, bardzo wysokie kary za naruszenie poszczególnych przepisów ustawy, które mogą wynosić nawet do 10 mln EUR i będą wielokrotnie przekraczać dotychczasowy pułap maksymalny za naruszenia, który według art. 73 ust. 5 wynosi 10 mln zł. W drugiej kolejności zauważamy, że redakcja przepisu powoduje, że będzie istniała nadmiarowa dowolność w zakresie interpretacji danego naruszenia jako stanowiącego poważne zagrożenie, czy skutkującego powstaniem poważnych szkód majątkowych lub poważnych utrudnień w świadczeniu usług. W praktyce, zasadniczo niemal każde naruszenie będzie obarczone ryzykiem nałożenia kary w wysokości do 100 mln zł. Ponadto zauważamy usunięcie z przepisu istotnego słowa, które znajdowało się w jego dotychczasowym brzmieniu, tj. wskazania na „uporczywość” danego naruszenia. Miało ono kluczowe znaczenie dla nadania stosowaniu aktualnego przepisu większej proporcjonalności i ograniczenia do naruszeń, których w szczególności podmiot miał świadomość, a nie podejmował w ich zakresie działań naprawczych. Poza tym, w projektowanym stanie prawnym nie będzie jasne jaka jest relacja do uprawnienia nałożenia kary z ust. 1 do kary z ust. 5. W naszej ocenie istnieje ryzyko podwójnego karania za te same naruszenia. Z tego względu przepis ten powinien zostać usunięty z projektu. Kary maksymalne w wysokości do 10/7 mln EUR są zdecydowanie wystarczające i spełniają funkcję prewencyjną, represyjną i będą adekwatnie dolegliwie odstraszać od naruszeń.	Uwaga nieuwzględniona należy zauważyć, że pułap kar w NIS 2 to minimalna wysokość górnych widełek kary - kara maksymalna nie może być niższa niż 10 mln euro lub 7 mln euro w zależności od podmiotu. Tym samym kara 100 mln zł jest zgodna z dyrektywą. Ponadto należy pamiętać, że ustawa nie ma na celu wyłącznie wdrożenia dyrektywy, a jej zapisy są również efektem analizy funkcjonowania jej rozwiązań na przestrzeni lat. Z tego względu dokonano szeregu zmian w tym przepisie zaczynając od eliminacji uporczywości, a kończąc na wysokości kary. Sytuacja geopolityczna oraz wielość ataków w cyberprzestrzeni powoduje, że państwo polskie nie może pozwolić na naruszenia, które zagrażą bezpośrednio jego obronności, bezpieczeństwa czy życia i zdrowia ludzi.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

				Są to wartości i dobra, które Rząd obowiązany jest chronić. Z tych samych powodów zdecydowano się na usunięcie przesłanki uporczywości. Już jednokrotne działanie o takich skutkach jest wysoce szkodliwe.
124.	Amerykańska Izba Handlowa	Rt. 73	Zgodnie z art. 36 dyrektywy NIS 2 państwa członkowskie zobowiązane są do ustanowienia przepisów dotyczących kar stosowanych wobec naruszeń krajowych środków przyjętych zgodnie z dyrektywą oraz podjęcia wszelkich niezbędnych środków, aby zapewnić ich wdrożenie. Przewidziane kary muszą być skuteczne i odstraszające, ale także proporcjonalne. Art. 73 ust.1 uksc w brzmieniu ustalonym przez art. 1 pkt 74 projektu ustawy określa zachowania podlegające ustalonym w ustawie karom finansowym, które mogą być nałożone na podmioty kluczowe lub ważne. Maksymalne kwoty kar przewidziane w projekcie są analogiczne do tych przewidzianych w dyrektywie NIS 2, z dwoma wyjątkami, w których organ właściwy może nałożyć wyższe kary tj. karę w wysokości do 100 000 000 PLN (art. 1 pkt 74 lit. g projektu) oraz karę w wysokości od 500 PLN do 100 000 PLN za każdy dzień opóźnienia (art. 1 pkt 79 projektu). iStoimy na stanowisku, że przewidziane kary mogą być nieproporcjonalne w stosunku do naruszeń. Wysokie kary za nieznaczne uchybienia mogą prowadzić do nadmiernej represji i nieproporcjonalnego obciążenia podmiotów kluczowych lub ważnych. Ponadto przyznanie organom władzy możliwość nakładania wysokich kar oraz decydowania o zawieszeniu lub cofnięciu licencji może prowadzić do ryzyka arbitralności i nadużycia władzy. Proponujemy ponowne przeanalizowanie wysokości kar oraz wprowadzenie mechanizmów zapewniających proporcjonalność i sprawiedliwość w egzekwowaniu przepisów.o	Uwaga wyjaśniona Nie można zgodzić się ze stwierdzeniem, że przewidziane w projekcie kryteria wymiaru kary są nieproporcjonalne i nie pozwolą różnicować wysokości kary. Projektodawca wskazuje, że kryteria wymiaru kary zostały ukształtowane w ten sposób, żeby właśnie spełniały to założenie tj. uwzględniały specyfikę każdego z obowiązków oraz stan faktyczny. Kary nie będą zatem arbitralne, a oparte na wielu przesłankach, które należy wziąć pod uwagę przy wydawaniu decyzji o jej nałożeniu. Jednocześnie należy wskazać, że pułap wymiaru kary został przewidziany bardzo szeroko co zapewnia dostosowywanie wymiaru kary do rodzaju naruszenia, a także sytuacji finansowej podmiotu.
125.	Fundacja Open Allies	art. 73	[Prawo odwołania się od decyzji nakładającej kary] Open Allies wnosi o zmianę przepisów nowelizacji UKSC w ten sposób, aby odwołanie od: decyzji nakładającej karę administracyjną, rozstrzygnięcia w zakresie zaleceń pokontrolnych, decyzji organu właściwego do spraw cyberbezpieczeństwa, o których mowa w art. 53 projektowanej UKSC. było kierowane do SOKiK. Weryfikacja rozstrzygnięć organów administracji przez sądy administracyjne ogranicza się do legalności wydania decyzji lub innego aktu. Sąd administracyjny nie bada merytorycznych przesłanek rozstrzygnięcia. Z kolei odwołanie do SOKiK zapewni podmiotowi cyberbezpieczeństwa prawo do ponownej oceny merytorycznej podstaw wydania rozstrzygnięcia przez organ właściwy do spraw cyberbezpieczeństwa.	Uwaga nieuwzględniona Należy zwrócić uwagę na fakt, że ze względu na specyfikę zaleceń pokontrolnych nie przysługuje od nich skarga do sądu. Jeśli natomiast chodzi o sądową kontrolę decyzji w zakresie kar administracyjnych czy środków nadzorczych to przede wszystkim jest to właściwość postępowania o charakterze administracyjnym czemu wyraz dają np. kary pieniężne przewidziane w kodeksie postępowania administracyjnego. Przepisy tego kodeksu w zakresie procedury i w zakresie nieuregulowanym stosuje się odpowiednio przy procedurze nakładania

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

				kar pieniężnych na podmiot kluczowy lub podmiot ważny. Podobnie w przypadku sprawowania nadzoru przeważającą rolę odgrywa tu prawo administracyjne. Tym samym właściwym jest stosowanie procedury sądowoadministracyjnej.
126.	Cybermadein poland	Art. 73	Art. 73. - doprecyzowanie zapisu “nie zarządził ryzykiem wystąpienia incydentu”.	Uwaga wyjaśniona Brzmienie przepisu w ocenie projektodawcy jest wystarczająco precyzyjne i odpowiada obowiązкови, o którym mowa w art. 8 ust. 1 pkt 1 ustawy. Uwaga zbyt ogólna aby wprowadzić zmiany.
127.	Centrum Wymiany i Analiz Informacji podsektora transportu kolejowego „ISAC-Kolej”	Art. 73	W art. 73 ust. 1 pkt 3 wprowadzić zmianę zapisu na: „3) nie wdrożył systemu zarządzania bezpieczeństwem informacji, systemu bezpieczeństwa automatyki przemysłowej i sterownia oraz systemu zarządzania ciągłości działania w systemie informacyjnym i technologii operacyjnej wykorzystywanej do świadczenia usługi albo system ten nie zapewnia funkcjonalności, o których mowa w art. 8 ust. 1”. Oprócz systemu zarządzania bezpieczeństwem informacji, jak wskazują wcześniejsze zapisy, powinna zostać również wdrożona dokumentacja systemu zarządzania ciągłością działania (wg normy ISO22301). Ponadto system zarządzania dla technologii operacyjnych użytkowanych może wynikać z normy ISO62443 czy z innych norm branżowych i standardów obowiązujących w danym sektorze lub podsektorze.	Uwaga częściowo uwzględniona Przepis zostanie dostosowany do art. 8 w zakresie uwzględnienia systemu zarządzania ciągłością działania.
128.	ZIPSEE Cyfrowa Polska	Art. 73	W dyrektywie możemy przeczytać (art. 36 Dyrektywy): “Państwa członkowskie ustanawiają przepisy dotyczące kar stosowanych wobec naruszeń krajowych środków przyjętych zgodnie z niniejszą dyrektywą oraz podejmują wszelkie niezbędne środki, aby zapewnić ich wdrożenie. Przewidziane kary muszą być skuteczne, proporcjonalne i odstraszające.” Polski projekt implementacji w art. 73 ust.1 określa kary finansowe, które mogą być nałożone na podmioty kluczowe lub ważne. Maksymalne kwoty kar przewidziane w polskim projekcie ustawy są takie same jak w NIS2, z dwoma wyjątkami, gdzie organ właściwy może nałożyć wyższe kary tj. karę w wysokości do 100 000 000 PLN oraz karę w wysokości od 500 PLN do 100 000 PLN za każdy dzień opóźnienia. Przewidziane kary mogą być nieproporcjonalne w stosunku do naruszeń. Wysokie kary za nieznaczne uchybienia mogą prowadzić do nadmiernej represji i nieproporcjonalnego obciążenia podmiotów kluczowych lub ważnych. Ponadto przyznanie organom władzy możliwości nakładania wysokich kar oraz decydowania o zawieszeniu lub cofnięciu licencji może prowadzić do ryzyka arbitralności i nadużycia władzy. Proponujemy ponowne przeanalizowanie wysokości kar oraz wprowadzenie mechanizmów zapewniających proporcjonalność i sprawiedliwość w egzekwowaniu przepisów.	Uwaga wyjaśniona Projektodawca wskazuje, że dyrektywa NIS 2 objęta jest wyłącznie minimalną harmonizacją, a państwa członkowskie mogą podejmować dalej idące środki, które pozostają w zgodzie z nadrzędnym celem tego aktu. Projekt nie stanowi wyłącznie implementacji a jego treść jest także odpowiedzią na zidentyfikowane problemy w trakcie obowiązywania obecnej ustawy o krajowym systemie cyberbezpieczeństwa. Jednocześnie wskazać należy, że kara 100 000 000 zł jest karą maksymalną i będzie miarkowana z uwzględnieniem kryteriów wskazanych w ustawie. Nie zajdzie zatem sytuacja, że za nieznaczne uchybienia nałożona zostanie maksymalna

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

				kara. W zakresie kar okresowych są one przewidziane w dyrektywie NIS 2, a ich wysokość pozostawiona jest kompetencji państw członkowskich. Po analizie zdecydowano o szerokim pałapie kar i z tego względu projektodawca stoi na stanowisku, że są one proporcjonalne i adekwatne.
129.	Krajowi Producenci Leków	Art. 73	Art. 1 pkt 74 lit a otrzymuje brzmienie: „ust. 2 otrzymuje brzmienie: „2. Karze pieniężnej może podlegać podmiot kluczowy lub podmiot ważny, który: (...) – jeżeli przemawia za tym czas, zakres lub charakter naruszenia. Uzasadnienie W obecnym brzmieniu art. 73 ust. 1 każde naruszenie ww. obowiązków obliguje do nałożenia kary pieniężnej. W ocenie Związku nieznaczne i nieintencjonalne naruszenie nie może skutkować automatyczną sankcją. Organ właściwy do spraw cyberbezpieczeństwa powinien za każdym razem uwzględniać czas, zakres oraz charakter naruszenia, podobnie jak w przypadku oceny naruszeń kierownika podmiotu kluczowego lub podmiotu ważnego (art. 73a). Powyższa zmiana ujednoliciłaby brzmienie art. 73 w zakresie ust. 1a projektu ustawy, przecinając wątpliwości interpretacyjne co do obligatoryjności administracyjnej kary pieniężnej, zwłaszcza w świetle możliwości odstąpienia od nałożenia kary przewidzianym w art. 76a ust. 6.	Uwaga nieuwzględniona Projektodawca wskazuje, że są inne przepisy, które umożliwiają odstąpienie od wymierzenia kary. Kary mają być obligatoryjne i pełnić funkcję prewencyjną oraz gwarancyjną. Powinny być również proporcjonalne dlatego przewidziane zostały kryteria wymiaru kary jakie należy wziąć pod uwagę właśnie z powodu różnego stopnia i wagi naruszenia.
130.	Krajowi Producenci Leków	Art. 73	Powrót do limitowania wysokości kary pieniężnej w zależności od rodzaju naruszenia ustawy Art. 1 pkt 74 lit c otrzymuje brzmienie: „ust. 2 otrzymuje brzmienie: „2. Wysokość kary pieniężnej, o której mowa w: 1) ust. 1 pkt 1, wynosi do _____ 2) ust. 1 pkt 2, wynosi do 150 000 zł; 3) ust. 1 pkt 3, wynosi do _____ 4) ust. 1 pkt 4, wynosi do 100 000 zł; 5) ust. 1 pkt 5, wynosi do 50 000 zł; 6) ust. 1 pkt 6, wynosi do _____ 7) ust. 1 pkt 7, wynosi do 20 000 zł za każdy stwierdzony przypadek zaniechania obsługi incydentu; 8) ust. 1 pkt 8, wynosi do 20 000 zł za każdy stwierdzony przypadek niezgłoszenia incydentu poważnego	Uwaga nieuwzględniona Dyrektywa NIS 2 nie przewiduje limitowania kar pieniężnych w różny sposób w zależności od naruszonych obowiązków. Analiza funkcjonowania obecnie obowiązujących przepisów, a także podejścia pozostałych państw członkowskich do problematyki kar prowadzi również do wniosku, że przyjęte w projekcie rozwiązanie w postaci kary zależnej od analizy konkretnej sytuacji na podstawie wskazanych w ustawie kryteriów jest rozwiązaniem najbardziej efektywnym, proporcjonalnym i

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			9) ust. 1 pkt 9, wynosi do _____ 10) ust. 1 pkt 10, wynosi do _____ 11) ust. 1 pkt 11, wynosi do _____ 12) ust. 1 pkt 12 i 13, wynosi do 20 000 zł; 13) ust. 1 pkt 14 i 17, wynosi do 200 000 zł; 14) ust. 1 pkt 15, wynosi do 50 000 zł 15) ust. 1 pkt 16, wynosi do _____ 16) ust. 1 pkt 18, wynosi do _____ 17) ust. 1 pkt 19, wynosi do _____ 18) ust. 1 pkt 20, wynosi do _____ 19) ust. 1 pkt 21, wynosi do _____ 20) ust. 1a pkt 2, wynosi do 20 000 zł; Uzasadnienie Postulujemy przywrócenie limitowania kar pieniężnych co do niektórych obowiązków, zwłaszcza tych, których naruszenie nie może prowadzić do wyrządzenia znacznej szkody. Nakładanie kary z uwzględnieniem sytuacji majątkowej podmiotu istniejącego w chwili wydania decyzji o nałożeniu kary nie może prowadzić do sytuacji, gdzie podmiot (np. wskutek niewyznaczenia osób odpowiedzialnych za utrzymywanie kontaktów z innymi podmiotami kluczowymi) może podlegać karze, której górna granica wynosi odpowiednio 7 milionów euro dla podmiotów ważnych, a 10 milionów euro w przypadku podmiotów kluczowych. Uwzględnienie specyfiki każdego z obowiązków oraz stopnia potencjalnego ich naruszenie pozwoli na ukształtowanie odpowiednich „limitów” kar pieniężnych, co ochroni podmioty kluczowe lub podmioty ważne przed nałożeniem nieproporcjonalnie wysokiej kary w stosunku do wagi naruszenia.	sprawiedliwym. Wiele kryteriów wymiaru kary zapobiegnie nieproporcjonalnej wysokości tej kary.
131.	Polskie Towarzystwo Informatyczne	Art. 73	Pkt 74, art. 73a), ust 1 ppkt 2) „nie przeprowadził systematycznego szacowania ryzyka lub nie zarządził ryzykiem wystąpienia incydentu, o których mowa w art. 8 ust. 1 pkt 1;” – zdanie niepoprawne gramatycznie, nie można trybu dokonanego używać do czynności systematycznych lub o charakterze ciągłym; proponuje się zmianę: nie przeprowadzał (..) lub nie zarządzał (..).	Uwaga uwzględniona Zmiany zostały wprowadzone w pkt 2 oraz w ustępie, który stanowi, że karze podlega również podmiot, którego działanie miało charakter jednorazowy. Wynika to z faktu, że znacznie utrudnione jest postawienie granicy w sytuacji, w której czyn określony jest w sposób ciągły.
132.	IAB Polska	Art. 73 ust. 5	Kara pieniężna w wysokości do 100 mln zł. [art. 1 ust. 74 lit. g) projektu nowelizacji / art. 73 ust. 5 nowelizowanego UKSC] W art. 73 ust. 5 nowelizowanego UKSC wprowadzono możliwość nałożenia na podmiot kluczowy lub podmiot ważny kary pieniężnej w wysokości do 100 mln zł, jeżeli taki podmiot naruszy przepisy ustawy, powodując: 1) bezpośrednie i poważne zagrożenie cyberbezpieczeństwa dla obronności, bezpieczeństwa państwa, bezpieczeństwa i porządku publicznego lub życia i zdrowia ludzi; lub 2) zagrożenie wywołania poważnej szkody majątkowej lub poważnych utrudnień w świadczeniu usług. Taka regulacja nie znajduje swojego odpowiednika w przepisach dyrektywy NIS 2, a także nie znajduje uzasadnienia dla jej wprowadzenia, jako że określony w dyrektywie NIS 2 oraz projekcie nowelizacji pułap	Uwaga nieuwzględniona W ocenie projektodawcy wprowadzanie przepisu, który określałby wykluczenie możliwości nałożenia kary pieniężnej na podstawie ust 3 i 4 a ust. 5 jest niezasadne, z uwagi na to, że po pierwsze ust. 5 znajduje zastosowanie wyłącznie wtedy, gdy spełnione zostaną konkretne

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			kar na poziomie nawet 10 mln euro zdecydowanie przewyższa obecnie obowiązujące limity kar, a tym samym w pełni realizuje prewencyjne i represyjne funkcje kar pieniężnych. Co więcej, taki sposób zredagowania analizowanego przepisu przyznaje organom właściwym dowolność co do sposobu interpretacji przesłanek do nałożenia kary pieniężnej, umożliwiając nałożenie kary w wysokości nawet 100 mln zł za praktycznie każde naruszenie przepisów. Przyjęcie tak niedookreślonych przesłanek do nałożenia kary pieniężnej narusza przy tym zasadę określoności przepisów prawnych, wyrażoną chociażby w § 75 ust. 1 w zw. z § 81a ust. 3 Zasad techniki prawodawczej, zgodnie z którym znamiona czynu zabronionego powinny zostać określone w sposób wyczerpujący. Nie jest także jasna zależność pomiędzy analizowaną karą a karą pieniężną wynikającą z art. 73 ust. 3 lub 4 nowelizowanego UKSC, ponieważ obecne brzmienie projektu nowelizacji nie wyklucza jednoczesnego nałożenia kar pieniężnych na podstawie art. 73 ust. 3 i 4 oraz art. 73 ust. 5 nowelizowanego UKSC. Mając to na uwadze, IAB Polska postuluje wykreślenie art. 73 ust. 5 nowelizowanego UKSC. Alternatywnie, w razie nieuwzględnienia powyższego postulatu, IAB Polska wskazuje na potrzebę doprecyzowania przesłanek do nałożenia kary pieniężnej na podstawie tego przepisu, a także wprowadzenie regulacji, która wykluczy równoczesne stosowanie art. 73 ust. 3 lub 4 i art. 73 ust. 5 nowelizowanego UKSC.	przesłanki, a po drugie zakaz łącznego nałożenia tych kar wynika przede wszystkim z zakazu podwójnego karania. Uzasadnienie zostanie doprecyzowane w tym zakresie. Co do zasadności przepisu art. 73 ust. 5 należy zauważyć, że pułap kar w NIS 2 to minimalna wysokość górnych widełek kary – kara maksymalna nie może być niższa niż 10 mln euro lub 7 mln euro w zależności od podmiotu. Tym samym kara 100 mln zł jest zgodna z dyrektywą. Ponadto należy pamiętać, że ustawa nie ma na celu wyłącznie wdrożenia dyrektywy, a jej zapisy są również efektem analizy funkcjonowania jej rozwiązań na przestrzeni lat. Z tego względu dokonano szeregu zmian w tym przepisie zaczynając od eliminacji uporczywości, a kończąc na wysokości kary. Sytuacja geopolityczna oraz wielość ataków w cyberprzestrzeni powoduje, że państwo polskie nie może pozwolić na naruszenia, które zagrażają bezpośrednio jego obronności, bezpieczeństwa czy życia i zdrowia ludzi. Są to wartości i dobra, które rząd obowiązany jest chronić.
133.	PGE SA	Art. 1 pkt 74 lit. g, Art. 73 ust. 5	Przepis w proponowanym brzmieniu powinien zostać usunięty z projektu ustawy z uwagi na nieprawidłowe sformułowanie przepisu karnego, które może powodować jego niezgodność z Konstytucją. Ponadto, tak sformułowany przepis karny nie będzie skutecznie realizował celu jakim jest karanie za poważne naruszenia, które spowodowały poważne skutki. Po pierwsze, zachowania, które skutkują nałożeniem kary pieniężnej są określone w art. 73 ust. 1 i w tym przepisie powinny być uregulowane wszystkie naruszenia, które skutkują nałożeniem kary pieniężnej. Po drugie, przepis nakładający sankcję powinien precyzyjnie określać naruszenie podlegające sankcji, a zwrot „narusza przepisy ustawy” nie spełnia tego kryterium – powinno zostać wskazane, o naruszenie jakich konkretnie przepisów chodzi.	Uwaga nieuwzględniona Art. 73 ust. 5 jest przepisem szczególnym do ust. 1. Wypełnienie znamion z przepisu art. 73 ust. 5 eliminuje karę z ust. 1 z uwagi na konieczność uniknięcia podwójnego karania. Co do zasadności przepisu art. 73 ust. 5 należy zauważyć, że pułap kar w NIS 2 to minimalna wysokość górnych widełek kary – kara maksymalna nie może być niższa niż

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

		Po trzecie, także zachowania podlegające karze nie są prawidłowo określone: „bezpośrednie i poważne zagrożenie”, „zagrożenie wywołania poważnej szkody majątkowej” są to pojęcie nieostre. Jakie będą kryteria oceny, czy zagrożenie cyberbezpieczeństwa było bezpośrednie i poważne (koniunkcja skazuje, że muszą być spełnione obydwie przesłanki). Jak definiować „zagrożenie wywołania poważnej szkody”? Jak definiować samo słowo „zagrożenie” i jak definiować „poważną szkodę” oraz „poważne utrudnienie”? W zakresie „poważnej szkody” powinna być wskazana konkretna kwota pieniężna lub odwołanie do przepisów, które definiują poważną szkodę majątkową, ewentualnie dodanie definicji „poważnej szkody” w niniejszej ustawie. Przepisy prawa, a w szczególności przepisy karne, nie powinny stosować pojęć ocennych w postaci przymiotników. Należy wziąć pod uwagę także sankcję w wysokości 100 mln złotych, która jest zagrożeniem za naruszenie przepisów, które nie zostały precyzyjnie określone, podobnie jak nie zostały precyzyjnie określone konsekwencje naruszeń, które skutkują wymierzeniem kary. Tak sformułowany przepis narusza zasadę demokratycznego państwa prawa, zasadę legalizmu oraz zasady wynikające z nauki prawa karnego dotyczące tworzenia przepisów nakładających sankcje. Konsekwencją wydawania decyzji nakładających kary pieniężne na podstawie tak sformułowanego przepisu będzie składanie skarg do sądów, które z dużym prawdopodobieństwem będą uchylać decyzje nakładające kary jako nałożone bez wyraźnej i bezspornej podstawy prawnej. Trudno będzie na podstawie tak sformułowanego przepisu wykazać, że podmiot dopuścił się naruszenia w nim opisanego. Środek w postaci sankcji za poważne naruszenia przepisów, który w zamyśle miał dotyczyć naruszeń powodujących bardzo poważne konsekwencje dla państwa i podmiotów gospodarczych będzie nieskuteczny. ~~„5. Jeżeli podmiot kluczowy albo podmiot ważny narusza przepisy ustawy, powodując:~~ ~~1) ——— bezpośrednie i poważne zagrożenie cyberbezpieczeństwa dla obronności, bezpieczeństwa państwa, bezpieczeństwa i porządku publicznego lub życia i zdrowia ludzi;~~ ~~2) ——— zagrożenie wywołania poważnej szkody majątkowej lub poważnych utrudnień w świadczeniu usług —organ właściwy do spraw cyberbezpieczeństwa nakłada karę w wysokości do 100 000 000 zł.”;~~	10 mln euro lub 7 mln euro w zależności od podmiotu. Tym samym kara 100 mln zł jest zgodna z dyrektywą. Ponadto należy pamiętać, że ustawa nie ma na celu wyłącznie wdrożenia dyrektywy, a jej zapisy są również efektem analizy funkcjonowania jej rozwiązań na przestrzeni lat. Z tego względu dokonano szeregu zmian w tym przepisie zaczynając od eliminacji uporczywości, a kończąc na wysokości kary. Sytuacja geopolityczna oraz wielość ataków w cyberprzestrzeni powoduje, że państwo polskie nie może pozwolić na naruszenia, które zagrożą bezpośrednio jego obronności, bezpieczeństwa czy życia i zdrowia ludzi. Są to wartości i dobra, które rząd obowiązany jest chronić. Jednocześnie wskazać należy, że zarzut nieprecyzyjności tego przepisu i w konsekwencji zarzut, że stanowi on naruszenie konstytucji jest niezasadny. Podobne przepisy wykorzystujące przesłanki nieostre funkcjonują w prawie powszechnie obowiązującym – również w kodeksie karnym (np. art. 231 Kodeksu karnego). Trybunał Konstytucyjny wypowiadał się już w tym przedmiocie np. w wyroku z dnia 9 czerwca 2010 r. w sprawie o sygn. akt SK 52/08. Znamiona czynu – choć ogólne i co do zasady ocenne – spełniają wymóg określoności. Powyższy wyrok odnosi się również do kwestii szerokiego odesłania, a więc gospodaruje uwagę, iż zwrot „narusza przepisy ustawy” jest nieprecyzyjny. W ustawie wskazano bowiem obowiązki podmiotów, a treść przepisów ustawy nie

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

				budzi wątpliwości, jakie obowiązki powinny być realizowane przez podmiot kluczowy czy podmiot ważny. W przywołanym powyżej wyroku rozpatrywana była kwestia jeszcze szersza bowiem uprawnienia i obowiązki funkcjonariusza publicznego nie wynikają bezpośrednio z kodeksu karnego, a z innych ustaw. Jeśli zatem w kodeksie karnym można posłużyć się odwołaniem do uprawnień lub obowiązków funkcjonariusza, które nie zostały wprost określone w tym przepisie, a nawet w całym Kodeksie karnym, a swoje źródło mają w innych ustawach, to projektodawca uważa, że tym bardziej możliwe jest odwołanie ogólne do naruszeń przepisów ustawy, jeśli znajduje się ono w tej samej ustawie, w której znajdują się obowiązki podmiotu karanego.
134.	Polskie Stowarzyszenie Fotowoltaiki	Art. 73	Art. 73 [Opowiedzialność PK i PW] W razie naruszenia określonych enumeratywnie obowiązków określonych w Projekcie, PK i PW podlegają karze pieniężnej w wysokości: - do 10 000 000 euro, wyrażonej w złotych i ustalonej przy zastosowaniu kursu średniego ogłaszanego przez Narodowy Bank Polski obowiązującego w dniu 31 grudnia w roku poprzedzającym rok wydania decyzji o wymierzeniu kary lub 2% przychodów osiągniętych przez podmiot kluczowy z działalności gospodarczej w roku obrotowym poprzedzającym wymierzenie kary, przy czym zastosowanie ma kwota wyższa. Kara ta nie może być jednak niższa niż 20 000 zł. – w odniesieniu do PK; - do 7 000 000 euro, wyrażonej w złotych i ustalonej przy zastosowaniu kursu średniego ogłaszanego przez Narodowy Bank Polski obowiązującego w dniu 31 grudnia w roku poprzedzającym rok wydania decyzji o wymierzeniu kary lub 1,4% przychodów osiągniętych przez podmiot ważny z działalności gospodarczej w roku obrotowym poprzedzającym wymierzenie kary. Kara ta nie może być jednak niższa niż 15 000 zł. – w odniesieniu do PW. Podstawa wysokości kary pieniężnej w odniesieniu do podmiotów, których okres wykonywania działalności gospodarczej jest krótszy niż 12 miesięcy albo gdy podmiot nie osiągnął przychodu wynosi 500.000 euro. W razie naruszenia przepisów KSC przez PK lub PW, które stwarza szczególne zagrożenie dla bezpieczeństwa, zdrowia, życia lub zagrożenie wywołania poważnej szkody majątkowej lub poważnych utrudnień w świadczeniu usług, wysokość kary może wynosić do 100.000.000 zł. Ogólny wpływ regulacji: W stosunku do poprzednio obowiązujących przepisów, Projekt zakłada podwyższenie maksymalnych kar pieniężnych z tytułu naruszenia obowiązków w zakresie	Uwaga nieuwzględniona Przepisy dotyczące nakładania kar pieniężnych mają na celu wdrożenie dyrektywy NIS 2 do porządku krajowego. Projekt ustawy nakłada na podmioty kluczowe i podmioty ważne szereg obowiązków, które nie mogą pozostać bez sankcji, gdy podmiot nie będzie ich wykonywał. Stanowiłoby to bowiem lukę w prawie, a także stało w sprzeczności z dyrektywą NIS2, która zobowiązuje państwa członkowskie do przyjęcia przepisów w zakresie kar, które m.in. będą odstrasżające. Należy wskazać, że wszystkie obowiązki nałożone na podmioty mają istotne znaczenie dla krajowego systemu cyberbezpieczeństwa. Wysokość kar nie stoi w sprzeczności z dyrektywą NIS 2.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			cyberbezpieczeństwa, zgodnie z postanowieniami Dyrektywy NIS2. Ponadto, niższa kwota maksymalna będzie miała zastosowanie do podmiotów prowadzących działalność krócej niż 12 miesięcy lub które nie osiągnęły przychodu. Ww. odstępstwa nie wynikają z Dyrektywy NIS2. Projekt wprowadza również podwyższony wymiar kary w razie kwalifikowanego naruszenia wymogów dot. cyberbezpieczeństwa – 100.000.000 PLN. Wpływ na sektor energetyczny: jw. – brak specyficznego wpływu na sektor energetyczny.	Karanie za jednokrotne naruszenie jest niezwykle istotne bowiem już takie naruszenie niekiedy może skutkować bardzo poważnymi konsekwencjami.
135.	Związek Telewizji Kablowych (ZTKIG)	Art. 73	Kary pieniężne Zdecydowanie należy się sprzeciwić opcji obliczania kary pieniężnej od przychodów osiągniętych przez podmiot kluczowy oraz przez podmiot ważny z całej działalności gospodarczej tych podmiotów osiągniętych w poprzednim roku obrotowym Za sprzeczne z konstytucyjnymi zasadami sprawiedliwości społecznej i demokratycznego państwa prawnego (art. 2 w zw. z art. 8 Konstytucji RP) uznać należy przyjęcie w art. 73 ust. 3 i ust. 4 ustawy o KSC podstawy wyliczenia kary pieniężnej dla podmiotu kluczowego i podmiotu ważnego obliczanej od całego przychodu osiągniętego przez tegoż przedsiębiorcę w poprzednim roku kalendarzowym. Jeżeli bowiem podmiotem ukaranym będzie spółdzielnia mieszkaniowa osiągająca wielomilionowe przychody z tytułu sprzedaży lokali, czynszów, pobierania opłat eksploatacyjno- użytkowych od lokali spółdzielczych, a także z tytułu zarządzania nieruchomościami i lokalami, zaś przychody uzyskiwane z tytułu prowadzenia działalności telekomunikacyjnej stanowią niewielką jedynie część tego przychodu, to doprawdy trudno byłoby wobec spółdzielni mieszkaniowej przyjmować podstawę wyliczenia kary od całego jej ubiegłorocznego przychodu z działalności gospodarczej obejmującego także przychody uzyskiwane z działalności inwestycyjnej oraz zarządzania lokalami, która to działalność poza umiejscowieniem sieci telekomunikacyjnej niewiele ma wspólnego z działalnością telekomunikacyjną, szczególnie jeśli się zważy, że kara wymierzana jest w związku z niewykonywaniem lub nienależytym wykonywaniem obowiązków opisanych w art. 73 ust. 1 , ust. 1 a i ust. 1 b ustawy o KSC, a nie w związku z wykonywaniem wadliwym lub też niewykonywaniem przez spółdzielnię mieszkaniową innych obowiązków. Ponadto w przypadku przedsiębiorcy telekomunikacyjnego świadczącego różnorakie usługi telekomunikacyjne oraz inne usługi i świadczenia (np. naprawa sprzętu komputerowego, handlowanie komputerami)także trudno byłoby jako podstawę wyliczenia kary pieniężnej z tytułu niewykonania lub nienależytego wykonania, obowiązków związanych z cyberbezpieczeństwem przyjmować przychód uzyskany przez przedsiębiorcę telekomunikacyjnego w poprzednim roku kalendarzowym z całej prowadzonej działalności telekomunikacyjnej oraz jeszcze innej działalności nie będącej działalnością telekomunikacyjną. aPodstawa bowiem obliczenia kary pieniężnej winna być ściśle powiązana z usługą telekomunikacyjną, w ramach której realizacji doszło do zarzucanych naruszeń, nie zaś w związku z przychodem podmiotu uzyskiwanym z całej działalności gospodarczej podmiotu. Jeżeli bowiem podmiotem ukaranym będzie spółdzielnia mieszkaniowa osiągająca wielomilionowe przychody z tytułu sprzedaży lokali, czynszów, pobierania opłat eksploatacyjno- użytkowych od lokali spółdzielczych, a także z tytułu zarządzania nieruchomościami i lokalami, zaś przychody uzyskiwane z tytułu prowadzenia działalności telekomunikacyjnej stanowią niewielką jedynie część tego przychodu, to	Uwaga nieuwzględniona Projekt ustawy wdraża w tym zakresie postanowienia dyrektywy NIS 2. Państwa członkowskie obowiązane są do stosowania wskazanych w niej kryteriów zgodnie z zasadą harmonizacji minimalnej. Ponadto wskazać należy, że obowiązki podmiotu kluczowego i podmiotu ważnego nie zależą od tego czy podmiot ten prowadzi również inną działalność poza tą, w stosunku do której nie wykonał obowiązków. Takie podejście prowadziłyby do nierówności podmiotów i niesprawiedliwego traktowania bowiem zachodziłaby różnica pomiędzy samymi podmiotami wewnątrz podmiotów kluczowych lub podmiotów ważnych. Każdy podmiot spełniający kryteria uznany za podmiot kluczowy lub podmiot ważny ma takie same obowiązki i podlega takim samym kryteriom wymiaru kary. Należy zwrócić uwagę, że zaproponowany system kar, wdrażany na podstawie dyrektywy NIS 2, cechuje się proporcjonalnością i adekwatnością. Umożliwia bowiem organowi właściwemu do spraw cyberbezpieczeństwa dostosowanie wysokości kary przy uwzględnieniu przesłanek merytorycznych – istotnych z punktu widzenia cyberbezpieczeństwa. Tylko takie przesłanki mogą stanowić podstawę wymiaru kary, a nie obliczanie przychodu uzyskiwanego przez podmiot z części swojej działalności.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			doprawdy trudno byłoby wobec spółdzielni mieszkaniowej przyjmować podstawę wyliczenia kary od całego jej ubiegłorooW tym stanie rzeczy wnioskujemy zatem o: a/ zmianę art. 1 pkt. 74 lit. d projektu ustawy zmieniającej ustawę o KSC w ten sposób, że w proponowanym art. 73 ust. 3 zd. 1 in fine ustawy o KSC alternatywnie określoną podstawę 2 %- owej kary pieniężnej liczonej od „przychodów osiągniętych przez podmiot kluczowy z działalności gospodarczej w roku obrotowym poprzedzającym wymierzenie kary” zastąpi się podstawą obliczenia 2 %- owej kary pieniężnej liczonej od „przychodów osiągniętych przez podmiot kluczowy z działalności telekomunikacyjnej w roku obrotowym poprzedzającym wymierzenie kary”,a b/ zmianę art. 1 pkt. 74 lit. f projektu ustawy zmieniającej ustawę o KSC w ten sposób, że w proponowanym art. 73 ust. 4 zd. 1 in fine ustawy o KSC alternatywnie określoną podstawę 1,4 %- owej kary pieniężnej liczonej od „przychodów osiągniętych przez podmiot ważny z działalności gospodarczej w roku obrotowym poprzedzającym wymierzenie kary” zastąpi się podstawą obliczenia 1,4 %- owej kary pieniężnej liczonej od „przychodów osiągniętych przez podmiot ważny z działalności telekomunikacyjnej w roku obrotowym poprzedzającym wymierzenie kary”.	
136.	Osoba fizyczna	Art. 73	Katalog kar art. 73 został zmieniony na formę trybu przeszłego dokonanego. Są to formy czasowników w trzeciej osobie liczby pojedynczej. „nie uzupełnił”, „nie wyznaczył”, „nie wdrożył”. Powoduje to, iż zapisy wskazują na jednokrotność czynności. W wersji poprzedniej ustawodawca zastosował formy, odpowiednio: nie uzupełnia, nie wyznacza, nie wdraża, co wskazuje na procesowość. W cyberbezpieczeństwie pożądaną jest forma procesowa.	Uwaga wyjaśniona W ocenie projektodawcy dokonane zmiany na tryb przeszły dokonany, a także doprecyzowanie, że karze podlega podmiot, którego działanie miało także charakter jednorazowy są niezbędne dla prawidłowego i skutecznego dochodzenia odpowiedzialności za naruszenia przepisów ustawy. Należy wskazać, że na wymiar kary będzie miała wpływ m.in. jednorazowość lub wielokrotność naruszenia. Przesłanki wymiaru kary zostały bowiem wskazane w art. 53 ust. 10 ustawy. Naruszenia nałożonych na podmioty obowiązków mogą mieć różne skutki dla samego podmiotu, innych podmiotów będących w łańcuchu dostaw a także dla państwa i jego obywateli. Nie można zatem zgodzić się na sytuację w której podmiot nie podlega odpowiedzialności za naruszenie jednokrotne, a wyłącznie za procesowe czyli trwające przez nieokreślony czas. Dokonując analizy obecnych postanowień

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

				ustawy zdecydowano o rezygnacji z dotychczasowego podejścia uznając je za nieefektywne i nieodpowiednie do założonego celu jakim jest zapewnienie wysokiego poziomu cyberbezpieczeństwa.
137.	Związek Cyfrowa Polska	Art. 73	W dyrektywie możemy przeczytać (art. 36 Dyrektywy): “Państwa członkowskie ustanawiają przepisy dotyczące kar stosowanych wobec naruszeń krajowych środków przyjętych zgodnie z niniejszą dyrektywą oraz podejmują wszelkie niezbędne środki, aby zapewnić ich wdrożenie. Przewidziane kary muszą być skuteczne, proporcjonalne i odstraszające.” Polski projekt implementacji w art. 73 ust.1 określa kary finansowe, które mogą być nałożone na podmioty kluczowe lub ważne. Maksymalne kwoty kar przewidziane w polskim projekcie ustawy są takie same jak w NIS2, z dwoma wyjątkami, gdzie organ właściwy może nałożyć wyższe kary tj. karę w wysokości do 100 000 000 PLN oraz karę w wysokości od 500 PLN do 100 000 PLN za każdy dzień opóźnienia. Przewidziane kary mogą być nieproporcjonalne w stosunku do naruszeń. Wysokie kary za nieznaczne uchybienia mogą prowadzić do nadmiernej represji i nieproporcjonalnego obciążenia podmiotów kluczowych lub ważnych. Ponadto przyznanie organom władzy możliwości nakładania wysokich kar oraz decydowania o zawieszeniu lub cofnięciu licencji może prowadzić do ryzyka arbitralności i nadużycia władzy. Proponujemy ponowne przeanalizowanie wysokości kar oraz wprowadzenie mechanizmów zapewniających proporcjonalność i sprawiedliwość w egzekwowaniu przepisów.	Uwaga wyjaśniona Do postępowania w sprawie nałożenia administracyjnej kary pieniężnej będą stosowane przepisy o miarkowaniu kary pieniężnej z KPA, co oczywiście będzie mogło podlegać kontroli sądu administracyjnego.
138.	Osoba fizyczna	Art. 73 i art. 73a	Jeżeli katalog kar jest zamknięty i wskazany jest bezpośrednio w przepisie prawa, a dotyczy przecież naruszenia obowiązków wynikających z przepisów prawa, zapis: organ właściwy do spraw cyberbezpieczeństwa może odstąpić od nałożenia kary pieniężnej, o której mowa w art. 73 i art. 73a, jeżeli waga naruszenia i znaczenie naruszonych przepisów jest znikome, a podmiot albo kierownik podmiotu kluczowego lub podmiotu ważnego zaprzestał naruszania prawa lub naprawił wyrządzoną szkodę. Wszystkie wskazane w wymienionych art. naruszenia mają charakter poziomu wysokiego.	Uwaga wyjaśniona Nie jest możliwe aby z góry założyć wpływ naruszenia dokonanego przez podmiot. Każda sytuacja będzie rozpatrywana indywidualnie przez organ właściwy do spraw cyberbezpieczeństwa na podstawie stanu faktycznego i wskazanych w projekcie ustawy przesłanek, które należy wziąć pod uwagę przy wymiarze kary. Jeśli zatem podmiot analizując sytuację uwzględniając przesłanki wymiaru kary dojdzie do wniosku, że naruszenie jest znikome, może odstąpić od nałożenia kary.
139.	KIGEIT	Art. 73 ust. 1 i art. 73a ust. 2	Art. 73 ust. 1 b oraz art. 73a ust. 2 - rozwiązania nieproporcjonalne, nie podlegający kwantyfikacji, bez żadnych ograniczeń, NIS2 mówi w art. 34 ust. 6 o karach okresowych w celu przymuszenia a nie jednorazowych, w ten sposób nie ma mowy o proporcjonalności	Uwaga wyjaśniona Dyrektywa NIS 2 w wielu miejscach nakłada na państwa członkowskie obowiązek zapewnienia, że osoby fizyczne pełniące funkcje kierownicze będą podlegały odpowiedzialności za

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

				uchybień w obowiązkach swoich lub podmiotu. Przepis jest zatem bezpośrednim wdrożeniem postanowień dyrektywy NIS 2.
140.	Krzysztof Rożko i Wspólnicy Kancelaria Prawna sp. k.	Art. 73	<u>UWAGA ZGŁOSZONA W RAMACH ZGŁOSZENIA LOBBINGOWEGO</u> Art. 1 pkt 74 lit. d) projektu nowelizacji uKSC wprowadza w art. 73 ust 3 uKSC wysokość kary minimalnej dla podmiotu kluczowego jako nie niższej niż 20 000 zł i odpowiednio w art. 1 pkt. 74 lit. f) karę minimalną dla podmiotu ważnego w wysokości nie niższej niż 15 000 zł, podczas, gdy dyrektywa NIS 2 nie określa kar minimalnych. Zważywszy na fakt, iż kary takiej wysokości nakładane mogłyby być na podmioty małe, o utrudnionym procesie adaptacji do zaostrzonych wymogów wprowadzonych w nowelizacji uKSC proponujemy zrezygnowanie z regulowania wysokości kary minimalnej.	Uwaga nieuwzględniona Wdrażana do porządku prawnego dyrektywa NIS 2 pozostawia państwom członkowskim swobodę w kształtowaniu sankcji, wskazując jedynie minimalną wysokość górnego pułapu kar. Państwa członkowskie są jednak zobowiązane do takiego ukształtowania sankcji, które zapewnią skuteczność egzekwowania przepisów, będą odstrasżające, a jednocześnie proporcjonalne. Mając na uwadze istotność obowiązków nałożonych na podmioty oraz ich zróżnicowanie pod kątem osiąganych przychodów należało wprowadzić minimalną wysokość kary pieniężnej.
141.	KIGEIT	Art. 73 ust. 5	Art. 73 ust 5 - jaka jest relacja tej kary do nowych przepisów karnych wynikających z NIS2? Brak jest podstawy prawnej stwierdzenia tego naruszenia.	Uwaga wyjaśniona Przepis znajdzie zastosowanie gdy zrealizują się wskazane w nim przesłanki tzn. wtedy gdy podmiot kluczowy lub podmiot ważny naruszy obowiązki wynikające z ustawy, a naruszenie to dodatkowo będzie realizowało przesłanki wskazane w pkt 1 lub 2 tego przepisu. Jednocześnie realizacja tych przesłanek wyklucza możliwość stosowania kary za naruszenia przewidziane w art. 73 ust. 1, ponieważ stoi to w sprzeczności z zakazem podwójnego karania za to samo naruszenie.
142.	ZIPSEE Cyfrowa Polska	Art. 73a	Państwa członkowskie zapewniają w NIS2, że organy zarządzające podmiotów kluczowych i ważnych zatwierdzają środki zarządzania ryzykiem cyberbezpieczeństwa podjęte przez te podmioty w celu przestrzegania artykułu 21, nadzorują ich wdrażanie oraz mogą ponosić odpowiedzialność za naruszenia tego artykułu przez te podmioty. Polski projekt implementacji określa obowiązki szefów podmiotów kluczowych i ważnych (art. 8c do 8e) oraz zasady związane z karami finansowymi, które mogą być na nich nałożone (art. 73a). Kara może być nałożona w dwóch przypadkach: a. jeśli szef jednostki nie wypełnił swoich obowiązków wynikających z polskiej implementacji NIS2, wymienionych w art. 73a projektu, lub	Uwaga wyjaśniona Art. 76a wskazuje co organ właściwy do spraw cyberbezpieczeństwa musi brać pod uwagę przy określaniu wymiaru kary. Bierze pod uwagę m.in. możliwości finansowe kierownika podmiotu kluczowego lub podmiotu ważnego.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			b. jeśli podmiot kluczowy ub ważny nie wypełnił swoich obowiązków wynikających z projektu implementacji NIS2, wymienionych w art. 73 krajowego projektu implementacji. Kwota kary nie może przekroczyć 600% wynagrodzenia otrzymanego przez ukaraną osobę, obliczonego zgodnie z zasadami dotyczącymi ustalania ekwiwalentu pieniężnego za urlop. Takie uszczegółowienie w sposób istotny odbiega od zasad określonych w dyrektywie. Kara taka powinna uwzględniać zdolność finansową szefa jednostki.	Wobec tego postulat o uzupełnienie, aby kara uwzględniała zdolność finansową szefa jednostki jest bezprzedmiotowa bowiem projekt już to przewiduje.
143.	Polskie Stowarzyszenie Fotowoltaiki	Art. 73a	Art. 73a [Odpowiedzialność kierownika PK lub PW] Projekt przewiduje odpowiedzialność kierownika PK lub PW w razie niewykonywania, w tym jednorazowego niewykonania, nałożonych na niego obowiązków wynikających z Projektu. Kara pieniężna może wynosić do 600% otrzymywanego przez ukaranego wynagrodzenia obliczanego według zasad obowiązujących przy ustalaniu ekwiwalentu pieniężnego za urlop Ogólny wpływ regulacji: Przepis określa podstawy nałożenia kary pieniężnej na kierownika PK lub PW. Jak zostało wskazane w uwagach do art. 8d-8f, obowiązki wskazane w przepisach Projektu odnoszą się bezpośrednio do kierownika PK lub PW i są niezależne od obowiązków PK i PW w zakresie cyberbezpieczeństwa. W rezultacie skutkuje to koniecznością zapewnienia przez PK i PW zgodności z wymogami na dwóch płaszczyznach. Wpływ na sektor energetyczny: jw. – brak specyficznego wpływu na sektor energetyczny. [Nadregulacja względem Dyrektywy NIS2] Dyrektywa NIS2 nie przewiduje nakładania kar pieniężnych na kierownika PK lub PW, a jedynie obowiązek zapewnienia możliwości pociągnięcia do odpowiedzialności za niewywiązanie się z obowiązku zapewnienia jej przestrzegania. Osoby te mogą ponosić niezależną odpowiedzialność na podstawie łączącego ją stosunku z PK lub PW (pracy lub innego cywilnoprawnego) jak również mogą ponosić odpowiedzialność karną na podstawie ogólnie obowiązujących przepisów. Tym samym, nałożenie dodatkowej odpowiedzialności administracyjnej jest nieproporcjonalne i stanowi zbędną nadregulację w stosunku do wymogów wynikających z Dyrektywy NIS2. (Zob. dodatkowe uwagi do art. 8d-8f KSC wg Projektu).	Uwaga nieuwzględniona Dyrektywa NIS 2 zobowiązuje państwa członkowskie do zapewnienia takich środków, które pozwolą na egzekwowanie odpowiedzialności kierownika podmiotu za niewywiązanie się z obowiązków. Jeśli podmioty ponoszą odpowiedzialność za naruszanie obowiązków przewidzianych ustawą to również kierownik podmiotu powinien ponosić taką odpowiedzialność.
144.	Amerykańska Izba Handlowa w Polsce	Art. 73a	Zgodnie z art. 20 ust. 1 dyrektywy NIS 2 na państwach członkowskich ciąży obowiązek zapewnienia, że organy zarządzające podmiotów kluczowych i ważnych zatwierdzają środki zarządzania ryzykiem cyberbezpieczeństwa podjęte przez te podmioty w celu przestrzegania artykułu 21 dyrektywy, nadzorują ich wdrażanie oraz mogą ponosić odpowiedzialność za naruszenia tego artykułu przez te podmioty. Projekt ustawy określa, w art. 1 pkt 13, obowiązki kierowników podmiotów kluczowych i ważnych (art. 8c do 8e wprowadzane do uksc) oraz, w art. 1 pkt 75m zasady związane z karami finansowymi, które mogą być na nich nałożone (art. 73a wprowadzany do uksc). Kara może być nałożona w dwóch przypadkach: jeżeli kierownik jednostki nie wypełnił swoich obowiązków wynikających z polskiej implementacji NIS 2, wymienionych w art. 73a wprowadzanym do uksc, lub jeśli podmiot kluczowy lub ważny nie wypełnił swoich obowiązków wynikających z art. 73 uksc. Kwota kary nie może przekroczyć 600% wynagrodzenia otrzymanego przez ukaraną osobę, obliczonego	Uwaga wyjaśniona Art. 76a wskazuje co organ właściwy do spraw cyberbezpieczeństwa musi brać pod uwagę przy określaniu wymiaru kary. Bierze pod uwagę m.in. możliwości finansowe kierownika podmiotu kluczowego lub podmiotu ważnego. Wobec tego postulat o uzupełnienie, aby kara uwzględniała zdolność finansową szefa jednostki jest bezprzedmiotowa bowiem projekt już to przewiduje.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			zgodnie z zasadami dotyczącymi ustalania ekwiwalentu pieniężnego za urlop. Takie uszczegółowienie w sposób istotny odbiega od zasad określonych w dyrektywie. Stoimy na stanowisku, że kara pieniężna powinna uwzględniać względy proporcjonalności i zdolność finansową kierownika jednostki.	
145.	Polska Izba Informatyki i Telekomunikacji	Art. 74	Art. 74 ust. 2 – możliwość nadania karze pieniężnej rygoru natychmiastowej wykonalności Jako Izba stoimy na stanowisku, że kara pieniężna nigdy nie powinna być nakładana pod rygorem natychmiastowej wykonalności. Możliwość nadania rygoru natychmiastowej wykonalności decyzji nakładającej karę pieniężną przewiduje art. 74 ust. 2 ustawy (w brzmieniu nadawanym projektowaną ustawą) i choć jest to możliwość (a nie ustawy rygor natychmiastowej wykonalności) to uważamy, że nie powinno być takiej możliwości. Kary pieniężne, w szczególności tak wysokie jak te, które przewiduje ustawa w brzmieniu nadawanym projektowaną ustawą, są bardzo dotkliwe i nie powinny nigdy być natychmiast wykonywane, a więc wykonywane zanim jeszcze decyzja o nałożeniu kary stanie się prawomocna i zakończy się ewentualne postępowanie sądowe zainicjowane odwołaniem się od decyzji. Konieczność uiszczenia wysokiej kary pieniężnej może oznaczać koniec działalności podmiotu kluczowego albo ważnego, a skutki mogą nieodwracalne, nawet jeśli po latach sąd przyzna rację podmiotowi skarżącemu decyzję o karze. Natychmiastowa wykonalność kary pieniężnej budzi zastrzeżenia natury konstytucyjnej, bo może być odczytywana jako ograniczenie prawa do sądu, w szczególności biorąc pod uwagę przeciętny czas oczekiwania na wydanie orzeczenia przez sąd. Właśnie z tych względów szereg przepisów obowiązującego prawa, traktujących o nakładaniu kar pieniężnych przez organy nadzorcze w różnych sektorach działalności regulowanej, wprost wyłączają możliwość nadania rygoru natychmiastowej wykonalności decyzji o nałożeniu kary pieniężnej. Dobrym przykładem jest tu obowiązująca ustawa – Prawo telekomunikacyjne, która w art. 210 ust. 1 zdanie drugie jednoznacznie i kategorycznie przesądza, że decyzjom o nałożeniu kary pieniężnej nie nadaje się rygoru natychmiastowej wykonalności. Projektowane przepisy powinny być zmienione na wzór przytoczonego przepisu ustawy – Prawo telekomunikacyjne. Projektowany art. 74 ust. 2 ustawy o krajowym systemie cyberbezpieczeństwa powinien wprost i jednoznacznie przesądzać, że decyzji o nałożeniu kary pieniężnej nie nadaje się rygoru natychmiastowej wykonalności.	Uwaga nieuwzględniona W ocenie projektodawcy pozostawienie możliwości nałożenia rygoru natychmiastowej wykonalności w określonych enumeratywnie przesłankach jest konieczne. Wskazać należy, że zasadą przyjętą w projekcie jest jednak brak nakładania rygoru natychmiastowej wykonalności. Wskazanie kilku wyjątków zapewnia jednak, że środek ten jest proporcjonalny i adekwatny. Zagadnienie to zostanie poddane dalszej analizie z uwzględnieniem uwag zgłoszonych przez pozostałe podmioty.
146.	Fundacja Open Allies	Art. 74	[RYGOR NATYCHMIASTOWEJ WYKONALNOŚCI] Zwracamy się o wykreślenie z Projektu art. 74 ust. 2 nowelizacji UKSC. Zgodnie z tym przepisem organ właściwy do spraw cyberbezpieczeństwa może nadać decyzji nakładającej karę pieniężną rygor natychmiastowej wykonalności w całości lub w części. Zdaniem Fundacji, decyzja nakładająca karę administracyjną nie powinna posiadać rygoru natychmiastowej wykonalności. Każdy podmiot cyberbezpieczeństwa powinien mieć prawo do odwołania się od nałożonej kary – przed jej zapłaceniem. Kara powinna być płacona dopiero po uprawomocnieniu się decyzji o nałożeniu kary – w szczególności po rozpatrzeniu decyzji przez niezależny sąd, o ile podmiot ukarany zdecyduje się na skargę (odwołanie do sądu).	Uwaga nieuwzględniona W ocenie projektodawcy pozostawienie możliwości nałożenia rygoru natychmiastowej wykonalności w określonych enumeratywnie przesłankach jest konieczne. Wskazać należy, że zasadą przyjętą w projekcie jest jednak brak nakładania rygoru natychmiastowej wykonalności. Wskazanie kilku wyjątków zapewnia jednak, że środek ten jest proporcjonalny i adekwatny.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			Nałożenie rygoru natychmiastowej wykonalności może doprowadzić również do uznania, że podmiot jest „recydywistą” (por. art. 53 ust. 10 nowelizowanego UKSC oraz art. 189d pkt 3) ustawy kodeks postępowania administracyjnego) bez wyroku sądowego.	
147.	Grupa MiŚOT	Art. 74	Należy wykreślić z KSC możliwość nałożenia rygoru natychmiastowej wykonalności na decyzję nakładającą karę administracyjną (art. 74 ust. 2 KSC).	Uwaga nieuwzględniona W ocenie projektodawcy pozostawienie możliwości nałożenia rygoru natychmiastowej wykonalności w określonych enumeratywnie przesłankach jest konieczne. Wskazać należy, że zasadą przyjętą w projekcie jest jednak brak nakładania rygoru natychmiastowej wykonalności. Wskazanie kilku wyjątków zapewnia jednak, że środek ten jest proporcjonalny i adekwatny.
148.	IAB Polska	Art. 74 i art. 76b	Natychmiastowa wykonalność decyzji o nałożeniu kar pieniężnych. [art. 1 ust. 76 i 79 projektu nowelizacji / art. 74 ust. 2 i art. 76b ust. 3 nowelizowanego UKSC] Nakładając którąkolwiek z kar pieniężnych opisanych powyżej, właściwy organ będzie uprawniony do nadania takiej decyzji rygoru natychmiastowej wykonalności, jeżeli wymaga tego ochrona bezpieczeństwa lub porządku publicznego. Trudno jest jednak wyobrazić sobie sytuację, w której konieczność natychmiastowej egzekucji kary pieniężnej (która z natury ma charakter represyjny i wtórny do zaistniałego naruszenia) może być wymagana do ochrona bezpieczeństwa lub porządku publicznego – a więc pojęcia bardzo nieostrego, umożliwiającego jego dowolną interpretację. Tym samym istnieje obawa, że proponowane regulacje dotyczące natychmiastowej wykonalności decyzji o nałożeniu kar pieniężnych będą nadużywane przez organy nadzoru, które będą mogły praktycznie natychmiastowo nałożyć i wyegzekwować karę pieniężną w wysokości nawet 100 mln zł, natomiast ocena zasadności tych działań będzie zależeć od dalszych rozstrzygnięć sądów administracyjnych, zapadłych w toku długotrwałych postępowań. Mając to na uwadze, IAB Polska postuluje wykreślenie art. 74 ust. 2 i art. 76b ust. 3 nowelizowanego UKSC.	Uwaga nieuwzględniona W ocenie projektodawcy pozostawienie możliwości nałożenia rygoru natychmiastowej wykonalności w określonych enumeratywnie przesłankach jest konieczne. Wskazać należy, że zasadą przyjętą w projekcie jest jednak brak nakładania rygoru natychmiastowej wykonalności. Wskazanie kilku wyjątków zapewnia jednak, że środek ten jest proporcjonalny i adekwatny.
149.	Konfederacja Lewiatan	Art. 74	Uwaga: Projektodawca wprowadził możliwość nałożenia na decyzję w sprawie kary rygoru natychmiastowej wykonalności w całości lub w części, jeżeli wymaga tego ochrona bezpieczeństwa lub porządku publicznego. Okoliczności te jednak są bez znaczenia dla określenia rygoru natychmiastowej wykonalności. Rygor ten bowiem co do zasady nie jest nakładany na decyzje administracyjne w sprawie kar ze względu na uzasadnione ryzyko naruszenia podstawowych praw podmiotu, uniemożliwiając mu odwołanie się od sankcji – nałożona kara pieniężna (szczególnie gdy może osiągnąć 100 mln zł) może bowiem spowodować zaprzestanie działalności bez możliwości odwołania się. Ogólna zasada nadawania rygoru natychmiastowej wykonalności określona w art. 108 kpa odwołuje się do takich kwestii jak ochrona zdrowia lub życia ludzkiego albo dla zabezpieczenia gospodarstwa narodowego przed ciężkimi stratami bądź też ze względu na inny interes społeczny lub wyjątkowo ważny interes strony. Niemniej w przypadku administracyjnej kary pieniężnej mamy do czynienia z relacją państwo – podmiot ukarany, stąd ewentualny	Uwaga nieuwzględniona Projekt zakłada odpowiednie stosowanie przepisów KPA w zakresie nieuregulowanym w projekcie. W pozostałym zakresie wprowadza własną procedurę, w tym również przesłanki nadania rygoru natychmiastowej wykonalności. W ocenie projektodawcy pozostawienie możliwości nałożenia rygoru natychmiastowej wykonalności w określonych enumeratywnie przesłankach

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			rygor natychmiastowej wykonalności mógłby być uzasadniony np. uzasadnionym podejrzeniem podejmowania działań, mających na celu bezprawne uniknięcie zapłaty wymierzonej kary (np. wyprowadzanie środków pieniężnych). Odwołanie się natomiast do ogólnych klauzul ochrona bezpieczeństwa lub porządku publicznego wypacza sens nadania rygoru natychmiastowej wykonalności, ponieważ w istocie oznacza możliwość arbitralnego nadawania takiego rygoru. Podczas gdy nadawanie rygoru natychmiastowej wykonalności dla decyzji administracyjnych wymierzających kary powinno być wyjątkiem. Analogicznej konstrukcji, do projektowanego art. 74 ust. 2 projektu KSC próżno szukać w ustawie – Prawo telekomunikacyjne, czy w ustawie o ochronie danych osobowych. Przykładowo w ustawie – Prawo telekomunikacyjne, zgodnie z art. 206 ust. 2aa, decyzje regulacyjne podlegają natychmiastowemu wykonaniu, ale z wyjątkiem decyzji w sprawie nałożenia kar, właśnie z uwagi na ich nieodwracalne skutki.	jest konieczne. Zasadą przyjętą w projekcie jest jednak brak nakładania rygoru natychmiastowej wykonalności.
150.	Konfederacja Lewiatan	Art. 74	W art. 74 ust. 3 projektu KSC proponuje się utrzymanie zasady, zgodnie z którą wpływy z kar nakładanych na podstawie ustawy o krajowym systemie cyberbezpieczeństwa stanowią przychody Funduszu Cyberbezpieczeństwa. Taki mechanizm budzi kontrowersje z kilku istotnych powodów. Przede wszystkim, powiązanie wpływów z kar z wynagrodzeniami osób odpowiedzialnych za ich nakładanie rodzi poważne wątpliwości co do bezstronności i obiektywizmu procesu nakładania tych kar. Mechanizm ten może prowadzić do sytuacji, w której osoby mające kompetencje do nakładania kar będą bardziej skłonne do ich stosowania, nawet w przypadkach, gdzie mogłyby one być nieadekwatne lub zbyt surowe. Zwiększenie wpływów Funduszu Cyberbezpieczeństwa poprzez nakładanie większej liczby kar bezpośrednio wpływa na wynagrodzenia osób odpowiedzialnych za te decyzje, co może stanowić bodziec do nadużyć. Takie rozwiązanie może być postrzegane jako konflikt interesów, podważając zaufanie do całego systemu cyberbezpieczeństwa. Działanie organów państwa musi być transparentne i wolne od konfliktu interesów. Przepisy prawa powinny być konstruowane w taki sposób, aby zapobiegać sytuacjom, w których decyzje administracyjne mogą być podejmowane z pobudek osobistych lub finansowych. W świetle tego proponowane brzmienie (choć utrzymujące dotychczasową konstrukcję art. 74 ustawy KSC może być uznane za sprzeczne z zasadą bezstronności działania organów państwowych. Choć idea Funduszu Cyberbezpieczeństwa jako źródła finansowania wynagrodzeń osób realizujących zadania z zakresu cyberbezpieczeństwa jest uzasadniona, to powiązanie wpływów z kar z tym funduszem rodzi poważne wątpliwości natury etycznej i prawnej. Dla zapewnienia bezstronności oraz zaufania do systemu cyberbezpieczeństwa, konieczne jest przemyślenie i zmodyfikowanie tego mechanizmu, tak aby unikać potencjalnych nadużyć oraz konfliktu interesów.	Uwaga nieuwzględniona Dochód z kar na podstawie obecnie obowiązującej ustawy również stanowi przychód funduszu cyberbezpieczeństwa. Funkcjonowanie funduszu cyberbezpieczeństwa jest ściśle związane z krajowym systemem cyberbezpieczeństwa - stanowi on jego część. Należy zauważyć, że nie ma bezpośredniego powiązania między nałożonymi karami a otrzymaniem środków z Funduszu Cyberbezpieczeństwa. Środki z tego Funduszu są przyznawane uprawnionym podmiotom na podstawie wniosków, które podlegają ocenie dokonywanej przez Kolegium ds. cyberbezpieczeństwa. W związku z tym, z samego faktu nałożenia kary nie wzrastają środki jaki dany podmiot ma do dyspozycji. Możliwa jest też sytuacja, w której podmiot nakładający kary nie otrzyma żadnych środków na świadczenie teleinformatyczne. W związku z tym organ nie uzyskuje bezpośrednich korzyści z nakładanych kar.
151.	PIKE i Mediakom	Art. 74 ust. 3	Izba zwraca uwagę na <i>korupcjogenny charakter tego przepisu</i> . Podmioty, dla których minister właściwy do spraw informatyzacji jest organem właściwym do spraw cyberbezpieczeństwa, mogą czuć się systemowo zagrożone tym przepisem, ponieważ powoduje on, że kary nakładane na te podmioty będą bezpośrednio zasilać fundusz, od zasobności którego będzie zależała wysokość wynagrodzenia osób kontrolujących.	Uwaga nieuwzględniona Dochód z kar na podstawie obecnie obowiązującej ustawy również stanowi przychód funduszu cyberbezpieczeństwa.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			Konsekwentnie należałoby również w przepisach przejściowych do projektu ustawy uchylić art. 2 ust. 4 pkt 1 ustawy z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa. Art. 74 [...] 3. Wpływy z tytułu kar pieniężnych, o których mowa w art. 73 i art. 73a, stanowią przychód <u>Funduszu Cyberbezpieczeństwa, o którym mowa w art. 2 ustawy z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa budżetu państwa.</u>	Funkcjonowanie funduszu cyberbezpieczeństwa jest ściśle związane z krajowym systemem cyberbezpieczeństwa - stanowi on jego część. Należy zauważyć, że nie ma bezpośredniego powiązania między nałożonymi karami a otrzymaniem środków z Funduszu Cyberbezpieczeństwa. Środki z tego Funduszu są przyznawane uprawnionym podmiotom na podstawie wniosków, które podlegają ocenie dokonywanej przez Kolegium ds. cyberbezpieczeństwa. W związku z tym, z samego faktu nałożenia kary nie wzrastają środki jaki dany podmiot ma do dyspozycji. Możliwa jest też sytuacja, w której podmiot nakładający kary nie otrzyma żadnych środków na świadczenie teleinformatyczne. W związku z tym, organ nie uzyskuje bezpośrednich korzyści z nakładanych kar.
152.	PIKE i Mediakom	Art. 74	Zgodnie z tym przepisem organ właściwy do spraw cyberbezpieczeństwa może nadać decyzji nakładającej karę pieniężną rygor natychmiastowej wykonalności w całości lub w części. Decyzji nakładającej karę administracyjną nie powinno nadawać się takiego rygoru. Każdy podmiot powinien mieć prawo do odwołania się od nałożonej kary bez konieczności jej uprzedniego uiszczenia, przede wszystkim ze względu na potencjalnie katastroficznie wysoki poziom tych kar. Zapłacenie kary powinno następować dopiero po uprawomocnieniu decyzji. Nałożenie rygoru natychmiastowej wykonalności mogłoby, ponadto, doprowadzić właściwy do uznania, że podmiot kluczowy działa w warunkach „powrotu do przestępstwa” (por. art. 53 ust. 10 pkt 1 lit. a oraz pkt 3, jak również art. 189d pkt 3 Kodeksu postępowania administracyjnego, lecz bez wyroku niezależnego sądu. Taki skutek byłby sprzeczny z motywem 143 dyrektywy NIS2 i Kartą Praw Podstawowych. PIKE wnosi o wykreślenie przepisu.	Uwaga nieuwzględniona W ocenie projektodawcy pozostawienie możliwości nałożenia rygoru natychmiastowej wykonalności w określonych enumeratywnie przesłankach jest konieczne. Wskazać należy, że zasadą przyjętą w projekcie jest jednak brak nakładania rygoru natychmiastowej wykonalności. Wskazanie kilku wyjątków zapewnia jednak, że środek ten jest proporcjonalny i adekwatny.
153.	ZBP	Art. 74 ust. 1 i 2	Art. 74.1. Karę pieniężną, o której mowa w art. 73 i art. 73a, nakłada, w drodze decyzji organ właściwy do spraw cyberbezpieczeństwa. 2. Organ właściwy do spraw cyberbezpieczeństwa może nadać decyzji, o której mowa w ust. 1, rygor natychmiastowej wykonalności w całości lub w części, jeżeli wymaga tego ochrona bezpieczeństwa lub porządku publicznego.	Uwaga wyjaśniona W ocenie projektodawcy pozostawienie możliwości nałożenia rygoru natychmiastowej wykonalności w określonych enumeratywnie przesłankach jest konieczne. Wskazać należy, że zasadą

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			Uwaga ogólna - rygor natychmiastowej wykonalności nie powinien dotyczyć kary pieniężnej w sytuacji, gdy jej nałożenie może utrudnić (np. spowolnić) wdrożenie zabezpieczeń cyberinformatycznych niwelujących cyberzagrożenia, co powinno być priorytetem.	przyjętą w projekcie jest jednak brak nałożenia rygoru natychmiastowej wykonalności. Wskazanie kilku wyjątków zapewnia jednak, że środek ten jest proporcjonalny i adekwatny.
154.	KIGEIT	Art. 76	Art. 76 - wątpliwe w kontekście zasady proporcjonalności jest nałożenie kar pomimo zaprzestania naruszenia prawa lub naprawienia szkody - takie przyjęcie penalizacji w KSC narusza podstawowe zasady TFUE; ponadto jest to sprzeczne z art. 76a ust 6 gdzie wskazano na możliwość odstąpienia od wymierzenia kary i jedną z możliwości odstąpienia jest zaprzestanie naruszenia - zastosowano tutaj alternatywę rozłączną	Uwaga uwzględniona Art. 76 zostanie uchylony.
155.	Polska Izba Informatyki i Telekomunikacji	Art. 76	Art. 76 - inne przyczyny nałożenia kary Za wątpliwe w kontekście zasady proporcjonalności jest nałożenie kar, pomimo zaprzestania naruszenia prawa lub naprawienia szkody - takie przyjęcie penalizacji w ksc narusza podstawowe zasady TFUE; ponadto jest to jednocześnie sprzeczne z art. 76a ust 6, gdzie wskazano na możliwość odstąpienia od wymierzenia kary i jedną z możliwości odstąpienia jest właśnie zaprzestanie naruszenia, za które jednocześnie jest penalizacja w art. 76 - zastosowano tutaj alternatywę rozłączną „albo”.	Uwaga uwzględniona Art. 76 zostanie uchylony.
156.	PIKE i Mediakom	Art. 76	Przepis budzi duży sprzeciw. W kontekście zasady proporcjonalności niedopuszczalne jest nałożenie kar pomimo zaprzestania naruszenia prawa lub naprawienia szkody - takie przyjęcie penalizacji w KSC narusza podstawowe zasady TFUE; ponadto jest to sprzeczne z art. 76a ust 6 gdzie wskazano na możliwość odstąpienia od wymierzenia kary i jedną z możliwości odstąpienia jest zaprzestanie naruszenia - zastosowano tutaj alternatywę rozłączną. Wykreślenie art. 76	Uwaga uwzględniona Art. 76 zostanie uchylony.
157.	Krzysztof Rożko i Wspólnicy Kancelaria Prawna sp. k.	Art. 76a	<u>UWAGA ZGŁOSZONA W RAMACH ZGŁOSZENIA LOBBINGOWEGO</u> Zważywszy, że art. 10 pkt 7) projektu ustawy wdrażającej DORA również przewiduje dodanie art. 76a do uKSC, który jednakże reguluje odmienną materię, niż art. 76a, w brzmieniu proponowanym projektem nowelizacji uKSC, zwracamy uwagę by w art. 1 pkt 79 ppkt 1) projektu nowelizacji uKSC, uwzględnione zostały stosowne zmiany w numeracji przepisów.	Uwaga wyjaśniona Projekty zostaną skoordynowane w tym zakresie.
158.	KIGEIT	Art. 76a ust. 4	Art. 76a ust. 4 - bardzo krótki termin płatności, zakładając maksymalną karę jest niemożliwością zgromadzenie równowartości 10 mln euro bez konsekwencji dla ciągłości prowadzenia działalności gospodarczej, ponadto płatność powinna nastąpić na podstawie prawomocnej decyzji.	Uwaga wyjaśniona Równowartość 10 mln euro jest maksymalną wysokością kary jaką można wymierzyć podmiotowi kluczowemu. Nie oznacza to, że jest to jedyna, automatyczna kara jaka będzie wymierzana wszystkim podmiotom niezależnie od rodzaju naruszenia. Rozpiętość pułapu kar pozwala na proporcjonalny wymiar również w odniesieniu do rodzaju podmiotu. Projektowaną ustawą objęte są zarówno

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

				mikroprzedsiębiorstwa jak i duże przedsiębiorstwa osiągające wielomiliardowe przychody. Kary muszą być dostosowane do podmiotu wobec czego również ich termin zapłaty nie będzie dla podmiotu uciążliwy.
159.	PIKE i Mediakom	Art. 76a ust. 4	Art. 76a ust. 4 Przepis przewiduje bardzo krótki termin płatności. Zakładając maksymalną karę jest niemożliwością zgromadzenie równowartości 10 mln euro bez konsekwencji dla ciągłości prowadzenia działalności gospodarczej, ponadto płatność powinna nastąpić na podstawie prawomocnej decyzji. Art. 76a [...] 4. ~~Karę~~ pieniężną <u>uiszcza się w terminie 14 dni od dnia, w którym decyzja o jej wymierzeniu stała się ostateczna lub od dnia doręczenia decyzji z klauzulą natychmiastowej wykonalności, na odrębny rachunek bankowy wskazany w decyzji organu właściwego do spraw cyberbezpieczeństwa o wymierzeniu kary pieniężnej podlega egzekucji w trybie przepisów o postępowaniu egzekucyjnym w administracji w zakresie egzekucji obowiązków o charakterze pieniężnym</u>	Uwaga wyjaśniona Równowartość 10 mln euro jest maksymalną wysokością kary jaką można wymierzyć podmiotowi kluczowemu. Nie oznacza to, że jest to jedyna, automatyczna kara jaka będzie wymierzana wszystkim podmiotom niezależnie od rodzaju naruszenia. Rozpiętość pułapu kar pozwala na proporcjonalny wymiar również w odniesieniu do rodzaju podmiotu. Projektowaną ustawą objęte są zarówno mikroprzedsiębiorstwa jak i duże przedsiębiorstwa osiągające wielomiliardowe przychody. Kary muszą być dostosowane do podmiotu wobec czego również ich termin zapłaty nie będzie dla podmiotu uciążliwy.
160.	Polskie Stowarzyszenie Fotowoltaiki	Art. 76a	[Informacje na potrzeby wymiaru kary pieniężnej] Obowiązek: - dostarczenia danych niezbędnych do określenia podstawy wymiaru kary pieniężnej na żądanie właściwego organu; - zapłaty kary pieniężnej w terminie 14 dni od kiedy decyzja stała się ostateczna lub doręczenia decyzji z klauzulą natychmiastowej wykonalności. Ogólny wpływ regulacji: Brak istotnego wpływu regulacji. Wpływ na sektor energetyczny: jw. – brak specyficznego wpływu na sektor energetyczny	Uwaga wyjaśniona Treść uwagi stanowi podsumowanie przepisu.
161.	IAB Polska	Art. 76b	Okresowa kara pieniężna. [art. 1 ust. 79 projektu nowelizacji / art. 76b nowelizowanego UKSC] W art. 77b nowelizowanego UKSC wprowadzono możliwość nałożenia na podmiot kluczowy lub podmiot ważny okresowej (dziennej) kary pieniężnej w wysokości do 100 tys. zł. Zdaniem IAB Polska górna wysokość takiej kary została ustalona na nieproporcjonalnie wysokim poziomie i nie jest ona niezbędna do zapewnienia skuteczności egzekwowania przepisów projektu nowelizacji. Mając to na uwadze, IAB Polska postuluje obniżenie maksymalnej wysokości okresowej kary pieniężnej do kwoty 5 tys. zł.	Uwaga nieuwzględniona Przepis jest wdrożeniem dyrektywy NIS 2 w zakresie okresowych kar pieniężnych. Jeśli natomiast chodzi o wysokość dziennej kary należy wskazać, że pułap został określony szeroko z uwagi na liczny katalog podmiotów objętych zakresem

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

				dyrektywy. Są nim objęci zarówno mikroprzedsiębiorcy jak i duże przedsiębiorstwa osiągające tak wysokie przychody, że kara na poziomie 5 tys. zł, jak proponuje podmiot zgłaszający uwagę, byłaby rażąco nieproporcjonalna i nieskuteczna. Nie stanowiłaby dla takiego podmiotu żadnej dolegliwości, która zmusiłaby podmiot do pojęcia określonych działań mających wpływ na cyberbezpieczeństwo.
162.	Konfederacja Lewiatan	Art. 76b	Kolejną formą kary pieniężnej nieprzewidzianą wprost w dyrektywie NIS2 jest możliwość nakładania kar dziennych „w celu przymuszenia podmiotu kluczowego albo podmiotu ważnego do wykonania nałożonych na niego obowiązków”. Jak wskazaliśmy wyżej, w naszej ocenie wysokość zwiększana wielokrotnie wysokości maksymalnych kar pieniężnych stanowi pełne i wystarczające narzędzie odstraszające. Jednocześnie, maksymalny pułap możliwe kary dziennej tj. 100 tys. zł został określony na zbyt wysokim poziomie. W przypadku utrzymania tego przepisu na kolejnych etapach prac maksymalną karę dzienną należy obniżyć do poziomu wynoszącego maksymalnie 5 tys. zł.	Uwaga nieuwzględniona Przepis jest wdrożeniem dyrektywy NIS 2 w zakresie okresowych kar pieniężnych. Jeśli natomiast chodzi o wysokość dziennej kary należy wskazać, że pułap został określony szeroko z uwagi na liczny katalog podmiotów objętych zakresem dyrektywy. Są nim objęci zarówno mikroprzedsiębiorcy jak i duże przedsiębiorstwa osiągające tak wysokie przychody, że kara na poziomie 5 tys. zł, jak proponuje podmiot zgłaszający uwagę, byłaby rażąco nieproporcjonalna i nieskuteczna. Nie stanowiłaby dla takiego podmiotu żadnej dolegliwości, która zmusiłaby podmiot do pojęcia określonych działań mających wpływ na cyberbezpieczeństwo.
163.	Polska Izba Informatyki i Telekomunikacji	Art. 76b	Art. 76b ust. 1 – dzienna kara pieniężna Kolejną formą kary pieniężnej nieprzewidzianą wprost w dyrektywie NIS2 jest możliwość nakładania kar dziennych „w celu przymuszenia podmiotu kluczowego albo podmiotu ważnego do wykonania nałożonych na niego obowiązków”. Jak wskazaliśmy wyżej, w naszej ocenie zwiększana wielokrotnie wysokości maksymalnych kar pieniężnych stanowi pełne i wystarczające narzędzie odstraszające. Jednocześnie, maksymalny pułap możliwe kary dziennej tj. 100 tys. zł został określony na zbyt wysokim poziomie. W przypadku utrzymania tego przepisu na kolejnych etapach prac maksymalną karę dzienną należy obniżyć do poziomu wynoszącego maksymalnie 5 tys. zł. Ponadto nieakceptowalny jest przepis, który pozwala na nakładanie okresowych (dziennych) kar pieniężnych za każdy dzień niewykonania przez podmiot kluczowy albo ważny ostrzeżenia wydanego przez organ, a taką właśnie możliwość przewiduje projektowany art. 76b ust. 1 pkt 1) ustawy. Przepis ten daje możliwość nakładania okresowej kary pieniężnej za każdy dzień opóźnienia w wykonaniu czynności określonych w	Uwaga częściowo uwzględniona Okresowa kara pieniężna wynika bezpośrednio z NIS 2. Organy właściwe do spraw cyberbezpieczeństwa – zgodnie z dyrektywą – muszą być wyposażone w takie środki, które pozwolą skutecznie egzekwować przestrzeganie przepisów dyrektywy oraz prawa ją wdrażającego. Jednym z takich instrumentów jest właśnie okresowa kara pieniężna. Przepis zostanie zmodyfikowany o wykreślenie kary

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			ostrzeżeniu wydanym na podstawie art. 53 ust. 4. Nie może być kar pieniężnych (ani okresowych ani żadnych innych) za niezastosowanie się przez przedsiębiorcę do ostrzeżenia (o którym mowa w art. 53 ust. 4 ustawy – w brzmieniu nadawanym projektowaną ustawą), a więc niewiążącego dla przedsiębiorcy instrumentu prawnego. Nowo dodawany art. 53 ust. 4 ustawy przewiduje, że w przypadku uzasadnionego podejrzenia, że działania lub zaniechania podmiotu kluczowego mogą naruszać przepisy ustawy, organ właściwy do spraw cyberbezpieczeństwa kieruje do tego podmiotu pismo w formie elektronicznej z ostrzeżeniem, w którym wskazuje czynności, jakie należy podjąć w celu zapobiegnięcia lub zaprzestania naruszania przepisów ustawy. Zatem ostrzeżenie zostało pomyślane jako narzędzie nie władcze (instrument „miękki”), dające podmiotowi kluczowemu albo ważnemu możliwość polubownego załatwienia sprawy bez wdawania się w postępowanie i spór z organem, z drugiej strony nie wymagające od organu wydającego ostrzeżenie wykazania i udowodnienia, że doszło do naruszenia (wystarczy uzasadnione podejrzenie po stronie organu), niewymagające również wydania decyzji administracyjnej (przepis mówi o pisemnym wystąpieniu). Ostrzeżenie nie jest narzędziem władczym, podmiot kluczowy i ważny nie ma prawnego obowiązku zastosowania się do ostrzeżenia, i z tych powodów projektowane przepisy wydają się nie przewidywać możliwości zaskarżenia ostrzeżenia przez podmiot kluczowy lub ważny. A skoro tak to nie może być mowy o nakładaniu na podmiot kluczowy albo ważny jakichkolwiek kar za niezastosowanie się do ostrzeżenia, skoro nie ma obowiązku zastosowania się do ostrzeżenia. Jeśli podmiot kluczowy albo ważny nie zastosuje się do ostrzeżenia, a organ ma uzasadnione podejrzenie, że doszło do naruszenia ustawy, to może skorzystać z instrumentu władczego jakim są „nakazy”, o których mowa w art. 53 ust. 5 i następne ustawy (w brzmieniu nadawanym projektowaną ustawą). Biorąc powyższe pod uwagę uważamy za konieczne usunięcie z projektowanego art. 76b ust. 1 punktu i fragmentu, który daje możliwość nakładania dziennych kar pieniężnych za niezastosowanie się do ostrzeżenia	okresowej za niewykonanie czynności, o których mowa w ostrzeżeniu.
164.	PIKE i Mediakom	Art. 76b	Art. 76b PIKE ma świadomość, że dyrektywa NIS2 dopuszcza możliwość nałożenia okresowej kary pieniężnej, jednakże jest to jedynie możliwość, a nie obowiązek spoczywający na państwie członkowskim. W świetle rewolucji, jaką będzie z pewnością stanowić projekt ustawy wdrażającej dyrektywę NIS2, w tym w zakresie szerokiego i oryginalnego katalogu środków wymuszających określone zachowanie podmiotów kluczowych i podmiotów ważnych, PIKE apeluje o rezygnację z instytucji okresowej kary pieniężnej. Wykreślenie art. 76b	Uwaga nieuwzględniona Okresowa kara pieniężna wynika bezpośrednio z NIS 2. Organy właściwe do spraw cyberbezpieczeństwa – zgodnie z dyrektywą – muszą być wyposażone w takie środki, które pozwolą skutecznie egzekwować przestrzeganie przepisów dyrektywy oraz prawa ją wdrażającego. Jednym z takich instrumentów jest właśnie okresowa kara pieniężna.
165.	Polskie Stowarzyszenie Fotowoltaiki	Art. 76b	Art. 76b [Okresowe kary pieniężne] Organ właściwy może nałożyć okresową w wysokości od 500 zł do 100 000 złotych za każdy dzień opóźnienia w celu przymuszenia PK albo PW do wykonania nałożonych na niego obowiązków: - określonych w ostrzeżeniu wydanym na podstawie art. 53 ust. 4 KSC wg Projektu; - w wykonaniu decyzji wydanych na podstawie art. 53 ust. 5 pkt. 2-7 KSC wg Projektu	Uwaga częściowo uwzględniona Okresowa kara pieniężna zostanie wykreślona w stosunku do ostrzeżenia. W zakresie określenia maksymalnej kary łącznej wskazać należy, że byłoby to nieefektywne z uwagi na wielość i

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			Ogólny wpływ regulacji: PK i PW, wobec których została wydana decyzja określająca powinno zachowanie lub ostrzeżenie zobowiązane są do jego wdrożenia pod rygorem zapłaty okresowej kary pieniężnej. W zależności od złożoności organizacyjnej PK i PW, zachowanie zgodności z ostrzeżeniem lub decyzją może wymagać dłuższego okresu. W rezultacie, w razie istotnego opóźnienia, kara okresowa może wielokrotnie przewyższać wymiar kary za stwierdzone naruszenie. Projekt nie zawiera również wskazania maksymalnej łącznej kwoty naliczonej kary okresowej. Wpływ na sektor energetyczny: jw. – brak specyficznego wpływu na sektor energetyczny [Nadregulacja względem Dyrektywy NIS2] Zgodnie z art. 34 ust. 6 Dyrektywy NIS2 okresowe kary pieniężne mogą być nakładane w celu przymuszenia podmiotu kluczowego lub ważnego do zaprzestania naruszenia niniejszej dyrektywy zgodnie z wcześniejszą decyzją właściwego organu. Tymczasem możliwość nałożenia kary pieniężnej o której mowa w przepisie ma mieć zastosowanie do ostrzeżeń wydawanych na podstawie art. 53 ust. 4 KSC wg Projektu, które nie spełniają formy decyzji administracyjnej. Postanowienia Projektu wykraczają zatem istotnie poza zakres przedmiotowy Dyrektywy NIS2 Rekomendacja: - Zawężenie przypadków, w których możliwe jest nałożenie okresowej kary pieniężnej; - Określenie maksymalnej łącznej kwoty kary okresowe	zróżnicowanie podmiotów krajowego systemu cyberbezpieczeństwa. Objęte nim mogą być zarówno mikroprzedsiębiorstwa jak i duże przedsiębiorstwa osiągające wielomilionowe przychody, dla których określona na maksymalnym łącznym wymiarze kara mogłaby być nadal zbyt niska aby spełniała swoją funkcję.
166.	Polskie Stowarzyszenie Fotowoltaiki	Art. 76d	Art. 76d [Nakładanie kar pieniężnych z wykorzystaniem pism generowanych automatycznie] Projekt przewiduje, że kara pieniężna w razie - niewdrożenia systemu zarządzania bezpieczeństwem informacji w systemie informacyjnym wykorzystywanym do świadczenia usługi lub gdy system ten nie zapewnia funkcjonalności, o których mowa w art. 8 ust. 1; może być nakładana zgodnie z art. 14 par. 1b Ustawy kodeks postępowania administracyjnego, tj. z wykorzystaniem pism generowanych automatycznie i opatrzonych kwalifikowaną pieczęcią elektroniczną organu administracji publicznej. Ogólny wpływ regulacji: Przewidziany sposób wydawania decyzji administracyjnych w przedmiocie nałożenia kar pieniężnych budzi istotne wątpliwości. Tylko jedna podstawa nakładania kar pieniężnych objęta jest przedmiotową regulacją, przy czym obejmuje on najszerszy obszar obowiązków PK lub PW. Brak uzasadnienia takiego rozróżniania w Projekcie lub jego uzasadnieniu. Zastosowanie przewidzianego trybu załatwiania spraw dla wydawania decyzji w przedmiocie nałożenia kary pieniężnej może skutkować ryzykiem nakładania kar pieniężnych z pominięciem dyrektyw wymiaru kary pieniężnej, w tym stosowania zasad proporcjonalności i adekwatności oraz z pominięciem okoliczności wymagających rzetelnej oceny indywidualnych w sprawie okoliczności. Wpływ na sektor energetyczny: jw. – brak specyficznego wpływu na sektor energetyczny [Nadregulacja względem Dyrektywy NIS2] Sposób załatwiania spraw określony w art. 76d KSC wg Projektu nie znajduje uzasadnienia w wymogach określonych w Dyrektywie NIS2. Rekomendacja Wycofanie proponowanego przepisu art. 76d z Projektu.	Uwaga nieuwzględniona Przepis nie zostanie wykreślony, natomiast uzupełnione zostanie uzasadnienie w zakresie art. 76d.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

167.	PTI	Art. 2	W zmienianej ustawie z dnia 21 marca 1991 o obszarach morskich Rzeczypospolitej Polskiej i administracji morskiej w ustępie 2a, stosownie do zmian proponowanych w Art.1 omawianej ustawy (pkt. 3 przedkładanych uwag) proponuje się usunięcie słowa „wspólnego”.	Uwaga nieuwzględniona
168.	PTI	Art. 3	W Art.3 omawianej ustawy zmieniającej ustawę z dnia 29 sierpnia 1997 r. – Ordynacja podatkowa w dodanym art. 299i w końcu akapitu należy uzupełnić enumeratywnie wymieniane w nawiasie pozycje (aktualny zapis – Dz. U. z 2023 r. poz. 913,1703 i ...).	Uwaga uwzględniona
169.	Cybermadein poland	Art. 3	W Art.3 omawianej ustawy zmieniającej ustawę z dnia 29 sierpnia 1997 r. – Ordynacja podatkowa w dodanym art. 299 i w końcu akapitu należy uzupełnić enumeratywnie wymieniane w nawiasie pozycje (aktualny zapis – Dz. U. z 2023 r. poz. 913,1703 i ...).	Uwaga uwzględniona
170.	Konfederacja Lewiatan	Art. 3	Przekazywanie danych operacji finansowych przez Szefa Krajowej Administracji Skarbowej organom właściwym do spraw cyberbezpieczeństwa oraz CRIST NASK Jednostka redakcyjna: art. 299i ustawy Ordynacja podatkowa Jednostka redakcyjna NIS2: art. 3 ust. 4 Uwaga: Zgodnie z projektowanym art. 299i ustawy – Ordynacja podatkowa, Szef Krajowej Administracji Skarbowej udostępnia organom właściwym do spraw cyberbezpieczeństwa oraz Zespołowi Reagowania na Incydenty Bezpieczeństwa Komputerowego (CRIST) działającemu na poziomie krajowym, prowadzonemu przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy, dane nieodpłatnie, w drodze teletransmisji, bez konieczności składania każdorazowo pisemnych wniosków o udostępnienie. Dane te obejmują roczne zatrudnienie, roczny obrót netto ze sprzedaży towarów, wyrobów i usług oraz <u>operacji finansowych</u>, w zakresie niezbędnym do dokonania przez te podmioty weryfikacji wielkości przedsiębiorstwa zgodnie z art. 5 ust. 1 i ust. 2 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Chociaż dane dotyczące rocznego obrotu netto ze sprzedaży towarów, wyrobów i usług mogą być uzasadnione, warto zaznaczyć, że nie są one tożsame z pojęciem przychodu. Zupełnie niezrozumiałe jest, dlaczego miałyby być przekazywane dane z operacji finansowych, które są objęte tajemnicą skarbową, na rzecz organów do spraw cyberbezpieczeństwa. Taki zakres przekazywania danych jest nadmiarowy i nieproporcjonalny. Narusza on podstawowe zasady prawa, w tym zasadę praworządności (por. art. 7 Konstytucji RP). Z art. 51 ust. 5 Konstytucji RP wynika, że zasady i tryb gromadzenia oraz udostępniania informacji o jednostce określa ustawa. Oznacza to, że organy władzy publicznej nie mogą dowolnie dysponować informacjami o jednostce, lecz wyłącznie na zasadach i w trybie ściśle określonym w ustawie. Trybunał Konstytucyjny wielokrotnie podkreślał, że w ustawie powinny być uregulowane takie zagadnienia, jak zobowiązanie do ujawnienia informacji o swojej osobie, określenie podmiotów zobowiązanych, okoliczności powstania obowiązku ujawnienia informacji oraz zakres tych informacji, a także zasady ich przechowywania, poprawiania, udostępniania i usuwania (wyrok z dnia 6 czerwca 2018 r., sygn. akt K 53/16, OTK-A z 2018 r., poz. 38; wyrok Trybunału Konstytucyjnego z dnia 19 lutego 2002 r., sygn. akt U 3/01, OTK z 2002 r., Nr 1/A, poz. 3). Wreszcie ustawa musi określać tryb gromadzenia i udostępniania informacji, a więc procedurę postępowania podmiotu, który tymi informacjami dysponuje	Uwaga wyjaśniona Dane te są potrzebne celem ustalenia wielkości podmiotu.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			(wyroki Trybunału Konstytucyjnego z dnia 19 lutego 2002 r., sygn. akt U 3/01; z dnia 16 lipca 2015 r., sygn. akt K 2/13; z dnia 6 czerwca 2018 r., sygn. akt K 53/16). Materia ustawowa powinna obejmować zasady gromadzenia i udostępniania informacji, w tym ich przetwarzanie. Ustawa musi także określać tryb gromadzenia i udostępniania informacji, a więc procedurę postępowania podmiotu, który tymi informacjami dysponuje. Warto również zauważyć, że w art. 43 ust. 2 projektu KSC proponuje się wprowadzenie kompetencji dla organów właściwych do spraw cyberbezpieczeństwa w zakresie przekazywania informacji z rejestrów publicznych, z zachowaniem przepisów o tajemnicach prawnie chronionych. Oznacza to, że dostęp do informacji został już zapewniony, co budzi głębokie wątpliwości co do potrzeby przyznawania dodatkowych uprawnień dotyczących danych podatkowych.	
171.	Konfederacja Lewiatan	Art. 3	Brak definicji rocznej liczby pracowników lub rocznej liczby ubezpieczonych w ustawie o systemie ubezpieczeń społecznych i w ustawie Ordynacja podatkowa Jednostka redakcyjna: art. 50 ust. 28 ustawy o systemie ubezpieczeń społecznych; art. 299i § 2 ustawy – Ordynacja podatkowa Jednostka redakcyjna NIS2: nie dotyczy Uwaga: W art. 50 ustawy o systemie ubezpieczeń społecznych proponuje się dodanie przepisu, zgodnie z którym Zakład Ubezpieczeń Społecznych miałby udostępniać organom właściwym do spraw cyberbezpieczeństwa i Zespołowi Reagowania na Incydenty Bezpieczeństwa Komputerowego działającemu na poziomie krajowym, prowadzonemu przez Naukową i Akademicką Sieć Komputerową - Państwowy Instytut Badawczy, drogą elektroniczną, dane zgromadzone na koncie płatnika składek, o których mowa w art. 45 tej ustawy. Dane te obejmowałyby roczną liczbę pracowników lub roczną liczbę ubezpieczonych, w zakresie niezbędnym do realizacji ich ustawowych zadań. Podobny przepis został zaproponowany w ustawie – Ordynacja podatkowa (art. 299i). Niemniej ani ustawa o systemie ubezpieczeń społecznych, ani ustawa – Ordynacja podatkowa nie posługują się pojęciem rocznej liczby pracowników czy ubezpieczonych. Brak definicji tych pojęć rodzi praktyczne i wymierne konsekwencje, ponieważ nie jest jasne, jak należy liczyć taką roczną liczbę pracowników – czy ma to być liczba na koniec roku (31 grudnia), średnioroczna, czy wystarczy przekroczenie 250 pracowników przez jeden dzień w roku. Kwestie te mają istotne znaczenie prawne z uwagi na konsekwencje dla podmiotu co do kwalifikacji jako podmiot ważny lub kluczowy. Bez precyzyjnej definicji, podmioty mogą mieć trudności w interpretacji przepisów i spełnieniu wymogów ustawy, co może prowadzić do niepewności i niezgodności z prawem.	Uwaga wyjaśniona Przepis zostanie doprecyzowany o wskazanie rocznej liczby ubezpieczonych.
172.	Konfederacja Lewiatan	Art. 8	Brak wystarczającego uzasadnienia dla wykluczenia w zamówieniach publicznych dla produktów, usług lub procesów ICT po wystosowaniu (niewiążących) rekomendacji Jednostka redakcyjna: art. 226 ust. 1 ustawy – Prawo zamówień publicznych Jednostka redakcyjna NIS2: nie dotyczy Uwaga: Projektodawca zakłada, że oferty składane w zamówieniach publicznych obejmujące produkty ICT, usługi ICT lub procesy ICT wskazane w rekomendacjach, o których mowa w art. 33 ust. 4 ustawy o	Uwaga wyjaśniona Dyrektywa NIS 2 nakazuje zapewnić szczególną ochronę łańcuchom dostaw. Ponadto wiele z głośnych cyberataków z ostatnich lat w tym np. sprawa Solarwinds wynikały z ataku na dostawców usług dla podmiotów rządowych, w związku z tym

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			krajowym systemie cyberbezpieczeństwa lub w decyzji w sprawie uznania dostawcy za dostawcę wysokiego ryzyka, będą odrzucane. Należy jednak odwołać się do art. 13 lit. a) Dyrektywy 2009/81/WE, który przewiduje wyłączenia związane z zamówieniami, w przypadku których stosowanie przepisów tej dyrektywy zobowiązywałoby państwo członkowskie do dostarczenia informacji, których ujawnienie uznaje ono za sprzeczne z jego podstawowymi interesami bezpieczeństwa. Należy rozważyć, czy rzeczywiście wyłączenie stosowania prawa zamówień publicznych jest adekwatne i ściśle związane z podstawowymi interesami bezpieczeństwa, w sytuacji gdy niemal każdy urząd i podmioty im podległe lub nadzorowane będą objęte wyłączeniem. Wynika to z bardzo szerokiego katalogu zadań obejmujących m.in. ochronę zdrowia, bezpieczeństwo ekonomiczne, dostawy energii, sprawiedliwość, ochronę środowiska, weterynaryjną ochronę zdrowia publicznego, nadzór sanitarny oraz zadania z zakresu ochrony ludności i obrony cywilnej, zarządzania kryzysowego, w tym zapewnienie ciągłości funkcjonowania i odtwarzania infrastruktury krytycznej Państwa. Proponowane przepisy wydają się nadmiernie szerokie, co budzi wątpliwości co do ich proporcjonalności i adekwatności do każdego zamówienia publicznego udzielanego na podstawie przepisów ustawy o zamówieniach publicznych. Taki szeroki zakres wyłączeń może prowadzić do destabilizacji systemu udzielania zamówień publicznych, ponieważ może dochodzić do sytuacji, w których konieczne będzie odrzucenie danej oferty ze względu na poboczne wykorzystywanie produktów, usług lub procesów ICT objętych rekomendacją lub decyzją o uznaniu dostawcy za dostawcę wysokiego ryzyka⁹⁾. Co więcej do wyłączeń z zamówień publicznych dojdzie w wyniku wydania rekomendacji, nie posiadających rangi źródła prawa.	konieczne jest zapewnienie narzędzi, które umożliwią podmiotom publicznym odrzucenie potencjalnie niebezpiecznych ofert.
173.	Konfederacja Lewiatan	Art. 9	Brak zwrotu niewydatkowanych lub nieprawidłowo wydatkowanych środków z Funduszu Cyberbezpieczeństwa do budżetu państwa Jednostka redakcyjna: art. 2 ust. 4 ustawy o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa Jednostka redakcyjna NIS2: nie dotyczy Uwaga: Projektodawca proponuje wprowadzenie przepisu, zgodnie z którym jakiekolwiek dotacje z budżetu państwa udzielane Funduszowi Cyberbezpieczeństwa nie podlegają zwrotowi. Przepis ten oznacza wyłom od naczelnej zasady finansów publicznych, tj. obowiązku zwrotu dotacji w przypadku ich niezgodnego z przeznaczeniem wykorzystania, pobrania nienależnie lub w nadmiernej wysokości, zgodnie z ustawą z dnia 27 sierpnia 2009 r. o finansach publicznych. Proponowana konstrukcja powoduje, że dotacje z budżetu państwa nie będą podlegać zwrotowi, nawet w przypadku niewykorzystania środków lub ich nieprawidłowego wydatkowania, co może prowadzić do szkód dla finansów publicznych. Taki przepis jest sprzeczny z zasadą odpowiedzialności za publiczne środki finansowe i może skutkować brakiem odpowiedniego nadzoru nad wydatkowaniem środków z Funduszu Cyberbezpieczeństwa. Przykładem bardziej zasadnego podejścia jest art. 43 § 15 kodeksu karnego wykonawczego, który tworzy Fundusz	Uwaga wyjaśniona Zapewnienia cyberbezpieczeństwa jest jednym z kluczowych zadań jakie spoczywają obecnie na administracji publicznej. Jest to obszar wymagający dużych nakładów zarówno w zakresie zakupu sprzętu i oprogramowania jak również jeśli chodzi o kwestię opłacenia odpowiednich specjalistów. Pensje dla osób zaczynających karierę w tej branży zaczynają się od 9000 – 10000 zł, a specjaliści mogą liczyć na kilkunastotysięczne zarobki. Celem Funduszu Cyberbezpieczeństwa jest wsparcie działań zmierzających do zapewniania bezpieczeństwa systemów

⁹⁾ W tym zakresie swoje wątpliwości podnosił także Minister ds. Unii Europejskiej do poprzedniej wersji tego projektu. Warto także w tym kontekście przywołać opinie: opinia nr DPUE.920.1030.2021.AR(43).

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			Pomocy Pokrzywdzonym oraz Pomocy Postpenitencjarnej, gdzie przewidziane są mechanizmy kontroli i zwrotu niewykorzystanych lub niewłaściwie wykorzystanych środków. Wprowadzenie podobnych zasad dla Funduszu Cyberbezpieczeństwa byłoby zgodne z zasadami finansów publicznych i zapewniłoby lepszą ochronę środków publicznych.¹⁰⁾	teleinformatycznych przed cyberzagrożeniami poprzez finansowanie świadczenia teleinformatycznego, tj. dodatku do wynagrodzenia za pracę, a w przypadku funkcjonariuszy i żołnierzy zawodowych świadczenia pieniężnego. Świadczenie teleinformatyczne jest przyznawane osobom realizującym zadania z zakresu cyberbezpieczeństwa w kluczowych, ze względu na bezpieczeństwo państwa, instytucjach. Należy wskazać, że brak możliwości płynnego zarządzania Funduszem może doprowadzić do odpływu specjalistów z ww. instytucji, a co za tym idzie – do utraty kadry odpowiadającej za utrzymywanie niezbędnego poziomu bezpieczeństwa. W dobie stale wzrastającej liczby incydentów oraz trwającej wojny hybrydowej, utrzymanie odpowiedniego poziomu wynagrodzeń jest istotnym instrumentem w zakresie ochrony struktur państwa przed próbami destabilizacji funkcjonowania Rzeczypospolitej Polskiej. W związku z tym konieczne jest zapewnienie dodatkowych źródeł finansowania dla Funduszu Cyberbezpieczeństwa.
174.	Konfederacja Lewiatan	Art. 7	Jednostka redakcyjna: art. 61 pkt 3 ustawy – Prawo przedsiębiorców Jednostka redakcyjna NIS2: nie dotyczy Uwaga: Artykuł 61 pkt 3 ustawy – Prawo przedsiębiorców określa wyłączenia stosowania przepisów Prawa przedsiębiorców, które dotyczą zakazu równoczesnych kontroli oraz ograniczonego czasu trwania kontroli. Projektodawca proponuje wyłączenie kolejnej kategorii kontroli dotyczących przedsiębiorców, tj. kontroli obowiązków związanych z cyberbezpieczeństwem. Taki wymóg nie wynika z treści NIS2 i wygląda na to, że zamiast dążyć do ograniczania obciążeń i równoczesnych kontroli, projektodawca nakłada kolejne ograniczenia na przedsiębiorców bez należytego uzasadnienia. Gdyby	Uwaga nieuwzględniona Należy podnieść, że projekt nowelizacji nie ma na celu wyłącznie wdrożenia dyrektywy NIS 2, a stanowi efekt dokonanej analizy funkcjonowania obecnie obowiązujących przepisów. Nieprawdziwe jest przy tym stwierdzenie, że kontrole

¹⁰⁾ Zgodnie z tym przepisem: „w przypadku wykorzystania dotacji niezgodnie z przeznaczeniem lub pobranych nienależnie lub w nadmiernej wysokości stosuje się odpowiednio przepisy ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych dotyczące dotacji udzielonych z budżetu państwa.”.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			brzmienie przepisu było ograniczone do nagłych przypadków lub zarządzania incydentami, miałyby to bardziej logiczne uzasadnienie. Natomiast projektodawca świadomie szeroko definiuje podmiotowe wyłączenie, co w praktyce iluzoryczną czyni ochronę praw przedsiębiorców. Dodatkowo, kontrole mogą być prowadzone w sposób nieograniczony w czasie, co – jak pokazuje praktyka – zachęca do przedłużania czynności kontrolnych. Takie podejście jest sprzeczne z duchem Konstytucji dla Biznesu, która ma na celu ochronę przedsiębiorców przed nadmiernym obciążeniem administracyjnym i zapewnienie im stabilnych warunków do prowadzenia działalności gospodarczej.	będą nieograniczone w czasie – przewidziano bowiem maksymalny czas kontroli tj. 48 dni. Przepis ten zostanie jeszcze doprecyzowany z uwzględnieniem uwag zgłoszonych w toku konsultacji. Równoczesne kontrole również są istotne z punktu widzenia NIS 2 - podmiot może bowiem podlegać pod nadzór różnych organów ponieważ zalicza się do kilku sektorów. Może zdarzyć się sytuacja, że naruszy przepisy ustawy w kilku sektorach. W tej sytuacji zakaz prowadzenia równoległej kontroli powodowałby szkodę zarówno dla podmiotu jak i dla krajowego systemu cyberbezpieczeństwa.
175.	Konfederacja Lewiatan	Art. 14	Art. 14 ustawy nowelizującej – termin realizacji obowiązków i wpis do rejestru Wyjaśnienia wymaga relacja projektowanego art. 14 ust. 1 ustawy nowelizującej, który wskazuje termin półroczny na realizację wszystkich obowiązków z rozdziału 3 wobec projektowanego art. 16 ustawy uksc, który również wskazuje termin 6 miesięczny od dnia spełnienia przesłanek uznania za podmiot kluczowy lub ważny, ale od wejścia w życie ustawy. W szczególności, w przypadku art. 14 mowa o wszystkich wymaganiach, w tym audycie, który wg art. 16 ma być wykonany w ciągu 12 miesięcy po raz pierwszy. Podobnie niejasna jest relacja art. 14 ust. 2 dot. „zarejestrowania się” w wykazie zgodnie z „komunikatem o harmonogramie” wobec art. 7 ust. 3, który termin na „złożenie wniosku o wpis” w wykazie składa się w terminie 2 miesięcy od dnia spełnienia wymogów. Kwestie te wymagają ponownej weryfikacji i szczegółowego opisanie w uzasadnieniu projektu.	Uwaga uwzględniona Przepisy w tym zakresie zostaną ujednolicone tak aby nie było wątpliwości co do momentu od kiedy będzie termin na dostosowanie do nowych przepisów. Art. 14 ustawy nowelizującej dotyczy podmiotów, które w dniu wejścia w życie ustawy spełniają kryteria uznania za podmiot kluczowy/podmiot ważny. Zaś art. 16 ustawy ksc w brzmieniu znnowelizowanym dotyczy podmiotów, które w przyszłości staną się podmiotami kluczowymi lub podmiotami ważnymi.
176.	Polska Izba Informatyki i Telekomunikacji	Art. 14	Art. 14 ustawy nowelizującej – termin realizacji obowiązków i wpis do rejestru Wyjaśnienia wymaga relacja projektowanego art. 14 ust. 1 ustawy nowelizującej, który wskazuje termin półroczny na realizację wszystkich obowiązków z rozdziału 3 wobec projektowanego art. 16 ustawy uksc, który również wskazuje termin 6 miesięczny od dnia spełnienia przesłanek uznania za podmiot kluczowy lub ważny, ale od wejścia w życie ustawy. W szczególności, w przypadku art. 14 mowa o wszystkich wymaganiach, w tym audycie, który wg art. 16 ma być wykonany w ciągu 12 miesięcy po raz pierwszy. Podobnie niejasna jest relacja art. 14 ust. 2 dot. „zarejestrowania się” w wykazie zgodnie z „komunikatem o harmonogramie” wobec art. 7 ust. 3, który termin na „złożenie wniosku o wpis” w wykazie składa się w terminie 2 miesięcy od dnia spełnienia wymogów. Kwestie te wymagają ponownej weryfikacji i szczegółowego opisanie w uzasadnieniu projektu.	Uwaga uwzględniona Terminy zawarte w projekcie ustawy zostaną ponownie przeanalizowane i zweryfikowane.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

177.	TVN S.A.	Uwaga ogólna	Termin wejścia w życie nowelizowanej ustawy – doprecyzowanie terminu wejścia w życie ustawy Mając na uwadze powyższe wątpliwości związane z kręgiem podmiotów zobowiązanych do stosowania przepisów nowelizowanej ustawy KSC, które wynikają zarówno z definicji proponowanych w treści nowelizowanej ustawy jak i z definicji przedsiębiorcy telekomunikacyjnego, znajdujących się procedowanej równolegle projekcie ustawy PKE, niezbędnym wydaje się prawidłowe określenie procesu legislacyjnego dla obu procesowanych aktualnie ustaw. Z uwagi na odwołania w treści nowelizowanej UKSC do definicji zawartych w procesowanym PKE niezbędne wydaje się w pierwszej kolejności uchwalenie nowego PKE a dopiero w konsekwencji przepisów UKSC, które w swojej treści odwołują się do definicji zawartych w PKE. Mając na uwadze powyższe niezbędne wydaje się, w toku prac nad nowelizacją UKSC, odpowiednie określenie kręgu podmiotów objętych obowiązkami wynikającymi z dyrektywy NIS2, aby rozwiązać wszelkie wątpliwości i zapewnić pełną zgodność z dyrektywą, co można osiągnąć odpowiednio doprecyzowując zaproponowane w UKSC definicji Podmiotu Kluczowego.	Uwaga wyjaśniona W związku z uchwaleniem ustawy PKE projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw zostanie dostosowany do jej przepisów dla zapewnienia spójności przepisów obydwu ustaw.
178.	KIKE	Art. 29	Na zakończenie Izba pragnie wskazać na nierealność zakładanego vacatio legis jednego miesiąca. Projekt wprowadza bardzo skomplikowane obowiązki, określone w sposób ogólny co wymaga dziesiątek spotkań roboczych pomiędzy CSIRT a podmiotami kluczowymi i podmiotami ważnymi w celu uzgodnienia szczegółów organizacyjnych i technicznych wdrożenia uKSC. Tego nie da się zrobić w terminie jednego miesiąca. Doświadczenia izby we wdrażaniu mechanizmów zwalczających nadużycia w komunikacji elektronicznej wskazują, że potrzebny jest okres przynajmniej 6 miesięcy na wzajemne uzgodnienia pomiędzy instytucjami publicznymi wdrażającymi a sektorem prywatnym. Z tego względu Izba postuluje wydłużenie vacatio legis do 6 miesięcy.	Uwaga wyjaśniona Należy zauważyć, że termin 1 miesiąca dotyczy ogólnie całej ustawy, a poszczególne przepisy przewidują dla określonych obowiązków okresy dostosowawcze. Na przykład na wprowadzenie SZBI podmioty obowiązane będą miały 6-miesięcy. Dlatego nie ma potrzeby zmiany ogólnego terminu wejścia w życie ustawy.
179.	Konfederacja Lewiatan	Art. 29	Termin wejścia w życie nowelizowanej ustawy – doprecyzowanie terminu wejścia w życie ustawy Mając na uwadze wątpliwości związane z kręgiem podmiotów zobowiązanych do stosowania przepisów nowelizowanej ustawy KSC, które wynikają zarówno z definicji proponowanych w treści nowelizowanej ustawy jak i z definicji przedsiębiorcy telekomunikacyjnego, znajdujących się procedowanej równolegle projekcie ustawy PKE, niezbędnym wydaje się prawidłowe określenie procesu legislacyjnego dla obu procesowanych aktualnie ustaw. Z uwagi na odwołania w treści nowelizowanej ustawy KSC do definicji zawartych w procesowanym PKE niezbędne wydaje się w pierwszej kolejności uchwalenie nowego PKE a dopiero w konsekwencji przepisów KSC, które w swojej treści odwołują się do definicji zawartych w PKE.	Uwaga wyjaśniona Kwestie te będą uwzględnione na dalszych etapach prac legislacyjnych, biorąc pod uwagę postępy w pracach nad poszczególnymi projektami tak aby zapewnić spójność rozwiązań.
180.	ISACA	Załącznik nr 1	Sektor: Bankowość i infrastruktura rynków finansowych wykreślenie podmiotów regulowanych przez DORA lub zharmonizowanie ustaw implementujących DORA i NIS2 na poziomie krajowym duplikowanie się wymagań DORA i NIS2.	Uwaga wyjaśniona Przepis wskazuje, że w zakresie w jakim stosowana jest DORA, to w takim zakresie nie stosuje się wymogów ustawy ksc.
181.	ISSA Polska	Załącznik nr 1	Nieuzasadnione zakwalifikowanie uczelni wyższych, instytucji kultury oraz zakładów opieki zdrowotnej jako podmiotów kluczowych Projekt nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa nieprawidłowo klasyfikuje wszystkie uczelnie wyższe, państwowe i samorządowe instytucje kultury (np. muzea, teatry) oraz sektor zdrowia (w tym hospicja, zakłady rehabilitacyjne, zakłady	Uwaga wyjaśniona Uczelnie wyższe od 2012 r. są obowiązane mieć wdrożony system zarządzania bezpieczeństwem informacji. Jest to

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			pielęgnacyjno-opiekuńcze) jako podmioty kluczowe. Taka regulacja jest całkowicie nieproporcjonalna i nieadekwatna do rzeczywistych potrzeb oraz specyfiki działalności tych jednostek. Oznacza to, że jednostki, których główna działalność w żaden sposób nie wpływa na bezpieczeństwo krytycznej infrastruktury państwa, będą zobowiązane do spełnienia wymogów, które są zbędne, kosztowne i nie przyczyniają się do podniesienia poziomu cyberbezpieczeństwa kraju. Proponujemy ograniczenie zakresu podmiotowego nowelizacji do podmiotów rzeczywiście kluczowych i ważnych dla bezpieczeństwa cyberprzestrzeni RP.	istotne, przetwarzają one dane studentów oraz informacje o ocenach, przedmiotach itd. A historie dotyczące niedostępności systemów obsługi studiów, zwłaszcza w trakcie rejestracji na egzaminy, są słynne wśród obecnych studentów i absolwentów uczelni wyższych. Odnosnie SPZOZ to będą podlegały obowiązkowi jako średnie przedsiębiorstwa w sektorze ochrony zdrowia. Państwowe i samorządowe instytucje kultury prowadzą strony internetowe, czasem także inne zasoby, biblioteki cyfrowe itd. Istotne jest zapewnienie dostępności tych zadań publicznych dla obywateli. Dlatego warto żeby te podmioty były w KSC i mogły w razie potrzeby uzyskać pomoc CSIRT.
182.	Konfederacja Lewiatan	Załącznik nr 1	Nieuzasadnione zakwalifikowanie uczelni wyższych, instytucji kultury oraz zakładów opieki zdrowotnej jako podmiotów kluczowych Jednostka redakcyjna: załącznik nr 1 Jednostka redakcyjna NIS2: nie dotyczy Uwaga: Projekt nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa nieprawidłowo klasyfikuje wszystkie uczelnie wyższe, państwowe i samorządowe instytucje kultury (np. muzea, teatry) oraz sektor zdrowia (w tym hospicja, zakłady rehabilitacyjne, zakłady pielęgnacyjno-opiekuńcze) jako podmioty kluczowe. Taka regulacja jest całkowicie nieproporcjonalna i nieadekwatna do rzeczywistych potrzeb oraz specyfiki działalności tych jednostek. Oznacza to, że jednostki, których główna działalność w żaden sposób nie wpływa na bezpieczeństwo krytycznej infrastruktury państwa, będą zobowiązane do spełnienia wymogów, które są zbędne, kosztowne i nie przyczyniają się do podniesienia poziomu cyberbezpieczeństwa kraju. Takie podejście może być przykładem nieefektywnego prawa, które zamiast zabezpieczać, generuje nadmierne obowiązki	Uwaga wyjaśniona Uczelnie wyższe od 2012 r. są obowiązane mieć wdrożony system zarządzania bezpieczeństwem informacji. Jest to istotne, przetwarzają one dane studentów oraz informacje o ocenach, przedmiotach itd. A historie dotyczące niedostępności systemów obsługi studiów, zwłaszcza w trakcie rejestracji na egzaminy, są słynne wśród obecnych studentów i absolwentów uczelni wyższych. Odnosnie SPZOZ to będą podlegały obowiązkowi jako średnie przedsiębiorstwa w sektorze ochrony zdrowia. Państwowe i samorządowe instytucje kultury prowadzą strony internetowe, czasem także inne zasoby, biblioteki cyfrowe itd. Istotne jest zapewnienie dostępności tych zadań publicznych dla obywateli. Dlatego warto żeby te podmioty były w KSC i mogły w razie potrzeby uzyskać pomoc CSIRT.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

183.	POLMED	Załącz. nr 1	Wątpliwości Izby POLMED koncentrują się wokół zaproponowanego kształtu załączników do ustawy. W opublikowanym Projekcie w wykazie podmiotów kluczowych znalazły się takie podmioty z branży wyrobów medycznych jak: • Podmioty produkujące wyroby medyczne uznane za mające krytyczne znaczenie podczas danego stanu zagrożenia zdrowia publicznego („wykaz wyrobów medycznych o krytycznym znaczeniu w przypadku stanu zagrożenia zdrowia publicznego”) w rozumieniu art. 22 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/123; • Podmioty produkujące wyroby medyczne w rozumieniu art. 2 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2017/745; • Podmioty produkujące wyroby medyczne do diagnostyki in vitro w rozumieniu art. 2 ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2017/746. Wskazana wyżej propozycja regulacji przekracza wymogi określone w przepisach dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii (dalej: „Dyrektywa NIS2”), na podstawie której wyłącznie pierwsza z ww. kategorii podmiotów została włączona do zbioru podmiotów kluczowych, natomiast pozostałe dwie kategorie podmiotów zostały wskazane jako podmioty ważne. W ocenie Izby POLMED przedstawiony Projekt przewiduje zdecydowanie zbyt daleko idące zmiany w stosunku do Dyrektywy NIS2. Autorzy Dyrektywy NIS2 w trakcie prac nad tym aktem dokonali podziału na sektory kluczowe i ważne, w zależności od tego, jak bardzo ich znaczenie jest zasadnicze dla ich sektorów lub świadczonych przez nie usług. Izba POLMED zwraca uwagę, że przyjęcie znacznie szerszego zakresu podmiotów kluczowych w Projekcie niż w Dyrektywie NIS2 może skutkować obniżeniem atrakcyjności prowadzenia działalności w Polsce względem pozostałych państw członkowskich Unii Europejskiej. Krajowi producenci, którzy zostaną objęci szerszym nadzorem w zakresie cyberbezpieczeństwa mogą z tego powodu znacznie ograniczyć rozwijanie w Polsce najnowocześniejszych cyfrowych wyrobów medycznych. Dodatkowo, producenci wyrobów medycznych oraz wyrobów medycznych do diagnostyki in vitro i tak objęci są stosownymi sektorowymi regulacjami, które nakładają na nich obowiązki w zakresie cyberbezpieczeństwa. Zarówno rozporządzenie UE 2017/745 w sprawie wyrobów medycznych i rozporządzenie UE 2017/746 w sprawie wyrobów medycznych do diagnostyki laboratoryjnej przewidują wysokie standardy dotyczące ryzyka w cyberprzestrzeni. Izba POLMED zwraca uwagę, że zostało to również zauważone na poziomie europejskim, gdzie Komisja Europejska zdecydowała się na wyłączenie wyrobów medycznych oraz wyrobów medycznych do diagnostyki in vitro z rozporządzenia UE w sprawie horyzontalnych wymogów cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi i zmieniające rozporządzenie (UE) 2019/1020.	Uwaga uwzględniona

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			Mając na uwadze powyższe, uprzejmie proszę o zwrócenie uwagi na opisywany powyżej problem oraz o zmianę klasyfikacji podmiotów produkujących wyroby medyczne oraz wyroby medyczne do diagnostyki in vitro jako podmiotów kluczowych na podmioty ważne, zgodnie z brzmieniem Dyrektywy NIS2.	
184.	PTI	Załącz. nr 1	Podmioty zajmujące się produkcją, przetwarzaniem i dystrybucją żywności zostały w projekcie ustawy sklasyfikowane jako podmioty kluczowe. Zważyć należy, że dyrektywa NIS 2 klasyfikuje te podmioty jako podmioty ważne. Podniesienie rangi tych podmiotów stanowi tzw. nadregulację i spowoduje zbędne obciążenie dla tych podmiotów i systemu nadzoru. Sugeruje się przeniesienie podmiotów tego sektora do ZAŁĄCZNIKA NR 2 PODMIOTY WAŻNE.	Uwaga uwzględniona
185.	PTI	Załącz. nr 1	Podmioty zajmujące się produkcją, wytwarzaniem i dystrybucją chemikaliów zostały w projekcie ustawy sklasyfikowane jako podmioty kluczowe. Zważyć należy, że dyrektywa NIS 2 klasyfikuje te podmioty jako podmioty ważne. Podniesienie rangi tych podmiotów stanowi tzw. nadregulację i spowoduje zbędne obciążenie dla tych podmiotów i systemu nadzoru. Sugeruje się przeniesienie podmiotów tego sektora do ZAŁĄCZNIKA NR 2 PODMIOTY WAŻNE.	Uwaga uwzględniona
186.	PTI	Załącz. nr 1	Podmioty zajmujące się produkcją (wyrobów medycznych i wyrobów medycznych do diagnostyki in vitro, komputerów, wyrobów elektronicznych i optycznych, urządzeń elektrycznych, maszyn i urządzeń, gdzie indziej niesklasyfikowana, pojazdów samochodowych, przyczep i naczip, pozostałego sprzętu transportowego) zostały w projekcie ustawy sklasyfikowane jako podmioty kluczowe. Zważyć należy, że dyrektywa NIS 2 klasyfikuje te podmioty jako podmioty ważne. Podniesienie rangi tych podmiotów stanowi tzw. nadregulację i spowoduje zbędne obciążenie dla tych podmiotów i systemu nadzoru. Sugeruje się przeniesienie podmiotów tego sektora do ZAŁĄCZNIKA NR 2 PODMIOTY WAŻNE.	Uwaga uwzględniona
187.	Stowarzyszenie Absolwentów Studiów Cyberbezpieczeństwa MBA	Załącz. nr 1	Rozszerzenie katalogu podmiotów ważnych o portale informacyjne Należy rozszerzyć istniejące definicje bądź wprowadzić nową kategorię podmiotów np. „dostawca internetowej platformy udostępniania informacji online” – przez którego rozumie się osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, która dostarcza użytkownikom usługę udostępniania treści w ramach tej platformy, jak i poza nią. Istotą zmiany byłoby uznanie za podmiot ważny – dostawcę usług cyfrowych również podmioty prowadzące portale informacyjne od pewnego progu istotności, określonego np. liczbą użytkowników unikalnych odwiedzających dany portal w miesiącu. Obecnie jest projektowane: Dostawca internetowej platformy handlowej, Dostawca wyszukiwarki internetowej, Dostawca platformy sieci usług społecznościowych. Jedną z metod walki w cyberprzestrzeni jest bowiem dezinformacja. Podmioty prowadzące duże portale informacyjne powinny być uznane za podmiot ważny nawet w sytuacji, gdy nie prowadzą wyszukiwarek internetowych ani internetowych platform handlowych.	Uwaga nieuwzględniona Projektodawca rozumie, że zwalczanie dezinformacji jest ważne, niemniej jednak wykracza to poza kwestie cyberbezpieczeństwa.
188.	Polskie Stowarzyszenie Fotowoltaiki	Załącz. nr 1	[Katalog PK] Projekt wprowadza załącznik nr 1 do KSC określający zakres podmiotów uznawanych za PK.	Uwaga częściowo uwzględniona Sektory produkcji; Produkcji, wytwarzania i dystrybucji chemikaliów; Produkcji,

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

		W odniesieniu do sektora energii, Projekt kwalifikuje poniższe podmioty jako PK: - w ramach podsektora Wydobywanie kopalin: • Podmioty prowadzące działalność gospodarczą w zakresie wydobywania gazu ziemnego na podstawie koncesji, o której mowa w art. 22 ust. 1 ustawy z dnia 9 czerwca 2011 r. – Prawo geologiczne i górnicze (Dz. U. z 2023 r. poz. 633, 1688 i 2029). • Podmioty prowadzące działalność gospodarczą w zakresie wydobywania ropy naftowej na podstawie koncesji, o której mowa w art. 22 ust. 1 ustawy z dnia 9 czerwca 2011 r. – Prawo geologiczne i górnicze. • Podmioty prowadzące działalność gospodarczą w zakresie wydobywania węgla brunatnego na podstawie koncesji, o której mowa w art. 22 ust. 1 ustawy z dnia 9 czerwca 2011 r. – Prawo geologiczne i górnicze. - Podmioty prowadzące działalność gospodarczą w zakresie wydobywania węgla kamiennego na podstawie koncesji, o której mowa w art. 22 ust. 1 ustawy z dnia 9 czerwca 2011 r. – Prawo geologiczne i górnicze. - Podmioty prowadzące działalność gospodarczą w zakresie wydobywania pozostałych kopalin na podstawie koncesji, o której mowa w art. 22 ust. 1 ustawy z dnia 9 czerwca 2011 r. – Prawo geologiczne i górnicze. - Przedsiębiorstwo energetyczne, o którym w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie wytwarzania energii elektrycznej. - Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 24 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie przesyłania energii elektrycznej. § Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 25 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie dystrybucji energii elektrycznej. § Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie obrotu energią elektryczną. § Podmioty o których mowa w art. 3 pkt 28b ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne. § Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne świadczący usługę o której mowa w art. 3 pkt. 6f tej ustawy. - Uczestnicy rynku świadczący usługę, o której mowa w art. 3 pkt 11j ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne. § Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, prowadzące działalność gospodarczą w zakresie przetwarzania albo magazynowania energii elektrycznej.	przetwarzania i dystrybucji żywności – zostaną przeniesione do sektorów ważnych.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

		§ Przedsiębiorcy odpowiedzialni za zarządzanie punktem ładowania i jego obsługę, świadczący usługę ładowania na rzecz użytkowników końcowych, w tym w imieniu i na rzecz dostawcy usług w zakresie mobilności; - w ramach podsektora Ciepło: § Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie wytwarzania ciepła. § Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie obrotu ciepłem. § Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie przesyłania ciepła. § Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie dystrybucji ciepła. § Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie wytwarzania ciepła. - W ramach podsektora Ropa i paliwa: § Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie wytwarzania paliw ciekłych, o której mowa w art. 32 ust. 1 ustawy z dnia 10 kwietnia 1997 r. –Prawo energetyczne. § Podmioty prowadzące działalność gospodarczą w zakresie przesyłania ropy naftowej. § Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie przesyłania paliw ciekłych siecią rurociągów, o której mowa w art. 32 ust. 1 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne. § Podmiot prowadzący działalność gospodarczą w zakresie magazynowania ropy naftowej, w tym w zakresie bezzbiornikowego podziemnego magazynowania ropy naftowej, o którym mowa w art. 22 ust. 1 ustawy z dnia 9 czerwca 2011 r. - Prawo geologiczne i górnicze. § Podmioty prowadzące działalność gospodarczą w zakresie przeładunku ropy naftowej. § Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, wykonujące działalność gospodarczą w zakresie magazynowania paliw ciekłych, o którym mowa w art. 32 ust. 1 ustawy z	

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

		dnia 10 kwietnia 1997 r. –Prawo energetyczne, oraz podmiot prowadzący działalność w zakresie bezzbiornikowego podziemnego magazynowania paliw ciekłych, o którym mowa w art. 22 ust. 1 ustawy z dnia 9 czerwca 2011 r. –Prawo geologiczne i górnictwo. § Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, wykonujące działalność gospodarczą w zakresie przeładunku paliw ciekłych, o którym mowa w art. 32 ust. 1 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne. § Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, wykonujące działalność gospodarczą w zakresie obrotu paliwami ciekłymi lub w zakresie obrotu paliwami ciekłymi z zagranicą, o którym mowa w art. 32 ust. 1 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne. § Podmioty prowadzące działalność gospodarczą w zakresie wytwarzania paliw syntetycznych. § Agencja wykonawcza utworzona na podstawie ustawy z dnia 17 grudnia 2020 r. o rezerwach strategicznych (Dz. U. z 2023 r. poz. 294) - W ramach podsektora Gaz: § Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, prowadzące działalność w zakresie wytwarzania paliw gazowych, o którym mowa w art. 3 pkt 45 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne. § Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. –Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie przesyłania paliw gazowych. § Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie obrotu gazem ziemnym z zagranicą lub na wykonywanie działalności gospodarczej w zakresie obrotu paliwami gazowymi. § Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 24 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, będące wyznaczonym przez Prezesa Urzędu Regulacji Energetyki operatorem systemu przesyłowego gazowego. § Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 25 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, będące wyznaczonym przez Prezesa Urzędu Regulacji Energetyki operatorem systemu dystrybucyjnego gazowego. § Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 26 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, będące wyznaczonym przez Prezesa Urzędu Regulacji Energetyki operatorem systemu magazynowania paliw gazowych. § Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 27 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, będące wyznaczonym przez Prezesa Urzędu Regulacji Energetyki operatorem systemu skraplania gazu ziemnego. § Przedsiębiorstwa energetyczne prowadzące działalność gospodarczą w zakresie rafinacji i przetwarzania gazu ziemnego. - W ramach podsektora Dostawy i usługi dla sektora energii:	

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

		§ Dostawcy usług zarządzanych w zakresie cyberbezpieczeństwa dla podmiotów kluczowych lub ważnych w sektorze energii. - W ramach podsektora Jednostki nadzorowane i podległe: § Jednostki organizacyjne podległe ministrowi właściwemu do spraw energii lub przez niego nadzorowane. § Jednostki organizacyjne podległe ministrowi właściwemu do spraw gospodarki złożami kopalin lub przez niego nadzorowane. - W ramach podsektora Wodór: § Operatorzy instalacji służących do produkcji wodoru. § Operatorzy instalacji służących do magazynowania wodoru. § Operatorzy instalacji służących do przesyłu wodoru. § Operatorzy instalacji służących do dystrybucji wodoru. Ponadto, dostawcy produktów i usług wykorzystywanych w sektorze energetyki mogą podlegać kwalifikacji jako następujące PK określone w Załączniku: - Dostawca usług zarządzanych; - Dostawca usług zarządzanych w zakresie cyberbezpieczeństwa w ramach sektora Zarządzanie usługami ICT; - Przedsiębiorca prowadzący którykolwiek z rodzajów działalności gospodarczej, o których mowa w sekcji C dział 26 klasyfikacji NACE Rev.2, ujętej w załączniku I do rozporządzenia (WE) nr 1893/2006 Parlamentu Europejskiego i Rady z dnia 20 grudnia 2006 r. w sprawie statystycznej klasyfikacji działalności gospodarczej NACE Rev. 2 i zmieniającego rozporządzenie Rady (EWG) nr 3037/90 oraz niektóre rozporządzenia WE w sprawie określonych dziedzin statystycznych (Dz. Urz. UE L 393 z 30.12.2006, str. 1, z późn. zm.). - Przedsiębiorca prowadzący którykolwiek z rodzajów działalności gospodarczej, o których mowa w sekcji C dział 27 klasyfikacji NACE Rev.2. - Przedsiębiorca prowadzący którykolwiek z rodzajów działalności gospodarczej, o których mowa w sekcji C dział 28 klasyfikacji NACE Rev.2; w ramach sektora Produkcja. Ogólny wpływ regulacji: Zob. uwagi wskazanie do Art. 5 ust 1 i 2 Wpływ na sektor energetyczny: jw. – brak specyficznego wpływu na sektor energetyczny. [Nadregulacja względem Dyrektywy NIS2] Względem Dyrektywy NIS2, katalog PK określony w Projekcie jest szerszy i obejmuje, oprócz podmiotów wskazanych w Dyrektywie NIS2, podmioty z poniższych podsektorów: - Wydobywanie kopalin, - Wytwarzanie paliw syntetycznych, - Obrót paliwami ciekłymi lub obrót paliwami ciekłymi z zagranicą, - Przeładunek paliw ciekłych, - Dystrybucja wodoru, - Produkcja, wytwarzanie i dystrybucja chemikaliów	

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			- Produkcja, przetwarzanie i dystrybucja żywności - Produkcja wyrobów medycznych i wyrobów medycznych do diagnostyki in vitro, - Produkcja komputerów, wyrobów elektronicznych i optycznych, - Produkcja urządzeń elektrycznych, - Produkcja maszyn i urządzeń, gdzie indziej niesklasyfikowana, - Produkcja pojazdów samochodowych, przyczep i naczep, - Produkcja pozostałego sprzętu transportowego. Powyższe wskazuje na istotną nadregulację w zakresie katalogu podmiotów objętych katalogiem PK, w szczególności podmiotów wskazanych w ramach sektora Energia. Rekomendacja: Dostosowanie wykazu w Załączniku nr 1 do KSC wg Projektu względem Załącznika nr 1 do Dyrektywy NIS2, w tym uwzględnienie podmiotów z ww. sektorów w ramach Załącznika nr 2 „Podmioty ważne”.	
189.	ZBP	Załącz. nr 1	Krajowa Izba Rozliczeniowa S.A. Uwzględnienie Krajowej Izby Rozliczeniowej S.A. w ramach sektora „Bankowość i infrastruktura rynków finansowych” Krajowa Izba Rozliczeniowa została wskazana w ramach sektora: Infrastruktura cyfrowa, podsektor: Infrastruktura cyfrowa z wyłączeniem komunikacji elektronicznej mimo, że jednocześnie jako podmiot działa na rynku przypisanym dla grupy Bankowość i infrastruktura rynków finansowych. Należy wskazać, że Krajowa Izba Rozliczeniowa jako podmiot gwarantujący możliwość przeprowadzania transakcji na polskim rynku, w ramach administrowanych systemów transakcyjnych, podlega pod uregulowania rozporządzenia o operacyjnej odporności cyfrowej – tj. rozporządzenia 2022/2554 z dnia 14 grudnia 2022 r. W związku z tym, umieszczenie KIR S.A. w ramach sektora Infrastruktura Cyfrowa może prowadzić do niespójności obowiązujących regulacji oraz nakładania na Izbę Rozliczeniową obowiązków, które będą dublowały się z regulacjami ww. rozporządzenia.	Uwaga uwzględniona KIR zostanie przeniesiony do sektora bankowości i infrastruktury rynków finansowych.
190.	Związek Firm Biotechnologicznych	Załącz. nr 1	W odpowiedzi na skierowanie projektu ustawy o Krajowym Systemie Cyberbezpieczeństwa, implementującego Dyrektywę NIS2 do konsultacji społecznych, przesyłam stanowisko Związku Firm Biotechnologicznych BioForum. Projekt nowelizacji ustawy rozszerza jej zakres podmiotowy na prawie 40 tysięcy podmiotów z 18 branż zdefiniowanych w ustawie, w tym sektora ochrony zdrowia. Ze zdziwieniem i niepokojem przyjęliśmy objęcie obowiązkami wynikającymi z nowelizacji podmiotów prowadzących działalność badawczo-rozwojową w obszarze biotechnologii. Uważamy, że jest to działanie nadmiarowe i może przynieść więcej strat niż korzyści. Nasze stanowisko wynika ze specyfiki sektora, która może umykać ministerialnym legislatorom, nie wnikającym głębiej w poszczególne działy w ramach 18 branż objętych ustawą. Podmioty prowadzące biotechnologiczne projekty badawczo-rozwojowe przez wiele lat swojej działalności nie posiadają przychodów z działalności operacyjnej. Swoje koszty pokrywają w znacznej mierze ze środków grantowych, które nie pozostawiają swobody kierowania dodatkowych strumieni na spełnienie	Uwaga nieuwzględniona Dyrektywa NIS 2 wprost wskazuje, że organizacje badawcze podlegają wymogom z zakresu cyberbezpieczeństwa. Dlatego nie można wyłączyć organizacji badawczych będących co najmniej średnimi przedsiębiorstwami z zakresu podmiotowego ustawy.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			nowych obowiązków w zakresie cyberbezpieczeństwa. W znacznej większości nie będą mogły skorzystać z ewentualnych programów ministerialnych, kierowanych do placówek medycznych ani pozyskać dedykowanych środków finansowych z innych źródeł. Firmy biotechnologiczne powoływane są zwykle przez naukowców przepełnionych pasją do poprawy dobrostanu życia człowieka. Nałożenie osobistej odpowiedzialności członków zarządu za zarządzanie ryzykiem związanym z cyberbezpieczeństwem nie znajduje powiązania z poziomem kompetencji, jaki musiałby iść w parze z możliwością realnego podjęcia obowiązków wynikających z nowego zakresu odpowiedzialności. Wdrażanie nowych obowiązków może stanowić nadmierne obciążenie wobec posiadanych możliwości. Jesteśmy przekonani, że obszary, które wykazują wrażliwość naruszeń danych, jak chociażby przetwarzane dane osobowe, znajdują się już obecnie pod dostateczną ochroną na poziomie procedur i zabezpieczeń technicznych. W związku z powyższym postulujemy o wyłączenie podmiotów prowadzących działalność badawczo-rozwojową w biotechnologii z katalogu podmiotów objętych nowelizacją ustawy. Zauważamy również, iż proponowane zmiany nie zostały poddane dyskusji przez zainteresowane podmioty z obszaru ochrony zdrowia. Z uwagi na ograniczone działania edukacyjne i informacyjne wiele podmiotów z branży medycznej nie ma w ogóle świadomości, iż będą objęte zakresem nowelizacji.	
191.	Polskie Stowarzyszenie Fotowoltaiki	Załącznik nr 2	[Katalog PW] Projekt wprowadza załącznik nr 2 do KSC określający zakres podmiotów uznawanych za PW. Ogólny wpływ regulacji: Zob. uwagi wskazanie do Art. 5 ust 1 i 2 Wpływ na sektor energetyczny: jw. – brak specyficznego wpływu na sektor energetyczny. Podmioty z sektora energetyki nie będą co do zasady podlegały kwalifikacji jako PW. (Zob. uwagi wskazane powyżej w odniesieniu do zakresu PK.) [Nadregulacja względem Dyrektywy NIS2] Katalog PW określony w Projekcie jest węższy niż określony w Dyrektywie NIS2 i nie obejmuje podmioty z poniższych sektorów, które zostały zakwalifikowane jako PK w ramach Załącznika nr 1 do KSC wg Projektu: - Produkcja, wytwarzanie i dystrybucja chemikaliów - Produkcja, przetwarzanie i dystrybucja żywności - Produkcja Powyższe wskazuje na istotną nadregulację. Rekomendacja: Dostosowanie wykazu w Załączniku nr 1 do KSC wg Projektu względem Załącznika nr 1 do Dyrektywy NIS2, w tym uwzględnienie podmiotów z ww. sektorów w ramach Załącznika nr 2 „Podmioty ważne”.	Uwaga uwzględniona Sektory produkcji; Produkcji, wytwarzania i dystrybucji chemikaliów; Produkcji, przetwarzania i dystrybucji żywności – zostaną przeniesione do sektorów ważnych.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

192.	Federacja przedsiębiorców Polskich	Załącznik nr 3	Proponuje się wykreślenie Załącznika nr 3 Zgodnie z propozycją poprawki w pkt 4 Minister właściwy do spraw informatyzacji, poprzez wydanie odpowiednich rozporządzeń, będzie mógł precyzyjnie wskazać, które funkcje w każdym z sektorów mają kluczowe znaczenie dla ich prawidłowego funkcjonowania i bezpieczeństwa. Dzięki temu podejściu, regulacje będą bardziej elastyczne i dostosowane do specyficznych potrzeb oraz charakterystyki każdego z 18 sektorów, co przyczyni się do zwiększenia poziomu bezpieczeństwa i odporności na potencjalne zagrożenia. Dlatego zbędne jest pozostawienie listy funkcji krytycznych w Załączniku nr 3.	Uwaga nieuwzględniona Ze względu na doniosłość decyzji o uznaniu za dostawcę wysokiego ryzyka zasadne jest wskazanie w załączniku do ustawy funkcji, w przypadku których należy wcześniej wycofać sprzęt.
193.	KIGEIT	Załącznik nr 3	Załącznik nr 3 do Projektu KSC Kluczowym elementem zapewnienia systemowego bezpieczeństwa usług łączności jest właściwa identyfikacja krytycznych obszarów architektury sieciowej, względem których niezbędne powinno być stosowanie wyższych poziomów bezpieczeństwa - negatywnie należy w tym zakresie ocenić określenie w ramach Załącznika nr 3 kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług. Patrząc na neutralne technologicznie procedury przyjęte w innych krajach UE, również w Polsce to Prezes UKE w porozumieniu z przedstawicielami rynku telekomunikacyjnego powinien przygotowywać dokument wskazujący w oparciu o specyfikacje i analizy techniczne funkcje krytyczne sieci telekomunikacyjnej. Warto w tym zakresie zwrócić uwagę na przykład Niemiec, gdzie lista przygotowywana jest przez stronę administracyjną, jednak konsultowana jest z przedsiębiorcami i podlega aktualizacjom. Innym przykładem technicznego i dokładnego podejścia do budowania listy funkcji krytycznych jest proces fiński, gdzie do identyfikacji dochodzi przez pryzmat podstawowych funkcji sieciowych opartych o standardy ETSI i specyfikacje techniczne 3GPP, takie podejście zapewnia neutralny technologicznie proces wskazywania krytycznych elementów infrastruktury. Również w Austrii dochodzi do określenia obowiązków względem produktów bezpośrednio zidentyfikowanych jako komponenty krytyczne w sieci 5G zgodnie z załącznikiem do rozporządzenia dotyczącym bezpieczeństwa sieci wydanego przez austriacki organ regulacyjny Rundfunk und Telekom Regulierungs-GmbH (RTR-GmbH).iW przypadku przedstawionego załącznika nr 3 elementem, który zdaniem Izby nie powinien zostać uwzględniony na liście jest pkt 3 „Zarządzanie łącznością z urządzeniami użytkowników i przydzielanie zasobów radiowych.” Takie podejście nie znajduje uzasadnienia zgodnie z międzynarodowymi dokumentacjami technicznymi, m.in. Raportem ETSI oraz dokumentami przyjętymi w ramach Unii Europejskiej (Raport on EU Coordinated Risk Assessment for 5G, s. 16 i 17 i Toolbox, s. 39 i 40), z których również wynika, iż RAN Radio Access Network nie stanowi krytycznego elementu sieci.iPonadto projekt jest niespójny terminologicznie i nieproporcjonalny nie tylko względem NIS2 ale w ogólności względem jednej z podstawowych zasad prawa europejskiego.iPrzykładem	Uwaga wyjaśniona Ze względu na ustawowy obowiązek wycofania sprzętu od dostawcy wysokiego ryzyka zasadne jest aby na poziomie ustawy były także określone zasoby, które podlegają wcześniejszemu wycofaniu. Odnosząc się do pkt 3 projektodawca wskazuje, że Radio Acces Network jest uznawana za krytyczny komponent sieci np. przez firmę Ericsson¹¹⁾ czy naukowców¹²⁾. Dlatego zasadne jest utrzymanie jej w załączniku nr 3.

¹¹⁾ RAN and core are both critical components of 5G networks because gNBs (5G base stations) terminate the encryption of user data, except when it is encrypted externally and is beyond the control of an operator's 5G network. As a result of this, gNBs have full access to all data to and from devices in cleartext. *Whitepaper on security in 5G RAN and core deployment*, <https://www.ericsson.com/en/reports-and-papers/white-papers/security-in-5g-ran-and-core-deployments>.

¹²⁾ *Radio access network (RAN) is the most critical component of a mobile network*. [w:] pkt 3 V.S. Pana, O.P. Babalola, V. Balyan, *5G radio access networks: A survey*, „Array” t. 14 (2022), DOI: 10.1016/j.array.2022.100170, <https://www.sciencedirect.com/science/article/pii/S2590005622000315>.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			powyższego może być kwestia polecenia zabezpieczającego, która w sposób nieproporcjonalny i nieuzasadniony wskazujący na 2 letni okres na jaki zostaje wydana decyzja w tej sprawie.	
194.	Związek Cyfrowa Polska	Załącz. nr 3	Załącznik nr 3 pkt 3 – proponujemy, by temu punktowi nadać brzmienie: “5G, 3GPP release 15 and onwards, Radio Base Station Baseband Unit and other features such as Radio Units and antennas” - zamiast istniejącego “5G Radio Base Station Baseband Unit and other features”. Pozwoli to uniknąć wątpliwości interpretacyjnych. Uzasadnienie: Zmiana brzmienia Punktu 3 Załącznika nr 3 poprzez odniesienie się do 3GPP release 15 i późniejszych, a także rozróżnienia elementów stacji bazowej na Baseband, Radio Unit oraz anteny pozwoli na jednoznaczne odniesienie się do międzynarodowych standardów 3GPP, w których po raz pierwszy pojawiła się technologia 5G (i jego kolejnych iteracji), a także wskazuje wprost elementy, z jakich składa się stacja bazowa i pozwoli na uniknięcie nadinterpretacji zapisu w jego pierwotnej formie.	Uwaga uwzględniona Załącznik zostanie zmieniony we wskazanym zakresie.
UWAGI do uzasadnienia i OSR				
195.	PTI	uzasad. str. 73	Str. 73, cyt. <i>„Zmitygowanie ryzyka sprzętu lub oprogramowania pochodzącego od dostawcy wysokiego ryzyka nie jest także możliwe poprzez obowiązkową certyfikację sprzętu lub oprogramowania. Standardy certyfikacyjne nie zawsze będą w stanie pomóc przy wykryciu ukrytych podatności, zwłaszcza jeśli sam producent chce je ukryć. Ponadto standardy te są znane samemu producentowi, który może to wykorzystać”</i>. Powyższy akapit jest wielokrotnie nieprawdziwy. 1. Zgodnie z art. 67b ust.: <i>12. Sporządzając opinię, o której mowa w ust. 10 zdanie pierwsze, Kolegium uwzględnia:</i> <i>1) certyfikaty wydane dla produktów ICT, usług ICT lub procesów ICT, wydane lub uznawane w państwach członkowskich Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, w szczególności certyfikaty wydane w ramach europejskich programów certyfikacji cyberbezpieczeństwa”</i>. Oznacza to, że czynnikiem ryzyka, który bierze pod uwagę Kolegium, jest obecność lub brak uznawanych certyfikatów. Obowiązkowa certyfikacja niewątpliwie wpływa na poziom ryzyka związanego z użyciem produktów/usług od „dostawcy wysokiego ryzyka.” 2. Następnie, w przepisach dot. opracowywania strategii (art. 69) ust. 2: <i>2) przy opracowywaniu strategii uwzględnia się: 2) Rozwiązania dotyczące uwzględniania w zamówieniach publicznych wymogów związanych z cyberbezpieczeństwem w odniesieniu do produktów ICT i usług ICT oraz specyfikacji tych wymogów na potrzeby takich zamówień, w tym w odniesieniu do certyfikacji cyberbezpieczeństwa (..)”</i> 3. Kolejno, należy podkreślić, że nie ma czegoś takiego jak „standardy certyfikacji”. Są normy referencyjne, które określają, w jaki sposób przeprowadzić analizę podatności. Realizując wymagania normy ewaluacyjnej, podatności mogą być wykrywane. Nikt nie może zagwarantować, że zostaną wykryte wszystkie podatności – nie ma takiej uniwersalnej magicznej formuły.	Uwaga uwzględniona Akapit zostanie wykreślony.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			4. Wreszcie, niezależnie od tego, że „standardy certyfikacji” nie istnieją, to znajomość ich przez dostawcę nie ma żadnego znaczenia dla procesu oceny bezpieczeństwa. Dostawca nie ma wpływu, w jaki sposób ewaluatorzy prowadzą analizę podatności. Wynik zależy od umiejętności ewaluatorów, a nie od tego, czy dostawca coś ukrywa albo nie. Z powyższych względów, sugeruje się wykreślenie wskazanego akapitu.	
196.	Centrum Łukasiewicz – Państwowy Instytut Badawczy	OSR	Centrum Łukasiewicz zgłasza również uwagi do Oceny skutków regulacji - pkt 6 pt. „Wpływ na sektor finansów publicznych” W powyższym punkcie jest mowa o tym, że: „W ramach Inwestycji C3.1.1. KPO Cyberbezpieczeństwo – CyberPL, infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo przewiduje się m.in. realizację projektu pn. „Wsparcie 500 podmiotów krajowego systemu cyberbezpieczeństwa w modernizacji i rozbudowie infrastruktury cyberbezpieczeństwa w sieciach IT, w tym wsparcie podmiotów wykorzystujących technologie informacyjne (IT) oraz operacyjne (OT) stosowane w przemysłowych systemach sterowania (ICS)”. Projekt ten zakłada udzielenie wsparcia o wartości – ok. 700,5 mln zł m.in. dla ok. 70 urzędów administracji centralnej i rządowej W ramach tego projektu urzędy administracji centralnej i rządowej będą mogły uzyskać wsparcie finansowe na dostosowanie się do niniejszej ustawy. Ponad 2 500 samorządów (blisko 90%) otrzyma w bieżącym roku wsparcie finansowe w postaci grantów finansowanych ze środków budżetu państwa oraz programu Fundusze Europejskie na Rozwój Cyfrowy 2021–2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa. Wsparcie to jednostki samorządu terytorialnego będą mogły wykorzystać na modernizację rozwiązań w obszarze cyberbezpieczeństwa. Łączna wartość wsparcia jaka zostanie przekazana wyniesie ok. 1,5 mld zł.” W ocenie Centrum Łukasiewicz finansowanie należy zapewnić również dla instytucji badawczych, w tym dla podmiotów tworzących Sieć Badawczą Łukasiewicz. Finansowanie powinno obejmować ewentualne utworzenie CSIRT, jak również dostosowanie procesów, infrastruktury i systemów do wymogów nowej ustawy. Nadmienić trzeba, że w poszczególnych jednostkach Sieci Badawczej Łukasiewicz, w oparciu o analizę ryzyk, powstaną potrzeby związane z inwestycjami w infrastrukturę informatyczną w celu zapewnienia ciągłości działania, wyeliminowania dostawców wysokiego ryzyka, zapewnienia kompetencji z obszaru cyberbezpieczeństwa w instytutach Sieci Badawczej Łukasiewicz. Prosimy o rozważenie możliwości utworzenia przez Sieć Badawczą Łukasiewicz utworzenia sektorowego CSIRT „Badania naukowe”. Kompetencje i możliwości technologiczne w tym zakresie posiada Sieć Badawcza Łukasiewicz- Instytut Technik Innowacyjnych EMAG z siedzibą w Katowicach.	Uwaga wyjaśniona W ramach Inwestycji C3.1.1. KPO Cyberbezpieczeństwo – CyberPL instytuty Sieci Łukasiewicz będą mogły być objęte wsparciem. Decyzję o powołaniu CSIRT sektorowego dla organizacji badawczych podejmie minister właściwy do spraw nauki. Zgodnie z projektem te zadania będą mogły być powierzone państwowej osobie prawnej. Instytuty Sieci Łukasiewicz są państwowymi osobami prawnymi, więc może być im powierzone to zadanie.
197.	ISSA Polska	OSR	Nierównomierność w rozdzielaniu wsparcia finansowego pomiędzy administracją centralną a jednostkami samorządu terytorialnego W kontekście przydzielania wsparcia finansowego dla administracji centralnej i rządowej oraz samorządów, analiza Oceny Skutków Regulacji (załącznik do ustawy KSC) ujawnia znaczącą dysproporcję. Planuje się udzielenie wsparcia w wysokości około 700,5 mln zł dla około 70 podmiotów administracji centralnej i rządowej, co przekłada się na średnio 10 mln zł na	Uwaga wyjaśniona Projekt pn. „Wsparcie 500 podmiotów krajowego systemu cyberbezpieczeństwa w modernizacji i rozbudowie infrastruktury cyberbezpieczeństwa w sieciach IT, w tym

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			każdą z tych jednostek. Tymczasem dla 2500 samorządów przeznaczono 1,5 mld zł, co oznacza średnio jedynie około 600 tys. zł na jednostkę samorządową. Tak duża dysproporcja w rozdzielaniu środków, gdzie samorządy otrzymują znacznie mniej środków na jednostkę, może prowadzić do nierówności w możliwościach wdrażania niezbędnych działań związanych z cyberbezpieczeństwem. Co więcej, środki przeznaczone dla samorządów pochodzą z Europejskiego Funduszu Rozwoju Regionalnego (FERC), co oznacza, że ich wykorzystanie wiąże się z dodatkowymi rygorami dofinansowania europejskiego, które są zwykle bardziej skomplikowane i czasochłonne w administracji niż bezpośrednie środki budżetowe dostępne dla administracji centralnej. Taka różnica w finansowaniu nie tylko wprowadza nierówności, ale także może skutkować różnicami w poziomie zabezpieczeń między różnymi poziomami administracji. W kontekście równości i sprawiedliwości w dostępie do publicznych zasobów, zasadne byłoby ponowne przemyślenie i potencjalne zrównoważenie wsparcia finansowego, tak aby wszystkie jednostki administracyjne miały równą szansę na wzmocnienie swojego cyberbezpieczeństwa.	wsparcie podmiotów wykorzystujących technologie informacyjne (IT) oraz operacyjne (OT) stosowane w przemysłowych systemach sterowania (ICS)” zakłada udzielenie wsparcia o wartości ok. 700,5 mln zł dla przynajmniej 500 podmiotów krajowego systemu cyberbezpieczeństwa, w tym m.in. dla ok. 70 urzędów administracji centralnej i rządowej. Jest to projekt współfinansowany ze środków UE w ramach inwestycji C3.1.1. KPO. Maksymalna wysokość wsparcia grantowego dla samorządów w ramach projektu „Cyberbezpieczny Samorząd”, realizowanego z programu FERC wynosi 850 tys. zł. Zgodnie z zapisami art. 41 ust. 6 ustawy z dnia 28 kwietnia 2022 r. o zasadach realizacji zadań finansowanych ze środków europejskich w perspektywie finansowej 2021–2027, wartość grantu przekazanego grantobiorcy nie może przekroczyć równowartości w złotych 200 000 euro.
198.	ISSA Polska	OSR	Brak jakiegokolwiek analizy wpływu regulacji na przedsiębiorców Projektodawca, przygotowując Ocenę skutków regulacji (OSR), nie dostarczył wyczerpującej analizy potencjalnych negatywnych skutków nowych regulacji zawartych w projekcie ustawy na konkurencyjność gospodarczą i działalność przedsiębiorców. Analiza ta zdaje się pomijać szereg istotnych aspektów dotyczących wpływu nowych przepisów na różne sektory rynku, w szczególności na mikro, małe i średnie przedsiębiorstwa, które często dysponują ograniczonymi zasobami na dostosowanie się do skomplikowanych wymagań prawnych. Zwraca uwagę brak szczegółowego rozpoznania, w jaki sposób nowe obowiązki, zwłaszcza te związane z cyberbezpieczeństwem, wpłyną na operacje biznesowe, zwłaszcza w kontekście kosztów przystosowania się do wymogów ustawy. Dla wielu przedsiębiorstw, szczególnie dla mniejszych, które mają ograniczone możliwości inwestycyjne, wprowadzenie takich wymogów może stanowić znaczące obciążenie finansowe i operacyjne. Dodatkowo, obawy budzi brak analizy wpływu tych regulacji na konkurencyjność przedsiębiorstw na rynku, gdzie dodatkowe obciążenia regulacyjne mogą wpływać na ich zdolność do konkurencji zarówno na rynku krajowym, jak i międzynarodowym. W związku z tym zalecamy przeprowadzenie bardziej szczegółowej analizy, która uwzględni różnorodność sektora przedsiębiorców oraz zmienną zdolność różnych firm do absorpcji nowych kosztów i wymogów. Takie podejście pozwoliłoby na stworzenie bardziej zrównoważonych i adekwatnych do rzeczywistych warunków	Uwaga wyjaśniona Koszty dostosowania się do nowych regulacji są bardzo trudne do oszacowania ze względu na to, że obejmuje ona podmioty o zróżnicowanej wielkości, sposobie i zakresie wykorzystania technologii ICT oraz zróżnicowanym zaawansowaniu w sprawach cyberbezpieczeństwa. Koszty te rosną proporcjonalnie do wielkości danego przedsiębiorstwa, w związku z czym mniejsze podmioty poniosą odpowiednio mniejsze koszty. Dla podmiotów, które dotychczas nie były objęte krajowym systemem cyberbezpieczeństwa, dostosowanie się do

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			funkcjonowania przedsiębiorstw regulacji, które wspierają zarówno bezpieczeństwo cyfrowe, jak i zdrowy rozwój gospodarczy.	nowych regulacji będzie oznaczało konieczność zwiększenia ich budżetów przeznaczonych na systemy teleinformatyczne. Niemniej jednak należy podkreślić, że koszty dostosowania się podmiotów do wymogów wynikających z projektu ustawy będą znacznie niższe niż ewentualne koszty wynikające ze skutków cyberataków, np. ransomware, które często wiążą się z zapłatą wielomilionowych okupów lub koniecznością odbudowy całych segmentów systemu informatycznego.
199.	Federacja Konsumentów	OSR	Uzasadnienie dla konieczności uzupełnienia OSR (koszty dla konsumentów) Chcielibyśmy podkreślić, że Polska proponuje najbardziej restrykcyjne regulacje w zakresie uznania dostawców za wysokiego ryzyka w UE, jako jedyne państwo dając możliwość wykluczenia dostawców ze wszystkich 18 sektorów (a nie z 5G, czy samej telekomunikacji). Takie podejście może prowadzić do znaczących kosztów dla konsumentów, zarówno w kontekście finansowym, jak i jakościowym, o czym zresztą wspomina się w Ocenie Skutków Regulacji: <i>"Pośrednie koszty związane z wycofaniem i wymianą produktów, usług i procesów dostarczanych przez dostawcę wysokiego ryzyka ponosić będą konsumenci. Ponieważ są to koszty zależne od tych poniesionych przez podmioty kluczowe i ważne, nie jest możliwe ich oszacowanie na obecnym etapie."</i> (str. 4 i 16). Jak wynika z informacji z innych krajów europejskich czy w Stanów Zjednoczonych¹³⁾ koszt zastąpienia infrastruktury telekomunikacyjnej może iść w miliardy złotych¹⁴⁾, a dotyczyłby on jedynie sieci 5G. W przypadku zastępowania urządzeń lub oprogramowania dla wszystkich podmiotów ważnych i kluczowych (18 sektorów), w tym sektorów „newralgicznych” dla konsumentów (takich jak dostawcy usług cyfrowych, gospodarka odpadami, usługi pocztowe, produkcja urządzeń elektrycznych, samochodów, produkcja i	Uwaga wyjaśniona Uznanie dostawcy za dostawcę wysokiego ryzyka to szczególny środek mający zapewnić bezpieczeństwo w przypadku gdy zmiętygowanie ryzyka związane z danym podmiotem nie byłoby możliwe w inny sposób. Jest to środek szczególny, który może być wykorzystany tylko w ostateczności. Istnieje również możliwość, że nigdy nie zostanie on zastosowany. Oszacowanie kosztów uznania dostawcy za dostawcę wysokiego byłoby możliwe tylko wówczas gdyby przyjął na etapie projektowania przepisów jaki podmiot potencjalnie jest takim dostawcą.

¹³⁾ (...) gdyby FCC sfinansowała wszystkie wnioski jakie skierowały do niej sieci i dostawcy usług, program zwrotu kosztów wymagałby około 4,98 miliarda dolarów. Tymczasem przeznaczona na to przez amerykańską administrację kwota to 1,9 miliarda dolarów. Brakuje więc nieco ponad 3 miliardów. Źródło: Rezygnacja z chińskich dostawców kosztuje amerykańskie firmy biliony dolarów - Forsal.pl

¹⁴⁾ W Wielkiej Brytanii, (...), koszty jego usunięcia i wymiany oszacowano na około 4 miliardy funtów (21 miliardów złotych).(...) polityka zrywania i zastępowania istniejącego sprzętu będzie kosztować jedynie niemieckiego państwowego operatora kolejowego Deutsche Bahn ponad 400 milionów euro (1.8 miliarda złotych). Źródło: Niemcy odetną Huawei od sieci "bez względu na koszt" (evertiq.pl). Koszt wymiany obecnie wyniósłby miliardy euro, zgodnie z notatką badawczą Barclays uzyskaną przez Light Reading. Według własnych szacunków operatorzy używają sprzętu Huawei na około 50% swoich stacji bazowych, co odpowiada łącznie 46 000 stacji. (Deutsche Telekom obsługuje około 38 000 stacji, według Barclays, podczas gdy Telefónica i Vodafone utrzymują po 27 000 stacji każda.) Szacując koszty wymiany na około 50 000 € (54 200 USD) za antenę, Barclays uważa, że Deutsche Telekom musiałby ponieść koszt w wysokości 1,1 miliarda € (1,2 miliarda USD), aby wyeliminować Huawei, a Telefónica i Vodafone musiałby wydać około 700 000 € (758 750 USD) każda [siedemset milionów – przyp. aut]. Źródło: German Huawei ban to cost €2.5B and take years, no thanks to EU (lightreading.com)

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			przetwarzanie żywności, ścieki i woda), należy szacować ten koszt na wielokrotnie wyższy. Taki wzrost kosztów przekładałby się wyraźnie i negatywnie na portfel przeciętnego konsumenta. Jednocześnie warto zwrócić uwagę, że na etapie wydawania decyzji przez ministra właściwego do spraw informatyzacji nie dojdzie do analizy kosztów i skutków takiej decyzji dla konsumentów. Wykluczając dane produkty, usługi i procesy, nie tylko brak jest wiedzy na etapie planowania takiego rozwiązania na poziomie legislacyjnym, ale także organ wydający decyzje nie będzie przeprowadzał takiej analizy. Stąd istnieje uzasadniona potrzeba uzupełnienia dołączonej do Projektu Ustawy Oceny Skutków Regulacji właśnie o przeprowadzone uprzednio analizy.	Ministerstwo Cyfryzacji nie identyfikuje takiego podmiotu w Polsce, w związku z czym nie jest możliwe oszacowanie kosztów związanych ze skutkami decyzji w tej sprawie. Istotne jest też, że w samej decyzji o uznaniu dostawcy za dostawcę wysokiego ryzyka zostaną wskazane typy produktów ICT, usług ICT lub procesów ICT, które mają być usunięte z tych systemów. Nie będzie to więc oznaczało konieczności usunięcia wszystkich produktów takiego dostawcy. To kolejny aspekt tych przepisów, który uniemożliwia precyzyjne określenie kosztu takiej decyzji. Należy również dodatkowo podkreślić, że na wycofanie sprzętu pochodzącego od takiego dostawcy podmioty kluczowe i ważne będą miały, co do zasady 7 lat. Do czasu upływu terminu sprzęt ten będzie mógł być dalej użytkowany, a także naprawiany i aktualizowany, tak aby zapewnić pełną ciągłość działania. 7 lat to termin, w którym w wielu wypadkach cykl życia danego sprzętu i tak uległby zakończeniu, a więc i tak często musiałby on zostać wymieniony.
200.	OPOR	OSR	Działając w imieniu Fundacji OPOR (Ogólnopolskie Porozumienie Organizacji Radioamatorskich), w związku z publikacją w dniu 24 kwietnia 2024 roku projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw¹⁵⁾, która ma implementować dyrektywę NIS2¹⁶⁾, wobec poddania projektu krótkim jak na przedmiot ustawy konsultacjom publicznym przedstawiamy następujące stanowisko i zwracamy się do Pana Ministra o dokonanie następujących zmian w Projekcie.	Uwaga wyjaśniona Uznanie dostawcy za dostawcę wysokiego ryzyka to szczególnie środek mający zapewnić bezpieczeństwo w przypadku gdy zmitigowanie ryzyka związane z danym podmiotem nie byłoby możliwe w inny sposób. Jest to środek szczególny, który może być wykorzystany tylko w

¹⁵⁾ <https://legislacja.rcl.gov.pl/projekt/12384504/katalog/13055201#13055201>, numer z wykazu: UC32 „Projekt”.

¹⁶⁾ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z 14 grudnia 2022 roku w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			Podkreślamy, że Projekt będzie miał duży wpływ na branżę ICT, ponieważ w stosunku do podmiotów ważnych i kluczowych objętych ustawą została wprowadzona instytucja dostawcy wysokiego ryzyka oparta na nietechnicznych przesłankach. W związku z tym zwracamy się z wnioskiem, żeby w ocenie skutków regulacji Ministerstwo dokonało dogłębnej analizy kosztowej wykluczenia na polskim rynku dostawców spoza UE i NATO jest to na tyle istotne bo na polskim rynku działają również podmioty z poza tego kręgu a regulacja może wpłynąć na ich pozycje. Brak takiej oceny skutków regulacji w odniesieniu do tych podmiotów jest zaprzeczeniem równego traktowania podmiotów w tego typu regulacjach. Zwracamy uwagę, że decyzja o HRV wpłynie nie tylko na przedsiębiorców, którzy będą musieli wymienić sprzęt, oprogramowanie, procesy ICT, ale również na konkurencyjność przedsiębiorstw działających na polskim rynku, co przełoży się na wyższe ceny oferowanych przez przedsiębiorców towarów i usług, uderzając bezpośrednio w klienta końcowego. W ocenie skutków regulacji także powinna zostać przedstawiona analiza kosztowa implementacji obowiązków nałożonych Projektem, a następnie jakie będą koszty operacyjne związane z utrzymaniem zgodności ze wspomnianymi obowiązkami.T	ostateczności. Istnieje również możliwość, że nigdy nie zostanie on zastosowany. Oszacowanie kosztów uznania dostawcy za dostawcę wysokiego byłoby możliwe tylko wówczas gdyby przyjąć na etapie projektowania przepisów jaki podmiot potencjalnie jest takim dostawcą. Ministerstwo Cyfryzacji nie identyfikuje takiego podmiotu w Polsce, w związku z czym nie jest możliwe oszacowanie kosztów związanych ze skutkami decyzji w tej sprawie. Istotne jest też, że w samej decyzji o uznaniu dostawcy za dostawcę wysokiego ryzyka zostaną wskazane typy produktów ICT, usług ICT lub procesów ICT, które mają być usunięte z tych systemów. Nie będzie to więc oznaczało konieczności usunięcia wszystkich produktów takiego dostawcy. To kolejny aspekt tych przepisów, który uniemożliwia precyzyjne określenie kosztu takiej decyzji. Należy również dodatkowo podkreślić, że na wycofanie sprzętu pochodzącego od takiego dostawcy podmioty kluczowe i ważne będą miały, co do zasady 7 lat. Do czasu upływu terminu sprzęt ten będzie mógł być dalej użytkowany, a także naprawiany i aktualizowany, tak aby zapewnić pełną ciągłość działania. 7 lat to termin, w którym w wielu wypadkach cykl życia danego sprzętu i tak uległby zakończeniu, a więc i tak często musiałyby on zostać wymieniony.
201.	ZPP	OSR	Zwracamy uwagę na fakt, że, przy braku wątpliwości co do celu regulacji, przewidziane w projekcie rozwiązania będą wiązały się z koniecznością poniesienia nakładów przez konkretne grupy firm. Ocena Skutków Regulacji w obecnym brzmieniu nie uwzględnia tego faktu i nie wskazuje choćby przewidywanych “widełek”, w których mogłyby się mieścić rzeczywiście poniesione koszty.	Uwaga wyjaśniona Koszty dostosowania się do nowych regulacji są bardzo trudne do oszacowania ze względu na to, że obejmuje ona podmioty o zróżnicowanej wielkości, sposobie i zakresie wykorzystania

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			Mając powyższe na uwadze, warto rozważyć uzupełnienie OSR o choćby szacunkowe dane, tak aby przedsiębiorcy mieli świadomość, jakie koszty będą musieli ponieść w związku z koniecznością dostosowania się do projektowanej nowelizacji.	technologii ICT oraz zróżnicowanym zaawansowaniu w sprawach cyberbezpieczeństwa. Koszty te rosną proporcjonalnie do wielkości danego przedsiębiorstwa, w związku z czym mniejsze podmioty poniosą odpowiednio mniejsze koszty. Dla podmiotów, które dotychczas nie były objęte krajowym systemem cyberbezpieczeństwa, dostosowanie się do nowych regulacji będzie oznaczało konieczność zwiększenia ich budżetów przeznaczonych na systemy teleinformatyczne. Niemniej należy podkreślić, że koszty dostosowania się podmiotów do wymogów wynikających z projektu ustawy będą znacznie niższe niż ewentualne koszty wynikające ze skutków cyberataków, np. ransomware, które często wiążą się z zapłatą wielomilionowych okupów lub koniecznością odbudowy całych segmentów systemu informatycznego.
202.	Konfederacja Lewiatan	OSR	Nierównomierność w rozdzielaniu wsparcia finansowego pomiędzy administracją centralną a jednostkami samorządu terytorialnego Jednostka redakcyjna: OSR Jednostka redakcyjna NIS2: nie dotyczy Uwaga: W kontekście przydzielania wsparcia finansowego dla administracji centralnej i rządowej oraz samorządów, analiza Oceny Skutków Regulacji (załącznik do ustawy KSC) ujawnia znaczącą dysproporcję. Planuje się udzielenie wsparcia w wysokości około 700,5 mln zł dla około 70 podmiotów administracji centralnej i rządowej, co przekłada się na średnio 10 mln zł na każdą z tych jednostek. Tymczasem dla 2500 samorządów przeznaczono 1,5 mld zł, co oznacza średnio jedynie około 600 tys. zł na jednostkę samorządową. Tak duża dysproporcja w rozdzielaniu środków, gdzie samorządy otrzymują znacznie mniej środków na jednostkę, może prowadzić do nierówności w możliwościach wdrażania niezbędnych działań związanych z cyberbezpieczeństwem. Co więcej, środki przeznaczone dla samorządów pochodzą z Europejskiego Funduszu Rozwoju Regionalnego (FERC), co oznacza, że ich wykorzystanie wiąże się z dodatkowymi	Uwaga wyjaśniona W ramach projektu na administrację rządową zostały nałożone obowiązki – stworzenia CSIRT sektorowych oraz pełnienia roli organów nadzorczych dla poszczególnych sektorów. Wiąże się z tym dodatkowe koszty, które będą musiały być poniesione. Zwłaszcza w przypadku CSIRT sektorowych oznacza to konieczność stworzenia nowej organizacji – zapewnienia jej infrastruktury oraz personelu. Należy też podkreślić, że wiele obowiązków nakładanych na jednostki samorządu terytorialnego nie jest nowych.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

		rygorami dofinansowania europejskiego, które są zwykle bardziej skomplikowane i czasochłonne w administracji niż bezpośrednie środki budżetowe dostępne dla administracji centralnej. Taka różnica w finansowaniu nie tylko wprowadza nierówności, ale także może skutkować różnicami w poziomie zabezpieczeń cybernetycznych między różnymi poziomami administracji. W kontekście równości i sprawiedliwości w dostępie do publicznych zasobów, zasadne byłoby ponowne przemyślenie i potencjalne zrównoważenie wsparcia finansowego, tak aby wszystkie jednostki administracyjne miały równą szansę na wzmocnienie swojego cyberbezpieczeństwa.	Obowiązek wdrożenia SZBI w tych jednostkach został wprowadzony w pierwszym rozporządzeniu Rady Ministrów w sprawie minimalnych wymagań dla systemów teleinformatycznych w 2005 r., w związku z czym nie są to nowe obowiązki. Równocześnie będą tworzone narzędzia, mające zapewnić dodatkowe środki dla samorządów. W ramach inwestycji C3.1.1 Cyberbezpieczeństwo - CyberPL, infrastruktura przetwarzania danych i dostarczania usług cyfrowych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo – Komponent Cyberbezpieczeństwo (subinwestycja C3.1.1.1), planowane jest uruchomienie czterech projektów dedykowanych dla wybranych grup podmiotów krajowego systemu cyberbezpieczeństwa, w tym dla jednostek sektora finansów publicznych. Aktualnie trwają prace do przygotowania naborów, z uwzględnieniem ich celu określonego w Krajowym Planie Odbudowy i zwiększania odporności. Docelowe grupy odbiorców wsparcia będą wynikały bezpośrednio z tych założeń. Uruchamianie naborów dla tych projektów planowane jest sukcesywnie w kolejnych kwartałach bieżącego roku. Najszerszy zakres wsparcia planowany jest w ramach projektu pn. „Wsparcie 500 podmiotów krajowego systemu cyberbezpieczeństwa w modernizacji i rozbudowie infrastruktury cyberbezpieczeństwa w sieciach IT, w tym wsparcie podmiotów wykorzystujących technologie informacyjne (IT) oraz

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

				operacyjne (OT) stosowane w przemysłowych systemach sterowania (ICS)”, o którym mowa jest w dokumencie, który stanowi Załącznik do decyzji wykonawczej Rady UE, dostępnym pod adresem https://www.gov.pl/web/planodbudowy/o-kpo (strona 125 - pozycja C23G w tabeli). Wsparcie umożliwi wzmocnienie cyberbezpieczeństwa w obszarach organizacji (procedur), kompetencji personelu oraz technologii. Informacje o ogłoszeniu naborów oraz ich szczegółowe warunki będą na bieżąco publikowane na stronie Jednostki wspierającej plan rozwojowy - Centrum Projektów Polska Cyfrowa (CPPC) https://www.gov.pl/web/cppc/. Zwrócić należy jednak uwagę na fakt, że zgodnie z zasadami obowiązującymi w KPO podatek VAT stanowi koszt niekwalifikowany, wobec czego niezbędne jest zaangażowanie na ten cel własnych środków pochodzących z budżetu jednostki.
203.	Konfederacja Lewiatan	OSR	Brak przeprowadzenia Oceny Skutków Regulacji (OSR) Jednostka redakcyjna: OSR Jednostka redakcyjna NIS2: nie dotyczy Uwaga: Nie dokonano analizy skutków nowych przepisów i zaniechano zapewnienia zasobów: Zgodnie z § 28 Regulaminu Prac Rady Ministrów odrębną część uzasadnienia projektu aktu normatywnego stanowi ocena skutków regulacji, która przedstawia wyniki oceny przewidywanych skutków społeczno-gospodarczych, a w szczególności przedstawienie wyników analizy wpływu projektowanego aktu normatywnego na podmioty, w tym na sektor finansów publicznych, w tym budżet państwa i budżety jednostek samorządu terytorialnego, rynek pracy, konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców, a zwłaszcza mikroprzedsiębiorców, małych i średnich przedsiębiorców. W tym zakresie jednak projektodawca zaniechał przeprowadzenia głębszej analizy: 1. Brak estymacji kosztów przeprowadzenia obowiązkowych cyklicznych audytów bezpieczeństwa - OSR nie zawiera estymacji kosztów związanych z obowiązkiem przeprowadzania cyklicznych audytów	Uwaga wyjaśniona Ad. 1. Należy podkreślić, że obowiązek przeprowadzania audytów nie jest nowy – dotyczył on już obecnie wyznaczonych operatorów usług kluczowych. Koszt audytu również bardzo różnił się w zależności od cech danego przedsiębiorstwa. Dlatego nie da się go oszacować dla tak zróżnicowanej grupy podmiotów. Ad. 2. Koszty dostosowania się do nowych regulacji są bardzo trudne do oszacowania ze względu na to, że obejmuje ona podmioty o zróżnicowanej wielkości,

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			bezpieczeństwa. Dokument nie oferuje analizy finansowej ani wpływu tych kosztów na mniejsze podmioty, które mogą być szczególnie obciążone tym wymogiem, a także na jednostki samorządu terytorialnego (str. 10-16 OSR). 2. Brak estymacji kosztów wdrożenia obowiązków przez podmioty kluczowe i ważne, w szczególności podmioty nieobjęte dotychczas ustawą o krajowym systemie cyberbezpieczeństwa, ani równoważnymi obowiązkami. OSR nie przedstawia szczegółowej analizy kosztów dla nowych podmiotów kluczowych i ważnych, które będą musiały dostosować swoje operacje do wymogów ustawy. Brak takiej analizy może prowadzić do nieprzewidzianych obciążeń finansowych dla tych podmiotów (str. 27-30 OSR). 3. Brak choćby próby estymacji wpływu wydania decyzji o uznaniu dostawcy sprzętu i oprogramowania za dostawcę wysokiego ryzyka. W OSR brakuje oszacowania wpływu decyzji o klasyfikacji dostawców jako dostawców wysokiego ryzyka na operacje podmiotów kluczowych i ważnych. Takie decyzje mogą prowadzić do konieczności wymiany infrastruktury IT, co generuje znaczące koszty, szczególnie dla mniejszych firm (str. 29 OSR). 4. Brak oceny, jak długo w praktyce przedsiębiorcy rzeczywiście wykorzystują sprzęt/oprogramowanie danego typu, przyjęcie za punkt odniesienia do obowiązku usuwania sprzętu jego „żywołności”. OSR nie zawiera analizy dotyczącej realnego okresu użytkowania sprzętu i oprogramowania przez podmioty. Brak takiej analizy może skutkować ustanowieniem niewykonalnych wymagań dotyczących czasu na wymianę sprzętu w sytuacji klasyfikacji dostawcy jako dostawcy wysokiego ryzyka (str. 29 OSR).	sposobie i zakresie wykorzystania technologii ICT oraz zróżnicowanym zaawansowaniu w sprawach cyberbezpieczeństwa. Koszty te rosną proporcjonalnie do wielkości danego przedsiębiorstwa, w związku z czym mniejsze podmioty poniosą odpowiednio mniejsze koszty. Dla podmiotów, które dotychczas nie były objęte krajowym systemem cyberbezpieczeństwa, dostosowanie się do nowych regulacji będzie oznaczało konieczność zwiększenia ich budżetów przeznaczonych na systemy teleinformatyczne. Niemniej należy podkreślić, że koszty dostosowania się podmiotów do wymogów wynikających z projektu ustawy będą znacznie niższe niż ewentualne koszty wynikające ze skutków cyberataków, np. ransomware, które często wiążą się z zapłatą wielomilionowych okupów lub koniecznością odbudowy całych segmentów systemu informatycznego. Ad. 3. Uznanie dostawcy za dostawcę wysokiego ryzyka to szczególny środek mający zapewnić bezpieczeństwo w przypadku gdy zmitigowanie ryzyka związane z danym podmiotem nie byłoby możliwe w inny sposób. Jest to środek szczególny, który może być wykorzystany tylko w ostateczności. Istnieje również możliwość, że nigdy nie zostanie on zastosowany. Oszacowanie kosztów uznania dostawcy za dostawcę wysokiego byłoby możliwe tylko wówczas gdyby przyjąć na etapie projektowania przepisów jaki podmiot

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

				potencjalnie jest takim dostawcą. Ministerstwo Cyfryzacji nie identyfikuje takiego podmiotu w Polsce, w związku z czym nie jest możliwe oszacowanie kosztów związanych ze skutkami decyzji w tej sprawie. Istotne jest też, że w samej decyzji o uznaniu dostawcy za dostawcę wysokiego ryzyka zostaną wskazane typy produktów ICT, usług ICT lub procesów ICT, które mają być usunięte z tych systemów. Nie będzie to więc oznaczało konieczności usunięcia wszystkich produktów takiego dostawcy. To kolejny aspekt tych przepisów, który uniemożliwia precyzyjne określenie kosztu takiej decyzji. Należy również dodatkowo podkreślić, że na wycofanie sprzętu pochodzącego od takiego dostawcy podmioty kluczowe i ważne będą miały, co do zasady 7 lat. Do czasu upływu terminu sprzęt ten będzie mógł być dalej użytkowany, a także naprawiany i aktualizowany, tak aby zapewnić pełną ciągłość działania. 7 lat to termin, w którym w wielu wypadkach cykl życia danego sprzętu i tak uległby zakończeniu, a więc i tak często musiałby on zostać wymieniony. Ad. 4. W tym zakresie należy zwrócić uwagę, że termin 7-letni na wycofanie sprzętu w przypadku wydania decyzji o uznaniu dostawcy za dostawcę wysokiego ryzyka jest efektem takich rozważań. Należy jednak podkreślić, że stanowi on pewne uśrednienie, które jest konieczne w przepisach.
204.	Polskie Stowarzyszenie Fotowoltaiki	OSR	Ocena Skutków Regulacji – uwagi w zakresie sektora energetycznego 1. W przedmiotowej Analizie wielokrotnie podkreślano, że sektorowi energetycznemu została przypisana kluczowa rola z punktu widzenia bezpieczeństwa państwa oraz planowania strategicznego. Jak wynika z Pr.	Uwaga wyjaśniona Koszty dostosowania się do nowych regulacji są bardzo trudne do oszacowania

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

		Energ., bezpieczeństwo energetyczne jest to stan gospodarki umożliwiający pokrycie bieżącego i perspektywicznego zapotrzebowania odbiorców na paliwa i energię w sposób technicznie i ekonomicznie uzasadniony przy zachowaniu wymagań ochrony środowiska. Strategicznym celem Polski w obszarze energii i klimatu jest prowadzenie polityki energetycznej w taki sposób, aby zagwarantować bezpieczeństwo energetyczne poprzez stabilne, niezakłócone dostawy energii po optymalnej cenie i w sposób zrównoważony środowiskowo. Co istotne, proces polskiej transformacji energetycznej wpływa także w sposób bezpośredni na cenę energii elektrycznej dla odbiorców końcowych. Udowodnione jest, że najbardziej skuteczną metodą obniżania kosztów wykorzystywanej energii jest stałe zwiększanie efektywności energetycznej, której skuteczność zależy od odpowiednio zmodernizowanej i wydajnej infrastruktury energetycznej¹⁷⁾. W naszej ocenie, proponowane w Projekcie regulacje mają bezpośredni wpływ na funkcjonowanie oraz finansowanie infrastruktury energetycznej. Zwracamy zatem uwagę, że projektowane regulacje oddziałują na transformację energetyczną w Polsce i mogą pośrednio wpływać na zakłócenie ciągłości dostaw energii elektrycznej. 2. Ocena wpływu wraz z konsultacjami publicznymi stanowi instrument doskonalenia otoczenia regulacyjnego zapewniający tworzenie potrzebnych i korzystnych regulacji prawnych. Co istotne, prawidłowo funkcjonujący system oceny wpływu, dzięki analitycznemu przedstawieniu prognozowanych skutków podejmowanych działań, pozwala na identyfikację najważniejszych szans i ryzyk, jakie niesie ze sobą nowa regulacja. Jednym z podstawowych elementów oceny skutków regulacji jest precyzyjne określenie podmiotów, na które planowana regulacja wpłynie w sposób pozytywny lub negatywny. Projektodawca aktu normatywnego powinien więc zidentyfikować wszystkie podmioty odnoszące korzyść z regulacji, jak i te, które na niej tracą – pośrednio lub bezpośrednio. Dokonując takiej oceny, należy pamiętać, iż adresaci danej regulacji nie zawsze zachowują się zgodnie z zasadami i dyspozycjami w niej zawartymi. Oznacza to, że trzeba zidentyfikować również niezamierzone skutki regulacji, w tym te negatywne, a następnie rozważyć możliwość modyfikacji proponowanej regulacji, aby zminimalizować te następstwa.¹⁸⁾ 3. Mając na uwadze powyższe, należy zauważyć, że OSR przygotowany dla Projektu w sposób lakoniczny odnosi się do oceny skutków projektowanej regulacji na podmioty z sektora energetycznego wskazując jedynie, iż na podmioty kluczowe z sektora energii zostaną nałożone nowe obowiązki w zakresie zarządzania ryzykiem cyberbezpieczeństwa, obowiązki zgłaszania incydentów do właściwych CSIRT sektorowych oraz obowiązek wycofania produktów ICT, usług ICT i procesów ICT w przypadku uznania dostawcy za dostawcę wysokiego ryzyka. 4. Szczegółowy wpływ na sektor energetyczny wszystkich nowych regulacji wprowadzonych w Projekcie został przez nas w sposób wyczerpujący omówiony w punkcie IV powyżej, niemniej jednak należy podkreślić, że rozwiązania przewidziane w Projekcie, takie jak wspomniane uznanie za dostawcę wysokiego ryzyka, czy możliwość ingerencji w urządzenia i oprogramowanie w ramach audytów bezpieczeństwa IT,	ze względu na to, że obejmuje ona podmioty o zróżnicowanej wielkości, sposobie i zakresie wykorzystania technologii ICT oraz zróżnicowanym zaawansowaniu w sprawach cyberbezpieczeństwa. Koszty te rosną proporcjonalnie do wielkości danego przedsiębiorstwa, w związku z czym mniejsze podmioty poniosą odpowiednio mniejsze koszty. Dla podmiotów, które dotychczas nie były objęte krajowym systemem cyberbezpieczeństwa, dostosowanie się do nowych regulacji będzie oznaczało konieczność zwiększenia ich budżetów przeznaczonych na systemy teleinformatyczne. Niemniej należy podkreślić, że koszty dostosowania się podmiotów do wymogów wynikających z projektu ustawy będą znacznie niższe niż ewentualne koszty wynikające ze skutków cyberataków, np. ransomware, które często wiążą się z zapłatą wielomilionowych okupów lub koniecznością odbudowy całych segmentów systemu informatycznego. Uznanie dostawcy za dostawcę wysokiego ryzyka to szczególnie środek mający zapewnić bezpieczeństwo w przypadku gdy zmiętygowanie ryzyka związane z danym podmiotem nie byłoby możliwe w inny sposób. Jest to środek szczególnie, który może być wykorzystany tylko w

¹⁷⁾ M. Ruszel, Infrastruktura energetyczna Polski filarem bezpieczeństwa energetycznego i konkurencyjności gospodarki, [w:] S. Domaradzki, M. Haczowska (red.), Ku przyszłości. O Polsce za 25 lat, Kancelaria Prezydenta RP, Warszawa 2015, s. 91–114.

¹⁸⁾ E. Osińska, Wpływ oceny skutków regulacji na jakość stanowionego prawa na przykładzie ustawy o kierujących pojazdami, PPP 2015, nr 6, s. 30-36.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

		mogą przyczynić się do zakłócenia pracy, czy też wykluczenia poszczególnych urządzeń, co może negatywnie oddziaływać w szczególności na inteligentne systemy opomiarowania (tzw. Smart Metering), których głównym celem jest poprawa zrównoważonego rozwoju całego systemu energetycznego. W konsekwencji, projektowane zmiany stwarzają ryzyko naruszenia integralności danych pozyskanych w ramach inteligentnych systemów opomiarowania, a zakłócenie pracy urządzeń może skutkować destabilizacją dostaw energii elektrycznej. 5. Ponadto, co szczególnie istotne, zgodnie z Projektem, minister właściwy ds. informatyzacji będzie mógł uznać poszczególnych dostawców za dostawców wysokiego ryzyka również w sektorze energetycznym. Dodatkowo, Projekt nie przewiduje wypłaty przedsiębiorcom rekompensaty z tytułu konieczności rezygnacji z określonych usług lub produktów. 6. Dodatkowo, regulacją szczególnie dotkliwą i niosącą za sobą potencjalnie negatywne konsekwencje jest możliwość stosowania poleceń zabezpieczających przez ministra właściwego ds. informatyzacji, którym nadano rygor natychmiastowej wykonalności. W tym kontekście, widzimy potencjalne ryzyko, że wprowadzenie możliwości wydawania poleceń zabezpieczających posiadających rygor natychmiastowej wykonalności, oprócz zaburzenia prowadzenia działalności gospodarczej przez określone podmioty, obciążania tych podmiotów dodatkowymi kosztami, może także pośrednio wpływać na ciągłość dostaw energii elektrycznej. Bezpieczeństwo energetyczne, jako gwarancja dostaw energii definiowane jest zwykle przez odporność systemu energetycznego na wyjątkowe i nieprzewidywalne wydarzenia, które mogą zagrozić fizycznej integralności przepływu energii lub prowadzić do niepostrzeżonego wzrostu jej cen niezależnie od podstaw ekonomicznych. Jest to zatem część systemu bezpieczeństwa narodowego, zwłaszcza, że niezawodny i stały dostęp do źródeł energii, po kosztach możliwych do poniesienia przez społeczeństwo, jest niezbędnym elementem każdej nowoczesnej gospodarki. 7. Ponadto, należy zwrócić szczególną uwagę na fakt, iż zapewnienie ciągłości dostaw energii elektrycznej jest w wielu przypadkach konieczne ze względu na opłacalność prowadzenia działalności biznesowej i prawidłowe funkcjonowanie różnego rodzaju obiektów, np. centra przetwarzania danych, szpitale, banki i instytucje finansowe. Przerwy w dostawie energii elektrycznej mogą mieć zatem katastrofalne konsekwencje w przypadku określonego rodzaju podmiotów. 8. Kolejnym elementem, który został całkowicie pominięty przez projektodawcę przy konstruowaniu oceny skutków regulacji jest aspekt finansowy proponowanych zmian i wpływ proponowanych zmian na budżety poszczególnych grup gospodarczych. Konsekwencją uznania danego dostawcy za dostawcę wysokiego ryzyka będzie konieczność wycofania sprzętu lub oprogramowania danego dostawcy, a co za tym idzie: konieczność zakupu nowego sprzętu lub oprogramowania, użycie wycofanego sprzętu, zawarciem nowych umów serwisowych i utrzymaniowych, wykształceniem kadry pod kątem nabycia kompetencji do obsługi nowego sprzętu lub oprogramowania. Wszystkie czynności będące następstwem wycofania określonego sprzętu będą pociągać za sobą dodatkowe i trudne do przewidzenia nakłady finansowe. Nie ulega zatem wątpliwości, iż ocena skutków regulacji powinna w sposób precyzyjny określać wpływ nowych regulacji na gospodarkę krajową, w skali zarówno mikro, jak i makroekonomicznej.	ostateczności. Istnieje również możliwość, że nigdy nie zostanie on zastosowany. Oszacowanie kosztów uznania dostawcy za dostawcę wysokiego byłoby możliwe tylko wówczas gdyby przyjąć na etapie projektowania przepisów jaki podmiot potencjalnie jest takim dostawcą. Ministerstwo Cyfryzacji nie identyfikuje takiego podmiotu w Polsce, w związku z czym nie jest możliwe oszacowanie kosztów związanych ze skutkami decyzji w tej sprawie. Istotne jest też, że w samej decyzji o uznaniu dostawcy za dostawcę wysokiego ryzyka zostaną wskazane typy produktów ICT, usług ICT lub procesów ICT, które mają być usunięte z tych systemów. Nie będzie to więc oznaczało konieczności usunięcia wszystkich produktów takiego dostawcy. To kolejny aspekt tych przepisów, który uniemożliwia precyzyjne określenie kosztu takiej decyzji. Należy również dodatkowo podkreślić, że na wycofanie sprzętu pochodzącego od takiego dostawcy podmioty kluczowe i ważne będą miały, co do zasady 7 lat. Do czasu upływu terminu sprzęt ten będzie mógł być dalej użytkowany, a także naprawiany i aktualizowany, tak aby zapewnić pełną ciągłość działania. 7 lat to termin, w którym w wielu wypadkach cykl życia danego sprzętu i tak uległby zakończeniu, a więc i tak często musiałby on zostać wymieniony.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			9. Projektowana regulacja może doprowadzić do przeregulowania krajowych mikro i małych przedsiębiorców, poprzez nałożenie na nich niewspółmiernie szerokich i wymagających obowiązków, zarówno w kontekście ich wdrożenia jak i utrzymania. Obowiązki przewidziane w Rozdziale 3 KSC wg Projektu, w tym wdrożenie skomplikowanych środków składających się na System Zarządzania Bezpieczeństwem Informacji projektowane było z myślą o średnich i dużych przedsiębiorstwach, które posiadają już pewne doświadczenie w zakresie wdrażania SZBI, jak również posiadają odpowiednie zasoby ludzkie i środki w celu wdrożenia tego typu wymagań. Ponadto, z uwagi na radykalne różnice w zakresie funkcji, jaką pełnią podmioty z sektora publicznego oraz podmioty z sektora prywatnego w sektorze energetycznym, różnice te powinny zostać wyraźnie zaakcentowane w Projekcie. Jednocześnie, w ramach OSR brak jest oceny wpływu Projektu w zakresie omówionym powyżej, na konkurencyjność polskich firm z sektora energetycznego. 10. Żaden z opisanych wyżej problemów nie został dostrzeżony i przeanalizowany na etapie dokonywania oceny skutków regulacji Projektu. 11. W tym miejscu pragniemy podkreślić, że konieczność przyjęcia przez państwa członkowskie UE regulacji wspólnotowych nie zwalnia krajowego ustawodawcy od dokonania wszechstronnej oceny skutków tych regulacji dla wewnętrznego porządku prawnego, zwłaszcza w sytuacji, w której ustawa implementująca zawiera daleko idące modyfikacje prawa unijnego. Zwracamy ponadto uwagę, że podmioty z sektora energetycznego stanowią istotną część operatorów usług kluczowych, dlatego tak ważnym jest przeprowadzenie rzetelnej i wyczerpującej oceny skutków regulacji dla tego sektora.	
Dodatkowe uwagi – nowe propozycje				
205.	ISAC-Kolej	Zmiany w ustawie z dnia 28 marca 2003 r. o transporcie kolejowym	W ustawie z dnia 28 marca 2003 r. o transporcie kolejowym (tj. Dz.U. z 2023 r. poz. 1786 z późn. zm.) wprowadza się następujące zmiany: 1. w art. 18a po ust. 2 dodać ust. 2a w brzmieniu „Do wniosku, o którym, mowa w ust. 2 przekazuje się dane, o których mowa w art. 7 ust. 2 pkt 1–17 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa” 2. w art. 18b po ust. 2 dodać ust. 2a w brzmieniu „Do wniosku o wydanie jednolitego certyfikatu bezpieczeństwa przekazuje się dane, o których mowa w art. 7 ust. 2 pkt 1–17 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa”.	Uwaga nieuwzględniona Nie wszystkie podmioty z podsektora transportu kolejowego będą podlegały pod znowelizowaną ustawę z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa - będą to podmioty, które mają co najmniej status średniego przedsiębiorstwa. Stąd nie jest zasadne nakładanie na wszystkich zarządców infrastruktury kolejowej oraz przewoźników kolejowych obowiązku podawania danych do wykazu podmiotów kluczowych i podmiotów ważnych do Prezesa UTK na etapie uzyskiwania autoryzacji lub certyfikatu.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

206.	ZBP	Zmiany w ustawie – Prawo bankowe Art. 4 ust. 1 pkt 59	Nowy przepis „59) centrum wymiany i analiz informacji – podmiot sektora finansowego, upoważniony do przetwarzania informacji na temat podatności, zagrożeń lub incydentów, mogących lub mających wpływ na bezpieczeństwo podmiotów, o których mowa w art. 106d ust. 1 lub ich klientów.” Wobec identyfikacji coraz liczniejszych podatności, zagrożeń i incydentów wpływających na bezpieczeństwo sektora finansowego i jego klientów, istnieje konieczność powołania nowej kategorii instytucji, której głównym zadaniem będzie koordynowanie obsługi incydentów wymierzonych w podmioty sektora finansowego i ich klientów oraz wymienianie informacji na temat podatności i zagrożeń. Powołanie centrum wymiany i analiz oraz nadanie mu stosownych ustawowych uprawnień istotnie wpłynie na wykrywanie, analizowanie i przeciwdziałanie przestępstwom popełnianym na szkodę instytucji finansowych lub ich klientów oraz wspieranie organów ścigania w zakresie wykrywania i ścigania sprawców tych przestępstw. W tym celu, centrum wymiany i analizy informacji oraz inne podmioty wymienione w art. 106d ust. 1 i 1a powinny mieć m. in. możliwość wymieniania się informacjami prawnie chronionymi, w tym informacjami objętymi tajemnicą bankową.	Uwaga nieuwzględniona Zmiany w ustawie – Prawo bankowe wykraczają poza zakres wpisu do wykazu prac legislacyjnych i programowych Rady Ministrów projektu.
207.	ZBP	Zmiany w ustawie z dnia 29 sierpnia 1997 r. – Prawo bankowe Art. 106 ust. 6-8	Nowe przepisy „6. Bankowa izba gospodarcza, wspólnie z bankami, może utworzyć centrum wymiany i analiz informacji, upoważnione do gromadzenia, przetwarzania i udostępniania informacji, w tym informacji prawnie chronionych, w przypadkach, o których mowa w art. 106d ust. 2, w celu i zakresie, o których mowa w art. 106d ust. 1 oraz w odrębnych przepisach. 7. Do zadań centrum wymiany i analiz informacji należy, w szczególności: 1) wykrywanie, analizowanie i przeciwdziałanie przestępstwom popełnianym na szkodę podmiotów, o których mowa w art. 106d ust. 1 lub ich klientów; 2) koordynowanie obsługi incydentów zagrażających bezpieczeństwu podmiotów, o których mowa w art. 106d ust. 1 lub ich klientów; 3) wymiana informacji, dobrych praktyk i doświadczeń dotyczących podatności, zagrożeń, obsługi incydentów oraz ich koordynacji; 4) wspieranie banków w wykonywaniu obowiązków, o których mowa w ust. 1. 8. Centrum wymiany i analiz informacji może wspierać organy ścigania w wykrywaniu i ściganiu sprawców przestępstw, o których mowa w ust. 7 pkt 1.” Centrum wymiany i analiz informacji powinno być tworzone przez bankową izbę gospodarczą, w ramach której działa FinCERT.pl – Bankowe Centrum Cyberbezpieczeństwa. Izba, wspólnie z bankami, powinna mieć prawną możliwość utworzenia centrum wymiany i analizy informacji, która będzie wspierać banki oraz inne instytucje rynku finansowego w zakresie identyfikacji podatności, neutralizacji zagrożeń oraz koordynacji obsługi incydentów zagrażających bezpieczeństwu oraz cyberbezpieczeństwu instytucji finansowych lub ich klientów. Szczegółowe zadania centrum wymiany i analizy informacji zostały określone w propozycji art. 106d ust. 6-8.	Uwaga nieuwzględniona Zmiany w ustawie – Prawo bankowe wykraczają poza zakres wpisu do wykazu prac legislacyjnych i programowych Rady Ministrów projektu.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			Dodatkowo, centrum wymiany i analiz informacji powinno mieć możliwość wspierania organów ścigania w zakresie wykrywania i ścigania sprawców tych przestępstw. Dotychczasowe doświadczenia FinCERT.pl – BCC ZBP, Prokuratury Krajowej i Komendy Głównej Policji pozwalają stwierdzić, że powoływane wspólnie tzw. Grupy Operacyjne pozwalają na sprawne skoordynowanie działań po stronie sektora finansowego oraz organów ścigania, co wydatnie wpływa na efektywność działań podejmowanych przez wszystkich interesariuszy.	
208.	ZBP	Zmiany w ustawie z dnia 29 sierpnia 1997 r. – Prawo bankowe Art. 106a ust. 3b	Nowy przepis „3b. W razie wystąpienia okoliczności, o których mowa w art. 106d ust. 2, w wypadkach niecierpiących zwłoki, Policja, za pośrednictwem centrum wymiany i analizy informacji, może złożyć do banku wnioski o przeprowadzenie analizy. W przypadku potwierdzenia uzasadnionych podejrzeń, bank dokonuje blokady, o której mowa w ust. 3. O dokonaniu blokady bank niezwłocznie zawiadamia Policję i prokuratora. W przypadku braku możliwości dokonania blokady, bank niezwłocznie zawiadamia o tym Policję.” W określonych sytuacjach, uzasadnione jest występowanie przez Policję do banków o przeprowadzenie przez bank analizy oraz dokonanie przez bank blokady, zgodnie z ust. 3. Przepis ten umożliwi szybszą wymianę informacji oraz koordynację działań.	Uwaga nieuwzględniona Zmiany w ustawie – Prawo bankowe wykraczają poza zakres wpisu do wykazy prac legislacyjnych i programowych Rady Ministrów projektu.
209.	ZBP	Zmiany w ustawie z dnia 29 sierpnia	„1. Poza przypadkami określonymi w art. 105, art. 106a oraz ust. 6 prokurator prowadzący postępowanie o przestępstwo lub przestępstwo skarbowe może żądać od banku, osób zatrudnionych w banku, osób, za pośrednictwem których bank wykonuje czynności bankowe oraz organizacji płatniczej, o których mowa	Uwaga nieuwzględniona Zmiany w ustawie – Prawo bankowe wykraczają poza zakres wpisu do wykazu

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

		1997 r. – Prawo bankowe Art. 106b ust. 1 oraz 6-7	w art. 2 pkt 19c ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych udzielenia informacji stanowiących tajemnicę bankową jedynie na podstawie postanowienia wydanego na jego wniosek przez właściwy miejscowo sąd okręgowy. 6. W wypadkach niecierpiących zwłoki, w razie wystąpienia okoliczności, o których mowa w art. 106d ust. 2 prokurator prowadzący postępowanie w sprawie o przestępstwo na szkodę banków lub ich klientów, może żądać w drodze postanowienia, od banku, osób zatrudnionych w banku, osób, za pośrednictwem których bank wykonuje czynności bankowe oraz od organizacji płatniczej, o której mowa w art. 2 pkt 19c ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych, udzielenia informacji stanowiących tajemnicę bankową. Wydając postanowienie, prokurator zobowiązany jest w szczególności do wskazania okoliczności uzasadniających żądanie, do określenia rodzaju i zakresu żądanych informacji, jak również podmiotu zobowiązanego do ich udostępnienia. 7. Na postanowienie prokuratora, o którym mowa w ust. 6, podmiotom wymienionym w ust. 1 przysługuje zażalenie do właściwego miejscowo sądu okręgowego. Przepisy Kodeksu postępowania karnego stosuje się odpowiednio.” W szczególnie uzasadnionych przypadkach, które dotyczą sytuacji niecierpiących zwłoki, a takimi są postępowania przygotowawcze w sprawach związanych z cyberprzestępstwami popełnianymi na szkodę banków lub ich klientów, uzasadnione jest, aby prokurator mógł samoistnie wydać postanowienie zwalniające bank z obowiązku zachowania tajemnicy bankowej. Istnieją sytuacje, w których jedynie bardzo szybkie działanie, jest w stanie odnieść efekt tj. zapobiec popełnieniu przestępstwa lub doprowadzić do ujęcia jego sprawców. Bardzo często, postanowienie sądu w tego rodzaju sprawach wydawane jest ze znacznym opóźnieniem, co uniemożliwia efektywne działanie prokuratora, Policji lub innych służb realizujących czynności pod jego nadzorem. Należy również rozszerzyć katalog podmiotów, od których prokurator może żądać informacji, bowiem niejednokrotnie Prokuratura dysponuje jedynie identyfikatorem transakcji lub kodem BLIK i wobec braku informacji o banku, do którego należy się zwrócić, w praktyce zwraca się do podmiotów prowadzących systemy płatności i schematy płatnicze. W konsekwencji zasadnym jest, aby te podmioty wprost wskazać w przepisach jako podmioty, od których również można żądać przekazania posiadanych przez nie informacji objętych tajemnicą bankową.	prac legislacyjnych i programowych Rady Ministrów projektu.
210.	ZBP	Zmiany w ustawie z dnia 29 sierpnia 1997 r. – Prawo bankowe Art. 106d	1. Banki, inne instytucje ustawowo upoważnione do udzielania kredytów, izby rozliczeniowe utworzone na podstawie art. 67, instytucje utworzone na mocy art. 105 ust. 4, jednostki zarządzające systemem ochrony, o których mowa w art. 22d ust. 1 pkt 2 ustawy o funkcjonowaniu banków spółdzielczych, ich zrzeszaniu się i bankach zrzeszających, jednostki zarządzające systemem ochrony, o których mowa w art. 130e ust. 1, instytucje pożyczkowe, instytucje finansowe, których podstawowa działalność polega na udostępnianiu składników majątkowych na podstawie umowy leasingu lub świadczeniu usług faktoringowych, podmioty, których podstawowa działalność polega na udostępnianiu składników majątkowych na podstawie umowy leasingu, oraz podmioty, o których mowa w art. 59d ustawy z dnia 12 maja 2011 r. o kredycie konsumenckim, mogą przetwarzać i wzajemnie udostępniać informacje, w tym informacje objęte tajemnicą bankową, w przypadkach:	Uwaga nieuwzględniona Zmiany w Prawie bankowym wykraczają poza zakres wpisu w wykazie prac legislacyjnych i programowych Rady Ministrów.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

		1) uzasadnionych podejrzeń, o których mowa w art. 106a ust. 3; 2) uzasadnionych podejrzeń popełnienia przestępstw dokonywanych na szkodę banków, innych instytucji ustawowo upoważnionych do udzielania kredytów, instytucji kredytowych, instytucji finansowych, instytucji pożyczkowych oraz podmiotów, o których mowa w art. 59d ustawy z dnia 12 maja 2011 r. o kredycie konsumenckim, i ich klientów, w celu i zakresie niezbędnym do zapobiegania tym przestępstwom; 3) wykonywania obowiązków w zakresie określonym w przepisach o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu. 2. Podmioty określone w ust. 1 mogą przetwarzać i wzajemnie udostępniać informacje, w tym informacje objęte tajemnicą bankową oraz informacje dotyczące wyroków skazujących, w przypadkach przestępstw dokonywanych na szkodę banków, innych instytucji ustawowo upoważnionych do udzielania kredytów, instytucji kredytowych, instytucji finansowych, instytucji pożyczkowych oraz podmiotów, o których mowa w art. 59d ustawy z dnia 12 maja 2011 r. o kredycie konsumenckim, i ich klientów, w celu i zakresie niezbędnym do zapobiegania tym przestępstwom. „Art. 106d 1. Podmiotami uprawnionymi do przetwarzania i wzajemnego udostępniania informacji, w tym informacji objętych tajemnicą bankową w przypadkach określonych w ust. 2 i 3 są: 1) banki, inne instytucje ustawowo upoważnione do udzielania kredytów, 2) izby rozliczeniowe utworzone na podstawie art. 67, 3) instytucje utworzone na mocy art. 105 ust. 4, 4) jednostki zarządzające systemem ochrony, o których mowa w art. 22d ust. 1 pkt 2 ustawy o funkcjonowaniu banków spółdzielczych, ich zrzeszaniu się i bankach zrzeszających, 5) jednostki zarządzające systemem ochrony, o których mowa w art. 130e ust. 1, 6) instytucje pożyczkowe, 7) podmioty, których podstawowa działalność polega na udostępnianiu składników majątkowych na podstawie umowy leasingu lub świadczeniu usług faktoringowych, 8) podmioty, o których mowa w art. 59d ustawy z dnia 12 maja 2011 r. o kredycie konsumenckim, 9) centra wymiany i analiz informacji, o których mowa w art. 106 ust. 6, 10) podmioty, które są członkami centrów wymiany i analiz informacji, o których mowa w pkt 10 lub zawarły z nimi stosowne porozumienie o współpracy w przypadkach, o których mowa w ust. 2, 11) bankowe izby gospodarcze, 12) organizacje płatnicze, o których mowa w art. 2 pkt 19c ustawy o usługach płatniczych, 13) przedsiębiorcy telekomunikacyjni, o których mowa w art. 2 pkt 17 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne, 14) dostawcy usług płatniczych, o których mowa w art. 4 ust. 2 ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych, w celu i zakresie niezbędnym do zapobiegania przestępstwom popełnianym na szkodę tych podmiotów lub ich klientów.	

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

		2. Podmioty, o których mowa w ust. 1, mogą przetwarzać i wzajemnie udostępniać informacje, w tym informacje objęte tajemnicą bankową, w przypadkach: 1) uzasadnionych podejrzeń, o których mowa w art. 106a ust. 3; 2) uzasadnionych podejrzeń popełnienia przestępstw dokonywanych na szkodę podmiotów, o których mowa w ust. 1 lub ich klientów; 3) wykonywania obowiązków w zakresie określonym w przepisach o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu. 3. Podmioty, o których mowa w ust. 1, mogą przetwarzać i wzajemnie udostępniać informacje dotyczące wyroków skazujących, w tym informacje objęte tajemnicą bankową w celu i zakresie, o których mowa w ust. 1. W związku z ewoluującymi zagrożeniami oraz coraz bardziej rozwiniętymi formami przestępczości zorganizowanej, coraz większe znaczenie ma zapewnienie efektywnej, międzysektorowej wymiany informacji prawnie chronionych. Proponujemy zatem rozszerzenie katalogu podmiotów uprawnionych do wymiany informacji prawnie chronionych o przedsiębiorców telekomunikacyjnych, centrum wymiany i analizy informacji, podmioty które zawarły z centrum wymiany i analizy informacji stosowne porozumienie oraz dostawców usług płatniczych. Umożliwiłoby to wielostronną wymianę informacji w celu zapobiegania przestępstwom. Ze względów na rozwój usług mobilnych i zależności pomiędzy podmiotami wskazana zmiana wydaje się być konieczna. Przepis ten koresponduje również z analogicznymi przepisem w ustawie o usługach płatniczych, a także przepisami zaproponowanymi w ustawie – prawo telekomunikacyjne. Stworzenie możliwości przekazywania danych objętych tajemnicą bankową podmiotom, które zawarły z centrum wymiany i analizy informacji stosowne porozumienie pozwoli na podejmowanie wspólnych, międzysektorowych działań wymierzonych w walkę z przestępczością – w tym także cyberprzestępczością. Doświadczenia sektora bankowego pokazują, że w celu skutecznej ochrony klientów oraz ich środków konieczne jest włączanie do współpracy w obszarze bezpieczeństwa podmiotów z innych sektorów, w tym sektora publicznego. Każdorazowo, przekazanie tego rodzaju informacji powinno odbywać się z zachowaniem wymogów poufności oraz wyłącznie w przypadkach opisanych w ww. propozycji art. 106d ust. 2. Związek Banków Polskich wielokrotnie, w ramach licznych procesów konsultacyjnych postulował rozszerzenie katalogu podmiotów upoważnionych do wymiany informacji objętych tajemnicą bankową w stosownych przypadkach. Rozszerzenie przedmiotowego katalogu pozwoli nie tylko na wzmocnienie zdolności sektora finansowego do przeciwdziałania przestępczości wymierzonej w jego klientów lecz także do podejmowania odpowiednich działań prewencyjnych – w sytuacjach gdy przekazanie informacji mogłoby pozwolić na uniknięcie strat po stronie klientów.	

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

211.	ZBP	Zmiany w ustawie z dnia 29 sierpnia 1997 r. – Prawo bankowe Art. 106e	Do przetwarzania danych osobowych przez banki, inne instytucje ustawowo upoważnione do udzielania kredytów oraz instytucje utworzone na podstawie art. 105 ust. 4, jednostki zarządzające systemem ochrony, o których mowa w art. 22d ust. 1 pkt 2 ustawy o funkcjonowaniu banków spółdzielczych, ich zrzeszaniu się i bankach zrzeszających, jednostki zarządzające systemem ochrony, o których mowa w art. 130e ust. 1, instytucje pożyczkowe, instytucje finansowe, których podstawowa działalność polega na udostępnianiu składników majątkowych na podstawie umowy leasingu lub świadczeniu usług faktoringowych, podmioty, których podstawowa działalność polega na udostępnianiu składników majątkowych na podstawie umowy leasingu, oraz podmioty, o których mowa w art. 59d ustawy z dnia 12 maja 2011 r. o kredycie konsumenckim, przepisu art. 15 rozporządzenia 2016/679 nie stosuje się w zakresie, w jakim jest to niezbędne dla prawidłowej realizacji zadań dotyczących przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu, zgodnie z art. 106, oraz zapobiegania przestępstwom, zgodnie z art. 106a i art. 106d. Do przetwarzania danych osobowych przez podmioty, o których mowa w art. 106d ust. 1, przepisu art. 15 rozporządzenia 2016/679 nie stosuje się w zakresie, w jakim jest to niezbędne dla prawidłowej realizacji zadań dotyczących przypadków, o których w art. 106 ust. 6-8, art. 106a i art. 106d ust. 2.” Konsekwencja zmiany art. 106d Prawa bankowego;	Uwaga nieuwzględniona Zmiany w ustawie – Prawo bankowe wykraczają poza zakres wpisu do wykazu prac legislacyjnych i programowych Rady Ministrów projektu.
212.	ZBP	Proponowane zmiany w zakresie ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych	Nowy przepis „3. Dostawcy usług płatniczych, organizacje, o których mowa w art. 2 oraz podmioty, o których mowa w art. 106d ust. 1 ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe mogą przetwarzać i wzajemnie udostępniać informacje, w tym informacje objęte tajemnicą zawodową, w przypadkach określonych w tych przepisach.” Przepis analogiczny do treści zaproponowanego nowego brzmienia art. 106d ust. 1 Prawa bankowego.	Uwaga nieuwzględniona Zmiany w ustawie o usługach płatniczych wykraczają poza zakres wpisu do wykazu prac legislacyjnych i programowych Rady Ministrów projektu.
213.	ZBP	Proponowane zmiany w zakresie ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne Art. 161 ust. 5	Nowy przepis „5. Przedsiębiorcy telekomunikacyjni mogą przetwarzać i wzajemnie udostępniać informacje, w tym informacje objęte tajemnicą telekomunikacyjną, w przypadkach przestępstw lub uzasadnionych podejrzeń popełnienia przestępstw dokonywanych na szkodę przedsiębiorców telekomunikacyjnych lub ich klientów, w celu i zakresie niezbędnym do zapobiegania tym przestępstwom.” Proponujemy wprowadzenie możliwości wymiany pomiędzy przedsiębiorcami telekomunikacyjnymi informacji, w przypadku uzasadnionych podejrzeń o popełnieniu przestępstw na szkodę tych przedsiębiorców i ich klientów. Współpraca wewnątrz sektora jest niezbędna do skutecznej ochrony klientów przed skutkami takich zdarzeń. Jednocześnie należy zwrócić uwagę, iż wymiana tych informacji jest pod ścisłym nadzorem prokuratora na każdym etapie postępowania przygotowawczego.	Uwaga nieuwzględniona Zmiany w ustawie – Prawo telekomunikacyjne wykraczają poza zakres wpisu w wykazie prac legislacyjnych i programowych Rady Ministrów projektu. Ponadto ustawa – Prawo telekomunikacyjne zostaje uchylona, w związku z wejściem w życie ustawy WPKE z dniem 10.11.2024 r.
214.	ZBP	Proponowane zmiany w zakresie ustawy z dnia 16	Nowy przepis „6. Przedsiębiorcy telekomunikacyjni oraz podmioty, o których mowa w art. 106d ust. 1 ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe mogą przetwarzać i wzajemnie udostępniać informacje, w	Uwaga nieuwzględniona Zmiany w ustawie – Prawo telekomunikacyjne wykraczają poza zakres wpisu do wykazu prac legislacyjnych i

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

		lipca 2004 r. – Prawo telekomunikacyjne Art. 161 ust. 6	tym informacje objęte tajemnicą telekomunikacyjną w przypadkach określonych w treści tych przepisów.” Przepis w brzmieniu analogicznym do art. 106d Prawa bankowego. Pomiędzy sektorem bankowym a sektorem telekomunikacyjnym konieczna jest wymiana informacji w celu zapobiegania przestępstwom. Należy wskazać, że incydenty mogą mieć międzysektorowe skutki oddziaływania na usługi świadczone przez sektor telekomunikacyjny oraz sektor finansowy. Dlatego, dla wskazanych podmiotów krytyczne jest szybkie otrzymanie informacji o zdarzeniach, które mogą mieć wpływ na świadczone przez nich usługi. W związku z rosnącą liczbą oszustw angażujących podmioty z różnych sektorów, konieczne jest nawiązanie efektywnej współpracy międzysektorowej. Przepis ten miałby pozwalać na zapobieganie przestępstwom popełnianym na szkodę instytucji finansowych, przedsiębiorców telekomunikacyjnych i ich klientów, przyczyniać się do ograniczania ryzyka operacyjnego tych podmiotów oraz zmniejszenia strat wynikających z przestępstw popełnianych na ich szkodę oraz szkodę ich klientów. Celem byłoby również umożliwianie przeprowadzania efektywnej analizy z obszaru Security Intelligence, w tym także eliminację tzw. false positive.	programowych Rady Ministrów projektu. Ponadto ustawa – Prawo telekomunikacyjne zostaje uchylona, w związku z wejściem w życie ustawy WPKE z dniem 10.11.2024 r.
215.	ZBP	Proponowane zmiany w zakresie ustawy z dnia 1 grudnia 2022 r. o Systemie Informacji Finansowej Art. 19 ust. 2 pkt 16-18 oraz ust. 5	Nowe przepisy „2. Podmiotami uprawnionymi do uzyskiwania informacji rejestrowanych zgromadzonych w SInF są: [...] „16)banki krajowe, oddziały banków zagranicznych, oddziały instytucji kredytowych, instytucje finansowe mające siedzibę na terytorium Rzeczypospolitej Polskiej oraz oddziały instytucji finansowych niemających siedziby na terytorium Rzeczypospolitej Polskiej, w rozumieniu ustawy z dnia 29 sierpnia 1997 r. - Prawo bankowe; 17) spółdzielcze kasy oszczędnościowo-kredytowe oraz Krajowa Spółdzielcza Kasa Oszczędnościowo-Kredytowa, w rozumieniu ustawy z dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych; 18) centra wymiany i analiz informacji, o których mowa w art. 106 ust. 6 ustawy z dnia 29 sierpnia 1997 r. - Prawo bankowe. 5. Podmiotom, o którym mowa w ust. 1 pkt 16-18, informacje o rachunku zgromadzone w SInF, udostępniane są za pośrednictwem centrów wymiany i analiz informacji w przypadkach, celu i zakresie, o których mowa w art. 106d ust. 2 ustawy z dnia 29 sierpnia 1997 r. - Prawo bankowe.” W obecnym stanie prawnym banki posiadają ograniczone możliwości wymiany informacji oraz aktywnego wykrywania działań przestępczych podejmowanych przez klientów, co niejednokrotnie wiąże się ze znacznymi stratami finansowymi dla banków. Banki monitorując tylko swój portfel nie znają szerszego kontekstu przez co pomijają istotne sygnały mogące pozwolić na szybsze wykrycie faktu prania pieniędzy.	Uwaga nieuwzględniona Zmiany w ustawie o systemie informacji finansowej wykraczają poza zakres wpisu do wykazu prac legislacyjnych i programowych Rady Ministrów projektu.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			Zdecydowanym wzmocnieniem obecnych rozwiązań byłoby umożliwienie bankom uzyskiwania z SInF informacji na temat konkretnego klienta, w celu sprawdzenia czy posiada on rachunki w innych instytucjach finansowych oraz jaki jest status tych rachunków, co przełożyłoby się zarówno na możliwość analizy, czy rachunek klienta nie jest wykorzystywany do celów przestępczych, w tym potencjalnie do prania pieniędzy oraz finansowania terroryzmu. Dodatkową, bardzo istotną kwestią jest wzmocnienie możliwości wymiany informacji oraz przeprowadzania sektorowych analiz w celu wykrywania przestępstw popełnianych z wykorzystaniem działalności banków. W związku z tym, należy wprowadzić prawną możliwość dostępu do Systemu SInF dla centrów wymiany i analiz informacji, utworzonych przez banki i izbę gospodarczą na podstawie art. 106 ust. 6 ustawy – Prawo Bankowe. Kierowanie zapytań za pośrednictwem centrów wymiany i analiz informacji, będzie gwarantować z jednej strony prawidłowość wniosków pod względem formalnym, a z drugiej ułatwi również przekazywanie oraz analizę informacji w ramach sektora. Ponadto, takie rozwiązanie wzmocni również bezpieczeństwo przekazywanych informacji.	
216.	ZBP	Ustawa z dnia 29 sierpnia 1997 r. – Ordynacja Podatkowa	Nowy przepis „3) wykonywania przez izbę rozliczeniową na rzecz centrum wymiany i analiz informacji, o którym mowa w art. 106 ust. 6 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe czynności niezbędnych do wykonywania przez centrum wymiany i analiz informacji zadań, o których mowa w art. 106 ust. 7 oraz uprawnień określonych w art. 106d tej ustawy.” Umożliwienie centrum wymiany i analiz informacji przetwarzania informacji pochodzących z systemu STIR wzmocniłoby zdolność do wykonywania działań związanych ze wspieraniem banków w przeciwdziałaniu przestępczości – w tym przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu – tj. działań określonych w proponowanym art. 106 ust. 7 ustawy – Prawo bankowe. W ramach STIR gromadzone są m.in. szczegółowe dane o rachunkach bankowych (w tym rachunkach rozliczeniowych, rachunkach lokat, rachunkach VAT, rachunkach oszczędnościowych), tj. m.in o ich otwarciu lub zamknięciu, saldzie, dokonanych transakcjach, a także o danych pełnomocnika do rachunku. Stworzenie podstawy prawnej do przekazywania niektórych z tych informacji przez izbę rozliczeniową do centrum wymiany i analiz informacji pozwoli wspólne prowadzenie przez izbę rozliczeniową oraz Centrum kompleksowych analiz dotyczących przeciwdziałaniu wykorzystywaniu sektora finansowego do działań przestępczych. Dzięki wprowadzonemu rozwiązaniu, blokowanie środków pochodzących z przestępstw ma szansę stać się dużo bardziej skuteczne, co przełoży się na zwiększenie możliwości ochrony środków klientów, którzy padli ofiarami przestępstw. Dodatkowo, informacje pochodzące ze STIR i ich analiza umożliwią wypracowanie mechanizmów prewencyjnych, uniemożliwiających wykonywanie transakcji oszukańczych. Dostępne obecnie rozwiązania technologiczne (m.in. uczenie maszynowe, sztuczna inteligencja) pozwalają na tworzenie bardzo zaawansowanych mechanizmów analitycznych. Skuteczność tego rodzaju rozwiązań	Uwaga nieuwzględniona Zmiany w ustawie – Ordynacja podatkowa wykraczają poza zakres wpisu do wykazu prac legislacyjnych i programowych Rady Ministrów projektu.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			uzależniona jest jednak od jakości dostarczanych danych, w tym zbiorów porównawczych. Sektor bankowy, w tym również bankowa izba gospodarcza, podejmuje liczne inicjatywy zmierzające do wzmocnienia potencjału analitycznego w tym zakresie, niemniej, brak informacji pochodzących ze STIR wpłynie negatywnie na jakość rezultatów prowadzonych analiz.	
217.	Konfederacja Lewiatan	Nowa propozycja	Wydłużenie vacatio legis Dodaje się art. 27a w brzmieniu: <i>„Podmioty, które nie zostały wpisane do wykazu operatorów usług kluczowych, o którym mowa w art. 7 ustawy zmienianej, na podstawie decyzji o uznaniu za operatora usługi kluczowej, o której mowa w art. 5 ust. 2 ustawy zmienianej - realizują obowiązki, o których mowa w rozdziale 3 w brzmieniu nadanym niniejszą ustawą, w terminie 12 miesięcy od dnia dokonania wpisu do wykazu, o którym mowa w art. 7 ust. 1., w brzmieniu nadanym niniejszą ustawą”</i> Proponowana nowelizacja Ustawy obejmie nowe podmioty wskazane w załączniku nr 1 i nr 2 (np. producentów leków), które będą zobowiązane realizować obowiązki wynikające zarówno z obecnie obowiązującej ustawy jak i z treści projektu. Mając na uwadze stopień ich skomplikowania oraz wysokie koszty wdrożenia – proponujemy wskazanie terminu 12 miesięcy dla podmiotów, które nie zostały wpisane do wykazu operatorów usług kluczowych w rozumieniu w art. 7 ustawy zmienianej.	Uwaga nieuwzględniona Z uwagi na konieczność wdrożenia dyrektywy NIS2 proponuje się pozostawienie terminu 6 miesięcy na dostosowanie się do obowiązków.
218.	Osoba fizyczna	Nowa propozycja (dodanie art. 15a)	Art. 15a. Przeprowadzanie audytów bezpieczeństwa 1. Każdy podmiot kluczowy oraz ważny, który jest częścią krajowego systemu cyberbezpieczeństwa, jest zobowiązany do przeprowadzania regularnych audytów bezpieczeństwa swoich systemów informacyjnych, infrastruktury i procedur zgodnie z wymogami niniejszej ustawy oraz Dyrektywy NIS2. 2. Audyty bezpieczeństwa powinny być przeprowadzane co najmniej raz na dwa lata przez niezależne podmioty certyfikowane w zakresie audytów bezpieczeństwa informatycznego lub przez audytorów zatrudnionych w organizacji, którzy posiadają odpowiednie uprawnienia. Audyty te powinny obejmować: 1) Ocena zgodności: Weryfikacja zgodności z obowiązującymi przepisami prawa, normami i standardami bezpieczeństwa, w tym normami ISO/IEC 27001. 2) Ocena ryzyka: Przegląd i ocena mechanizmów zarządzania ryzykiem cybernetycznym w tym identyfikacja zagrożeń i ocena ich potencjalnego wpływu. 3) Testy penetracyjne: Regularne testy penetracyjne mające na celu identyfikację podatności w systemach informatycznych i infrastrukturze sieciowej. 4) Ocena skuteczności środków zaradczych: Sprawdzenie skuteczności wdrożonych środków zapobiegawczych i naprawczych oraz rekomendacja dalszych działań.	Uwaga wyjaśniona Naszym zdaniem przepis jest nadmiarowy. Wystarczające jest zapewnienie, że w przypadku podmiotów kluczowych będzie przeprowadzany audyt przez niezależnego audytora.
219.	Osoba fizyczna	Nowa propozycja (dodanie art. 15b)	Art. 15b. Weryfikacja zgodności przez niezależne podmioty 1. Niezależne podmioty certyfikowane w zakresie audytów bezpieczeństwa informatycznego powinny być akredytowane przez właściwe organy krajowe lub międzynarodowe, które zapewniają ich kompetencje i bezstronność. 2. Niezależne podmioty są zobowiązane do przestrzegania najwyższych standardów zawodowych i etycznych podczas przeprowadzania audytów oraz weryfikacji zgodności.	Uwaga nieuwzględniona W ocenie projektodawcy przepis jest nadmiarowy. Wystarczające jest zapewnienie, że w przypadku podmiotów kluczowych będzie przeprowadzany audyt przez niezależnego audytora.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			3. Weryfikacja zgodności obejmuje: 1) Przegląd polityk i procedur: Ocena, czy polityki i procedury bezpieczeństwa są zgodne z obowiązującymi przepisami i normami. 2) Inspekcje techniczne: Szczegółowe inspekcje techniczne infrastruktury informatycznej, systemów oraz urządzeń zabezpieczających. 3) Weryfikacja dokumentacji: Sprawdzenie kompletności i dokładności dokumentacji związanej z zarządzaniem bezpieczeństwem informacyjnym 4) Wywiady z pracownikami: Przeprowadzanie wywiadów z kluczowymi pracownikami odpowiedzialnymi za bezpieczeństwo informacyjne w celu oceny ich wiedzy, świadomości i kompetencji. 4. Niezależne podmioty powinny sporządzać szczegółowe raporty z przeprowadzonych weryfikacji zgodności, które zawierają: 1) Wnioski i rekomendacje: Szczegółowe wnioski dotyczące zgodności z obowiązującymi wymogami oraz rekomendacje dotyczące dalszych działań. 2) Analiza ryzyka: Ocena ryzyka związanego z wykrytymi niezgodnościami oraz potencjalnymi zagrożeniami. 3) Plan działań naprawczych: Propozycje działań naprawczych mających na celu usunięcie wykrytych niezgodności i poprawę bezpieczeństwa. 5. Raporty z weryfikacji zgodności powinny być przekazywane do właściwego CSIRT-u sektorowego oraz organu nadzoru w terminie 30 dni od zakończenia weryfikacji.	
220.	Konfederacja Lewiatan	Nowa propozycja	Brak wdrożenia Rozporządzenia PE i Rady (UE) 2019/881 Jednostka redakcyjna: nie dotyczy Jednostka redakcyjna NIS2: nie dotyczy Uwaga: Ustawa KSC pomimo odniesień do Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. dotyczącego ENISA (Europejskiej Agencji ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w obszarze technologii informacyjno-komunikacyjnych, nie zawiera konkretnych rozwiązań ani procedur wdrażających wspomniane przepisy. Brak jest jasnych wskazań dotyczących sposobu implementacji wymogów rozporządzenia, co stawia pod znakiem zapytania skuteczność przyszłych działań w zakresie zwiększenia cyberbezpieczeństwa na poziomie krajowym. Poprzednie konsultacje projektów ustawy podkreślały potrzebę wdrożenia rozporządzenia 2019/881, a nie dyrektywy NIS2, co czyni tę zaniechaną implementację szczególnie problematyczną.	Uwaga wyjaśniona Kwestia certyfikacji cyberbezpieczeństwa to odrębna materia, w związku z czym znalazła się w projekcie odrębnej ustawy – ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa (UC42).
221.	Konfederacja Lewiatan	Nowa propozycja	Brak udziału ministra ds. informatyzacji w ramach prac Rządowego Zespołu Zarządzania Kryzysowego Jednostka redakcyjna: nie dotyczy Jednostka redakcyjna NIS2: art. 9 Uwaga: Umocowanie ministra właściwego do spraw informatyzacji (Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa) jako organu wiodącego w zakresie cyberbezpieczeństwa nie znajduje odzwierciedlenia we włączeniu tego organu do działalności Rządowego Zespołu Zarządzania Kryzysowego, o którym mowa w art. 8 ustawy o zarządzaniu kryzysowym. Minister do spraw	Uwaga wyjaśniona Co do zasady się z przedstawiony postulat jest słuszny, niemniej jednak w związku z trwającymi pracami nad wdrożeniem dyrektywy CER zostanie przeprowadzona nowelizacja ustawy o zarządzaniu kryzysowym. W ramach tych prac zgłoszony został postulat dodania Ministra

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III

			informatyzacji może być jedynie doproszony do tego gremium na podstawie art. 8 ust. 3 ustawy o zarządzaniu kryzysowym. Z uwagi na znaczenie ministra właściwego do spraw informatyzacji, zasadne byłoby wprowadzenie odpowiedniej zmiany w tej jednostce redakcyjnej ustawy o zarządzaniu kryzysowym w celu zapewnienia spójności i koordynacji reagowania organów administracji publicznej w obliczu sytuacji kryzysowych.	Cyfryzacji do Rządowego Zespołu Zarządzania Kryzysowego. Wobec tego materia ta będzie przedmiotem innej ustawy.
222.	Związek Pracodawców Technologii Cyfrowych Lewiatan	Nowa propozycja	Nowelizacja ustawy o działaniach antyterrorystycznych Wprowadzenie stopni alarmowych w polskim systemie prawnym jest przeniesieniem odpowiadających im stopni alarmowych NATO. Polski system dodatkowo wprowadził stopnie alarmowe dla cyberprzestrzeni (art. 15 ust. 2). Proponowana zmiana związana jest z uwzględnieniem zapisu z kodeksu karnego (art. 269a). Ma również znaczenie dla podniesienia cyberbezpieczeństwa podmiotów kluczowych i ważnych, a także dotyczy dalszej synchronizacji z systemami NATO. Jest: <i>Art. 2 p.7) zdarzeniu o charakterze terrorystycznym – należy przez to rozumieć sytuację, co do której istnieje podejrzenie, że powstała na skutek przestępstwa o charakterze terrorystycznym, o którym mowa w art. 115 § 20 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny, lub zagrożenie zaistnienia takiego przestępstwa.</i> Propozycja <i>Art. 2 p.7) zdarzeniu o charakterze terrorystycznym – należy przez to rozumieć sytuację, co do której istnieje podejrzenie, że powstała na skutek przestępstwa o charakterze terrorystycznym, o którym mowa w art. 115 § 20 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny, lub sabotażu komputerowego, o którym mowa w art. 269a ustawy z dnia 6 czerwca 1997 r. – Kodeks karny lub zagrożenie zaistnienia takich przestępstw.</i>	Uwaga wyjaśniona Zmiana w ustawie o działaniach antyterrorystycznych wykracza poza zakres wpisu do wykazu prac legislacyjnych i programowych Rady Ministrów projektu.
223.	Polska Izba Informatyki i Telekomunikacji	Uwagi redakcyjne	Uwagi redakcyjne: • Projektowany art. 2 pkt 8a – odesłanie do ustawy o rachunkowości powinno dotyczyć art. 3 ust. 1 pkt 6, a nie art. 3 pkt 6, ponieważ ta jednostka redakcyjna jest podzielona na ustępy. • W dotychczasowym art. 15 ust. 6 pozostało sformułowanie „operator usługi kluczowej”.	Uwaga uwzględniona

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. IV

Lp.	Zgłaszający uwagę	Jednostka redakcyjna	Treść uwagi	Stanowisko Ministra Cyfryzacji
1.	PFRON	Uwaga ogólna	Państwowy Fundusz Rehabilitacji Osób Niepełnosprawnych wnosi o: a) dodanie Państwowego Funduszu Rehabilitacji Osób Niepełnosprawnych do załącznika nr 1 do projektu ww. ustawy w Sektorze „Administracja publiczna”. b) dołączenie w art. 9 projektu ww. ustawy Państwowego Funduszu Rehabilitacji Osób Niepełnosprawnych do listy podmiotów uprawnionych do stosowania ustawy z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa (Dz. U. z 2023 r. poz. 667). Zmiana polegałaby na dopisaniu w art. 5 pkt 2) tej ustawy Państwowego Funduszu Rehabilitacji Osób Niepełnosprawnych, co upoważniałoby pracowników Funduszu do pobierania dodatku do wynagrodzenia z tytułu realizacji zadań związanych z cyberbezpieczeństwem. W projekcie ustawy w sektorze „Administracja publiczna” wskazane zostały jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 1-6, 8 i 10-13 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2023 r., poz. 1270, z późn. zm.). Z zestawienia wyłączono państwowe fundusze celowe. Zgodnie z art. 45 ustawy z dnia 27 sierpnia 1997 r. o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych (Dz. U. z 2024 r. poz. 44, z późn. zm.) Państwowy Fundusz Rehabilitacji Osób Niepełnosprawnych został powołany jako państwowy fundusz celowy, w rozumieniu przepisów o finansach publicznych, z zastrzeżeniem, że Fundusz posiada osobowość prawną. Zgodnie z załącznikiem do obwieszczenia Ministra Rodziny, Pracy i Polityki Społecznej z dnia 21 grudnia 2023 r. Państwowy Fundusz Rehabilitacji Osób Niepełnosprawnych jest jednostką nadzorowaną przez Ministra Rodziny, Pracy i Polityki Społecznej. Celem działalności PFRON jest realizacja szerokiego spektrum zadań ukierunkowanych na wspieranie rehabilitacji zawodowej i integracji społecznej osób z niepełnosprawnością oraz kreowanie postaw tolerancji i szacunku społeczeństwa w stosunku do osób za szczególnymi potrzebami. Fundusz dostarcza szeroki zakres usług publicznych zarówno na rzecz osób niepełnosprawnych jak i pracodawców zatrudniających osoby niepełnosprawne. Środki PFRON przekazywane są na realizację zadań na rzecz osób z niepełnosprawnościami: samorządom powiatowym i wojewódzkim oraz fundacjom i organizacjom pozarządowym. Przerwanie ciągłości świadczenia tych usług może nieść poważne negatywne konsekwencje dla osób i podmiotów korzystających ze wsparcia Funduszu oraz będzie miało bezpośredni wpływ na realizację zadań publicznych. PFRON gromadzi w swoich zasobach teleinformatycznych dużą ilość danych wrażliwych oraz danych osobowych beneficjentów. Dane te należy chronić, niezależnie od ponoszonych kosztów poprzez intensyfikację działań w obszarze cyberbezpieczeństwa, w tym realizację projektów zwiększających bezpieczeństwo i ochronę danych, zwiększających kompetencje zespołów funkcjonujących w PFRON oraz inicjowanie nowych projektów i współpracę z innymi podmiotami. Zgłoszenie motywowane jest nie tylko wielkością infrastruktury Funduszu, na którą składa się 660 serwerów (60 fizycznych oraz 600 serwerów wirtualnych) oraz 150	Uwaga częściowo uwzględniona PFRON zostanie dodany do sektora podmioty publiczne. Nie przewiduje się szerszych zmian w ustawie o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. IV

			urządzeń aktywnych (switch, router, firewall), ale również ilością uruchomionych na niej systemów, których łącznie jest 90. Na wartość tą składa się 11 systemów strategicznych, w tym 7 wspierających usługi operacyjne wynikające z misji PFRON oraz 4 systemy krytyczne wspierające działalność uwarunkowaną wymogami prawnymi lub względami bezpieczeństwa, jak również 79 systemów wspierających codzienną działalność organizacji. Uwzględnienie Państwowego Funduszu Rehabilitacji Osób Niepełnosprawnych w krajowym systemie cyberbezpieczeństwa poprzez dodanie go do podmiotów kluczowych w załączniku nr 1 w Sektorze „Administracja publiczna”, a w konsekwencji w systemie zarządzania cyberbezpieczeństwem jest dużą szansą dla Funduszu w kwestii wzmocnienia technicznego oraz kompetencyjnego potencjału do zapobiegania i reagowania na incydenty cyberbezpieczeństwa. Działania takie pozwolą lepiej dbać o bezpieczeństwo przetwarzanych w wyżej wymienionych systemach informacji kontrahentów oraz beneficjentów PFRON. Przetwarzane informacje, w szczególności te wrażliwe mogą być celem potencjalnego cyberataku, gdzie Funduszu od początku roku 2024 do dnia 08.07.2024 r. zarejestrowanych zostało na Next Generation Firewall 31424 zdarzeń o charakterze cyberzagrożenia, bądź cyberataku. Jednocześnie Fundusz zwraca się o dodanie Państwowego Funduszu Rehabilitacji Osób Niepełnosprawnych do katalogu organów i podmiotów uprawnionych do przyznania pracownikom realizującym zadania w zakresie cyberbezpieczeństwa dodatku do wynagrodzenia za pracę lub świadczenia pieniężnego - w przypadku funkcjonariuszy i żołnierzy zawodowych świadczenie pieniężne, zwane dalej „świadczeniem teleinformatycznym”. Ochrona dużej liczby danych przetwarzanych w systemach należących do Funduszu w dobie wzrastających w cyberprzestrzeni zagrożeń staje się coraz większym wyzwaniem, szczególnie w sytuacji braku odpowiedniego wsparcia technologicznego oraz kompetencyjnego. PFRON zdając sobie sprawę z konieczności podnoszenia poziomu dojrzałości cyberbezpieczeństwa m.in. dbania o bezpieczeństwo informacji, ciągłego doskonalenia technologii oraz kompetencji, jak i dbania o niezawodną komunikację z organami administracji publicznej czy też organami właściwymi do spraw cyberbezpieczeństwa. Powyższe działania są niezbędne w celu zapewnienia bezpieczeństwa przetwarzanych danych oraz infrastruktury Funduszu, a ich realizacja wiąże się z koniecznością postawienia na kompetencje z zakresu cyberbezpieczeństwa. Uwzględnienie Państwowego Funduszu Rehabilitacji Osób Niepełnosprawnych nie tylko jako podmiotu kluczowego, ale również w art. 5 pkt. 2 ustawy z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa (Dz. U. z 2023 r. poz. 667) umożliwi sprawniejszą realizację projektów związanych z cyberbezpieczeństwem, umożliwi dostęp do szerszego grona specjalistów oraz da możliwość na nawiązanie współpracy i wymianę doświadczeń z innymi podmiotami kluczowymi, jak i jednostkami je nadzorującymi. Art. 5 pkt 2 lit. d obecnie obowiązującej ustawy wskazuję, iż do świadczenia teleinformatycznego uprawnione są osoby realizujące zadania w jednostkach organizacyjnych podległych Prezesowi Rady Ministrów lub ministrom. PFRON nie mieści się w tym katalogu,	

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. IV

			albowiem Fundusz, jak wskazano powyżej nie jest jednostką podległą Ministrowi Rodziny, Pracy i Polityki Społecznej lecz jednostką nadzorowaną. Jednocześnie Fundusz zwraca uwagę, iż pismem z dnia 8 listopada 2022 r. znak: DZ.WPL.0211.18.2022.GB Państwowy Fundusz Rehabilitacji Osób Niepełnosprawnych wnioskował o dodanie go do listy podmiotów uprawnionych do stosowania ustawy z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa przy pracach nad projektem ustawy o zmianie ustawy o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa oraz niektórych innych ustaw (UD390). W konsekwencji powyższego pisma PFRON został uwzględniony w projekcie niniejszej ustawy z dnia 13 grudnia 2022 r. Powyższe zgłoszenie wskazanej propozycji nastąpiło na tym etapie prac legislacyjnych, z uwagi na fakt nie otrzymania przez Fundusz niniejszego projektu ustawy do opiniowania na wcześniejszym etapie procedowania.	
2.	PSNM	Uwaga ogólna	W związku z powyższym, PSNM wnioskuje o zapewnienie dodatkowych 30 dni na konsultacje publiczne. Pozwoli to na szeroką i merytoryczną ocenę wpływu nowelizacji na sektor nowej mobilności oraz umożliwi skuteczniejsze wypracowanie propozycji, które z jednej strony zapewnią tak potrzebne cyberbezpieczeństwo, a z drugiej nie obciążą nadmiernie branży motoryzacyjnej. Uwzględniając potencjalne, istotne konsekwencje wprowadzenia nowych przepisów, wyrażamy przekonanie, że ich projekt wymaga dalszych, pogłębionych analiz. W związku z proponowanym przesunięciem klasyfikacji sektora produkcji z podmiotów ważnych (zgodnie z punktem 5 Załącznika II dyrektywy 2022/2555) na podmioty kluczowe, PSNM zwraca uwagę na znaczące implikacje tej decyzji dla branży nowej mobilności. Przedmiotowa zmiana obejmuje podsektory takie jak produkcja komputerów, wyrobów elektronicznych i optycznych, urządzeń elektrycznych, maszyn oraz pojazdów samochodowych i sprzętu transportowego. Reklasyfikacja prowadzi do zwiększonego nadzoru oraz wyższych kar za nieprzestrzeganie nowych przepisów, co znacząco podnosi koszty zgodności dla całego sektora produkcyjnego. Podsumowując, PSNM apeluje o wydłużenie okresu konsultacji publicznych, co pozwoli na bardziej aktywny i merytoryczny udział w procesie legislacyjnym. Stowarzyszenie jest zdecydowane na kontynuowanie dialogu z Ministerstwem Cyfryzacji, aby wspólnie kształtować przyszłość prawa w sposób, który będzie sprzyjał rozwojowi innowacyjnej gospodarki i bezpieczeństwu cybernetycznemu Polski.	Uwaga wyjaśniona Termin 30 dni to standardowy termin na konsultacje publiczne projektu ustawy.
3.	PSML	Uwaga ogólna	Działając w imieniu Polskiego Stowarzyszenia Menedżerów Logistyki i Zakupów, w związku z prowadzonymi przez Ministerstwo Cyfryzacji konsultacjami publicznymi projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw z 23 kwietnia 2024 r. (nr UC32 w wykazie prac legislacyjnych), niniejszym zwracamy się z wnioskiem o wydłużenie procesu konsultacji publicznych przedmiotowego projektu o 30 dni. Nasz wniosek o wydłużenie konsultacji publicznych wynika z szerokiego zakresu regulacji, który ma obejmować 18 sektorów polskiej gospodarki – tak przedsiębiorców, jak i podmioty publiczne, jednostki samorządu terytorialnego oraz urzędy państwowe. Jednocześnie należy	Uwaga wyjaśniona Termin 30 dni to standardowy termin na konsultacje publiczne projektu ustawy.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. IV

			podkreślić, że w naszej ocenie, na dzisiaj świadomość zakresu zmian wprowadzanych niniejszą nowelą wśród przedsiębiorstw działających w Polsce jest nikła. Wydłużony czas konsultacji pozwoli nam jako podmiotowi zrzeszającemu szereg firm działających w rozmaitych sektorach gospodarki poszerzyć świadomość zagadnienia wśród polskich przedsiębiorstw i oraz zebrać i przekazać wartościowe, z perspektywy przyszłej regulacji, uwagi i sugestie od podmiotów, które będą bezpośrednio dotknięte skutkami przedmiotowej regulacji. Nasza organizacja zrzesza 350 członków oraz dociera do kilku tysięcy osób realizujących zakupy w przedsiębiorstwach, odpowiedzialnych zatem również za relacje z dostawcami usług i produktów, To te osoby odpowiedzialne są za zarządzanie ryzykami związanymi z dostawcami i ew. zmiany źródeł zaopatrzenia. Współpracujemy z pełnym przekrojem przedsiębiorstw w Polsce w różnych formatach Z naszych wstępnych konsultacji wynika, że świadomość implikacji wprowadzanych zmian jest nikła oraz że specyfika poszczególnych branż, inaczej podchodzących do zarządzania ryzykiem stwarza przestrzeń do lepszego dopasowania przepisów do realiów prowadzenia biznesu. Z perspektywy zakupowej oraz analizy bezpieczeństwa łańcucha dostaw dostrzegamy, że dyrektywa NIS2 nakłada na podmioty kluczowe i ważne obowiązek wprowadzania odpowiednich środków technicznych, operacyjnych i organizacyjnych, mających na celu zarządzanie ryzykiem dla bezpieczeństwa sieci i systemów informatycznych. Widzimy jednak również, że proponowana ustawa daje możliwość uznania dostawcy za dostawcę wysokiego ryzyka i wykluczania podmiotów ze względu na państwo pochodzenia. Budzi to nasze wątpliwości i wymaga pogłębionej analizy wśród przedsiębiorstw działających w Polsce – członków naszego stowarzyszenia, zwłaszcza w kontekście potencjalnych kosztów takich decyzji. Jak wspomnieliśmy powyżej projektowane przepisy mogą mieć negatywne konsekwencje dla wielu podmiotów. Ocena Skutków Regulacji (OSR) nie zawiera kompleksowej analizy kosztów, jakie pracodawcy i przedsiębiorcy będą musieli ponieść, aby dostosować się do ostawionych przed nimi wymagań. W OSR wskazano, że takie szacunki nie są możliwe do wykonania, jednak nie podjęto próby wskazania minimalnej czy też ich maksymalnej wysokości. Dla wielu przedsiębiorców regulacja może oznaczać znaczące koszty związane z koniecznością wymiany stosowanej technologii, urządzeń, oprogramowania, ale też koszty związane z koniecznością zatrudnienia wysoko wykwalifikowanych specjalistów z dziedziny IT. Mówiąc o kosztach wdrożenia proponowanych rozwiązań należy mieć na uwadze nie tylko budżety największych korporacji, ale także ograniczone możliwości finansowe mniejszych przedsiębiorców. Mając powyższe na uwadze wnioskujemy o wydłużenie procesu konsultacji publicznych przedmiotowego projektu o 30 dni.	
4.	IAB Polska	Uwaga ogólna	Związek Pracodawców Branży Internetowej IAB Polska pragnie wyrazić poparcie dla wniosków innych organizacji oraz we własnym imieniu zwraca się z prośbą o wydłużenie do 60 dni terminu przewidzianego na konsultacje publiczne projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (dalej „Projekt”) opublikowanego na stronach Rządowego Centrum Legislacji w dniu 24 kwietnia 2024 r.	Uwaga wyjaśniona Termin 30 dni to standardowy termin na konsultacje publiczne projektu ustawy.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. IV

			(UC32). Podzielamy opinie, że z uwagi na kompleksowość i zakres Projektu obecnie wskazany termin konsultacji może znacząco utrudnić przeprowadzenie rzetelnej i gruntownej analizy jego treści, a tym samym nie sprzyja zachowaniu właściwej jakości procesu legislacyjnego. Poza powyższymi, podobnie do wniosków innych organizacji prosimy o udostępnienie tabeli zgodności oraz odwróconej tabeli zgodności, o których mowa w §30 Regulaminu Prac Rady Ministrów, a które nie zostały opublikowane wraz z Projektem.	
5.	Krajowa Izba Gospodarcza	Uwaga ogólna	Przedstawiony przez Ministerstwo Cyfryzacji termin 30 dni na konsultacje Projektu KSC (wliczając tzw. majówkę) jest zdaniem naszym terminem zbyt krótkim by możliwe było poinformowanie i zebranie uwag od rzeszy przedsiębiorców reprezentujących wiele branż gospodarki, którzy potencjalnie mogą zostać obciążeni nowymi regulacjami, z tego względu na obecnym etapie Krajowa Izba Gospodarcza przedstawia uwagi kierunkowe do opublikowanego Projektu KSC oraz prowadzonego procesu legislacyjnego. Pragniemy podkreślić, że akt prawny o tak dużym oddziaływaniu na przedsiębiorców – zarówno organizacyjnie, jak i kosztowo, w tym poprzez ograniczanie swobody działalności – powinien zostać szeroko skonsultowany z organizacjami zrzeszającymi przedsiębiorców oraz samymi przedsiębiorcami, którzy zakwalifikowani będą jako podmioty kluczowe i ważne. Liczymy, że zgodnie z wstępnymi zapowiedziami Pana Premiera, Ministra Cyfryzacji proces legislacyjny będzie prowadzony w sposób transparentny i zapewniony zostanie dialog Ministerstwa Cyfryzacji z podmiotami zainteresowanymi, m.in. poprzez możliwość udziału w konferencji uzgodnieniowej, a także możliwość konsultacji i zgłaszania krytycznych uwag do kolejnej wersji projektu ustawy. Krajowa Izba Gospodarcza z perspektywy konieczności zapewnienia przede wszystkim stabilności funkcjonowania przedsiębiorców, zwraca uwagę na kluczowe elementy i braki w procesie legislacyjnym Projektu KSC. Izba zauważa, że zgodnie z przedstawioną Oceną Skutków Regulacji Projektodawca nie przeprowadził prawidłowej oceny proporcjonalności nakładanych w ramach aktu prawnego obciążeń oraz analizy oddziaływania nakładanych obowiązków na przedsiębiorców – w zakresie obciążenia organizacyjnego obowiązkami z zakresu zarządzania ryzykiem oraz incydentami, ale przede wszystkim w odniesieniu do możliwości zakazu wykorzystywania oraz nakazu wycofania produktów, usług i procesów ICT tzw. dostawcy wysokiego ryzyka oraz wprowadzanego polecenia zabezpieczającego. Wprowadzane regulacje sformułowane są w sposób ogólny i objąć swoimi konsekwencjami mogą kilkanaście różnych sektorów, w tym wiele podmiotów wyspecjalizowanych. Zauważamy, że Projektodawca – jako jedyny przedstawiciel unijnych państw członkowskich – bez przeprowadzenia szczegółowych analiz sektorowych i szacowania konsekwencji swoich działań dla polskiej gospodarki chce procedurą tzw. dostawcy wysokiego ryzyka objąć wszystkie sektory gospodarki. Ocena Skutków Regulacji wskazuje na to, że nie dokonano żadnych szczegółowych analiz sektorowych/podsektorowych w zakresie wprowadzanych obciążeń (Punkt 7 Oceny Skutków Regulacji „Wpływ na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców oraz na rodzinę, obywateli i	Uwaga wyjaśniona Oszacowanie skutków projektu na przedsiębiorców jest trudne z uwagi dużą liczbę, zróżnicowaną działalność przez nich prowadzoną.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. IV

			gospodarstwa domowe” Krajowa Izba Gospodarcza zwraca się z prośbą, aby Projektodawca zapewnił w ramach wprowadzanych regulacji brak dyskryminacji przedsiębiorców oraz stabilność wprowadzanych regulacji, aby uniknąć w przyszłości kosztownych procesów związanych z wdrożeniem i realizacją ustawy. Dodatkowe obawy Izby budzi brak planów Ministerstwa Cyfryzacji w zakresie dokonania notyfikacji technicznej Projektu KSC, gdy oczywistym jest, że wprowadzane przepisy mają wpływ na swobodny przepływ towarów, a inne państwa członkowskie dokonywały notyfikacji wprowadzając przepisy o mniejszych konsekwencjach i oddziałujące na węższe grupy przedsiębiorców. Niedokonanie notyfikacji technicznej również może mieć daleko idące konsekwencje gospodarcze i wprowadzić chaos prawny – jak potwierdza Ministerstwo Rozwoju i Technologii https://www.gov.pl/web/rozwoj-technologie/notyfikacja-przepisow-technicznych Krajowa Izba Gospodarcza z pewną obawą stwierdza, że przy Projekcie KSC mającym oddziaływać na kilkanaście różnych sektorów gospodarki nie zostały przeprowadzone szczegółowe analizy konsekwencji gospodarczych, a wskazywane w Ocenie Skutków Regulacji szacunki dot. przedsiębiorców, na których oddziaływać będą proponowane regulacje oparte są w większości wyłącznie na danych statystycznych, bez dokładnych analiz dokonanych przez właściwe dla tych sektorów ministerstwa lub regulatorów.	
6.	Krajowa Izba Gospodarcza	Uwaga ogólna	Krajowa Izba Gospodarcza zrzeszającą ponad 160 Izb Gospodarczych w Polsce jest największą organizacją gospodarczą w naszym kraju. Przedsiębiorcy zrzeszeni w naszych Izbach zgłaszają szereg uwag i wniosków do nowelizacji istotnej ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (implementacja dyrektywy NIS2). Przyszła znowelizowana ustawa będzie bardzo ważnym aktem prawnym szczególnie dla podmiotów związanych z techniką cyfrową i bezpieczeństwem cyfrowym społeczeństwa i organów Państwa. Przyszła ustawa będzie zawierała elementy prawa wspólnotowego, jak również będzie definiowała zasady ładu prawnego w otaczającej nas cyfrowej rzeczywistości. Ponadto przyszła ustawa ma wymiar wielowektorowy i wielowątkowy. Całość nowego aktu prawnego wymaga przede wszystkim wnikliwej i bardzo głębokiej analizy. Wyznaczony, 30-to dniowy czas na odniesienie się do przedstawionego tekstu oraz przygotowanie propozycji zmian jest w praktyce zadaniem niewykonalnym W związku z pismem DP.MC.WL.0211.16.2024, z dnia 24 kwietnia 2024 roku Krajowa izba Gospodarcza wnioskuje o przedłużenie terminu konsultacji nad nowelizacją w/w ustawy do 28 czerwca 2024r	Uwaga wyjaśniona Termin 30 dni to standardowy termin na konsultacje publiczne projektu ustawy.
7.	Federacja Przedsiębiorców Polskich	Uwaga ogólna	Działając w trosce o zapewnienie prawidłowego procesu legislacyjnego, zwracam się z uprzejmą prośbą, w ramach posiadanych przez Pana Ministra kompetencji, jako osoby odpowiedzialnej za współpracę z Unią Europejską, o spowodowanie notyfikacji technicznej TRIS projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32, dalej "Projekt Ustawy"), w zakresie dotyczącym uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, zgodnie z dyrektywą (UE) 2015/1535 Parlamentu Europejskiego i Rady z dnia 9 września 2015 r. ustanawiającą	Uwaga wyjaśniona Nie przewiduje się notyfikacji, notyfikowana może być sama decyzja o uznaniu za dostawcę wysokiego ryzyka.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. IV

			procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego ("Dyrektywa 2015/1535"). W uzasadnieniu Projektu Ustawy wskazano, że "nie zawiera [on] przepisów technicznych w rozumieniu przepisów rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. poz. 2039 oraz z 2004 r. poz. 597) i w związku z tym nie podlega procedurze notyfikacji."1 Z tym twierdzeniem nie można się zgodzić. Ja bowiem wynika z załączonej opinii prawnej autorstwa Pana Profesora Piotra Bogdanowicza przepisy art. 67c Projektu w zw. z art. 67b Projektu Ustawy mieszczą się w kategorii zakazujących przepisów technicznych, przez które należy rozumieć przepisy zakazujące produkcji, przywozu, wprowadzania do obrotu lub stosowania produktu lub zakazujące świadczenia bądź korzystania z usługi lub ustanawiania dostawcy usług, a tym samym stanowią przepisy techniczne w rozumieniu Dyrektywy 2015/1535. W związku z powyższym Projekt Ustawy podlega przekazaniu (notyfikacji) Komisji Europejskiej na podstawie art. 5 ust. 1 Dyrektywy 2015/1535. Podobne projekty przepisów uchwalone w innych państwach członkowskich (Irlandia, Hiszpania) zostały przekazane (notyfikowane) Komisji Europejskiej. Zgodnie z art. 5 ust. 1 Dyrektywy 2015/1535, państwa członkowskie są, co do zasady, obowiązane do niezwłocznego przekazania Komisji Europejskiej ("Komisja") wszelkich projektów przepisów technicznych. Jak wskazał Trybunał Sprawiedliwości Unii Europejskiej ("Trybunał" lub "TSUE"), taka notyfikacja ma na celu ochronę – za pomocą kontroli prewencyjnej – swobodnego 1 Przy czym niektóre z wcześniejszych wersji Projektu Ustawy były przewidziane do notyfikacji. 2 przepływu towarów, który jest jedną z podstaw Unii Europejskiej, a kontrola ta jest przydatna ze względu na to, iż przepisy techniczne objęte tą dyrektywą mogą stanowić przeszkody w handlu między państwami członkowskimi, które to przeszkody dopuszczalne są jedynie wówczas, gdy są one niezbędne, aby spełnić wymogi nadrzędne, których przestrzeganie leży w interesie ogólnym2. W konsekwencji, Komisja musi mieć dostęp do niezbędnych informacji przed przyjęciem przepisów technicznych3. . Wobec powyższego uprzejmie proszę o podjęcie zapewniających notyfikowanie Projektu Ustawy zgodnie z przepisami wykonującymi postanowienia Dyrektywy 2015/1535 (rozporządzenie Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych). Załącznik: Kopia opinii pana prof. UW dr. hab. Piotra Bogdanowicza z Katedry Prawa Europejskiego WPiA UW z 14 czerwca 2023 r. (zaktualizowana 5 lipca 2023 r. oraz 10 maja 2024 r.) pt. „Opinia prawna w sprawie obowiązku notyfikacji projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw w zakresie dotyczącym uznania dostawcy sprzętu lub oprogramowania za dostawę wysokiego ryzyka	
8.	Związek Pracodawców Technologii	Uwaga ogólna	Mechanizm mający na celu uzyskanie autentycznego, a nie papierowego cyberbezpieczeństwa Idea: Wykorzystanie systemu S46 dla oceny stanu na poziomie sektorowym i krajowym, a także wydawania zaleceń i rekomendacji Analiza: Potencjalna wykorzystanie i precyzyjniejszy zapis	Uwaga nieuwzględniona Przed wszystkim należy wskazać, że cytowany w uwadze art. 8 ust. 4 nie

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. IV

Cyfrowych Lewiatan		w art. 8 ust. 4 [Zakreślenie w tym miejscu], · art. 9 [Obowiązek podmiotów kluczowych i ważnych] art. 13 [informacje przekazywane przez podmioty kluczowe i ważne] art. 46 ust. 1 p 4) Propozycje zmian: Art. 8 ust. 4 Jest: 4. Podmiot kluczowy lub podmiot ważny jest zobowiązany do raportowania w systemie, o którym mowa w art. 46 ust. 1, ryzyka utraty lub obniżenia jakości świadczenia usługi. Zmiana: 4. Podmiot kluczowy lub podmiot ważny jest zobowiązany do raportowania w systemie, o którym mowa w art. 46 ust. 1, ryzyka utraty lub obniżenia jakości świadczenia usługi oraz informacji wymaganych przez krajowe lub sektorowe organy właściwe mających na celu szacowanie ryzyka na poziomie krajowym lub sektorowym. Art. 9 Dodaje się p 3) w brzmieniu: 3) przekazuje w wyznaczonym terminie do krajowych lub sektorowych organów właściwych informacje wymagane mające na celu szacowanie ryzyka na poziomie krajowym lub sektorowym. Art. 13 Dodaje się ust. 2 w brzmieniu: 2. Podmiot kluczowy i podmiot ważny jest zobowiązany w wyznaczonym terminie przekazywać do właściwego CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT sektorowego informacje wymagane dla szacowania ryzyka na poziomie krajowym lub sektorowym. Dokonuje się zmiany numeracji dwóch pozostałych ust. w tym artykule, w związku z czym ust. 3 przyjmuje brzmienie: Jest: 3. Informacje, o których mowa w ust. 1, są (...) Zmiana: 3. Informacje, o których mowa w ust. 1 i 2, są (...) Art. 46 ust. 1 p. 4) Jest: 4) szacowanie ryzyka na poziomie krajowym; Zmiana: 4) System S46 jest uniwersalnym narzędziem komunikacji pomiędzy organami właściwymi a podmiotami kluczowymi i ważnymi. Może być nie tylko narzędziem zbierania informacji o incydentach lub przekazywania zaleceń, ale także zbierania informacji mających znaczenie dla krajowego lub sektorowego bezpieczeństwa. Może to mieć charakter wyrywkowy, sektorowy, nawet terytorialny np. ograniczony do województwa. Podmioty powinny mieć obowiązek składania takich informacji w terminach wyznaczonych przez organy właściwe, ponieważ takie wymaganie znajduje się w art. 8 stąd staje się także obowiązkiem kierownika podmiotu kluczowego lub ważnego. Rozwiązanie może mieć charakter formularza w formie elektronicznej, który należy wypełnić i odesłać. Art. 13 ust. 3 gwarantuje bezpieczeństwo przekazywanych informacji. Na podstawie takich zbiorczych danych władze odpowiedzialne za cyberbezpieczeństwo mogą określić dalsze działania, w tym także działania na poziomie sektorowym lub krajowym. Będzie to także doskonały materiał do współpracy z organami właściwymi w innych krajach. Przykłady prostych zapytań i reakcji organów właściwych: Pytanie: Podać liczbę komputerów/urządzeń mobilnych wykorzystujących niewspierane systemy operacyjne. Podać liczbę komputerów/urządzeń mobilnych wykorzystujących systemy operacyjne, które przestaną być wspierane w ciągu 12 miesięcy. W zależności od zbiorczej odpowiedzi organy właściwe mogą wydać rekomendację by dokonać aktualizacji, zmienić urządzenia na nowe – w obu przypadkach z własnego budżetu	istnieje w projekcie skierowanym w konsultacji publicznych. Ponadto propozycja sugeruje dodatkowe raportowanie informacji, które nie jest wymagane przez dyrektywę NIS2.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. IV

			i we własnym zakresie, ale także może wypracować lepsze warunki aktualizacji dla całego sektora/kraju lub wykupić dodatkowy okres wsparcia u producenta.	
9.	PERN	Uwaga ogólna	Biorąc pod uwagę skalę nowych obowiązków nakładanych na adresatów projektowanej ustawy wydaje się, że przewidziane miesięczne vacatio legis jest zbyt krótkie na rzetelne wdrożenie zmian w organizacjach. Proponuje się zatem przedłużyć vacatio legis przynajmniej do 12 miesięcy.	Uwaga nieuwzględniona Termin dostosowania się do wymogów ustawy pozostał 6 miesięczny
10.	Osoba Fizyczna	Art. 2	Definitywnie niniejszy projekt krajowy UKSC, pozostaje w niezgodności semantycznej z przywoływaną definicją rozporządzenia 2019/881 art. 2 pkt 1. UKSC kładzie najsilniejszy akcent na bezpieczeństwo systemów <u>informatycznych</u> , gdzie w rzeczywistości definicja, na którą powołano się w projekcie art. 2 pkt 4 kładzie nacisk na bezpieczeństwo systemów <u>informatycznych</u> (podobnie definicje Dyrektywy 2016/1148 art. 4). Wg poprzedniej <i>Odwróconej Tabeli Zgodności UD68 (październik 2022)</i> proces taki zauważono jako proces dostosowawczy do NIS. Jednakże należy pamiętać, iż definicja wyrażona przywołanymi powyżej dyrektywami unijnymi są definicjami węższymi niż definicja krajowa. Podobnie, proponowana definicja art. 2 pkt 5 dotycząca incydentu, rozszerza znaczenie definicji art. 4 pkt 7 Dyrektywy 2016/1148. Należy rozważyć, czy krajowa legislacja, może poszerzać definicję unijną.	Uwaga wyjaśniona Definicja systemu informacyjnego wdraża definicję z NIS 2, obejmując systemy IT jak i OT.
11.	PIKE	Art. 3, art. 10 ust. 1 i in. – uwaga ogólna	W projekcie ustawy zachowano konstrukcję z obowiązującej ustawy o krajowym systemie cyberbezpieczeństwa, polegającą na tym, że w ustawie, nawet znowelizowanej projektem ustawy, jest mowa o świadczeniu usług. Np. w art. 10 ust. 1 jest mowa o tym, że „ <i>Podmiot kluczowy i podmiot ważny opracowuje, stosuje i aktualizuje dokumentację dotyczącą bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi</i> ”. Przyczyną tego stanu rzeczy jest, jak się zdaje, objęcie reżimem podobnym do reżimu regulującego dotychczas działalność operatorów usług kluczowych, podmiotów kluczowych i podmiotów ważnych. Tymczasem wśród podmiotów kluczowych i podmiotów ważnych – zarówno w dyrektywie NIS2, jak i w projekcie ustawy – mowa jest o działalności, która może polegać nie tylko na świadczeniu usług, lecz również na produkcji (produkcja, wytwarzanie i dystrybucja produktów; produkcja, przetwarzanie i dystrybucja żywności; produkcja wyrobów medycznych, wyrobów medycznych do diagnostyki in vitro; komputerów, wyrobów elektroinżynierskich i optycznych; urządzeń elektrycznych; maszyn i urządzeń, gdzie identyfikacja i klasyfikacja; pojazdów samochodowych, przysięg i itp.; pozostałego sprzętu transportowego), czy prowadzeniu badań naukowych . W związku z powyższym wszystkie przepisy w projekcie ustawy (oraz w obowiązującej ustawie o krajowym systemie cyberbezpieczeństwa, jeżeli projekt ustawy nie przewidywał dotąd ich zmiany) należy przeredagować w taki sposób, aby była w nich mowa o prowadzeniu działalności, w tym świadczenia usług – zamiast o świadczeniu usług.	Uwaga nieuwzględniona Należy odwołać się raczej do świadczenia usług. Produkcja też może być usługą w szerokim znaczeniu.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. IV

			Pytanie: Podać liczbę urządzeń/oprogramowania, które zostały uznane za produkty wysokiego ryzyka W zależności od odpowiedzi organy właściwe mogą przygotować zalecenie by usunąć takie urządzenia w jak najkrótszym czasie, ale także – o co mogą zabiegać niektóre podmioty – wprowadzić zasady rekompensaty konieczności zmiany. Pytanie: Podać liczbę osób posiadających certyfikat dla Na poziomie krajowym lub sektorowym można ocenić zapotrzebowanie na szkolenia i odpowiednio kierować zadaniami w takim zakresie. Pytanie: Wskazać technologię wykorzystywaną dla Na podstawie takiego zadania można określić czy pewne technologie mają kluczowe znaczenie w sektorze lub dla całego kraju. W wyniku uzyskania takich informacji można np. określić potrzeby supportu technicznego, zadań w ramach programu PWCyber, poleceń instalacji aktualizacji itd. Warto zauważyć, że DORA wprowadza taki mechanizm (art. 31) wskazujący, że niektórzy producenci (tzw. kluczowi) są objęci dodatkowym nadzorem ze strony Europejskich Urzędów Nadzoru. Oczywiście, na podstawie takich informacji organy właściwe mogą kierować odpowiednie zalecenia do konkretnych podmiotów kluczowych i ważnych. Zwracamy uwagę, że zapisy art. 53c projektu ustawy są właściwe dla sprawowania nadzoru i kontroli nad podmiotami nadzorowanymi, ale nie służą do celów szacowania ryzyka i zbierania informacji mających znaczenie dla krajowego lub sektorowego bezpieczeństwa. Wydaje się, że taki rozdział celów zbierania informacji będzie właściwy.	
12.	Osoba fizyczna	Art. 2	Propozycje zapisów do zawarcia w nowej ustawie o krajowym systemie cyberbezpieczeństwa Art. 2. Definicje: Incydent cybernetyczny - każde niepożądane zdarzenie lub okoliczność związane z bezpieczeństwem sieci i systemów informatycznych, które mają lub mogą mieć negatywny wpływ na integralność, poufność, dostępność lub autentyczność danych, usług lub systemów informatycznych. Incydenty cybernetyczne klasyfikuje się według skali na następujące kategorie: 1. Incydenty niskiej skali: Zdarzenia mające minimalny wpływ na działalność organizacji, które nie powodują przerwania krytycznych usług ani utraty danych i mogą być rozwiązane w krótkim czasie przez wewnętrzny zespół IT. <i>(Niewielkie próby phishingu, które zostały zidentyfikowane i zablokowane, Błędy konfiguracyjne, które nie wpływają na dostępność lub bezpieczeństwo danych, Oprogramowanie malware wykryte i usunięte przez systemy antywirusowe bez wpływu na działalność organizacji)</i> 2. Incydenty średniej skali: Zdarzenia mające umiarkowany wpływ na działalność organizacji, mogące powodować przerwy w dostępności niektórych usług lub danych, ale nie wpływające na krytyczne operacje. Wymagają interwencji specjalistów IT oraz mogą wiązać się z koniecznością wdrożenia dodatkowych środków zaradczych <i>(Atak DDoS, który powoduje tymczasową niedostępność niektórych usług online, Utrata danych z jednego działu organizacji)</i>	Uwaga nieuwzględniona Zarówno obecna ustawa jak i projekt definiują różne poziomy incydentów.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do *projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw* (UC32) cz. IV

			spowodowana błędem systemowym, Wykrycie nieautoryzowanego dostępu do niewrażliwych danych, które nie powoduje znaczących szkód) 3. Incydenty wysokiej skali: Zdarzenia mające poważny wpływ na działalność organizacji, powodujące przerwanie krytycznych usług, utratę lub kradzież wrażliwych danych. Wymagają natychmiastowej reakcji i mogą wiązać się z koniecznością powiadomienia odpowiednich organów nadzoru (<i>Masowy wyciek danych osobowych klientów, Poważne naruszenie zabezpieczeń, które prowadzi do przerwania działalności operacyjnej, Atak ransomware, który zaszyfrował krytyczne dane i wymaga specjalistycznej interwencji w celu ich odzyskania</i>).	
13.	PERN	Art. 2	Art. 1 pkt 2 lit. i (art. 2 pkt 11 ustawy) – jak wynika z informacji CSIRT Ministerstwa Obrony Narodowej podatność jest definiowana, jako usterka w oprogramowaniu lub komponencie usługi, która może zostać wykorzystana na szkodę. W związku z powyższym definicji podatności proponuje się nadać następujące brzmienie: „i) podatność – cechy produktu ICT lub usługi ICT, które mogą być wykorzystane przez przestępców do groźby”;	Uwaga nieuwzględniona Obecnie brzmienie trafniej wdraża pojęcie z dyrektywy NIS2
14.	PERN	Art. 2	Art. 1 pkt 2 lit. j (art. 2 pkt 11a ustawy) – w celu wyeliminowania wątpliwości interpretacyjnych proponuje się w definicji platformy sieci usług społecznościowych doprecyzować, że wymiary, udostępni i odkrywa treści są równe do treści publiczne;	Uwaga nieuwzględniona W przypadku zamkniętych grup na portalach społecznościowych treści nie są wymieniane publicznie.
15.	Forum Przewoźników Ekspresowych	Art. 5	Pierwsza wątpliwość pojawia się na etapie interpretacji definicji legalnych podmiotu kluczowego oraz podmiotu ważnego (art. 1 pkt 8 ustawy nowelizującej). Zgodnie z zaproponowaną treścią definicji podmiotu kluczowego może być nim między innymi podmiot wskazany w załącznikach nr 1 i nr 2 do ustawy nowelizującej, który przewyższa wymogi dla średniego przedsiębiorstwa określone w art. 2 ust. 1 załącznika I do rozporządzenia Komisji (UE) nr 651/2014 z dnia 17 czerwca 2014 r. uznającego niektóre rodzaje pomocy za zgodne z rynkiem wewnętrznym w zastosowaniu art. 107 i 108 Traktatu (Dz. Urz. UE L 187 z 26.06.2014, str. 1) (dalej jako: „rozporządzenie 651/2014/UE”). Użycie spójnika „i” (konjunkcji) prowadzi do wniosku, że podmiotem kluczowym jest wyłącznie podmiot wskazany w załączniku nr 1 jak i w załączniku nr 2. A contrario – jeżeli podmiot nie został uwzględniony w załączniku nr 1 to nie uzyska statusu podmiotu kluczowego choćby znalazł się w wykazie stanowiącym załącznik nr 2 i spełniał pozostałe wymogi ustawowe, oraz na odwrót. Sytuacja, gdy podmiot wpisany jest jednocześnie do obu załączników jest niemożliwa do wyobrażenia, albowiem zakres obu załączników nie pokrywa się, a w każdym załączniku znajdują się podmioty innego sektora gospodarki.	Uwaga uwzględniona Usunięte zostanie odwołanie do zał. 2.
16.	Forum Przewoźników Ekspresowych	Art. 5	W ocenie FPE wątpliwości budzi również sposób kwalifikowania podmiotów wskazanych w załącznikach nr 1 lub nr 2 z uwagi na spełnienie lub odpowiednio przewyższenie wymogów dla średniego przedsiębiorstwa określonych w art. 2 ust. 1 załącznika I do rozporządzenia 651/2014/UE. Precyzując, w świetle art. 1 pkt 8 ustawy nowelizującej niejasne jest czy operator	Uwaga wyjaśniona Operator pocztowy będzie podmiotem ważnym, jeżeli spełnia kryteria wielkościowe.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. IV

			pocztowy, który przewyższy ww. wymogi uzyskuje status podmiotu kluczowego czy nadal pozostaje podmiotem ważnym wskazanym w załączniku nr 2 do ustawy nowelizującej?	
17.	PIKE	Art. 5 ust. 1 pkt 2 lit. f	Zgodnie z omawianym przepisem podmiotem kluczowym może być podmiot zidentyfikowany jako podmiot kluczowy na podstawie art. 7c ust. 2 pkt 1. Tymczasem art. 7c ust. 2 pkt 1 stanowi „2. Podmiot uznaje się za: 1) podmiot kluczowy, jeżeli prowadzi działalność określoną w <i>załączniku nr 1 do ustawy</i>”; Taka treść art. 7c ust. 2 pkt 1 powoduje, że cały art. 5 ust. 1 i art. 7c ust. 1 staje się niepotrzebnym <i>superfluum</i>. Wydaje się, że art. 5 ust. 1 pkt 2 lit. f oraz art. 7c miały służyć wdrożeniu art. 2 ust. 2 lit. b-f oraz art. 3 ust. 1 lit. e dyrektywy NIS2. W takim przypadku art. 7c ust. 2 należałoby wykreślić, a odesłanie w art. 5 ust. 1 pkt 2 lit. f powinno dotyczyć art. 7c ust. 1. „Art. 5. 1. Podmiotem kluczowym jest: [...] f) podmiot zidentyfikowany jako podmiot kluczowy na podstawie art. 7c ust. ~~1 2 pkt 1~~,” Art. 7c ust. 2 należy wykreślić.	Uwaga nieuwzględniona Przepis ten jest konieczny i nie może zostać usunięty z projektu.
18.	PIKE	Art. 5 ust. 2 pkt 4	Zgodnie z omawianym przepisem podmiotem ważnym może być podmiot zidentyfikowany jako podmiot kluczowy na podstawie art. 7c ust. 2 pkt 2. Tymczasem art. 7c ust. 2 pkt 2 stanowi „2. Podmiot uznaje się za: [...] 2) podmiot ważny, jeżeli prowadzi działalność określoną w <i>załączniku nr 2 do ustawy</i>”; Taka treść art. 7c ust. 2 pkt 2 powoduje, że cały art. 5 ust. 1 i art. 7c ust. 1 staje się niepotrzebnym <i>superfluum</i>. Wydaje się, że art. 5 ust. 2 pkt 4 oraz art. 7c miały służyć wdrożeniu art. 2 ust. 2 lit. b-f oraz art. 3 ust. 1 lit. e dyrektywy NIS2. W takim przypadku art. 7c ust. 2 należałoby wykreślić, a odesłanie w art. 5 ust. 2 pkt 4 powinno dotyczyć art. 7c ust. 1. „Art. 5. 2. Podmiotem kluczowym jest: [...] f) podmiot zidentyfikowany jako podmiot kluczowy na podstawie art. 7c ust. ~~1 2 pkt 1~~,” Art. 7c ust. 2 należy wykreślić.	Uwaga nieuwzględniona Przepis ten jest konieczny i nie może zostać usunięty z projektu
19.	Technomed	Art. 5	Analiza art. 1 pkt 8) projektu ustawy, a dotyczącego modyfikacji art. 5 zmienianej ustawy prowadzi do konkluzji, iż katalog podmiotów kluczowych oraz ważnych został uregulowany odmiennie od tego przyjętego w treści art. 3 dyrektywy NIS 2. Jak wynika z propozycji ustawodawcy krajowego: Przez podmiot kluczowy należy rozumieć m.in. • osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej wskazaną w załączniku nr 1 i nr 2 do ustawy, która przewyższa wymogi dla średniego przedsiębiorstwa określone w art. 2 ust. 1 <i>załącznika I do rozporządzenia 651/2014/UE</i>; Przez podmiot ważny należy rozumieć m.in. • osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej wskazaną w załączniku nr 1 i nr 2 do ustawy, która spełnia	Uwaga uwzględniona Odwwołanie do zał. nr 2 zostanie usunięte z przepisu.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. IV

			wymogi dla średniego przedsiębiorstwa określone w rozporządzeniu 651/2014/UE, oraz która jest podmiotem kluczowym; Mającą na uwadze powyższe należy przyjąć w pierwszej kolejności, że a) Nazewnictwo załączników jako odpowiednio PODMIOTY KLUCZOWE (Załącznik I) i PODMIOTY WAŻNE (Załącznik II) traci rację bytu, a to z tego względu, że kryterium rozróżniające stanowi rozmiar podmiotu, nie zaś sektor lub podsektor, w którym działa; b) Podmiot różni się od tego proponowanego w art. 3 dyrektywy NIS 2, zgodnie z którym za podmiot kluczowy rozumie się podmiot, który kumulatywnie: i) przekracza pułap dla średniego przedsiębiorcy ii) prowadzi działalność wskazaną w załączniku I do dyrektywy NIS 2 („Do celów niniejszej dyrektywy następujące podmioty uznaje się za podmioty kluczowe: podmiot w rodzaju tych, o których mowa w załączniku I, przekraczający pułapy dla średnich przedsiębiorstw, określone w art. 2 ust. 1 załącznika do zlecenia 2003/361/WE”). W związku z powyższym proponujemy dokonanie modyfikacji art. 1 pkt 8) w ten sposób, że: art. 5 w ust. 1 pkt 1) otrzymuje brzmienie: • „osoba fizyczna, osoba prawna albo jednostka organizacyjna nieposiadająca osobowości prawnej wskazana w załączniku nr 1 do ustawy, która przewyższa wymogi dla średniego przedsiębiorstwa określone w art. 2 ust. 1 załącznika I do rozporządzenia Komisji (UE) nr 651/2014 z dnia 17 czerwca 2014 r. uznającego niektóre rodzaje pomocy za zgodne z rynkiem wewnętrznym w zastosowaniu art. 107 i 108 Traktatu (Dz. Urz. UE L 187 z 26.06.2014, str. 1), którego dla „rozporządzenia 651/2014/UE;” Art. 5 ust. 2 pkt 1) otrzymuje brzmienie: • „osoba fizyczna, osoba prawna albo jednostka organizacyjna nieposiadająca osobowości prawnej wskazana w załączniku nr 2 do ustawy, która spełnia wymogi dla średniego Organizacja Pracodawców Przemysłu Medycznego TECHNOMED ul. Stefana Czarnieckiego 21/23 lok. 1, 01 -548 Warszawa; telefon: +48 734 718 742; e-mail: biuro@technomed.org.pl; www.technomed.org.pl przedsiębiorcy określono w rozporządzeniu 651/2014/UE oraz która nie jest podmiotem kluczowym”.	
20.	Technomed	Art. 5	Zgodnie z brzmieniem dyrektywy NIS 2, do podmiotów kluczowych z rynku wyrobów medycznych (załącznik nr I, sektory kluczowe, pkt 5 tiret 5) należy zaliczyć: - „podmioty produkujące wyroby medyczne uznane za mające krytyczne znaczenie podczas danego stanu zagrożenia zdrowia publicznego ("wykaz wyrobów medycznych o krytycznym znaczeniu w przypadku stanu zagrożenia zdrowia publicznego") w rozumieniu art. 22 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/123” Natomiast do podmiotów ważnych (załącznik nr II, sektory ważne, pkt 5 lit. a) dyrektywa NIS 2 zaliczyła: - „podmioty produkujące wyroby medyczne zdefiniowane w art. 2 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2017/745 oraz podmioty produkujące wyroby medyczne do diagnostyki in vitro zdefiniowane w art. 2 ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2017/746, z wyjątkiem podmiotów produkujących wyroby medyczne wymienione w załączniku I pkt 5 tiret piąte niniejszej dyrektywy” W projekcie ustawy jednak znacznie rozszerzono zakres podmiotów uznanych za kluczowe z branży wyrobów medycznych, przez uwzględnienie w	Uwaga uwzględniona Sektory krytyczne i ważne zostaną ukształtowane zgodnie z dyrektywą NIS2.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. IV

			załączniku nr 1 do ustawy, w którym wymienione są podmioty kluczowe: w kategorii „Ochrona zdrowia”: - „Podmioty produkujące wyroby medyczne uznane za mające krytyczne znaczenie podczas danego stanu zagrożenia zdrowia publicznego („wykaz wyrobów medycznych o krytycznym znaczeniu w przypadku stanu zagrożenia zdrowia publicznego”) w rozumieniu art. 22 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/123.” w kategorii „Produkcja”: - „Podmioty produkujące wyroby medyczne w rozumieniu art. 2 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2017/745”; - „Podmioty produkujące wyroby medyczne do diagnostyki in vitro w rozumieniu art. 2 ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2017/746, z wyjątkiem podmiotów produkujących wyroby medyczne uznane za mające krytyczne znaczenie podczas danego stanu zagrożenia zdrowia publicznego”. Takie rozszerzenie katalogu podmiotów kluczowych nie znajduje uzasadnienia. Założeniem dyrektywy przy tworzeniu katalogu podmiotów kluczowych i ważnych było z jednej strony dookreślenie odbiorców określonych obowiązków w zakresie cyberbezpieczeństwa, z drugiej natomiast ujednolicenie na terenie całej UE katalogu podmiotów, które mają być uznane za kluczowe, a które za ważne. Organizacja Pracodawców Przemysłu Medycznego TECHNOMED ul. Stefana Czarnieckiego 21/23 lok. 1, 01 -548 Warszawa, tel. +48 734 718 742; e-mail: biuro@technomed.org.pl; www.technomed.org.pl Dodatkowo, zgodnie z dyrektywą NIS 2, wszystkie Państwa członkowskie powinny poinformować Komisję Europejską co najmniej o liczbie podmiotów kluczowych i ważnych dla każdego sektora i podsektora, o których mowa w załącznikach. Biorąc pod uwagę, że kategoria „produkcja” i podmioty z rynku wyrobów medycznych w projekcie ustawy zostały uznane za kluczowe, a dyrektywa uznaje je za ważne, pojawiać się będą rozbieżności w podejściu poszczególnych państw co może rodzić problemy praktyczne. Zachowanie jednolitości w podejściu wynika także z założenia, że Komisja wyda wytyczne dla krajów członkowskich, aby wiedziały, jak należy klasyfikować podmioty o złożonych modelach biznesowych lub środowiskach operacyjnych, co pozwoli na zachowanie jednolitego podejścia przez wszystkie kraje członkowskie i jednolitego podejścia do klasyfikacji podmiotów na kluczowe i ważne. Jednocześnie zauważa się, że uznanie wszystkich podmiotów produkujących wyroby medyczne za podmioty kluczowe, a co za tym idzie możliwość nakładania na nie kar, jak w zmienianym art. 73 ust. 3 projektu ustawy, czy też prowadzenia czynności nadzorczych zarówno ex post jak i ex ante wydaje się pozostawać w sprzeczności z zasadą proporcjonalności projektowanych zmian. Postulujemy o nierozszerzanie zakresu stosowania ustawy i zmianę w nadanych dla podmiotów z rynku wyrobów medycznych klasyfikacji podmiotów jako kluczowe i ważne, zgodnie z brzmieniem dyrektywy.	
21.	Technomed	Art. 7	Finalnie, zwracamy się z prośbą o wydłużenie terminu przewidzianego w art. 7 ust. 3 zmienianej ustawy, a dotyczącego złożenia wniosku o wpis w wykazie podmiotów kluczowych lub ważnych (2 miesiące). Aktualnie przewidziany przez ustawodawcę termin, w konfrontacji z treścią art. 15 („Minister właściwy do spraw informatyzacji uruchomi wykaz podmiotów	Uwaga nieuwzględniona Zawarty w ustawie termin wynika z nałożonego na państwa członkowskie obowiązku przekazania Komisji

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. IV

			kluczowych i podmiotów ważnych, w terminie miesiąca od dnia wejścia w życie niniejszej ustawy.”) daje podmiotom realnie 1 miesiąc na dokonanie stosownego wpisu. Mając na uwadze powyższe zasadnym jest postulat wydłużenia terminu na dokonanie wpisu do 3 miesięcy.	Europejskiej list podmiotów ważnych i kluczowych do 17 kwietnia 2025 roku.
22.	PIKE	Art. 7 ust. 15 (powiązane z propozycją dodania ust. 1 ¹ do art. 11)	W przypadku każdego podmiotu i kluczowego będzie istniał obowiązek zgłoszenia incydentu poważnego do właściwego CSIRT sektorowego, przekazanie CSIRT sektorowemu sprawozdania okresowego z obsługi incydentu poważnego oraz sprawozdania końcowego z obsługi incydentu poważnego. CSIRT sektorowy może zostać ustanowiony dla jednego sektora lub podsektora. Wśród przedsiębiorców telekomunikacyjnych dość często występuje sytuacja, gdy świadczą oni nie tylko usługi telekomunikacyjne, lecz również usługi takie jak np. DNS, usługi chmurowe, a czasami usługi przyporządkowane pod całkiem inny sektor. W związku z tym, dla sprawności działania podmiotów kluczowych i ważnych, w szczególności dla sprawności obsługi incydentów poważnych, istotne jest, aby tylko jeden CSIRT sektorowy był właściwych dla jednego podmiotu kluczowego lub ważnego, szczególnie wówczas, gdy taki podmiot prowadzi działalność w więcej niż jednym sektorze lub podsektorze. Art. 7 15. Minister właściwy do spraw informatyzacji przesyła na adres do doręczeń elektronicznych albo na adres poczty elektronicznej zaświadczenie o wpisie podmiotu do wykazu, zmianie wpisu albo jego wykreśleniu. <u>W zaświadczeniu wskazuje się jeden CSIRT sektorowy właściwy dla danego podmiotu.</u>	Uwaga wyjaśniona Z całą pewnością wystąpi multisektorowość – i wtedy właściwe będą różne CSIRT które będą musiały wypracować wspólne procedury postępowania w takich działaniach.
23.	PIKE	Art. 7b ust. 2	Art. 7b ust. 2 stanowi, że „W przypadku stwierdzenia, że dane w wykazie [podmiotów kluczowych i podmiotów ważnych – wstawienie moje] są niezgodne ze stanem faktycznym organ właściwy do spraw cyberbezpieczeństwa wzywa podmiot do zmiany wpisu do wykazu w terminie 7 dni od doręczenia wezwania, pod rygorem nałożenia kary pieniężnej. Zawiadomienie przekazuje się na adres do doręczeń elektronicznych podmiotu”. Zdaniem PIKE, podobnie jak w przypadku wpisania do wykazu podmiotów kluczowych i podmiotów ważnych (art. 7a ust. 4), jak i w przypadku odmowy (art. 7b ust. 3) wykreślenia z tego wykazu, podmiotowi kluczowemu i podmiotowi ważnemu powinno przysługiwać prawo skargi do sądu administracyjnego. Art. 7b [...] 2. W przypadku stwierdzenia, że dane w wykazie są niezgodne ze stanem faktycznym organ właściwy do spraw cyberbezpieczeństwa wzywa podmiot do zmiany wpisu do wykazu w terminie 7 dni od doręczenia wezwania, pod rygorem nałożenia kary pieniężnej. Zawiadomienie przekazuje się na adres do doręczeń elektronicznych podmiotu. <u>Zawiadomienie jest inną czynnością z zakresu administracji publicznej, na którą przysługuje skarga do sądu administracyjnego.</u>	Uwaga uwzględniona

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. IV

24.	PIKE	Art. 7b ust. 4 (dodanie nowego ust. 4a)	Podobnie, jak w przypadku art. 7b ust. 2, także w przypadku art. 7b ust. 4 podmiotowi kluczowemu i podmiotowi ważnemu powinno przysługiwać prawo wniesienia skargi do sądu administracyjnego. Wykreślenie podmiotu z rejestru podmiotów kluczowych lub podmiotów ważnych może być, w niektórych sytuacjach, wbrew interesom takiego podmiotu. Art. 7b [...] <u>4a. Wykreślenie na podstawie ust. 4 z wykazu, o którym mowa w art. 7 ust. 1, jest inną czynnością z zakresu administracji publicznej, na którą przysługuje skarga do sądu administracyjnego.</u>	Uwaga uwzględniona
25.	PIKE	Art. 7c ust. 6 (uwaga powiązana z uwagą do art. 15 ust. 1 i art. 16)	I. Zbyt krótkie terminy Zgodnie z tym przepisem podmiot, który został wyznaczony jako podmiot kluczowy lub ważny na podstawie decyzji, o której mowa w art. 7c ust. 1, realizuje obowiązki, o których mowa w rozdziale 3, w terminie 6 miesięcy oraz zapewnia przeprowadzenie audytu, o którym mowa w art. 15 ust. 1 w terminie 12 miesięcy. Terminy są analogiczne w przypadku podmiotów, które uznaje się za podmioty kluczowe lub ważne bezpośrednio na podstawie przepisów ustawy. Termin 6 miesięcy to termin zbyt krótki dla wielu podmiotów kluczowych i ważnych, przede wszystkim dla tych podmiotów, które nie uzyskały certyfikatu zgodności z normą ISO 27001 i ISO 22301. Niezależnie od dalszych uwag PIKE w zakresie ww. norm (regulacje w tych normach powinny stanowić punkt odniesienia, lecz nie być bezwzględnie wiążące – o czym będzie mowa w uwadze dot. art. 10 ust. 1 pkt 1 3), należy podkreślić, że rzetelne wdrożenie obowiązków określonych w projekcie ustawy wymaga konsultacji z podmiotem, który ma doświadczenie w tworzeniu systemu zarządzania bezpieczeństwem informacji, aby następnie realistyczne było uzyskanie pozytywnego wyniku audytu. Z kolei audyt będzie mógł być przeprowadzony przez podmioty spełniające wymogi określone w art. 16 ust. 2-3. <u>Takich podmiotów na rynku jest ograniczona liczba, a w krótkim czasie zgłosi się do nich po konsultacje ponad 38 000 nowych klientów. Z pewnością ani w ciągu pół roku, ani nawet roku (w kontekście potrzeby przeprowadzenia audytu w podmiotach kluczowych i ważnych) polski rynek nie będzie w stanie zaspokoić nagłego wzrostu popytu ani na konsultacje w związku z wdrażaniem systemów zarządzania bezpieczeństwem informacji czy ciągłością działania, ani na przeprowadzenie audytów w tym zakresie.</u> II. Nadregulacja – regularne audyty bezpieczeństwa oraz brak różnicy pomiędzy podmiotami kluczowymi i ważnymi Omawiany przepis zakłada przeprowadzenie audytu, o którym mowa w art. 15 ust. 1, nie tylko przez podmioty kluczowe, lecz również przez podmioty ważne, co w sposób oczywisty wykracza poza obowiązki przewidziane w tej dyrektywie: w art. 32 ust. 2 lit. b dyrektywy NIS2 mowa jest o możliwości objęcia podmiotów kluczowych „regularnymi ukierunkowanymi audytami bezpieczeństwa prowadzonymi przez niezależną instytucję lub właściwy organ”.	Uwaga częściowo uwzględniona Terminy na przeprowadzenie audytów zostaną wydłużone

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. IV

			Odpowiednika takiej regulacji nie ma w art. 33 dyrektywy NIS2, który dotyczy podmiotów ważnych. Co więcej, zgodnie z art. 32 ust. 2 lit. b dyrektywy NIS2, to właściwe organy powinny być były uprawnione do objęcia podmiotów kluczowych regularnymi ukierunkowanymi audytami bezpieczeństwa. Projekt ustawy zakłada jednak, że to nie organ będzie decydował, w których przypadkach takie regularne audyty będą zasadne, lecz z góry przesądza się w projekcie ustawy, że regularny audyt bezpieczeństwa będą musiały prowadzić wszystkie podmioty kluczowe i ważne, niezależnie od tego, czy jest to zasadne w przypadku danego podmiotu, czy też nie. Tak ukształtowany obowiązek jest nie tylko wyraźnie nadmiernym obciążeniem przedsiębiorców i traktowanie różnych sytuacji jednakową miarą (<u>zatem obowiązek jest sprzeczny z zasadą proporcjonalności</u>), lecz również – ze względu na ograniczony krąg osób uprawnionych do prowadzenia audytów – <u>całkowicie nierealny do przeprowadzenia w określonym terminie, ze względu na ograniczoną podaż, o czym była mowa powyżej.</u> III. Sytuacja podmiotów, które zostały objęte reżimem ustawy w drodze innej niż z mocy prawa lub na podstawie decyzji, o której mowa w art. 7 ust. 1 Z takimi podmiotami mamy do czynienia w przypadku, gdy podmiot zostanie wpisany na podstawie art. 7a ust. 1 do wykazu, o którym mowa w art. 7 ust. 1. W takim przypadku podmiot powinien mieć odpowiedni czas na wdrożenie obowiązków wynikających z ustawy. Art. 7c [...] 6. Podmiot, wobec którego wydano decyzję <u>o uznaniu go za podmiot kluczowy</u>, o której mowa w ust. 1: 1) realizuje obowiązki, o których mowa w rozdziale 3, w terminie <u>12 6</u>-miesięcy, 2) zapewnia przeprowadzenie audytu, o którym mowa w art. 15 ust. 1, <u>jeżeli zostanie do tego zobowiązany w drodze decyzji przez organ właściwy do spraw cyberbezpieczeństwa, przy czym taka decyzja nie może zostać wydana wcześniej niż</u> w terminie 12 miesięcy – od dnia doręczenia tej decyzji. <u>6a. Podmiot, który na podstawie art. 7a ust. 1 zostanie wpisany do wykazu, o którym mowa w art. 7 ust. 1:</u> <u>1) realizuje obowiązki, o których mowa w rozdziale 3, w terminie 12 miesięcy,</u> <u>2) zapewnia przeprowadzenie audytu, o którym mowa w art. 15 ust. 1, jeżeli zostanie do tego zobowiązany w drodze decyzji przez organ właściwy do spraw cyberbezpieczeństwa, przy czym taka decyzja nie może zostać wydana wcześniej niż w terminie 12 miesięcy</u> <u>- od dnia doręczenia zawiadomienia, o którym mowa w art. 7a ust. 3.</u>	

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. IV

			Alternatywnie, na wypadek nie uwzględnienia powyższej uwagi, proponujemy alternatywne brzmienie ust. 6 oraz dodanie ust. 6a i 6b: Art. 7c [...] 6. Podmiot, wobec którego wydano decyzję <u>o uznaniu go za podmiot kluczowy</u>, o której mowa w ust. 1: 1) realizuje obowiązki, o których mowa w rozdziale 3, w terminie <u>12 6</u> miesięcy, 2) zapewnia przeprowadzenie audytu, o którym mowa w art. 15 ust. 1, w terminie <u>12 24</u> miesięcy – od dnia doręczenia tej decyzji. <u>6a. Uznaje się, że podmiot kluczowy nie naruszył art. 7c ust. 6 pkt 2 jeżeli do przeprowadzenia audytu dojdzie w terminie późniejszym, lecz podmiot kluczowy wykaże, że zachował należyta staranność w toku aktywnego poszukiwania audytora, spełniającego przesłanki określonego w art. 15 ust. 2-3.</u> <u>6b. Podmiot, który na podstawie art. 7a ust. 1 zostanie wpisany do wykazu, o którym mowa w art. 7 ust. 1:</u> <u>1) realizuje obowiązki, o których mowa w rozdziale 3, w terminie 12 miesięcy,</u> <u>2) zapewnia przeprowadzenie audytu, o którym mowa w art. 15 ust. 1, w terminie 24 miesięcy - od dnia doręczenia zawiadomienia, o którym mowa w art. 7a ust. 3.</u> <u>Ustęp 6a stosuje się odpowiednio.</u>	
26.	Osoba fizyczna	Art. 7d	Art. 7 d. Obowiązki podmiotów: Podmioty, które są częścią krajowego systemu cyberbezpieczeństwa, są zobowiązane do: 1) monitorowania swoich systemów informatycznych w celu wykrywania i reagowania na incydenty cybernetyczne, 2) raportowania incydentów do odpowiednich CSIRT-ów sektorowych w terminach określonych w niniejszej ustawie, 3) udziału w krajowych i międzynarodowych mechanizmach wymiany informacji o zagrożeniach i incydentach cybernetycznych, 4) wdrożenia środków zapobiegawczych i naprawczych w celu minimalizacji ryzyka cybernetycznego.	Uwaga wyjaśniona Wskazywane kwestie są już zawarte w innych przepisach projektu.
27.	Osoba fizyczna	Art. 8	Art. 8. System zarządzania bezpieczeństwem informacji Podmiot kluczowy lub podmiot ważny wdraża system zarządzania bezpieczeństwem informacji w procesach wpływających na świadczenie usług przez ten podmiot, zapewniający:	Uwaga nieuwzględniona Projekt już zawiera przepisy o SZBI.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. IV

			Prowadzenie systematycznego szacowania ryzyka wystąpienia incydentu oraz zarządzanie tym ryzykiem; Wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, uwzględniających najnowszy stan wiedzy, koszty wdrożenia, wielkość podmiotu, prawdopodobieństwo wystąpienia incydentów, narażenie podmiotu na ryzyka, w szczególności: - Polityki szacowania ryzyka oraz bezpieczeństwa systemu informacyjnego w tym polityki tematyczne, - Utrzymanie i bezpieczną eksploatację systemu informacyjnego w tym: Procedury Audytów i Przeglądów Bezpieczeństwa, - Bezpieczeństwo fizyczne i środowiskowe, uwzględniające kontrolę dostępu, - Bezpieczeństwo i ciągłość łańcucha dostaw produktów ICT, usług ICT i procesów ICT, od których zależy świadczenie usługi, z uwzględnieniem związków pomiędzy dostawcą sprzętu lub oprogramowania a podmiotem kluczowym lub podmiotem ważnym, w tym: Procedury Zarządzania Dostawcami i Partnerami, - Wdrażanie, dokumentowanie i utrzymywanie planów działania umożliwiających ciągłe i niezakłócone świadczenie usługi oraz zapewniających poufność, integralność, dostępność i autentyczność informacji, oraz planów awaryjnych umożliwiających odtworzenie systemu informacyjnego po katastrofie, z regularnymi testami tych planów, w tym: Procedury Zarządzania Kontynuacją Działalności i Odzyskiwania Danych po Awarii, - Objęcie systemu informacyjnego wykorzystywanego do świadczenia usługi systemem monitorowania w trybie ciągłym, w tym automatyczne wykrywanie i powiadamianie o anomaliach i zagrożeniach, w tym: Procedury Przetwarzania Logów i Monitoringu, - Polityki i procedury oceny skuteczności środków technicznych i organizacyjnych, w tym: Procedury Zarządzania Zmianami w Systemach IT, - Edukację z zakresu cyberbezpieczeństwa dla personelu podmiotu, w tym podstawowe zasady cyberhigieny, specjalistyczne szkolenia dla personelu IT oraz kampanie podnoszące świadomość, w tym: - Procedury Szkoleniowe i Podnoszenia Świadomości, - Polityki i procedury stosowania kryptografii, w tym szyfrowania danych w spoczynku i w transporcie oraz zarządzania kluczami kryptograficznymi; Zbiórki informacji o cyberzagrożeniach i podatnościach na incydenty systemu informacyjnego wykorzystywanego do świadczenia usługi; - Zarządzanie incydentami, w tym opracowanie i wdrożenie procedur reagowania na incydenty, ich analizę, dokumentowanie oraz podejmowanie działań naprawczych i zapobiegawczych, w tym: Procedury raportowania incydentów, - Procedury Zarządzania Incydentami;	

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. IV

			- Stosowanie środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego wykorzystywanego do świadczenia usługi w tym: Stosowanie mechanizmów zapewniających poufność, integralność, dostępność i autentyczność danych przetwarzanych w systemie informacyjnym, - Regularne przeprowadzanie aktualizacji oprogramowania, stosownie do zaleceń producenta, z uwzględnieniem analizy wpływu aktualizacji na bezpieczeństwo świadczonej usługi oraz poziomu krytyczności poszczególnych aktualizacji, z minimalizacją przerw w świadczeniu usług, - Ochronę przed nieuprawnioną modyfikacją w systemie informacyjnym w tym stosowanie mechanizmów kontroli dostępu oraz rejestrowanie i monitorowanie działań użytkowników, - Niwelowanie podjęmów i działań po dostrzeżeniu lub wybrzeżeniu; - Stosowanie bezpiecznych środków komunikacji elektronicznej w ramach krajowego systemu cyberbezpieczeństwa, uwzględniających uwierzytelnianie wieloskładnikowe oraz bezpieczne protokoły komunikacyjne (p. TL/LL); - Istotowe procedury i doświadczenia, w tym: Procedury Zarządzania Dostępem; - Istotowe procedury ochrony danych w tym: Procedury Ochrony Danych; - Raportowanie i komunikacja z organami nadzoru, w tym: Procedury Raportowania i Komunikacji z Organami Nadzoru.	
28.	PIKE	Art. 8 ust. 1 pkt 2 lit. a	Zgodnie z tym przepisem podmiot kluczowy lub podmiot ważny wdraża system zarządzania bezpieczeństwem informacji w procesach wpływających na świadczenie usług przez ten podmiot, zapewniający wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, uwzględniających najnowszy stan wiedzy, koszty wdrożenia, wielkość podmiotu, prawdopodobieństwo wystąpienia incydentów, narażenie podmiotu na ryzyka, w szczególności polityki szacowania ryzyka oraz bezpieczeństwa systemu informacyjnego, w tym polityki tematyczne. Z przepisu tego wynika obowiązek stworzenia polityk tematycznych. Wydaje się, że obowiązek stworzenia polityk tematycznych jest nadmiarowy, nie w przypadku wszystkich podmiotów kluczowych i podmiotów ważnych zasadne byłoby obowiązkowe określenie polityk tematycznych. Art. 8. 1. Podmiot kluczowy lub podmiot ważny wdraża system zarządzania bezpieczeństwem informacji w procesach wpływających na świadczenie usług przez ten podmiot, zapewniający: [...] 2) wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, uwzględniających najnowszy stan wiedzy, koszty wdrożenia, wielkość podmiotu, prawdopodobieństwo wystąpienia incydentów, narażenie podmiotu na ryzyka, w szczególności: a) polityki szacowania ryzyka oraz bezpieczeństwa systemu informacyjnego, w tym, <u>jeżeli to będzie zasadne, w szczególności ze względu na działalność danego podmiotu w więcej niż jednym sektorze</u>, polityki tematyczne,	Uwaga wyjaśniona Polityki tematyczne mają być tworzone proporcjonalnie, czyli wtedy kiedy podmiot uzna to za stosowne.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. IV

29.	PIKE	Art. 8 ust. 1 pkt 2 lit. d	Wiele podmiotów kluczowych i ważnych nie ma wpływu na procesy ICT i nie ma wiedzy o procesach ICT w podmiotach, od których nabywa produkty ICT i usługi ICT [„proces ICT” oznacza zestaw czynności wykonywanych w celu projektowania, rozwijania, dostarczania lub utrzymywania produktów ICT lub usług ICT]. PIKE postuluje doprecyzowanie przepisu w taki sposób, aby zawrzeć w nim odniesienie do związków bezpośrednich pomiędzy podmiotami, aby nie dawać możliwości interpretacji rozszerzającej Art. 8. 1. Podmiot kluczowy lub podmiot ważny wdraża system zarządzania bezpieczeństwem informacji w procesach wpływających na świadczenie usług przez ten podmiot, zapewniający: [...] 2) wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, uwzględniających najnowszy stan wiedzy, koszty wdrożenia, wielkość podmiotu, prawdopodobieństwo wystąpienia incydentów, narażenie podmiotu na ryzyka, w szczególności: [...] d) bezpieczeństwo i ciągłość łańcucha dostaw produktów ICT, usług ICT i procesów ICT, od których zależy świadczenie usługi z uwzględnieniem bezpośrednich związków pomiędzy dostawcą sprzętu lub oprogramowania a podmiotem kluczowym lub podmiotem ważnym,	Uwaga uwzględniona Zostanie wprowadzone odniesienie do bezpośrednich dostawców.
30.	PIKE	Art. 8 ust. 1 pkt 2 lit. e	Przepis ten posługuje się pojęciem “katastrofy”, choć w projekcie ustawy takiego pojęcie nie zostało zdefiniowane. Art. 8. 1. Podmiot kluczowy lub podmiot ważny wdraża system zarządzania bezpieczeństwem informacji w procesach wpływających na świadczenie usług przez ten podmiot, zapewniający: [...] 2) wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, uwzględniających najnowszy stan wiedzy, koszty wdrożenia, wielkość podmiotu, prawdopodobieństwo wystąpienia incydentów, narażenie podmiotu na ryzyka, w szczególności: [...] e) wdrażanie, dokumentowanie i utrzymywanie planów działania umożliwiających ciągłe i niezakłócone świadczenie usługi oraz zapewniających poufność, integralność, dostępność i autentyczność informacji, oraz planów awaryjnych umożliwiających odtworzenie systemu informacyjnego po <u>katastrofie-incydencie poważnym lub krytycznym</u>.	Uwaga uwzględniona Pojęcie katastrofy zostanie zdefiniowane.
31.	PIKE	Art. 8 ust. 1 pkt 2 lit. f	W przepisie mowa jest o objęciu systemu informacyjnego wykorzystywanego do świadczenia usługi systemem monitorowania w trybie „ciągłym”. W dyrektywie NIS2 brak jest odniesienia do wymogu monitorowania w takim trybie. W przypadku, gdyby przyjąć, że w przepis ten dotyczy systemu monitorowania bezpieczeństwa (SIEM), obowiązek ten łączyłby się z ogromnymi kosztami ze względu na: -zakup rozwiązania SIEM -zatrudnienie osób lub firmy zewnętrznej, która ten system będzie utrzymywać i pisać reguły korelacyjne	Uwaga wyjaśniona W monitorowaniu w trybie ciągłym chodzi o zapewnienie rozliczalności działania systemu. Nie oznacza to automatycznego zatrudnienia osób. Istnieją też open source’ owe SIEM.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. IV

			-zatrudnienie specjalistów lub firmy zewnętrznej, która będzie pełniła rolę SOC (Security Operation Centre) 24h/dobę 7 dni w tygodniu i monitorowała SIEM oraz analizowała incydenty. Dodatkowo zapis ten powoduje trudności interpretacyjne: nie jest jasne, czym miałyby być monitorowanie „w trybie ciągłym”, jak ono miałyby wyglądać, czym miałyby się odznaczać, jakie dane i informacje zbierać? Art. 8. 1. Podmiot kluczowy lub podmiot ważny wdraża system zarządzania bezpieczeństwem informacji w procesach wpływających na świadczenie usług przez ten podmiot, zapewniający: [...] 2) wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, uwzględniających najnowszy stan wiedzy, koszty wdrożenia, wielkość podmiotu, prawdopodobieństwo wystąpienia incydentów, narażenie podmiotu na ryzyka, w szczególności: [...] f) ~~monitorowanie obięcie~~ systemu informacyjnego wykorzystywanego do świadczenia usługi ~~systemem monitorowania w trybie ciągłym~~.	
32.	PIKE	Art. 8 ust. 1 pkt 5 lit. b	Przepis mówi o tym, że „system zarządzania bezpieczeństwem informacji” powinien zapewniać „regularne przeprowadzanie aktualizacji oprogramowania”. Podczas gdy systemy duży podmiotów często składają się ze skomplikowanej sieci powiązań różnych elementów oprogramowania i bezmyślna aktualizacja jednego z komponentów może spowodować przerwy w działaniu usług i brak ciągłości biznesowej. Dlatego PIKE wskazuje, że aktualizacja oprogramowania nie powinna być przeprowadzana automatycznie przez „system zarządzania bezpieczeństwem informacji”, natomiast powinna być audytowana pod kątem zarówno bezpieczeństwa (przez „system zarządzania bezpieczeństwem informacji”), jak również konieczności zapewnienia ciągłości działania i dlatego powinna być realizowana zgodnie z polityką danej firmy. Takie podejście jest zgodnie z motywem 49 i 89 dyrektywy NIS2, które nakazują ujęcie aktualizacji oprogramowania w polityce podmiotu kluczowego i ważnego, a nie wskazują na potrzebę automatycznego stosowania każdej dostępnej aktualizacji. Art. 8. 1. Podmiot kluczowy lub podmiot ważny wdraża system zarządzania bezpieczeństwem informacji w procesach wpływających na świadczenie usług przez ten podmiot, zapewniający: [...] 5) stosowanie środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego wykorzystywanego do świadczenia usługi, w tym: [...] b) ~~ujęcie zagadnienia regularne~~przeprowadzaniea aktualizacji oprogramowania <u>w polityce szacowania ryzyka oraz bezpieczeństwa systemu informacyjnego, stosownie do zaleceń producenta pżgodnie</u>, z uwzględnieniem analizy wpływu aktualizacji na bezpieczeństwo świadczonej usługi oraz poziomu krytyczności poszczególnych aktualizacji,	Uwaga wyjaśniona W ocenie projektodawcy obecne brzmienie przepisu odpowiednio adresuje problem.
33.	PIKE	Art. 8 ust. 1 pkt 6	Zgodnie z tym przepisem podmioty kluczowe i podmioty ważne zobowiązane będą do stosowania bezpiecznych środków komunikacji elektronicznej w ramach krajowego systemu	Uwaga częściowo uwzględniona

Tabela uwag zgłoszonych w ramach konsultacji publicznych do *projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw* (UC32) cz. IV

			cyberbezpieczeństwa, uwzględniających uwierzytelnianie wieloskładnikowe. Pojawiają się dwie wątpliwości w kontekście tego przepisu: 1) po pierwsze, w dyrektywie NIS2 (art. 21 ust. 2 lit. j dyrektywy NIS2) mowa jest m.in. o stosowaniu takiego uwierzytelniania w sytuacjach nadzwyczajnych, na dodatek w uzasadnionych przypadkach – zatem to do podmiotu kluczowego i do podmiotu ważnego powinna należeć decyzja, czy do danego typu komunikacji uwierzytelnianie wieloskładnikowe jest zasadne, czy też nie, 2) po drugie, zgodnie z art. 4 krajowy system cyberbezpieczeństwa obejmuje podmioty kluczowe, podmioty ważne, CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT sektorowe, organy właściwe do spraw cyberbezpieczeństwa, Pojedynczy Punkt Kontaktowy do spraw cyberbezpieczeństwa, Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa i Kolegium do Spraw Cyberbezpieczeństwa. Wydaje się, że stosowanie bezpiecznych środków komunikacji elektronicznej „w ramach krajowego systemu cyberbezpieczeństwa” oznacza komunikowanie się w ramach systemu, o którym mowa w art. 46. To w ramach tego systemu powinny porozumiewać się pomiędzy sobą podmioty krajowego systemu cyberbezpieczeństwa (porozumiewające się „w ramach krajowego systemu cyberbezpieczeństwa”). Stosowanie uwierzytelniania wieloskładnikowego w tym systemie zależy od administratora tego systemu, czyli formalnie od ministra właściwego do spraw informatyzacji. Z kolei w art. 8 mowa jest o systemach komunikacji w ramach jednej organizacji (w ramach podmiotu kluczowego lub podmiotu ważnego). Art. 8. 1. Podmiot kluczowy lub podmiot ważny wdraża system zarządzania bezpieczeństwem informacji w procesach wpływających na świadczenie usług przez ten podmiot, zapewniający: [...] 6) <u>w uzasadnionych przypadkach</u> stosowanie bezpiecznych środków komunikacji elektronicznej <u>w ramach krajowego systemu cyberbezpieczeństwa</u>, uwzględniających uwierzytelnianie wieloskładnikowe	Uwierzytelnianie wieloskładnikowe będzie obowiązkiem w stosownych przypadkach.
34.	PERN	Art. 8 ust. 1	Art. 1 pkt 12 (art. 8 ust. 1 pkt 2 lit. i ustawy) – proponuje się doprecyzować projektowane brzmienie przepisu poprzez dookreślenie o jaki rodzaj kryptografii chodzi, tzn. kryptografię ~~symetryczną~~, w ~~której~~ ~~zastosowano~~ ~~zastosowane~~ ~~są~~ pliki;	Uwaga nieuwzględniona Rodzaj stosowanej kryptografii to jest kwestia do ustalenia przez sam podmiot.
35.	PERN	Art. 8 ust. 1	art. 1 pkt 12 (art. 8 ust. 1 pkt 3 ustawy) – proponuje się doprecyzowanie projektowanego przepisu o wskazanie czy przechowywane mają być wyłącznie historyczne informacje dotyczące każdego zidentyfikowanego przez systemy wewnętrzne zagrożenia cyberbezpieczeństwa czy też informacje dotyczące każdego zagrożenia cyberbezpieczeństwa zidentyfikowanego przez systemy brzegowe. Jaki zakres cyberzagrożeń ma być objęty historią przechowywaną;	Uwaga wyjaśniona W przepisie chodzi o każde zidentyfikowane cyberzagrożenie przez systemy brzegowe.
36.	PIKE	Art. 8 ust. 2	Zgodnie z tym przepisem „2. Wymagania, o których mowa w ust. 1, uznaje się za spełnione, gdy podmiot kluczowy i podmiot ważny zapewnia system zarządzania bezpieczeństwem informacji,	Uwaga wyjaśniona

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. IV

			z uwzględnieniem wymagań określonych w Polskiej Normie PN-EN ISO/IEC 27001 oraz PN-EN ISO/IEC 22301". O ile przepis ten może stanowić zachętę do stosowania europejskich i międzynarodowych norm i specyfikacji technicznych istotnych z punktu widzenia bezpieczeństwa sieci i systemów informatycznych (o czym jest mowa w art. 25 ust. 1 dyrektywy NIS2, o tyle: 1) powinna istnieć możliwość uznania, że wymagania, o których mowa w art. 8 ust. 1 uznaje się za spełnione, gdy podmiot kluczowy i podmiot ważny zapewnia system zarządzania bezpieczeństwem informacji, z uwzględnieniem wymagań określonych także w normach równoważnych w krajowym systemie norm ISO; 2) norma PN-EN ISO/IEC 22301 nie dotyczy systemu zarządzania bezpieczeństwem informacji, lecz ciągłości działania całego przedsiębiorstwa, niezależnie od tego, jaką działalność dany przedsiębiorca prowadzi, 3) w dyrektywie NIS2 brak jest odniesień do normy ISO 22301 – takie odniesienia można co najwyżej odnaleźć w wytycznych ENISA wydanych na podstawie art. 40 i 41 Europejskiego kodeksu łączności cyfrowej, uchylonych dyrektywą NIS2; w dyrektywie NIS2 w kontekście zapewnienia ciągłości działania mowa jest o zarządzaniu kopiami zapasowymi i przywracaniu normalnego działania po wystąpieniu sytuacji nadzwyczajnej, i zarządzaniu kryzysowym (art. 21 ust. 2 lit. a dyrektywy NIS2); 4) brak odniesienia w dyrektywie NIS2 ma istotne znaczenie, ponieważ ta norma nie dotyczy systemu zarządzania bezpieczeństwem informacji, lecz zapewnienia ciągłości działania całego podmiotu, w dużej mierze w kontekście zapewnienia płynności finansowej podmiotu; przepisy dotyczące płynności finansowej już wymogi dla prowadzącej działalność bankowej, czy ubezpieczeniowej, lecz rozszerzanie regulacji tego typu na wszystkie podmioty kluczowe i podmioty wydające usługi publiczne jest drogą; 5) co więcej, o ile niektórzy przedsiębiorcy telekomunikacyjni przeszli certyfikację w zakresie normy ISO 27001, która z pewnością powinna być punktem odniesienia przy zarządzaniu cyberbezpieczeństwem, o tyle zbiór przedsiębiorców posiadających certyfikację w zakresie zarówno normy ISO 27001, jak i ISO 22301 jest wyraźnie mniejszy. Art. 8 [...] 2. Wymagania, o których mowa w ust. 1, uznaje się za spełnione, gdy podmiot kluczowy i podmiot ważny zapewnia system zarządzania bezpieczeństwem informacji, z uwzględnieniem wymagań określonych w Polskiej Normie PN-EN ISO/IEC 27001 ~~oraz PN-EN ISO/IEC 22301~~ lub normie jej równoważnej.	Zrezygnowano z tej koncepcji pod wpływem różnych uwag zgłoszonych w trakcie konsultacji projektu.
37.	Osoba fizyczna	Art. 8, art. 10	Projekt UKSC przywołuje w swej treści PN/EN/ISO oraz standardy „europejskie i międzynarodowe”, jednakże nie przywołuje krajowych <i>Narodowych Standardów Cyberbezpieczeństwa</i> realizujących interwencję 2.1 celu szczegółowego 2 Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019 – 2024 w zakresie opracowania i wdrożenia Narodowych Standardów Cyberbezpieczeństwa.	Uwaga wyjaśniona NSC będą mogły być wydawane jako rekomendacje Pełnomocnika Rządu.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. IV

38.	PERN	Art. 8 ust. 2	Art. 1 pkt 12 (art. 8 ust. 2 ustawy) – projektowany przepis wymaga doprecyzowania poprzez wskazanie mechanizmów, za pomocą których będzie weryfikowane spełnienie wymagań, wskazania procedury jaka będzie miała zastosowanie do weryfikacji wymagań oraz konsekwencji twierdzenia braku płać i wymogów;	Uwaga wyjaśniona Zrezygnowano z tej koncepcji.
39.	Osoba fizyczna	Art. 8 ust. 2	System Zarządzania Bezpieczeństwem Informacji. Katalog wymagań dla SZBI uznaje się za spełniony, gdy podmiot kluczowy i podmiot ważny zapewnia system zarządzania bezpieczeństwem informacji, z uwzględnieniem wymagań określonych w Polskiej Normie PN-EN ISO/IEC 27001 oraz PN-EN ISO/IEC 22301. Niestety zdanie to w jednoznaczny sposób nie implikuje konieczności certyfikowania podmiotu.	Uwaga wyjaśniona Nie wprowadzono obowiązkowej certyfikacji ponieważ nie ma tylu jednostek certyfikujących, aby certyfikować wszystkie podmioty ksc.
40.	PERN	Art. 8 ust.4	Art. 1 pkt 12 (art. 8 ust. 4 pkt 2 ustawy) – projektowane brzmienie przepisu jest niejasne, bowiem z przedłożonego projektu nowelizacji nie wynika, w jaki sposób ma być mierzona jakość produktów ICT, usług ICT i procesów ICT. Wyjaśnienia wymaga również czy przewidywane jest powstanie ogólnodostępnego źródła wiedzy dotyczącego uśrednionych wymogów jakościowych produktów ICT, usług ICT i procesów ICT;	Uwaga wyjaśniona Jakość może być mierzona np. poprzez liczbę wykrytych podatności. Poleca się w tym zakresie publikację ENISA https://www.enisa.europa.eu/publications/good-practices-for-supply-chain-cybersecurity
41.	XOPERO	Art. 8	8.1.2 (Art 8. pkt 2, ppkt 2) Dodanie punktora j) polityki i procedury kopii zapasowej i przywracania danych w przypadku awarii Opis i uzasadnienie w dokumencie “Propozycja - konsultacje - projekt ustawy KSC”	Uwaga wyjaśniona Taka polityka może zostać opracowana przez podmiot jako polityka tematyczna.
42.	XOPERO	Art. 8	8.1.5 (art. 8. Pkt 1, ppkt 5c) ochronę przed nieuprawnioną modyfikacją w systemie informacyjnym Propozycja doprecyzowania tutaj i dodania podpunktu 5e) ochronę przed nieuprawnioną modyfikacją wykonanej kopii zapasowej systemów informatycznych 5f) ochronę przed nieuprawnioną modyfikacją wykonanej kopii zapasowej danych wrażliwych w postaci plików 5f) ochronę danych zapisanych na storku niezmiennym, natychmiastowym oraz nienaruszalnym (Immutable, immediate, intact)	Uwaga nieuwzględniona W ocenie projektodawcy dotychczasowy ogólny punkt konsumuje uwagę. Pamiętać należy o wynikającej z NIS 2 zasadzie proporcjonalności przy stosowaniu środków technicznych i organizacyjnych.
43.	XOPERO	Uwaga ogólna	Dostawcy usług cyfrowych Wydaje się być stosownym aby wskazać w ustawie dostawcę usług poczty elektronicznej, która to usługa umożliwia połączenie się za pomocą bezpiecznych połączeń w celu przeprowadzenia kopii zapasowej - przyrostowej i umożliwiająca przywracanie danych (nawet na poziomie pojedynczej wiadomości email) Propozycja - dodanie do podmiotów ważnych Dostawca usługi poczty elektronicznej.	Uwaga wyjaśniona Dostawcy poczty elektronicznej już są uwzględnieni w projekcie jako przedsiębiorcy komunikacji elektronicznej.
44.	PIKE	Art. 8a	Zgodnie z projektowanym art. 8a „Rada Ministrów może określić, w drodze rozporządzenia, odrębnie dla danego rodzaju działalności wykonywanej przez podmioty kluczowe lub podmioty	Uwaga nieuwzględniona

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. IV

			ważne szczegółowe wymagania dla systemu zarządzania bezpieczeństwem informacji, o którym mowa w art. 8 ust. 1, biorąc pod uwagę rekomendacje międzynarodowe o charakterze specjalistycznym, w tym rekomendacje Agencji Unii Europejskiej do spraw Cyberbezpieczeństwa, zwanej dalej „ENISA”, skalę działalności wykonywanej przez te podmioty oraz potrzebę podejmowania przez te podmioty działań zapewniających cyberbezpieczeństwo”. W opinii Izby przepis ten stanowi szkodliwą nadregulację, stojącą w wyraźnej sprzeczności z zasadą proporcjonalności. Każdy podmiot powinien mieć możliwość samodzielnie dobierać odpowiednie i proporcjonalne do swojej działalności środki zarządzania bezpieczeństwem informacji – w tym celu dokonuje przecież analizy ryzyka (art. 21 ust. 1 NIS2). W opinii PIKE rekomendacje międzynarodowe o charakterze specjalistycznym, w tym rekomendacje Agencji Unii Europejskiej do spraw Cyberbezpieczeństwa, zwanej dalej „ENISA” powinny być brane pod uwagę nie przy wydawaniu rozporządzenia, o którym mowa w projektowanym art. 8a, lecz przy wydawaniu rekomendacji, o których mowa w art. 33 ust. 4. Należy również zauważyć, że istnieje konflikt tego przepisu z faktem przyszłego powstania aktów wykonawczych do NIS2. Powstanie chaos regulacyjny. Art. 21 ust. 5 dyrektywy daje m.in. podstawę KE do przyjęcia aktów wykonawczych, w których określić ma ona wymogi techniczne i metodykę dotyczącą środków zarządzania ryzykiem w cyberbezpieczeństwie w odniesieniu do niektórych rodzajów podmiotów. Tj. dostawców usług DNS, rejestrów nazw TLD, dostawców usług chmurowych, dostawców usług ośrodka przetwarzania danych, dostawców sieci dostarczania treści, dostawców usług zarządzanych, dostawców usług zarządzanych w zakresie bezpieczeństwa, dostawców internetowych platform handlowych, wyszukiwarek internetowych oraz platform sieci społecznościowych i dostawców usług zaufania. Jako fakultatywne należy potraktować wskazanie przez KE w akcie wykonawczym wymogów technicznych i metodyk oraz wymogów sektorowych dotyczących tych środków w odniesieniu do podmiotów kluczowych i ważnych innych, niż wymienione wyżej. Projektowany art. 8a należy wykreślić.	Konfliktu między aktami Komisji a rozporządzeniami nie będzie, ponieważ rozporządzenia mają charakter fakultatywny a i tak z uwagi na prymat prawa unijnego muszą być z nimi zgodne. Podtrzymujemy zasadność odwołania się do rekomendacji ENISA w wytycznych w upoważnieniu.
45.	Osoba fizyczna	Art. 8a	Art. 8a. Procedury oceny ryzyka: Podmioty kluczowe oraz ważne są zobowiązane do przeprowadzania regularnych ocen ryzyka cybernetycznego, które obejmują: 1) identyfikację i analizę potencjalnych zagrożeń, 2) ocenę prawdopodobieństwa wystąpienia incydentów oraz ich potencjalnych skutków, 3) wdrożenie odpowiednich środków zaradczych i prewencyjnych, 4) dokumentowanie wyników oceny ryzyka i działań naprawczych, 5) regularny przegląd i aktualizację ocen ryzyka.	Uwaga nieuwzględniona W ramach SZBI podmiot ma prowadzić systematyczne szacowanie ryzyka.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. IV

46.	PIKE	Art. 8h ust. 1	Zgodnie ze wspomnianym przepisem „Podmioty kluczowe i podmioty ważne wymieniają między sobą informacje dotyczące cyberbezpieczeństwa, w tym informacje o cyberzagrożeniach, potencjalnych zdarzeniach dla cyberbezpieczeństwa, podatnościach, technikach i procedurach, oznakach naruszenia integralności systemu, wrogich taktykach, a także informacje o grupach przestępczych, ostrzeżenia dotyczące cyberbezpieczeństwa i zalecenia dotyczące konfiguracji narzędzi bezpieczeństwa mających wykrywać cyberataki”. Takie sformułowanie przepisu jest równoznaczne w wprowadzeniu obowiązku wymiany informacji pomiędzy podmiotami kluczowymi i ważnymi, przy spełnieniu przesłanek z art. 8h ust. 2. Tymczasem taka wymiana informacji powinna odbywać się na zasadzie dobrowolności: zgodnie z art. 29 NIS2 „Państwa członkowskie zapewniają, aby podmioty objęte zakresem stosowania niniejszej dyrektywy, a w stosownych przypadkach również inne podmioty nieobjęte zakresem niniejszej dyrektywy <u>mogły dobrowolnie wymieniać się odpowiednimi informacjami</u> na temat cyberbezpieczeństwa, w tym informacjami o cyberzagrożeniach, potencjalnych zdarzeniach dla cyberbezpieczeństwa, podatnościach, technikach i procedurach, oznakach naruszenia integralności systemu, wrogich taktykach, a także informacjami o grupach przestępczych, ostrzeżeniami dotyczącymi cyberbezpieczeństwa i zaleceniami dotyczącymi konfiguracji narzędzi bezpieczeństwa mających wykrywać cyberataki, jeżeli wymiana takich informacji [...]”. Propozycja projektodawcy jest niezrozumiała tym bardziej, że jest to obowiązek penalizowany. Obowiązkiem powinna być objęta tylko wymiana informacji z CSIRT, jak w dyrektywie NIS 2. Art. 8h. 1. Podmioty kluczowe i podmioty ważne <u>mogą</u> wymieniać między sobą informacje dotyczące cyberbezpieczeństwa, w tym informacje o cyberzagrożeniach, potencjalnych zdarzeniach dla cyberbezpieczeństwa, podatnościach, technikach i procedurach, oznakach naruszenia integralności systemu, wrogich taktykach, a także informacje o grupach przestępczych, ostrzeżenia dotyczące cyberbezpieczeństwa i zalecenia dotyczące konfiguracji narzędzi bezpieczeństwa mających wykrywać cyberataki.	Uwaga uwzględniona
47.	PERN	Art. 9	Art. 1 pkt 14 (art. 9 pkt 1 i 2 ustawy) – wyjaśnienia wymaga czy projektodawca przewiduje możliwość zgłaszania osób z wykorzystaniem dedykowanej platformy komunikacji (S46). Analogiczna wątpliwość dotyczy kontaktów z Ministerstwem oraz Rządowym Centrum Bezpieczeństwa. Ponadto w zakresie pkt 2 wyjaśnienia wymaga czy intencją ustawodawcy było udo	Uwaga wyjaśniona Elementem wniosku o wpis do wykazu podmiotów kluczowych i podmiotów ważnych będzie wskazanie osób kontaktowych. Co do strony to chodzi o stronę internetową.
48.	PIKE	Art. 10 ust. 3 pkt 1 i 3	Zgodnie z art. 10 ust. 1 „Podmiot kluczowy i podmiot ważny opracowuje, stosuje i aktualizuje dokumentację dotyczącą bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi”. Z kolei zgodnie z art. 10 ust. 3 pkt 1 „Dokumentację normatywną stanowią: 1) dokumentacja dotycząca systemu zarządzania bezpieczeństwem informacji	Uwaga uwzględniona Odniesienia do norm ISO zostaną usunięte z projektu.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. IV

			wytworzona zgodnie z wymaganiami Polskiej Normy PN-EN ISO/IEC 27001 lub normy jej równoważnej; [...] 3) dokumentacja systemu zarządzania ciągłością działania usługi wytworzona zgodnie z wymaganiami Polskiej Normy PN-EN ISO 22301 lub normy jej równoważnej;”. Należy w tym kontekście podkreślić, że powyższa konstrukcja przepisu powoduje, iż: 1) podmioty kluczowe i podmioty ważne powinny stworzyć dokumentację dotyczącą systemu zarządzania bezpieczeństwem informacji – nie, jak w art. 8 ust. 1 pkt 2 „uwzględniając najnowszy stan wiedzy”, czyli m.in. normy ISO jako punkt odniesienia, lecz wprost zgodnie z konkretnymi normami ISO, 2) <u>konsekwencją takiej redakcji przepisu jest konieczność dowodzenia – w razie kontroli systemu zarządzania bezpieczeństwem informacji – że system ten i odpowiednia dokumentacja jest zgodna z wymaganiami normy ISO, a nie – że wynika z analizy ryzyka wykonanej przez dany podmiot</u>, który powinien móc dowodzić, że w jego przypadku nie wszystkie szczegółowe rozwiązania przewidziane w normach ISO są w jego przypadku adekwatne i uzasadnione, 3) <u>polski ustawodawca ceduje regulację podstawowych obowiązków spoczywających na podmiotach kluczowych i podmiotach ważnych w dużym zakresie na prywatną organizację międzynarodową</u>, która zresztą cyklicznie zmienia wymagania ujęte w swoich normach. Art. 10 [...] 3. Dokumentację normatywną stanowią: 1) dokumentacja dotycząca systemu zarządzania bezpieczeństwem informacji wytworzona <u>zgodnie z uwzględnieniem najnowszego stanu wiedzy wymaganiami Polskiej Normy PN-EN ISO/IEC 27001 lub normy jej równoważnej</u>; [...] 3) dokumentacja systemu zarządzania ciągłością działania <u>usługi wytworzona zgodnie z wymaganiami Polskiej Normy PN-EN ISO 22301 lub normy jej równoważnej, obejmująca w szczególności zarządzanie kopiami zapasowymi i przywracanie normalnego działania po wystąpieniu sytuacji szczególnego zagrożenia, i zarządzanie kryzysowe</u>;”.	
49.	Osoba fizyczna	Art.10	Dokumentacja. Zapisy niniejszego projektu UKSC zapisami ustawy znoszą istnienie rozporządzenia dotyczącego dokumentacji koniecznej dla PK/WP. Tym samym powodują, iż każdorazowo, w przypadku konieczności aktualizacji tych zapisów koniecznym będzie aktualizacja aktu wyższego poziomu. Przypadki takie mogą zdarzyć się niejednokrotnie w wyniku zmian technologicznych, czy pojawienia się nowych standardów europejskich czy międzynarodowych. Jednocześnie zapisy te nie konsumują zapisów art. 21 <i>Środki zarządzania ryzykiem w cyberbezpieczeństwie dyrektywy NIS II</i>, bazujące na podejściu uwzględniającym wszystkie	Uwaga wyjaśniona Wprowadzone przepisy są na takim stopniu ogólności jakiego wymaga poziom ustawy.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do *projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw* (UC32) cz. IV

			zagrożenia i mające na celu ochronę sieci i systemów informatycznych oraz środowiska fizycznego tych systemów przed incydentami. Zakres dokumentacji w przywołanym art. jest szerszy. Bardzo wartościowym są zapisy dotyczące postępowania z dokumentacją.	
50.	PERN	Art.10	Art. 1 pkt 14 (art. 10 ust. 1 ustawy) – proponuje się przeanalizowanie możliwości uzupełnienia przepisów projektowanej ustawy o regulacje dotyczące wymagań co do lokalizacji i podległości komórek do spraw bezpieczeństwa w strukturach organizacji podmiotów kluczowych i w [];	Uwaga wyjaśniona Nie wprowadzono takich regulacji, gdyż byłyby to nadmierna ingerencja w decyzje podmiotu.
51.	PERN	Art. 10	Art. 1 pkt 14 (art. 10 ust. 3 pkt 2 lit. d ustawy) – wyjaśnienia wymaga czy dokumentacja ochrony infrastruktury, z wykorzystaniem której świadczona jest usługa, obejmować ma opis zabezpieczeń technicznych wszystkich obiektów infrastruktury czy tylko tych, które zawierają systemy informatyczne.	Uwaga wyjaśniona Chodzi o opis zabezpieczeń infrastruktury systemu informacyjnego.
52.	Osoba fizyczna	Art. 11	Zgłaszanie incydentów. Rada Ministrów w ramach prac operacyjnych i konsultacji międzyresortowych, w zgodzie z przepisami niniejszej ustawy, winna ujednolicić sposoby zgłaszania incydentów do właściwych CSIRT. W chwili obecnej zgłaszanie incydentów, mimo to, iż odbywa się na podstawie jednolitej dla wszystkich ustawy o KSC, w każdym z CSIRT wygląda []; [] różni [] kr[] tr[] gło[], różni m[]ody t[] h[] J[] d[] b[] [] warto zwrócić uwagę, iż zgłoszenia określają zakresy godzinowe z osobą do kontaktu, w przedziałach czasowych. Wydaje się to błędne w momencie, gdy zgłoszenia dotyczą przecież incydentów najwyższych poziomów zagrożeń dla PK/PW.	Uwaga wyjaśniona Od tej pory zgłaszanie incydentów będzie odbywało się za pomocą systemu s46, co ujednolici praktykę.
53.	Osoba fizyczna	Art. 11	Zgłaszanie incydentów. Przepisy ustawy zawierają wytyczne techniczne co do zawartości zgłoszeń. Należy rozważyć przeniesienie tych treści do właściwego rozporządzenia jako przepisów wykonawczych. Jednocześnie treści te wskazują, iż w każdym zgłoszeniu należy zawrzeć m.in. takie dane jak: imię i nazwisko, numer telefonu oraz adres poczty elektronicznej osoby dokonującej zgłoszenia czy imię i nazwisko, numer telefonu oraz adres poczty elektronicznej osoby uprawnionej do składania wyjaśnień dotyczących zgłaszanych informacji. Brak jest tutaj doprecyzowania, czy osobą dokonującą zgłoszenia winien być reprezentant PK/PW, czy osoba techniczna. Podobnie nie doprecyzowano, czy osobą uprawnioną do składania wyjaśnień jest osoba zgłoszona zgodnie z art. 9.1 UKSC.	Uwaga wyjaśniona Zbieranie informacji, zwłaszcza tak wrażliwych, musi mieć podstawę prawną w ustawie.
54.	Osoba fizyczna	Art. 11	Zgłaszanie incydentów. Należy rozważyć obowiązek zgłaszania incydentów w ramach UKSC do Prezesa Urzędu Danych Osobowych. Art.46 projektu deleguje PUODO jako organ zobowiązany do korzystania z systemu teleinformatycznego w celu realizacji swoich zadań ustawowych, jednakże nie stawia na równi incydentów cyberbezpieczeństwa z pozostałymi CSIRT. Statystyka naruszeń odo (statystyki krajowe) wyraźnie wskazują, iż większość ich odbywa się w przestrzeni cyfrowej. Obowiązek taki podnosiłby wagę incydentów	Uwaga wyjaśniona S46 będzie umożliwiał przekazywanie zgłoszeń naruszeń ochrony danych osobowych.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. IV

			cyberbezpieczeństwa i nie pozwalał, tak jak odbywa się w to chwili obecnej, na dowolność postępowania podmiotów, których dotknęło naruszenie poufności, dostępności czy integralności. Obecnie formularz zgłaszanie incydentów do PUODO sugeruje jedynie zgłaszanie tego typu incydentów do krajowego CERT (nie uwzględniając przy tym nawet innych CSIRT).	
55.	Osoba fizyczna	Art. 11	Zgłaszanie incydentów. Projekt ustawy stanowi, iż „<i>W przypadku zaistnienia znaczącego cyberzagrożenia podmiot kluczowy i podmiot ważny informuje swoich użytkowników, na których takie cyberzagrożenie może mieć wpływ, o możliwych środkach zapobiegawczych, które użytkownicy ci mogą podjąć.</i>” W lakoniczny sposób określono bardzo ważne czynności techniczno-administracyjne: informowanie. Brak jest określenia w jaki sposób miałby PK/PW wykonać to wobec swoich użytkowników, nie określając również kim są użytkownicy. Przykładowo w zakresie ochrony zdrowia: szpital będzie miał innych użytkowników jak przedsiębiorstwo energetyczne, na terenie którego będzie się znajdować sporo tego typu placówek, czy apteka szpitalna. Podobnie urzędy publiczne, KRUS, ZUS czy NFZ. Pojęcie sposobu „informowania” winno być doprecyzowane, również w zakresie rozliczalności procesów. Sam proces „informowania” w wielu miejscach ustawy jest określony w sposób jednoznaczny i rozliczalny (drogą elektroniczną, system, ePUAP) w innych natomiast jest niedookreślony.	Uwaga wyjaśniona Opis tego procesu można znaleźć na stronie internetowej (link poniżej) https://www.enisa.europa.eu/publications/cyber-threats-outreach-in-telecom
56.	PIKE	Art. 11 ust. 1 pkt 2	Zgodnie z tym przepisem, podmiot kluczowy i ważny zapewniają dostęp do informacji o rejestrowanych incydentach właściwemu CSIRT sektorowemu, CSIRT MON, CSIRT NASK lub CSIRT GOV w zakresie niezbędnym do realizacji jego zadań. PIKE uważa, że – po pierwsze – <u>podmioty kluczowe i ważne powinny być zobowiązane do współpracy z jednym tylko CSIRT</u>. Po drugie, projekt ustawy nakłada tak wiele nowych obowiązków na podmioty kluczowe i ważne (np. w zakresie kilku sprawozdań z obsługi incydentów), że <u>każdy kolejny obowiązek nałożony projektem ustawy nałożony na podmioty, którego jednocześnie dyrektywa NIS2 nie wymaga, jest niepożądany</u>. Omawiany przepis wymagałby, ponadto (w praktyce) od podmiotów kluczowych i ważnych analizy zadań wykonywanych przez CSIRT MON, CSIRT NASK i CSIRT GOV w celu oceny, czy może przekazać mu informacje o rejestrowanym konkretnym incydencie, czy też nie, co wydaje się całkowicie nieuzasadnionym obciążeniem dla przedsiębiorcy. <u>Dostęp do informacji o incydentach innych niż poważne powinien być udzielany wyłącznie na zasadzie dobrowolności (np. w ramach ISAC), a nie obowiązku</u>. Art. 11 1. Podmiot kluczowy i podmiot ważny: [...]	Uwaga wyjaśniona Zapewnienie dostępu do rejestru incydentów jest konieczne do realizacji zadań CSIRT, które mogą np. zmienić klasyfikację incyduentu.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. IV

			2) <u>może</u> zapewnić dostęp do informacji o rejestrowanych incydentach właściwemu CSIRT sektorowemu, ~~CSIRT MON, CSIRT NASK lub CSIRT GOV w zakresie niezbędnym do realizacji jego zadań na zasadzie dobrowolności.~~	
57.	PIKE	Art. 11 ust. 1 pkt 5	Projekt ustawy zakłada obowiązek współdziałania przez podmiot kluczowy lub ważny z CSIRT sektorowym, CSIRT MON, CSIRT NASK lub CSIRT GOV podczas obsługi incydentu poważnego, polegającego na przekazywaniu niezbędnych danych, w tym danych osobowych. Zdaniem PIKE taki przepis może spowodować, że podmiot kluczowy i ważny, zamiast całość wysiłków przeznaczać na obsługę incydentu, będzie zmuszony do przekazywania informacji co najmniej dwóm CSIRTom (sektorowemu oraz CSIRT MON, CSIRT NASK lub CSIRT GOV). W takim scenariuszu nie sposób wykluczyć, że te CSIRTy będą żądały częściowo takich samych informacji, zatem tak skonstruowany obowiązek współpracy z CSIRTami może generować nadmierne i niepotrzebne obciążenie dla podmiotów kluczowych i ważnych, które powinny koncentrować się na obsłudze incydentu. W związku z tym przepis budzi wątpliwości co do zgodności z motywem 102 dyrektywy NIS2, który stanowi: „Państwa członkowskie powinny zapewnić, aby obowiązek takiego wczesnego ostrzeżenia lub późniejszego zgłoszenia incydentu <u>nie powodował przekierowania zasobów podmiotu zgłaszającego przeznaczonych na obsługę incydentów, które powinno być traktowane priorytetowo, tak by zapobiec sytuacji, w której obowiązki dotyczące zgłaszania incydentów powodowałyby przekierowanie zasobów przeznaczonych na reagowanie na poważne incydenty albo w inny sposób utrudniałyby działania danego podmiotu w tym zakresie</u>”. Podmiot kluczowy i ważny powinny współpracować co najwyżej z CSIRT sektorowym, a z CSIRT MON, NASK lub GOV – za pośrednictwem CSIRT sektorowego. Art. 11 1. Podmiot kluczowy i podmiot ważny: [...] 5) współdziała podczas obsługi incydentu poważnego i incydentu krytycznego z właściwym CSIRT ~~MON, CSIRT NASK lub CSIRT GOV~~ sektorowym, przekazując niezbędne dane, w tym dane osobowe, <u>przy czym podczas obsługi incydentu poważnego i krytycznego termin przekazania danych właściwemu CSIRT sektorowemu wynosi co najmniej 24 godziny.</u>	Uwaga nieuwzględniona CSIRT sektorowe będą musiały wprowadzić wewnętrzne procedury współpracy przy podmiotach które podlegają pod kilka CSIRT.
58.	PIKE	Art. 11 ust. 1 pkt 6 (powiązane z uwagą dot. art. 32 ust. 2)	W opinii PIKE bardzo złym rozwiązaniem, sprzecznym z zasadą proporcjonalności i zasadą analizy ryzyka przez każdy podmiot kluczowy i ważny oraz doбором środków adekwatnych do sytuacji takiego podmiotu, jest możliwość nałożenia obowiązku „usunięcia podatności”. Po pierwsze, w przypadku oprogramowania istnieje ryzyko, że „usunięcie” podatności wymagałoby wprowadzenia takich zmian, które wymagałoby uzyskania zgody dostawcy oprogramowania. Po drugie, dosłowne „usunięcie” podatności może być w praktyce niemożliwe bez wymiany sprzętu, podczas gdy zazwyczaj istnieje wiele sposobów zarządzania nawet najbardziej krytyczną podatnością tzn. możliwe jest zablokowanie możliwości wykorzystania ujawnionej podatności przez cyberzagrożenie. Po trzecie, „usunięcie” podatności (w razie potrzeby razem ze sprzętem) lub zablokowanie możliwości	Uwaga nieuwzględniona Żądanie usunięcia podatności na wezwanie CSIRT jest szczególną okolicznością – i takie uprawnienie powinno pozostać.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. IV

			wykorzystania podatności, czy też inne działania wobec podatności powinny być dobrane przez podmiot kluczowy i podmiot ważny na podstawie wykonywanej przez te podmioty analizy ryzyka. Idea możliwości nakazania „usunięcia” podatności jest sprzeczna z ideą prowadzenia analizy ryzyka indywidualnie przez każdy podmiot kluczowy i podmiot ważny. Art. 11. 1. Podmiot kluczowy i podmiot ważny: [...] 6) <u>zarządza ujawnionymi podatnościami występującymi w sprzęcie i oprogramowaniu, którymi się posługuje usuwa podatności, o których mowa w art. 32 ust. 2, oraz informuje o ich usunięciu organ właściwy do spraw cyberbezpieczeństwa.</u>	
59.	PIKE	Art. 11 ust. 1 ¹ (propozycja powiązana z uwagą do art. 7 ust. 15)	Propozycja dodania do art. 11 ustępu, który jednoznacznie przesądza, że jeden podmiot – kluczowy lub ważny – będzie podlegał pod jeden CSIRT sektorowy. Art. 11 [...] <u>1¹. Dla podmiotu kluczowego i podmiotu ważnego właściwy jest tylko jeden CSIRT sektorowy, nawet w przypadku, gdy ten podmiot kluczowy i podmiot ważny prowadzi działalność w więcej niż jednym sektorze lub podsektorze wskazanym w załączniku nr 1 lub załączniku nr 2 do ustawy.</u>	Uwaga nieuwzględniona Wprowadzenie takiego przepisu jest niemożliwe, ponieważ podmioty prowadzą zróżnicowaną działalność.
60.	PIKE	Art. 11 ust. 1a	Przepis zakłada skrócenie czasu zgłoszenia wczesnego ostrzeżenia o incydencie poważnym dla przedsiębiorców telekomunikacyjnych względem wszystkich pozostałych podmiotów kluczowych i ważnych: z 24 godzin do 12 godzin. Tak drastyczne skrócenie czasu zgłoszenia wczesnego ostrzeżenia o incydencie – po pierwsze – wykracza poza wymagania dyrektywy NIS2, czyli będzie stanowiło obciążenie, które nie wynika z prawa UE, a – po drugie – budzi wątpliwości co do zgodności z motywem 102 dyrektywy NIS2, który stanowi: „Państwa członkowskie powinny zapewnić, aby obowiązek takiego wczesnego ostrzeżenia lub późniejszego zgłoszenia incydentu <u>nie powodował przekierowania zasobów podmiotu zgłaszającego przeznaczonych na obsługę incydentów, które powinno być traktowane priorytetowo</u>, tak by zapobiec sytuacji, w której obowiązki dotyczące zgłaszania incydentów powodowałyby przekierowanie zasobów przeznaczonych na reagowanie na poważne incydenty albo w inny sposób <u>utrudniałyby działania danego podmiotu w tym zakresie</u>”. Trzeba zwrócić uwagę, że w przypadku incydentu należy: - wykonać analizę zdarzenia, znaleźć przyczynę/źródło ataku, zweryfikować całą infrastrukturę teleinformatyczną celem ustalenia pełnych skutków ataku i wyłapania wszystkich dotkniętych systemów, - dokonać modyfikacji na sieci, aby zablokować pozostałe potencjalne źródła ataku lub np. update urządzeń wykonuje w celu usunięcia podatności (zero-day), - przywrócić jak najszybciej działanie systemów, które zostały zaatakowane (np. w przypadku ransomware).	Uwaga uwzględniona Czas na wczesne ostrzeżenie zostanie wydłużone do 24 h.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. IV

			W przeciągu 12 godzin może nie być możliwości, aby przygotować odpowiednie ostrzeżenie i przekazać do odpowiedniego zespołu CSIRT. Jednocześnie ze względu na analizę możliwy jest brak pełnej wiedzy o incydencie, przez co zostanie wskazane błędne źródło ataku oraz potencjalne skutki. Dodatkowo zespół zajmujący się incydem ze względu na zbliżające się 12-godzin, może popełniać błędy lub pominąć ważne czynniki lub wydłużyć czas przywracania systemów, aby tylko komunikat wysłać. 24-godzinna informacja jest odpowiednim czasem na analizę zdarzenia i wysłanie komunikatu i należy go przywrócić. Postulat wykreślenia projektowanego ust. 1a z art. 11.	
61.	PIKE	Art. 11 ust. 4	Zgodnie z art. 11 ust. 4 Rada Ministrów określi, w drodze rozporządzenia, progi uznania incydentu za poważny według rodzaju zdarzenia w poszczególnych sektorach i podsektorach określonych w załącznikach nr 1 oraz nr 2 do ustawy. Określenie takich progów może być pomocne dla podmiotów kluczowych i ważnych, zwiększając poziom pewności prawnej. Jednocześnie jednak, dla porządku i jasności regulacji, warto byłoby zasygnalizować w tym przepisie również możliwość pojawienia się aktów wykonawczych Komisji Europejskiej w tym zakresie (o których mowa w art. 23 ust. 1 akapit drugi dyrektywy NIS2: „Do dnia 17 października 2024 r. Komisja, w odniesieniu do dostawców usług DNS, rejestrów nazw TLD, dostawców usług chmurowych, dostawców usług ośrodka przetwarzania danych, dostawców sieci dostarczania treści, dostawców usług zarządzanych, dostawców usług zarządzanych w zakresie bezpieczeństwa, jak również dostawców internetowych platform handlowych, wyszukiwarek internetowych i platform usług sieci społecznościowych, przyjmuje akty wykonawcze doprecyzowujące przypadki, w których incydent uznaje się za poważny zgodnie z ust. 3. Komisja może przyjąć takie akty wykonawcze w odniesieniu do innych podmiotów kluczowych i ważnych”). Art. 11 [...] 4. Rada Ministrów określi, w drodze rozporządzenia, progi uznania incydentu za poważny według rodzaju zdarzenia w poszczególnych sektorach i podsektorach określonych w załącznikach nr 1 oraz nr 2 do ustawy, uwzględniając: 1) liczbę użytkowników, których dotyczy zakłócenie świadczenia usługi kluczowej, 2) czas oddziaływania incydentu na świadczone usługi, 3) zasięg geograficzny obszaru, którego dotyczy incydent, 4) inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują, <u>5) akty wykonawcze Komisji Europejskiej</u> - kierując się potrzebą zapewnienia ochrony przed zagrożeniem życia lub zdrowia ludzi, znacznymi stratami majątkowymi oraz obniżeniem jakości świadczonej usługi kluczowej.	Uwaga wyjaśniona Rozporządzenia te muszą być zgodne z bezpośrednio stosowanymi aktami wykonawczymi Komisji Europejskiej.
62.	Osoba fizyczna	Art. 11a	Art. 11a. Odpowiedzialność za raportowanie i przekazywanie sprawozdań	Uwaga nieuwzględniona

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. IV

			Każdy podmiot kluczowy oraz ważny, który jest częścią krajowego systemu cyberbezpieczeństwa, jest zobowiązany do natychmiastowego raportowania incydentów cybernetycznych do właściwego CSIRT-u sektorowego. Raportowanie to obejmuje następujące etapy: 1) Wstępne zgłoszenie incyduentu: Powinno zostać dokonane w ciągu 24 godzin od momentu wykrycia incyduentu i zawierać podstawowe informacje na temat zdarzenia, jego potencjalnego wpływu oraz podjętych środków zaradczych. 2) Pełne zgłoszenie incyduentu: Powinno zostać dokonane w ciągu 72 godzin od momentu wykrycia incyduentu i zawierać szczegółowe informacje na temat przyczyn incyduentu, jego wpływu na działalność organizacji oraz wszystkich podjętych działań naprawczych i prewencyjnych. Podmiot kluczowy oraz ważny jest odpowiedzialny za regularne przekazywanie sprawozdań okresowych do właściwego CSIRT-u sektorowego. Sprawozdania te powinny być przekazywane w terminach uzgodnionych z CSIRT-em i zawierać: 1) Podsumowanie zgłoszonych incydentów: W tym liczba i rodzaj zgłoszonych incydentów, działania podjęte w odpowiedzi na te incydenty oraz ich wpływ na działalność organizacji. 2) Analizę trendów: Identyfikację wzorców i trendów dotyczących incydentów cybernetycznych oraz ocenę skuteczności podjętych środków zaradczych. 3) Rekomendacje: Propozycje dodatkowych środków zapobiegawczych i ulepszeń w zakresie zarządzania ryzykiem cybernetycznym. Podmiot kluczowy oraz ważny jest również zobowiązany do przekazywania sprawozdań końcowych do właściwego CSIRT-u sektorowego po zakończeniu działań naprawczych związanych z każdym poważnym incydentem cybernetycznym. Sprawozdanie końcowe powinno zawierać: 1) Szczegółowy opis incyduentu: W tym przyczyny, skutki oraz wszystkie podjęte działania naprawcze. 2) Ocena skuteczności działań: Analiza skuteczności podjętych działań naprawczych oraz wnioski dotyczące dalszych działań zapobiegawczych.	Podnoszone kwestie wynikają już z innych przepisów projektu.
63.	Osoba fizyczna	Art. 15a-15b	Art. 15a. Przeprowadzanie audytów bezpieczeństwa 1. Każdy podmiot kluczowy oraz ważny, który jest częścią krajowego systemu cyberbezpieczeństwa, jest zobowiązany do przeprowadzania regularnych audytów bezpieczeństwa swoich systemów informacyjnych, infrastruktury i procedur zgodnie z wymogami niniejszej ustawy oraz Dyrektywy NIS2. 2. Audyty bezpieczeństwa powinny być przeprowadzane co najmniej raz na dwa lata przez niezależne podmioty certyfikowane w zakresie audytów bezpieczeństwa informatycznego lub przez audytorów zatrudnionych w organizacji, którzy posiadają odpowiednie uprawnienia. Audyty te powinny obejmować:	Uwaga nieuwzględniona Kwestie audytów są już uregulowane w projekcie.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. IV

			1) Ocena zgodności: Weryfikacja zgodności z obowiązującymi przepisami prawa, normami i standardami bezpieczeństwa, w tym normami ISO/IEC 27001. 2) Ocena ryzyka: Przegląd i ocena mechanizmów zarządzania ryzykiem cybernetycznym w tym identyfikacja zagrożeń i ocena ich potencjalnego wpływu. 3) Testy penetracyjne: Regularne testy penetracyjne mające na celu identyfikację podatności w systemach informatycznych i infrastrukturze sieciowej. 4) Ocena skuteczności środków zaradczych: Sprawdzenie skuteczności wdrożonych środków zapobiegawczych i naprawczych oraz rekomendacja dalszych działań. 3. Audyty mogą być przeprowadzane przez audytorów zatrudnionych w organizacji, którzy posiadają odpowiednie uprawnienia, takie jak: audytor wiodący ISO 27001, Certified Information Systems Auditor (CISA), Certified Internal Auditor (CIA), Certified Government Auditing Professional (CGAP) lub inne równoważne kwalifikacje. 4. Wyniki audytów powinny być dokumentowane w formie raportów, które zawierają szczegółowe informacje na temat wykrytych nieprawidłowości, zaleceń dotyczących ich usunięcia oraz oceny skuteczności wdrożonych środków zaradczych. Raporty te powinny być przekazywane do właściwego CSIRT-u sektorowego oraz organu nadzoru w terminie 30 dni od zakończenia audytu. 5. Podmiot kluczowy oraz ważny jest zobowiązany do niezwłocznego wdrożenia zaleceń wynikających z audytu bezpieczeństwa oraz do poinformowania właściwego CSIRT-u sektorowego o podjętych działaniach naprawczych w terminie 60 dni od otrzymania raportu z audytu. Art. 15b. Weryfikacja zgodności przez niezależne podmioty 1. Niezależne podmioty certyfikowane w zakresie audytów bezpieczeństwa informatycznego powinny być akredytowane przez właściwe organy krajowe lub międzynarodowe, które zapewniają ich kompetencje i bezstronność. 2. Niezależne podmioty są zobowiązane do przestrzegania najwyższych standardów zawodowych i etycznych podczas przeprowadzania audytów oraz weryfikacji zgodności. 3. Weryfikacja zgodności obejmuje: 1) Przegląd polityk i procedur: Ocena, czy polityki i procedury bezpieczeństwa są zgodne z obowiązującymi przepisami i normami. 2) Inspekcje techniczne: Szczegółowe inspekcje techniczne infrastruktury informatycznej, systemów oraz urządzeń zabezpieczających. 3) Weryfikacja dokumentacji: Sprawdzenie kompletności i dokładności dokumentacji związanej z zarządzaniem bezpieczeństwem informacyjnym.	

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. IV

			4) Wywiady z pracownikami: Przeprowadzanie wywiadów z kluczowymi pracownikami odpowiedzialnymi za bezpieczeństwo informacyjne w celu oceny ich wiedzy, świadomości i kompetencji. 4. Niezależne podmioty powinny sporządzać szczegółowe raporty z przeprowadzonych weryfikacji zgodności, które zawierają: 1) Wnioski i rekomendacje: Szczegółowe wnioski dotyczące zgodności z obowiązującymi wymogami oraz rekomendacje dotyczące dalszych działań. 2) Analiza ryzyka: Ocena ryzyka związanego z wykrytymi niezgodnościami oraz potencjalnymi zagrożeniami. 3) Plan działań naprawczych: Propozycje działań naprawczych mających na celu usunięcie wykrytych niezgodności i poprawę bezpieczeństwa. Raporty z weryfikacji zgodności powinny być przekazywane do właściwego CSIRT-u sektorowego oraz organu nadzoru w terminie 30 dni od zakończenia weryfikacji.	
64.	PERN	Art. 15	Art. 1 pkt 20 lit. a (art. 15 ust. 1 ustawy) – doprecyzowania wymaga czy audyt bezpieczeństwa, o którym mowa w projektowanym przepisie dotyczy audytu zgodności z nowelizowaną ustawą czy audytu z normą ISO 27001 czy też audytu w formie przeprowadzanych pentestów.	Uwaga uwzględniona Audyt zgodności z ustawą. Uzasadnienie zostanie doprecyzowane w tym zakresie.
65.	PIKE	Art. 15 ust. 1	Obowiązkowy cykliczny audyt bezpieczeństwa systemu informacyjnego dla podmiotów ważnych nie występuje w dyrektywie NIS2 ani w przypadku podmiotów kluczowych (art. 32 ust. 2 pkt 2 oraz ust. 2 akapit drugi dyrektywy NIS2), ani podmiotów ważnych (art. 33 ust. 1 i 2 dyrektywy NIS2). Zgodnie z art. 32 ust. 2 pkt 2 dyrektywy NIS2, to właściwe organy powinny być uprawnione do objęcia podmiotu kluczowego regularnymi ukierunkowanymi audytami bezpieczeństwa. Wprowadzenie odgórnego obowiązku prowadzenia cyklicznych audytów bezpieczeństwa stanowi nadregulację. Jest to zaprzeczenie zasady proporcjonalności, ponieważ nie w przypadku każdego podmiotu kluczowego i ważnego będzie istniała potrzeba przeprowadzania takich audytów cyklicznie. Ponadto, zgodnie z art. 32 ust. 2 akapit drugi dyrektywy NIS2 „Ukierunkowane audyty bezpieczeństwa, o których mowa w akapicie pierwszym lit. b), opierają się na oszacowaniach ryzyka przeprowadzonych przez właściwy organ lub badany podmiot bądź na innych dostępnych informacjach dotyczących ryzyka”. Zatem regularne audyty bezpieczeństwa powinny być audytami ukierunkowanymi, a nie audytami obejmującymi za każdym razem cały system informacyjny wykorzystywany do świadczenia usługi. Ponadto, należy zaznaczyć, że w projekcie ustawy usunięto faktyczne różnice pomiędzy obrazem kontroli działalności podmiotów kluczowych i ważnych. W praktyce w projekcie	Uwaga częściowo uwzględniona Uwaga została uwzględniona w zakresie wyłączenia spod regularnych audytów podmiotów ważnych oraz wydłużenia regularnych audytów dla podmiotów kluczowych do 3 lat. W pozostałym zakresie należy wskazać, że obowiązek przeprowadzania audytu funkcjonuje na podstawie już obecnie obowiązującej ustawy. Jednocześnie państwa członkowskie mogą podejmować dalej idące środki niż przewiduje dyrektywa NIS 2, jeżeli środki te są zgodne z celem dyrektywy. Związane jest to z harmonizacją minimalną.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. IV

			ustawy istnieją tylko dwie różnice pomiędzy podmiotami kluczowymi i ważnymi: przesłanki wszczęcia kontroli oraz maksymalny wymiar kary. W pozostałym zakresie rozróżnienie na podmioty kluczowe i ważne nie ma praktycznego znaczenia. Obrazuje to skalę nadregulacji w przypadku projektu ustawy. Art. 15. <u>1. Organ właściwy do spraw bezpieczeństwa może nałożyć na ~~Podmiot~~ podmiot kluczowy w drodze decyzji lub podmiot ważny ma obowiązek ~~zapewnić~~ przeprowadzenia, na własny koszt, ~~co najmniej~~ raz na ~~2~~ 3 lata lub rządziej, audytu bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi, zwanego dalej „audytem”, jeżeli przemawia za tym charakter i częstotliwość występowania cyberzagrożeń w sektorze, w którym podmiot ten prowadzi działalność. Zakres audytu organ właściwy do spraw cyberbezpieczeństwa określa na podstawie wyników oszacowania ryzyka dla podmiotu kluczowego, wykonanego przez ten podmiot lub przez organ lub innych dostępnych informacjach dotyczących ryzyka.</u> <u>1a. Uznaje się, że podmiot kluczowy nie naruszył terminu przeprowadzenia audytu, o którym mowa w ust. 1, jeżeli do przeprowadzenia audytu dojdzie w terminie późniejszym, lecz podmiot kluczowy wykaże, że zachował należyłą staranność w toku aktywnego poszukiwania audytora, spełniającego przesłanki określonego w art. 15 ust. 2-3.</u>	Ponadto wprowadzenie regulacji, że podmiot nie naruszył terminu, jeżeli zachował należyłą staranność w toku aktywnego poszukiwania audytora stanowiłoby pole do naruszeń i obejścia przepisów prawa. Ponadto stanowiłoby niezgodność z dyrektywą NIS 2.
66.	PIKE	Art. 15 ust. 1b	Wydaje się, że art. 15 ust. 1b dotyczy audytu, o którym mowa w art. 32 ust. 2 lit. c i art. 33 ust. 2 lit. b dyrektywy NIS2. Niezbędne wydaje się określenie realistycznego terminu na przeprowadzenie takiego audytu. PIKE wnosi nadto o powstrzymanie się od nadregulacji i o wierne wdrożenie ww. przepisów dyrektywy NIS2. Art. 15 [...] 1b. Organ właściwy do spraw cyberbezpieczeństwa może nakazać, w drodze decyzji: <u>1) podmiotowi kluczowemu, przeprowadzenie audytu, o którym mowa w ust. 1, doraźnie i w uzasadnionych przypadkach w związku z wystąpieniem incydentu poważnego lub z naruszeniem przez podmiot kluczowy obowiązków określonych w ustawie, wraz z określeniem adekwatnego terminu przekazania sprawozdania z przeprowadzonego audytu, nie krótszego jednak niż 3 miesiące od dnia doręczenia podmiotowi kluczowemu decyzji ostatecznej,</u> <u>2) podmiotowi ważnemu przeprowadzenie audytu, o którym mowa w ust. 1, wraz z określeniem adekwatnego terminu przekazania sprawozdania z przeprowadzonego audytu, nie krótszego jednak niż 3 miesiące od dnia doręczenia podmiotowi kluczowemu decyzji ostatecznej, przy czym zakres audytu organ właściwy do spraw cyberbezpieczeństwa określa na podstawie wyników oszacowania ryzyka dla podmiotu ważnego, wykonanego przez ten podmiot lub przez organ lub innych dostępnych informacjach dotyczących ryzyka.</u> <u>1b¹. Uznaje się, że podmiot kluczowy i podmiot ważny nie naruszył terminu przeprowadzenia audytu, o którym mowa w ust. 1b, jeżeli do przeprowadzenia audytu dojdzie w terminie</u>	Uwaga wyjaśniona Wskazać należy, że organ właściwy do spraw cyberbezpieczeństwa zlecając w ramach czynności nadzorczych przeprowadzenie audytu określa termin jego przeprowadzenia. Wprowadzenie regulacji, że podmiot nie naruszył terminu jeśli zachował należyłą staranność w toku aktywnego poszukiwania audytora stanowiłoby pole do naruszeń i obejścia przepisów prawa. Ponadto stanowiłoby niezgodność z dyrektywą NIS 2. W pozostałym zakresie należy zauważyć, że państwa członkowskie mają swobodę we wdrożeniu dalej idących środków, jeżeli pozostają one w zgodności z celem dyrektywy.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. IV

			<u>późniejszym niż określony zgodnie z ust. 1b, lecz podmiot ten wykaże, że zachował należytą staranność w toku aktywnego poszukiwania audytora, spełniającego przesłanki określonego w art. 15 ust. 2-3.</u>	
67.	Osoba fizyczna	Art. 16	Art. 16. Sankcje za naruszenia: Podmioty, które nie przestrzegają przepisów niniejszej ustawy, podlegają następującym sankcjom: 1) Kary finansowe do 5% rocznych przychodów lub budżetu podmiotu, w zależności od skali i powagi naruszenia. 2) Odpowiedzialność karna dla członków zarządu lub innych osób odpowiedzialnych za bezpieczeństwo cybernetyczne. 3) Zakazy działalności lub świadczenia usług do czasu pełnego wdrożenia zaleconych środków naprawczych. 4) Publiczne ostrzeżenia o naruszeniach oraz obowiązek naprawy szkód wyrządzonych przez incydent.	Uwaga wyjaśniona Sankcje za naruszenia zostały przewidziane w rozdziale 14 ustawy i zostały odpowiednio zmodyfikowane w taki sposób, aby zapewniały właściwe wdrożenie dyrektywy NIS 2. Przewiduje się zarówno kary finansowe oparte na % obrotu jak i kary finansowe dla kierownika podmiotu. W pozostałym zakresie organy właściwe do spraw cyberbezpieczeństwa sprawują nadzór nad podmiotami kluczowymi i podmiotami ważnymi. W związku z tym propozycje określone w niniejszej uwadze zostały już przez projektodawcę przewidziane w projekcie.
68.	PIKE	Art. 16 ust. 1	Oprócz argumentacji wskazanej w uwagach dot. w art. 7c ust. 6 należy dodać, że wdrożenie wszystkich obowiązków ujętych w projekcie ustawy łączyć się będzie w szczególności z zakupem oraz wdrożeniem rozwiązań wspierających spełnienie wymagań (które może trwać kilka miesięcy), ale także przygotowaniem, przetestowaniem oraz wdrożeniem polityk, procedur dla całej organizacji. Dla tych dokumentów należy przeprowadzić odpowiednie szkolenia dla pracowników, personelu IT, przygotowanie partnerów, a także środowiska, co także proces może przedłużyć. Mając na uwadze zakres i ilość branż objętych ustawą, niemożliwe może stać się znalezienie odpowiedniego partnera na wdrożenie rozwiązania, a firmy wdrożeniowe + dostawcy oprogramowania mogą znacząco podnieść ceny swoich usług, co negatywnie może wpłynąć na sytuację finansową. Należy mieć też na uwadze, że dla spełnienia wymagań konieczne może być zatrudnienie personelu, który ponownie przy ilości branż objętych ustawą, może być problem z zatrudnieniem odpowiednich kandydatów, a i koszty zatrudnienia ze względu na zapotrzebowanie rynkowe, mogą być znacznie podwyższone (zwiększenie wymagań płacowych). Z kolei proponowane zmiany w art. 15 uzasadniają wykreślenie art. 16 ust. 1 pkt 2. Art. 16. 1. Podmiot kluczowy i podmiot ważny:	Uwaga nieuwzględniona Termin 6 miesięczny pozostanie z uwagi na konieczność wdrożenia NIS2.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. IV

			1) realizuje obowiązki, o których mowa w niniejszym rozdziale, w terminie <u>12 6-miesięcy od dnia spełnienia przesłanek uznania za podmiot kluczowy lub podmiot ważny;</u> <u>2) zapewnia przeprowadzenie audytu, o którym mowa w art. 15 ust. 1 lub ust. 1b, po raz pierwszy w terminie 12 miesięcy</u> <u>— od dnia spełnienia przesłanek uznania za podmiot kluczowy lub podmiot ważny.</u>	
69.	Osoba fizyczna	Art. 18	Art. 18. Współpraca międzynarodowa: Podmioty kluczowe oraz ważne są zobowiązane do aktywnego uczestnictwa w międzynarodowych mechanizmach współpracy w zakresie cyberbezpieczeństwa w tym: 1) Wymiany informacji o zagrożeniach i incydentach cybernetycznych z organami cyberbezpieczeństwa innych krajów oraz instytucjami międzynarodowymi. 2) Udziału w międzynarodowych ćwiczeniach i symulacjach incydentów cybernetycznych. 3) Współpracy z organami ścigania innych państw w zakresie zwalczania przestępczości cybernetycznej. 4) Przestrzegania międzynarodowych standardów i norm dotyczących cyberbezpieczeństwa.	Uwaga nieuwzględniona W ocenie projektodawcy są to nadmiarowe obowiązki i nie zostaną wprowadzone w projekcie.
70.	PIKE	Art. 32 ust. 2	PIKE postuluje wykreślenie tego przepisu. Szczegółowe uzasadnienie uwagi znajduje się przy uwadze dot. art. 11 ust. 1 pkt 6. Wykreślenie at. 32 ust. 2.	Uwaga nieuwzględniona
71.	PIKE	Art. 32 ust. 3	PIKE postuluje: 1) jak wskazano wyżej: aby podmiot kluczowy i podmiot ważny były zobowiązane do współpracy tylko z jednym CSIRTem (sektorowym), a pozostałe CSIRTy (MON, NASK, GOV) uzyskiwały te informacje od CSIRTu sektorowego, 2) aby w toku obsługi incydentu minimalizować dodatkowe obowiązki nakładane na podmiot kluczowy i podmiot ważny. Art. 32 [...] 3. CSIRT <u>sektorowy, na polecenie CSIRT MON, CSIRT NASK lub CSIRT GOV, może</u> wystąpić <u>pośrednio</u> do podmiotu kluczowego lub podmiotu ważnego o udostępnienie informacji technicznych związanych z incydentem poważnym lub krytycznym, które będą niezbędne do przeprowadzenia analizy lub koordynacji obsługi takiego incydentu. <u>Przepis art. 11 1 pkt 5 [w brzmieniu określonym w niniejszych uwagach – wtrącenie moje] stosuje się odpowiednio.</u>	Uwaga nieuwzględniona Proponowane regulacje są niemożliwe do wprowadzenia, z uwagi na zróżnicowaną działalność podmiotów kluczowych i ważnych.
72.	PIKE	Art. 33 ust. 1b	Testy penetracyjne, o których mowa w przepisie wymagają uwzględnienia w umowach licencyjnych, a to oznacza czas potrzebny na renegotiacje umów. Jako alternatywę można zaproponować chociaż, aby uwzględnić w omawianej procedurze możliwość poinformowania dostawcy produktu/usługi/procesu ICT, ograniczenie do prowadzenia ich tylko w warunkach testowych lub dodanie przepisów o odpowiedzialności podmiotów prowadzących testy za zakłócenia w działaniu usług.	Uwaga uwzględniona Przepis zostanie odpowiednio zmieniony.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. IV

			Art. 33 [...] 1b. CSIRT MON, CSIRT NASK i CSIRT GOV prowadz ~~ają~~ <u>ę</u> badanie, o którym mowa w ust. 1, <u>w środowisku testowym i</u> jest uprawniony do stosowania technik mających na celu: obserwację i analizę pracy urządzenia lub oprogramowania, uzyskanie dostępu do przetwarzanych danych, odtworzenie postaci źródłowej oprogramowania, zwielokrotnienie (powielenie) kodu programowego oraz tłumaczenie (translacja) jego formy, odtworzenie algorytmu przetwarzania danych, identyfikację realizowanych funkcji, usunięcie lub przełamanie zabezpieczeń przed badaniem, identyfikację podatności lub identyfikację nieudokumentowanych funkcji realizowanych przez produkt ICT, usługi ICT lub procesu ICT.	
73.	Osoba fizyczna	Art. 33	Badania produktów ICT. Zapis w projekcie ustawy stanowi, iż badania produktu, usługi lub procesu ICT przez poszczególne CSIRTy nie narusza autorskich praw osobistych oraz majątkowych, oraz nie wymaga zgody licencjodawcy lub dysponenta produktu ICT, usługi ICT lub procesu ICT. W ocenie autora uwag, zapis taki jest nieprawdziwy, gdyż badanie takie będzie naruszało prawa autorskie, czy majątkowe, jak i często patentowe (o których nie wspomniano) i zapis taki nie będzie zwalniał a'priori z odpowiedzialności procesowej. Dodatkowo nie wskazano zapisów o ochronie wyników tychże badań.	Uwaga wyjaśniona Przepis jest konieczny aby zapewnić licencję ustawową dla zespołów CSIRT przeprowadzających badanie.
74.	PIKE	Art. 36b ust. 1 pkt 2	Przepis art. 36b ust. 1 pkt 2 stanowi: „Art. 36b. 1. Ocena bezpieczeństwa systemu informacyjnego może być przeprowadzona: 1) za zgodą podmiotu krajowego systemu cyberbezpieczeństwa, wyrażoną w formie pisemnej lub formie elektronicznej pod rygorem nieważności lub 2) na zlecenie organu właściwego do spraw cyberbezpieczeństwa. [...]” Powyższy przepis zdecydowanie wykracza poza wymagania dyrektywy NIS2. Zgodnie z art. 11 ust. 3 lit. e dyrektywy NIS2 ocena bezpieczeństwa systemu informacyjnego powinna następować na wniosek podmiotu kluczowego lub ważnego. W opinii PIKE bez uprzedzenia i bez wniosku podmiotu kluczowego lub podmiotu ważnego ocena bezpieczeństwa systemu informacyjnego powinna następować wyłącznie w środowisku testowym. Alternatywnie, podmioty prowadzące testy penetracyjne (ocenę bezpieczeństwa systemu informacyjnego) w środowisku produkcyjnym powinny ponosić odpowiedzialność za szkodę wynikającą z zakłóceń w świadczeniu usług na zasadach ogólnych. Art. 36b 1. 1. Ocena bezpieczeństwa systemu informacyjnego może być przeprowadzona: ~~1) za zgodą podmiotu krajowego systemu cyberbezpieczeństwa, wyrażoną w formie pisemnej lub formie elektronicznej pod rygorem nieważności~~ <u>lub</u> ~~2) na zlecenie organu właściwego do spraw cyberbezpieczeństwa.~~	Uwaga nieuwzględniona Dyrektywa NIS 2 dopuszcza security scans jako działanie nadzorcze – w polskiej propozycji zostało to wdrożone jako ocena bezpieczeństwa.
75.	PIKE	Art. 36b	Ocena bezpieczeństwa. W projekcie UKSC wskazuje się, iż poszczególne CSIRT może wytwarzać lub pozyskiwać urządzenia i oprogramowanie przystosowane do popełnienia przestępstw komputerowych (art. 269b. KK). Jednocześnie zaproponowano zapis, iż ocenę bezpieczeństwa systemu informacyjnego prowadzi się z uwzględnieniem zasady minimalizacji	Uwaga wyjaśniona W ocenie projektodawcy przepis jest potrzebny i powinien pozostać w projekcie. Ocena bezpieczeństwa może

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. IV

			zakłócenia pracy systemu informacyjnego lub ograniczenia jego dostępności i nie może prowadzić do <u>nieodwracalnego zniszczenia danych</u> przetwarzanych w systemie informacyjnym podlegającym tej ocenie. Zapisy te w sposób oczywisty zapewniają i zabezpieczają swobodę działania organów wykonujących badanie, jednakże, nie zabezpieczają PK/PW przed efektem takich działań. Należy pamiętać, iż oprogramowanie tego typu (za art. 269b), usuwające dane w sposób trwały (Darik's Boot and Nuke), Blancco, czy Secure Eraser), służące niszczeniu danych (File Shredder, czy BleachBit), wszelkie oprogramowanie brute-force czy też exploity działają w sposób nieodwracalny. Zapisy art. 36 wydaje się, iż służą jedynie działaniom związanym z wykonywaniem testów penetracyjnych. Jednakże delegacja do art. 269b znacznie poszerza katalog tegoż oprogramowania, a co za tym idzie działań i nieodwracalnych efektów tych czynności.	się odbyć na kopii systemu i wtedy będzie można w bezpieczny sposób sprawdzić odporność systemu na tego typu oprogramowanie.
76.	PIKE	Art. 46 ust. 6	Przepis stosuje zwrot "zapewnienie zgodności systemów", postanowienia te ograniczają swobodę działalności gospodarczej w obecnym kształcie - takie brzmienie idzie zdecydowanie za daleko, można użyć zwrotu „zapewnia kompatybilność systemów”. Art. 46 [...] 6. Podmioty kluczowe i podmioty ważne obowiązane są zapewnić ~~zgodność~~ kompatybilność swoich systemów informacyjnych z minimalnymi wymaganiami technicznymi i funkcjonalnymi korzystania z systemu teleinformatycznego, o którym mowa w ust. 1, w terminie 3 miesięcy od udostępnienia tych wymagań.	Uwaga wyjaśniona Zapewnienie zgodności systemów należy rozumieć jako kompatybilność.
77.	Osoba fizyczna	Art. 53	Działania organu ds. cyberbezpieczeństwa. Zapis projektu stanowi, iż w celu egzekwowania przepisów ustawy organ właściwy do spraw cyberbezpieczeństwa w stosunku do podmiotów kluczowych, może: nakazać podjęcie określonych czynności dotyczących obsługi incydentu. W przypadku nie podjęcia tychże działań organ właściwy do spraw cyberbezpieczeństwa, może zwrócić się do: organu, który udzielił koncesji podmiotowi kluczowemu albo podmiotowi ważnemu o jej zawieszenie, ograniczenie jej zakresu albo cofnięcie do czasu gdy podmiot kluczowy albo podmiot ważny podejmie działania niezbędne do usunięcia uchybień lub zaprzestania naruszeń. Semantycznie zapisy te rozszerzają treść odniesienia (pkt 5.1). Zapisy powyższe mogą spowodować, iż ustawa o KSC będzie ingerować tym samym na poziomie koncesjonowania sektora energetycznego, w tym wydobywczego (gazu, ropy, węgla). Należy pamiętać, iż incydenty KSC mogą nie mieć nic wspólnego z procesami wydobywczymi, a odbieranie koncesji może wstrzymać podstawową produkcję zakładu. Środek zaradczy, w ten sposób zapisany, wykracza poza zakres merytoryczny ustawy krajowego systemu cyberbezpieczeństwa.	Uwaga wyjaśniona Przepis jest bezpośrednim wdrożeniem postanowień dyrektywy NIS 2. Zgodnie z postanowieniami tej dyrektywy konieczne jest wyposażenie organu nadzorczego w kompetencje do nakazywania podjęcia określonych czynności dotyczących obsługi incydentu oraz – w przypadku braku realizacji tych czynności – kompetencje do podjęcia dalej idących działań, w tym np. zawieszenie, ograniczenie albo cofnięcie koncesji podmiotu. Nie można zgodzić się z zarzutem, że przepis wykracza poza to, co nakłada na państwa członkowskie dyrektywa NIS 2. Po pierwsze organ

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. IV

			Podobnie w pozostałych sektorach waga ograniczenia działalności podstawowej podmiotu, przykładowo przez wykreślenia z rejestru działalności gospodarczej, czy działalności regulowanej, wykracza poza nakaz usunięcia czynności związanych z obsługą incydentu.	właściwy do spraw cyberbezpieczeństwa sam nie dokonuje cofnięcia ani zawieszenia koncesji, a zwraca się do odpowiedniego organu, który jest kompetentny. Nie jest to także cofnięcie, zawieszenie czy ograniczenie koncesji o charakterze permanentnym. Po drugie należy wskazać, że akt jakim jest dyrektywa wiąże państwa członkowskie wyłącznie w zakresie harmonizacji minimalnej. Tym samym państwa członkowskie – jeśli widzą taką potrzebę i przyczyni się to do osiągnięcia założonego przez Unię Europejską celu – mogą przyjąć bardziej rygorystyczne środki służące – w tym przypadku – nadzorowi i egzekwowaniu przepisów. Projektodawca dąży do zapewnienia wysokiego poziomu skuteczności w zapewnieniu odpowiedniego poziomu bezpieczeństwa, realizacji obowiązków przez podmioty kluczowe lub podmioty ważne i tym samym nie może uznać przedmiotowej uwagi za uzasadnioną.
78.	PIKE	Art. 53 ust. 8	Przepis służy wdrożeniu art. 32 ust. 5 dyrektywy NIS2, przy czym ten przepis dyrektywy opiera się na założeniu, że niezwykle dotkliwe sankcje, o których mowa w tym przepisie, mają charakter tymczasowy - do czasu gdy podmiot kluczowy albo podmiot ważny podejmie działania niezbędne do usunięcia uchybień lub zaprzestania naruszeń. Wykreślenie podmiotu z rejestru działalności regulowanej jest środkiem, który nie ma tymczasowego charakteru, a przywrócenie wpisu (zatem wznowienie prowadzenia regulowanej działalności gospodarczej) będzie zależne od rozpatrzenia przez właściwy organ wniosku o ponowny wpis do rejestru. W przypadku rejestru przedsiębiorców telekomunikacyjnych, przykładowo, termin na wpisanie podmiotu do rejestru wynosi 7 dni. To oznacza, że nawet przez tydzień podmiot kluczowy nie będzie mógł prowadzić działalności. Taka sytuacja byłaby niezwykle szkodliwa dla każdego przedsiębiorcy. PIKE nalega, aby art. 33 ust. 5 dyrektywy NIS2 wdrożyć tylko w niezbędnym zakresie i zrezygnować z możliwości wykreślenia podmiotu kluczowego z rejestru.	Uwaga częściowo uwzględniona Przepis został zmodyfikowany w ten sposób, że zastosowanie znajdzie wyłącznie do podmiotów kluczowych. Środki te nie będą mogły być stosowane do momentu rozpatrzenia sprawy przez sąd, jeśli zostanie złożona skarga. Ponadto wykreślono środek polegający na wykreśleniu podmiotu z rejestru działalności regulowanej i określono w odrębnym przepisie procedurę stosowania środków określonych w art. 53 ust. 8.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. IV

			Ponadto, zniesienie wszystkich pozostałych tymczasowych sankcji powinno następować automatycznie, już od chwili, gdy podmiot kluczowy podejmie działania niezbędne do usunięcia uchybień lub zaprzestania naruszeń. W projekcie ustawy brak jest wskazania, w jaki sposób dochodzi do ustalenia, że podmiot kluczowy podjął działania niezbędne do usunięcia uchybień lub zaprzestania naruszeń. Warto dodać, że art. 32 ust. 5 dyrektywy NIS2 nie ma swojego odpowiednika w przypadku podmiotów ważnych ani nie znajduje odpowiedniego zastosowania do podmiotów ważnych. W związku z tym środki przewidziane w tym przepisie nie powinny dotyczyć podmiotów ważnych. Dodatkowo, w art. 53 ust. 8 pkt 4 mowa jest o możliwości nałożenia przez sąd tymczasowego zakazu zajmowania stanowiska przez osoby kierujące podmiotem kluczowym. We wszystkich pozostałych przepisach projektu ustawy występuje pojęcie „kierownika”. Art. 53 [...] 8. Organ właściwy do spraw cyberbezpieczeństwa, w przypadku gdy podmiot kluczowy nie zastosował się do nakazu, o którym mowa w ust. 5 pkt 1 lub postanowień decyzji, o której mowa w ust. 5 pkt 2–5 lub 6, może zwrócić się do: 1) organu, który udzielił koncesji podmiotowi kluczowemu albo podmiotowi ważnemu o jej zawieszenie, ograniczenie jej zakresu albo cofnięcie do czasu gdy podmiot kluczowy <u>albo podmiot ważny</u> podjął działania niezbędne do usunięcia uchybień lub zaprzestania naruszeń; <u>2) organu, który dokonał wpisu podmiotu kluczowego albo podmiotu ważnego do rejestru działalności regulowanej, o wykreślenie podmiotu z tego rejestru;</u> 3) organu, który wydał podmiotowi <u>kluczowemu albo podmiotowi ważnemu</u> zezwolenie na prowadzenie działalności gospodarczej, o cofnięcie tego zezwolenia do czasu gdy podmiot kluczowy <u>albo podmiot ważny</u> podejmie działania niezbędne do usunięcia uchybień lub zaprzestania naruszeń; 4) sądu o nałożenie tymczasowego zakazu zajmowania stanowiska przez <u>osoby kierujące podmiotem kluczowym-kierownika podmiotu kluczowego.</u> <u>8a. Tymczasowe rozstrzygnięcia, o których mowa w ust. 8, zapadają w formie decyzji i zawierają w swojej sentencji rozstrzygnięcie o automatycznym zakończeniu obowiązywania tymczasowych rozstrzygnięć z chwilą podjęcia pierwszej czynności prowadzącej do usunięcia uchybień lub zaprzestania naruszeń.</u>	
79.	Związek Pracodawców Technologii Cyfrowych Lewiatan	Art. 53d	Art. 53d. Uprawnienia urzędnika monitorującego w zakresie nadzorowania wykonywania obowiązków przez podmiot kluczowy Jest: Art. 53d. 1. Urzędnik monitorujący, o którym mowa w art. 53 ust. 5 pkt 7, w zakresie nadzorowania wykonywania przez podmiot kluczowy obowiązków, o których mowa w rozdziale 3, jest uprawniony w szczególności do: 1) swobodnego wstępu i poruszania się po terenie podmiotu kluczowego bez obowiązku uzyskiwania przepustki; 2) wglądu do dokumentów dotyczących działalności podmiotu	Uwaga wyjaśniona Przepis art. 53d został zmodyfikowany w ten sposób, że realizował będzie swoje zadania po uzyskaniu przepustki oraz w pewnym zakresie po uprzednim zawiadomieniu podmiotu

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. IV

		kluczo-; 3) przetwarzanych osobowych w krajowym będącym do realizacji celu; 4) żądania złożenia uchwały lub piśmie- w prawach dotyczących kraju; 5) przeprowadzić ogląd urzędników, osób i systemów informacyjnych. 2. Urzędnik monitorujący realizuje powierzone mu zadania z zachowaniem przepisów o tajemnicy prawnie chronionej. Propozycja Art. 53d. 1. Urzędnik monitorujący, o którym mowa w art. 53 ust. 5 pkt 7, prowadzi nadzór wykonywania przez podmiot kluczowy obowiązków, o których mowa w rozdziale 3, z zachowaniem: 1) przedstawionego planu kontroli; podmiot kluczowy może zgłosić trudności do planu kontroli pod warunkiem wykazania, że naruszają one zasady zapisane w punktach 3) i 4) 2) procedur i polityk bezpieczeństwa i cyberbezpieczeństwa obowiązujących w podmiocie kluczowym; 3) utrzymania ciągłości działania, dostępności, integralności i poufności danych i systemów informacyjnych podmiotu kluczowego; 4) utrzymywania ciągłości dostępu, integralności i poufności danych i systemów informacyjnych i innych podmiotów; 5) zgodności z przepisami przetwarzania danych osobowych pracowników i kontrahentów podmiotu kluczowego w krajowym będącym do realizacji celu; 6) transparentności i pełnego udokumentowaniu zakresu prowadzenia nadzoru, zakresu uzyskanej dokumentacji i wyjaśnień, protokołu i wniosków pokontrolnych. 2. Urzędnik monitorujący, o którym mowa w art. 53 ust. 5 pkt 7, prowadzi nadzór wykonywania przez podmiot kluczowy obowiązków, o których mowa w rozdziale 3, jest w ramach planu kontroli uprawniony w szczególności do: 1) żądania złożenia uchwały lub piśmie- w prawach dotyczących kraju; 2) wglądu do dokumentów dotyczących działalności podmiotu kluczowego w zakresie związanym z niniejszą ustawą 3. Urzędnik monitorujący realizuje powierzone mu zadania z zachowaniem przepisów o tajemnicy prawnie chronionej 4. W sytuacjach zagrażających bezpieczeństwu publicznemu lub bezpieczeństwu narodowemu urzędnik monitorujący może odstąpić od zasad zapisanych w ust. 1-3 Uzasadnienie: Ust. 1 Przedstawienie planu kontroli pozwala podmiotowi kluczowemu przygotować się w sposób nie naruszający normalnego funkcjonowania (patrz punkty 3) i 4). Warto zaznaczyć, że dla większych podmiotów kluczowych przedmiotem kontroli może być wycinek ich działalności. Praktyka przedstawiania planu kontroli jest znana z działań innych regulatorów. Podmiot kluczowy może zgłosić zastrzeżenia do planu kontroli jeśli jest w stanie wykazać, że w wyniku kontroli mogą być naruszone ciągłość działania, dostępność, integralność lub poufność danych i systemów informacyjnych tego podmiotu lub innych podmiotów. Kontrola w podmiocie kluczowym musi być przeprowadzona zgodnie z obowiązującymi w tym podmiocie procedurami i politykami. Po pierwsze, nie będzie to naruszało przyjętych polityk, a prowadzenie nadzoru zostanie odnotowane we właściwych dokumentach. Po wtóre, jeśli w ramach tych polityk i procedur zostaną zauważone niedociągnięcia będzie można zaproponować w protokole pokontrolnym właściwe środki zaradcze i ich poprawę. Po trzecie, jeśli podmiot kluczowy został certyfikowany na zgodność z odpowiednimi normami to	monitorowanego. Będzie musiał mieć ściśle wyznaczone zadania przez organ właściwy do spraw cyberbezpieczeństwa oraz będzie mógł zostać wyznaczony na czas określony nie dłuższy niż miesiąc.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. IV

			naruszenie przyjętych praktyk może oznaczać zanegowanie takiej certyfikacji. Proces nadzoru nie może w żaden sposób naruszyć ciągłości działania, dostępności, integralności i poufności danych i systemów informacyjnych podmiotu kluczowego. Proces nadzoru nie może także naruszać ciągłości działania, dostępności, integralności i poufności danych i systemów informacyjnych innych podmiotów – ta sytuacja może mieć miejsce w przypadku podmiotu kluczowego będącego częścią grupy podmiotów (polskich i zagranicznych) ze współdzielonymi usługami, a także wykorzystywane są takie formy przetwarzania jak outsourcing, hosting, kolokacja lub chmura obliczeniowa wykorzystujące zewnętrzną infrastrukturę. Podmiotem kluczowym mogą być także dostawcy usług chmurowych, w których infrastrukturze przetwarza wiele podmiotów. Interesy tych podmiotów – nie objętych kontrolą! - muszą być chronione w trakcie prowadzenia nadzoru. Proces nadzoru może – w zakresie i dla realizacji celu nadzoru – być związany z przetwarzaniem danych osobowych. Zakres ten należy zawęzić do danych osobowych pracowników i kontrahentów podmiotu kluczowego. Sposób przetwarzania danych osobowych nie może powodować powstawania wątpliwości co do charakteru przetwarzania w trakcie nadzoru np. czy urzędnik monitorujący staje się administratorem tych danych, współadministratorem, następuje powierzenie danych, celu przetwarzania itp. itd. Proces nadzoru musi być prowadzony w sposób transparentny i prawidłowo udokumentowany . Ust. 2 Urzędnik monitorujący może zapoznawać się z dokumentami podmiotu kluczowego mającymi związek z ustawą, a nie do wszelkich dokumentów. Zakres musi być prawidłowo określony. Ust. 4 Wszystkie zapisane powyżej zasady dotyczą nadzoru rutynowego i przebiegającego w normalnych warunkach mogą jednak być zawieszane jeśli sytuacja zagraża bezpieczeństwu narodowemu lub publicznemu.	
80.	PIKE	Art. 67b ust. 1 i nast. – uwaga ogólna dot. dostawcy wysokiego ryzyka	W opinii PIKE z projektu ustawy wszystkie regulacje w zakresie dostawcy wysokiego ryzyka powinny być ujęte w rekomendacjach Pełnomocnika Rządu ds. Cyberbezpieczeństwa, a ostateczne decyzje w zakresie stosowania sprzętu i oprogramowania od takiego dostawcy powinny należeć do podmiotów kluczowych i ważnych, podejmowane w ramach analizy ryzyka. Takie rozwiązanie byłoby zgodne z 5G Toolbox i zarazem zgodne z celami dyrektywy NIS2: NIS2 opiera się na założeniu, że każdy podmiot indywidualnie powinien oceniać swoje ryzyka, w tym ryzyka w łańcuchu dostaw. . Z kolei rozwiązanie ujęte w ustawie stanowi pogwałcenie zasady proporcjonalności.	Uwaga nieuwzględniona Kwestia dostawcy wysokiego ryzyka jest ujęta w projekcie jako sprawa mająca istotne znaczenie dla bezpieczeństwa narodowego.
81.	PIKE	Art. 67b ust. 2-4	W razie nieuwzględnienia naszej uwagi ogólnej powyżej, wskazujemy, że w postępowaniu w sprawie uznania dostawcy sprzętu/oprogramowania za dostawcę wysokiego ryzyka wyłączono stosowanie art. 28, art. 31, art. 51, art. 66a i art. 79 KPA. Oznacza to, że zasadniczo przedsiębiorcy telekomunikacyjni (ani inne podmioty korzystające ze sprzętu/oprogramowania, które planuje się wykluczyć z rynku) nie mogą brać udziału w charakterze strony w tym postępowaniu. Wyjątek: przedsiębiorcy telekomunikacyjni osiągający roczny przychód z tytułu prowadzenia działalności telekomunikacyjnej w wysokości co najmniej 20.000-krotności przeciętnego wynagrodzenia (ok. 143 109 600 PLN). Organizacje społeczne	Uwaga nieuwzględniona Wyłączenia KPA są niezbędne celem zapewnienia sprawności postępowania.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. IV

			także nie będą mogły brać udziału w takim postępowaniu w charakterze strony. Z kolei podmioty, które mogą przyłączyć się do postępowania w charakterze strony będą pozbawione ważnych praw z art. 79 KPA. Biorąc pod uwagę daleko idące skutki finansowe dla przedsiębiorców w razie wydania przez organ właściwy decyzji o uznaniu dostawcy sprzętu i oprogramowania za dostawcę wysokiego ryzyka (szacujemy, że w razie obowiązku wymiany sprzętu pełniącego funkcje krytyczne dla bezpieczeństwa w sieci 5G należałoby liczyć się z kosztami rzędu kilkudziesięciu milionów euro, a w przypadku sieci stacjonarnej przedsiębiorcy średniej wielkości – ok. 2,5 mln zł – załączamy do stanowiska symulację takich kosztów), <u>wylączenie stosowania art. 28, art. 31, art. 51, art. 66a i art. 79 Kodeksu postępowania administracyjnego jest niedopuszczalne i sprzeczne z motywem 143 dyrektywy NIS i Kartą Praw Podstawowych UE.</u> Art. 67b [...] <u>2. Stroną postępowania w sprawie uznania za dostawcę wysokiego ryzyka jest każdy wobec kogo zostało wszczęte postępowanie w sprawie uznania za dostawcę wysokiego ryzyka</u> Do postępowania w sprawie uznania za dostawcę wysokiego ryzyka, <u>jeżeli ustawa nie stanowi inaczej</u>, stosuje się przepisy ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego, <u>z wyłączeniem art. 28, art. 31, art. 51, art. 66a i art. 79 tej ustawy.</u> <u>3. Stroną postępowania w sprawie uznania za dostawcę wysokiego ryzyka jest każdy wobec kogo zostało wszczęte postępowanie w sprawie uznania za dostawcę wysokiego ryzyka.</u> <u>4. Do postępowania w sprawie uznania za dostawcę wysokiego ryzyka może przystąpić, na wniosek na prawach strony, przedsiębiorca komunikacji elektronicznej, który w poprzednim roku obrotowym uzyskał przychód z tytułu prowadzenia działalności telekomunikacyjnej w wysokości co najmniej dwudziestotysięcznej krotności przeciętnego wynagrodzenia w gospodarce narodowej wskazanego w ostatnim komunikacie Prezesa Głównego Urzędu Statystycznego, o którym mowa w art. 20 pkt 1 lit. a ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych (Dz. U. z 2023 r. poz. 1251, 1429 i 1672). Przepisy art. 31 § 2 i 3 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego stosuje się odpowiednio.</u> <u>5. Za poprzedni rok obrotowy uznaje się rok, przed którym postępowanie zostało wszczęte. Za ostatni komunikat Prezesa Głównego Urzędu Statystycznego uznaje się ostatni komunikat Prezesa Głównego Urzędu Statystycznego przed wszczęciem postępowania.</u>	
82.	PIKE	Art. 67b ust. 11 i 15	Decyzja dotycząca uznania dostawcy za dostawcę wysokiego ryzyka zostaje wydana, jeżeli dostawca ten stanowi poważne zagrożenie dla obronności, bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego, lub życia i zdrowia ludzi. Przed wydaniem tej decyzji właściwy minister zasięga opinii Kolegium, obejmującej szereg zagadnień, z których część ma charakter wyłącznie polityczny (art. 67b ust. 11 pkt 1).	Uwaga nieuwzględniona Identyfikacja dostawcy wysokiego ryzyka musi obejmować wszystkie kwestie techniczne jak i nietechniczne.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. IV

			Art. 67b ust. 15 nie gwarantuje, że warunkiem uznania, iż dostawca stanowi zagrożenie, jest np. wystąpienie choćby jednego incydentu poważnego w związku z podatnością sprzętu/oprogramowania, które będzie musiało być usunięte. Istnieje możliwość, że sam fakt, iż państwo spoza UE/NATO może ingerować w swobodę działalności gospodarczej dostawcy przesądzi o uznaniu tego dostawcy za dostawcę wysokiego ryzyka. Jednocześnie postępowanie będzie częściowo utajnione, więc okoliczności, które ostatecznie przesądziły o wydaniu decyzji, mogą być nieznane stronom postępowania – a tym bardziej wszystkim przedsiębiorcom, którzy będą musieli mierzyć się ze skutkami tej decyzji (czyli usuwać sprzęt). Zapewnienie bezpieczeństwa powinno oznaczać usuwanie sprzętu dostawcy, który rzeczywiście nie jest bezpieczny tzn. w jego sprzęcie pojawiają się podatności albo celowo umieszczano w nim backdoory. <u>Ponadto sprzeciw budzi usuwanie sprzętu bez rekompensaty.</u> Art. 67b [...] 11. Opinia, o której mowa w ust. 10, zawiera analizę: [...] 2) prawdopodobieństwa z jakim dostawca sprzętu lub oprogramowania znajduje się pod kontrolą <u>innego podmiotu, w szczególności osób sprawujących władzę w dowolnym państwie, państwa spoza terytorium Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego</u>, z uwzględnieniem: a) przepisów prawa regulujących stosunki między dostawcą sprzętu lub oprogramowania, a tym <u>państwem podmiotem</u> oraz praktyki stosowania prawa w tym zakresie, b) prawodawstwa oraz stosowania prawa w zakresie ochrony danych osobowych, w szczególności w przypadku, gdy nie ma porozumień w zakresie ochrony tych danych między Unią Europejską i tym państwem, c) struktury własnościowej dostawcy sprzętu lub oprogramowania, d) zdolności ingerencji tego <u>państwa podmiotu</u> w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania [...] 15. Minister właściwy do spraw informatyzacji, w drodze decyzji, uznaje dostawcę sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, jeżeli: - dostawca ten stanowi poważne zagrożenie dla obronności, bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego, lub życia i zdrowia ludzi <u>oraz</u> <u>- sprzęt ten lub oprogramowanie zawierały podatności, które doprowadziły do co najmniej jednego incydentu poważnego w Rzeczypospolitej Polskiej lub innym państwie członkowskim Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, a dostawca nie przystąpił natychmiast do skutecznego zneutralizowania takiej podatności lub</u>	

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. IV

			<u>- w sprzęcie tym lub oprogramowaniu jego dostawca celowo umieścić backdoor, który doprowadził do incydentu poważnego w Rzeczypospolitej Polskiej lub innym państwie członkowskim Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego.</u>	
83.	PIKE	Art. 67c ust. 1-3	Przepisy te przewidują obowiązek wycofania z użytkowania typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT dostarczanych przez dostawcę wysokiego ryzyka oraz zakaz wprowadzania do użytkowania produktów ICT, rodzajów usług ICT i konkretnych procesów ICT w zakresie objętym decyzją, dostarczanych przez dostawcę wysokiego ryzyka: co do zasady w ciągu 7 lat (4 lata w przypadku sprzętu/oprogramowania pełniącego funkcje krytyczne dla bezpieczeństwa w sieci 5G). Okres ten jest rażąco krótki. Twierdzenia Ministerstwa Cyfryzacji, ujęte w uzasadnieniu projektu ustawy, że termin 5-7 jest „często” uznawany za średni okres użytkowania sprzętu lub oprogramowania, czyli tzw. cykl życia urządzenia, jest o tyle nietrafione, że okres użytkowania sprzętu abonenckiego oraz sprzętu w sieci dostępowej „blisko” abonenta jest skrajnie różny (krótki) w porównaniu ze sprzętem i oprogramowaniem w sieci szkieletowej, pełniącym funkcje krytyczne dla bezpieczeństwa sieci. Co więcej, w uzasadnieniu wskazuje się, że w przypadku sprzętu 5G wykorzystywanego w radiowej sieci dostępowej (RAN) cykl życia urządzenia wynosi w większości przypadku od 5 do 10 lat. Tymczasem sam Minister Cyfryzacji zmierza do nakazania usunięcia tego sprzętu w ciągu 4 lat! Ponadto, niezależnie od cyklu życia urządzenia, należy wziąć pod uwagę inne czynniki. Otóż podstawowym problemem związanym z wymianą sprzętu dla sieci 5G jest konieczność wymiany sprzętu również dla 4G (wykorzystywana obecnie konfiguracja 5G non-standalone), nie tylko na tych samym lokalizacjach, ale de facto w całej sieci. W konsekwencji jest to dużo bardziej złożony projekt niż budowa sieci 5G, obejmujący wielokrotnie więcej lokalizacji fizycznych. Skala inżynieryjna projektu jest tak duża, że próba jego realizacji w ciągu 4 lat byłaby ograniczona ze względu na brak dostępności wyspecjalizowanych ekip instalacyjnych. Co więcej, wymiana sprzętu i oprogramowania jest równoznaczna z uruchomieniem bardzo dużego programu obejmującego nie jeden, ale co najmniej kilka projektów, dotyczących równoległe zmiany kilku systemów w tym samym czasie oraz dostosowanie pozostałych systemów do współpracy z nowym rozwiązaniem. Podkreślić należy, że ryzyko niedotrzymania wskazanego w Projekcie KSC 4 lat na usunięcie sprzętu i oprogramowania może być całkowicie niezależne od przedsiębiorcy telekomunikacyjnego w sytuacji, gdy pozostali dostawcy oferujący dany typ rozwiązania (ilość ich jest również ograniczona), nie będą w stanie wywiązać się z zamówień od nowych klientów w określonym czasie.	Uwaga nieuwzględniona Z uwagi na kwestie bezpieczeństwa należy wprowadzić krótszy 4-letni okres wycofania sprzętu dla funkcji krytycznych.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. IV

			Należy także zwrócić uwagę, że uznanie dostawcy za dostawcę wysokiego ryzyka niekoniecznie doprowadzi do tego, że nastanie w Polsce wyższy poziom cyberbezpieczeństwa. Wręcz przeciwnie: rozwiązania ujęte w projekcie ustawy mogą zachwiać stabilnością finansową przedsiębiorców prowadzących działalność w Polsce. Gdyby jednak regulacje w zakresie dostawcy wysokiego ryzyka miały zostać utrzymane, należałoby określić precyzyjnie okres, od którego należy liczyć bieg terminu na usunięcie sprzętu i oprogramowania dostawcy stanowiącego dostawcę wysokiego ryzyka. Należy także dopuścić serwis wszystkich kategorii sprzętu i oprogramowania do czasu jego całkowitego usunięcia. Art. 67c. 1. W przypadku wydania decyzji, o której mowa w art. 67b ust. 15, podmioty, o których mowa w art. 67b ust. 1: 1) nie wprowadzają do użytkowania typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT w zakresie objętym decyzją, do czasu wycofania z użytkowania typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT w zakresie objętym decyzją dostarczanych przez dostawcę wysokiego ryzyka nie później niż <u>7-10</u> lat od dnia <u>ogłoszenia lub udostępnienia informacji o</u> uprawomocnienia decyzji, o której mowa w art. 67b ust. 15. 2. Przedsiębiorcy telekomunikacyjni, o których mowa w art. 67b ust. 1 pkt 2, wycofują w ciągu <u>4-8</u> lat typy produktów ICT, rodzaje usług ICT, konkretne procesy ICT wskazane w decyzji i określone w wykazie kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług w załączniku nr 3 do ustawy. 3. Do czasu wycofania sprzętu lub oprogramowania, o którym mowa w ust. 1 pkt 2 <u>oraz w ust. 2</u>, dopuszcza się użytkowanie dotychczas posiadanych typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT w zakresie objętym decyzją, dostarczanych przez dostawcę wysokiego ryzyka, w zakresie naprawy, modernizacji, wymiany elementu lub aktualizacji, jeżeli jest to niezbędne dla zapewnienia odpowiedniej jakości i ciągłości świadczonych usług, w szczególności dokonywania niezbędnych napraw awarii lub uszkodzeń.	
84.	PIKE	Art. 67g ust. 3, 9, 10, 12, 13	Zgodnie z tym przepisem minister właściwy do spraw informatyzacji w przypadku wystąpienia incydentu krytycznego może, w drodze decyzji, wydać polecenie zabezpieczające podlegające natychmiastowej wykonalności. Nie ma jednak możliwości, aby z dnia na dzień (lub z godziny na godzinę) można było przestać stosować sprzęt lub oprogramowanie bez konsekwencji dla działalności gospodarczej i ciągłości świadczenia usługi (prowadzenia działalności). Z drugiej strony każdy racjonalnie działający podmiot kluczowy będzie miał wdrożone systemy zarządzania bezpieczeństwem informacji i odpowiednie polityki i procedury które de facto wstrzymają używania tego co przyczyniło się do incydentu krytycznego. Doprecyzowanie jest konieczne przynajmniej za pomocą zwrotu „nie później niż” dla celów ewentualnych kontroli organów właściwych.	Uwaga nieuwzględniona Polecenie zabezpieczające musi być decyzją generalną, więc należy wyłączyć część przepisów KPA, które nie są dostosowane do decyzji generalnych.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. IV

		Polecenie zabezpieczające może zawierać m.in.: - nakaz zastosowania określonej poprawki bezpieczeństwa w produkcie ICT, procesie ICT lub usłudze ICT posiadającym daną podatność, - zakaz korzystania z określonego produktu ICT, usługi ICT lub procesu ICT, które posiada podatność, która przyczyniła się do zaistnienia incydentu krytycznego, - nakaz wprowadzenia ograniczenia ruchu sieciowego z adresów IP lub adresów URL wchodzącego do infrastruktury podmiotu kluczowego lub podmiotu ważnego, który skutkując zakłóceniem usług świadczonych przez ten podmiot został sklasyfikowany przez CSIRT MON, CSIRT NASK lub CSIRT GOV jako przyczyna trwającego incydentu krytycznego, - nakaz wstrzymania dystrybucji lub zakaz instalacji określonej wersji oprogramowania. Oprócz tego, że artykuł ten zakłada wyłączenie stosowania art. 10, art. 34, art. 79, art. 81, art. 81a, art. 107 § 1 pkt 3, art. 145 § 1 pkt 4 i art. 156 § 1 pkt 4 oraz rozdziału 8 działu I KPA, co poważnie ogranicza możliwość wejścia w dialog z organem i zweryfikowania, czy organ nie popełnił w swoim rozumowaniu błędów, najważniejszym problemem jest czas trwania polecenia zabezpieczającego: „Polecenie zabezpieczające wydaje się na czas koordynacji obsługi incydentu krytycznego lub na czas oznaczony, nie dłużej niż na dwa lata.. Tymczasem polecenie zabezpieczające powinno być ściśle związane z incydem krytycznym i czasem jego trwania/obsługi – nie powinno być możliwości, że polecenie zostanie wydane na dwa lata pomimo, że incydent został już skutecznie zakończony. Art. 67g. [...] 3. Do postępowania w sprawie o wydanie polecenia zabezpieczającego <u>nie</u> stosuje się <u>art. 10, art. 34, art. 79, art. 81, art. 81a, art. 107 § 1 pkt 3, art. 145 § 1 pkt 4 i art. 156 § 1 pkt 4 oraz rozdziału 8 działu I</u> ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego, <u>pozostałe przepisy tej ustawy stosuje się odpowiednio</u>. [...] 9. Polecenie zabezpieczające zawiera: 1) wskazanie rodzaju lub rodzajów podmiotów, których dotyczy; 2) obowiązek określonego zachowania zmniejszającego skutki incydentu krytycznego lub pobiętego jego rozprzestrzenienia; 3) termin <u>rozpoczęcia</u> jego wdrożenia, <u>nie krótszy niż 48 godzin od ogłoszenia polecenia zabezpieczającego, o którym mowa w ust. 15.</u> 10. Obowiązkiem określonego zachowania, o którym mowa w ust. 9 pkt 2, jest: 1) nakaz przeprowadzenia szacowania ryzyka związanego ze stosowaniem określonego produktu ICT, usługi ICT lub procesu ICT i wprowadzenie środków ochrony proporcjonalnych do identyfikowanych ryzyk; 2) nakaz przeglądu planów ciągłości działania i planów odtworzenia działalności pod kątem ryzyka wyłączenia ciągłości działania krytycznego świadczonego dla podmiotów;	

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. IV

			3) nakaz <u>podjęcia działań zmierzających do zneutralizowania podatności ujawnionej zastosowania określonej poprawki bezpieczeństwa</u> w produkcie ICT, procesie ICT lub usłudze ICT <u>posiadającym daną podatność, przy czym polecenie zabezpieczające może wskazywać przykładowe sposoby neutralizacji podatności, lecz ostateczna decyzja w tym zakresie należy do adresata polecenia zabezpieczającego.</u> ~~4) nakaz szczególnej konfiguracji produktu ICT, usługi ICT lub procesu ICT, bpi i p d wykorzyst i m okr sło i podat o i;~~ 5) k wmozo go mo itorow i i h i y t mu; ~~6) zakaz korzystania z określonego produktu ICT, usługi ICT lub procesu ICT, które p i d podat o i, któr p y y il i e do i t i i i yd tu kryty go;~~ 7) nakaz wprowadzenia ograniczenia ruchu sieciowego z adresów IP lub adresów URL wchodzącego do infrastruktury podmiotu kluczowego lub podmiotu ważnego, który skutkując zakłóceniem usług świadczonych przez ten podmiot został sklasyfikowany przez CSIRT MON, CIRT NAK lub CIRT GOV jako p y y trw ją go i yd tu kryty go; ~~8) nakaz wstrzymania dystrybucji lub zakaz instalacji określonej wersji oprogram i;~~ 9) k b pi i okr sło y h i form ji, w tym d i ików y t mowy h; 10) nakaz wytworzenia obrazów stanu określonych urządzeń zainfekowanych złośliwym oprogramowaniem. 11. Wskazanie obowiązku określonego zachowania, o którym mowa w ust. 9 pkt 2, następuje z uwzględnieniem środków adekwatnych, w szczególności w świetle analizy, o której mowa w ust. 5. 12. Polecenie zabezpieczające wydaje się na czas koordynacji obsługi incydentu krytycznego <u>lub na czas oznaczony, nie dłużej niż na dwa lata. W przypadku, gdy polecenie zabezpieczające obejmuje nakaz, o którym mowa w ust. 10 pkt 7, minister właściwy do spraw informatyzacji publikuje w sposób określony w ust. 15 informację o zniesieniu tego nakazu natychmiast po zakończeniu koordynacji obsługi incydentu krytycznego lub po zakończeniu obsługi incydentu krytycznego przez podmiot, o którym mowa w ust. 10 pkt 7.</u> 13. Polecenie zabezpieczające wygasa: <u>1) z dniem wskazanym w ogłoszeniu o zakończeniu koordynacji obsługi incydentu w dzienniku urzędowym ministra właściwego do spraw informatyzacji, lub</u> <u>2) po upływie czasu, na który zostało wydane.</u> 14. Polecenie zabezpieczające podlega natychmiastowej wykonalności.	
85.	PERN	Art. 69	Art. 1 pkt 71 (art. 69 ust. 2 pkt 2 ustawy) – wyjaśnienia wymaga czy projektowany przepis obejmuje swoim zakresem regulacji również podmioty nie podlegające PZP a posiadające wewnętrzny regulamin zakupów.	Uwaga wyjaśniona Przepis nie obejmuje podmiotów, które nie podlegają PZP i które posiadają wewnętrzny regulamin zakupów.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. IV

86.	Osoba fizyczna	Załącznik	Załącznik. Brak numeracji z możliwością odwołań do pozycji.	Uwaga wyjaśniona Szablon aktu prawnego przygotowany przez Rządowe Centrum Legislacji ma domyślnie wyłączone numerowanie, co utrudnia wprowadzenie numeracji przy takich tabelach.
87.	Osoba fizyczna	Załącznik	Załącznik w sposób jednoznaczny wskazuje wiele podmiotów z różnych sektorów działalności gospodarczej. Jednakże brak tutaj wskazanej korelacji z definicją art. 5.1. W definicji wspomnianego art. wskazuje się, iż podmiotem kluczowym jest m.in: osoba fizyczna, osoba prawna albo jednostka organizacyjna nieposiadająca osobowości prawnej wskazana w załączniku nr 1 i nr 2 do ustawy, która przewyższa wymogi dla średniego przedsiębiorstwa określone w art. 2 ust. 1 załącznika I do rozporządzenia Komisji (UE) nr 651/2014 z dnia 17 czerwca 2014 r. uznającego niektóre rodzaje pomocy za zgodne z rynkiem wewnętrznym w zastosowaniu art. 107 i 108 Traktatu (Dz. Urz. UE L 187 z 26.06.2014, str. 1), zwanego dalej „rozporządzeniem 651/2014/UE”; Rozporządzenie Komisji (UE) nr 651/2014 z dnia 17 czerwca 2014 r., często nazywane ogólnego zwolnienia blokowego (General Block Exemption Regulation, GBER), określa kryteria, według których pewne rodzaje pomocy państwa mogą być uznane za zgodne z rynkiem wewnętrznym. Wymogi dotyczące klasyfikacji przedsiębiorstw na mikro, małe, średnie i duże są zawarte w Załączniku I tego rozporządzenia. Zgodnie z tym rozporządzeniem, średnie przedsiębiorstwo jest zdefiniowane jako firma, która: - Zatrudnia mniej niż 250 osób, - Osiąga roczny obrót nie przekraczający 50 milionów euro lub - Posiada roczny bilans ogółem nie przekraczający 43 milionów euro. Warto zaznaczyć, że przedsiębiorstwo musi spełniać warunek dotyczący zatrudnienia oraz jeden z dwóch pozostałych warunków finansowych (obróć lub bilans) aby być klasyfikowane jako średnie przedsiębiorstwo. Dodatkowo, przedsiębiorstwo nie może być własnością lub być kontrolowane przez jedno lub więcej przedsiębiorstw (z wyjątkiem publicznych instytucji inwestycyjnych, uniwersytetów lub instytucji non-profit prowadzących badania), które nie spełniają definicji MŚP (mikro, małych i średnich przedsiębiorstw). Przedsiębiorstwo, które przewyższa te wymogi, generalnie klasyfikuje się jako duże przedsiębiorstwo. To oznacza, że zatrudnia co najmniej 250 osób i/lub osiąga roczny obrót przekraczający 50 milionów euro, lub ma roczny bilans ogółem przekraczający 43 miliony euro.	Uwaga uwzględniona Załącznik i art. 5 zostaną uszeregowane.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. IV

			W poszczególnych sektorach, przykładowo zdrowia, zapis załącznika stanowi. iż podmiotem kluczowym jest: Przedsiębiorca prowadzący działalność w formie apteki ogólnodostępnej w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne. Przedsiębiorca prowadzący działalność w formie apteki ogólnodostępnej, według ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne, to osoba fizyczna, prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej, która uzyskała odpowiednie zezwolenie od właściwego organu do prowadzenia apteki. Apteka ogólnodostępna jest placówką, która zapewnia realizację recept oraz wydawanie produktów leczniczych i środków medycznych pacjentom. Brak tutaj wskazanej korelacji z definicją art. 5.1. Jednakże, przyjmując, iż załącznik w sposób bezpośredni wskazywałby podmioty kluczowe wg definicji zamieszczonych w przywołanych w nim przepisach (kolumna ostatnia), wydaje się być wielce nieprawdopodobne, aby przedsiębiorcy tego typu (apteki ogólnodostępne) spełnili/ały wszystkie obowiązki wynikające z przepisów UKSC.	
88.	Technomed	Nowa propozycja	Trzecią istotną kwestią wymagającą zmiany jest konieczność doprecyzowanie co należy rozumieć pod pojęciem „Podmioty produkujące wyroby medyczne w rozumieniu art. 2 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2017/745”. We wskazanym rozporządzeniu w art. 2 pkt 1 wskazana jest definicja wyrobu medycznego. Jesteśmy świadomi, że dyrektywa NIS 2 w Załącznikach I i II posługuje się pojęciem „podmiotu produkującego” niemniej zwraca się uwagę, że zarówno rozporządzenie 2017/745, jak i ustawa o wyrobach medycznych, nie zawiera w sobie definicji „podmiotu produkującego wyroby medyczne”, w konsekwencji czego trudno jest stwierdzić, jaka grupa podmiotów miałaby być objęta zakresem tej definicji. W związku z powyższym postulujemy by zakresem regulacji objęte zostały podmioty najbliższej definicyjnie „podmiotom produkującym” wyroby medyczne tj. producenci wyrobów medycznych. Jednocześnie pragniemy zwrócić uwagę, że Producent wyrobu medycznego nie jest zawsze podmiotem produkującym taki wyrób, co wynika z legalnej definicji producenta (osoba fizyczna lub prawna, która wytwarza lub całkowicie odtwarza wyrób lub która zleca zaprojektowanie, wytworzenie lub całkowite odtworzenie wyrobu i oferuje ten wyrób pod własnym imieniem i nazwiskiem lub nazwą lub znakiem towarowym;”),	Uwaga nieuwzględniona Przyjęcie definicji tego pojęcia w prawie krajowym stanowiłoby zawężenie w stosunku do przepisów dyrektywy NIS 2
89.	Polskiej Federacji Producentów Żywności Związek Pracodawców z siedzibą w Warszawie	Uwaga ogólna	Działając imieniem Polskiej Federacji Producentów Żywności Związek Pracodawców z siedzibą w Warszawie, uprzejmie informuję, iż projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) wdrażający dyrektywę NIS2 w Polsce może być postrzegany jako niekorzystny dla przedsiębiorstw produkujących żywność z następujących powodów: 1. Zakres regulacji Nowelizacja ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa, dalej jako: „ustawa KSC”, obejmuje nowe sektory gospodarki, w tym produkcję żywności, co może oznaczać, że więcej przedsiębiorstw będzie	Uwaga wyjaśniona Sektor produkcji żywności zostanie przeniesiony do sektorów ważnych.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. IV

			musiało spełniać wymogi dyrektywy, niezależnie od ich dotychczasowego doświadczenia w obszarze cyberbezpieczeństwa. 2. Dyrektywa unijna Sam fakt, że dyrektywa NIS2 uznaje producentów żywności za podmioty ważne, a nie kluczowe, sugeruje, że ich rola w kontekście cyberbezpieczeństwa jest istotna, ale nie na tyle krytyczna, aby wymagać najwyższego poziomu regulacji. Potencjalne opóźnienia w transpozycji Polska, podobnie jak inne państwa członkowskie UE, może napotkać trudności z terminową transpozycją dyrektywy NIS2, co sugeruje potrzebę przyjęcia bardziej elastycznego podejścia do klasyfikacji podmiotów. 4. Zwiększone obciążenia regulacyjne Nowe przepisy wprowadzają bardziej rygorystyczne wymogi dotyczące cyberbezpieczeństwa, co może oznaczać konieczność inwestycji w lepsze systemy zabezpieczeń i procedury zarządzania ryzykiem. 5. Wpływ na konkurencyjność Nadmierne obciążenia regulacyjne mogą wpłynąć negatywnie na konkurencyjność polskich producentów żywności na rynku europejskim, gdzie inne kraje mogą przyjąć mniej restrykcyjne podejście do klasyfikacji podmiotów w swoich krajowych transpozycjach dyrektywy NIS2. 6. Zróżnicowanie sektora Sektor produkcji żywności jest bardzo zróżnicowany, a zastosowanie jednolitych, rygorystycznych wymogów dla wszystkich podmiotów może nie uwzględniać specyfiki poszczególnych przedsiębiorstw. 7. Koszty implementacji Przedsiębiorstwa będą musiały ponieść znaczne koszty związane z dostosowaniem się do nowych wymogów, co może być szczególnie obciążające dla nowych sektorów gospodarki objętych projektem ustawy, w tym producentów żywności. 8. Wpływ na łańcuch dostaw Dyrektywa NIS2 dotyczy nie tylko producentów żywności, ale również firm należących do ich łańcuchów dostaw, co może komplikować współpracę i zwiększać koszty operacyjne. 9. Administracyjne kary pieniężne Za niewywiązanie się z obowiązków wynikających z dyrektywy NIS2 mogą zostać nałożone wysokie kary finansowe, niekoniecznie realistyczne w odniesieniu do polskich przedsiębiorstw, co stanowi dodatkowe ryzyko finansowe. 10. Odpowiedzialność indywidualna Osoby fizyczne odpowiedzialne za przedsiębiorstwo mogą być pociągnięte do odpowiedzialności za niewywiązanie się z obowiązków, co zwiększa presję na zarządzających i może wpływać na decyzje biznesowe. Głównym celem dyrektywy NIS2 jest zwiększenie bezpieczeństwa cyfrowego, co dla przedsiębiorstw produkujących żywność oznacza konieczność zmierzenia się z nowymi wyzwaniami i obciążeniami, które mogą i zapewne mocno wpłyną, na ich działalność gospodarczą. Istotne pozostaje, iż choć produkcja żywności jest ważna dla bezpieczeństwa społecznego i gospodarczego, powyższe argumenty wskazują, że nie musi być ona automatycznie uznawana za sektor kluczowy w kontekście wymogów NIS2, zwłaszcza jeśli dyrektywa unijna klasyfikuje te przedsiębiorstwa jako podmioty ważne, a nie kluczowe	
90.	MPA	Uwaga ogólna	Wdrożenie dyrektywy NIS2: realizacja celu art. 28 dotyczącego publicznego dostępu do wiarygodnych informacji WHOIS Motion Picture Association (MPA) pełni rolę słyszalnego na skalę globalną głosu i rzecznika międzynarodowej branży filmowej, telewizyjnej i streamingowej. Naszymi członkami są Walt Disney Studios Pictures, Netflix Studios, LLC,	Uwaga wyjaśniona Dostęp do danych zgromadzonych przez rejestr TLD oraz rejestratorów powinien być za pośrednictwem sądu/prokuratora

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. IV

		Paramount Pictures Corporation, Sony Pictures Entertainment Inc, Universal City Studios LLC i Warner Bros. Discovery. Firmy członkowskie MPA w znacznym stopniu produkują i inwestują w produkcję europejskich treści audiowizualnych, które poprzez ich dystrybucję znajdują również globalną publiczność. MPA odgrywa wiodącą rolę w zwalczaniu nielegalnego rozpowszechniania treści chronionych prawem autorskim i prawami pokrewnymi, które szkodzi dobrze prosperującemu ekosystemowi cyfrowemu. Celem MPA jest ograniczenie i złagodzenie piractwa poprzez skuteczne strategie egzekwowania prawa wymierzone w operatorów nielegalnych witryn i usług, a także pośredników, którzy je umożliwiają. MPA z zadowoleniem przyjęło przyjęcie Dyrektywy w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii (dyrektywa NIS2), a w szczególności przepisów dotyczących rejestrów nazw domen i usługi rejestracji nazw domen zawartych w art. 28 i motywach 109-112. Zapewnienie dostępu do wiarygodnych danych dotyczących rejestracji nazw domen ("dane WHOIS") ma zasadnicze znaczenie dla zwalczania nielegalnych i szkodliwych treści w internecie, w tym treści naruszających prawa autorskie, oraz ochrony zdrowia i bezpieczeństwa obywateli. W badaniu Komisji Europejskiej z 2022 r. dotyczącym nadużyć DNS weryfikacja danych WHOIS została uznana za jedno z głównych zaleceń w zakresie zapobiegania nadużyciom DNS, ich wykrywania i łagodzenia. Komisja Europejska uznała również niedawno w zaleceniu z 2024 r. w sprawie zwalczania obrotu towarami podrobionymi, że "dokładność i kompletność danych rejestracyjnych nazw domen może również odgrywać kluczową rolę w egzekwowaniu praw własności intelektualnej". Podkreślono również potrzebę, aby dostarczone dane rejestrowe były dokładne, zweryfikowane i odnosiły się do rzeczywistego użytkownika nazwy domeny, a nie tylko do dostawcy usług prywatności lub proxy. W związku z tym MPA z zadowoleniem przyjmuje fakt, że Polska jest w trakcie transpozycji dyrektywy NIS2 i pragnie zwrócić uwagę na następujące priorytety w celu zapewnienia solidnego wdrożenia art. 28 i znacznego zwiększenia dostępności i dokładności danych WHOIS: • Wnioskodawcy ubiegający się o prawnie uzasadniony dostęp: Motyw 110 dyrektywy NIS2 opisuje "wnioskodawców ubiegających się o prawnie uzasadniony dostęp," do danych WHOIS, o których mowa w art. 28 (5), jako "każdą osobę fizyczną lub prawną występującą z wnioskiem na podstawie prawa Unii lub prawa krajowego". Przepisy krajowe, w tym również prawo polskie, powinny zatem wyjaśniać, że "wnioskodawcy ubiegający się o prawnie uzasadniony dostęp" powinni być zdefiniowani nie tylko jako agencje rządowe, takie jak organy ścigania, ale także każda osoba fizyczna lub prawna składająca wniosek o dostęp do danych WHOIS w celu zbadania niezgodności z prawem, w tym między innymi w celu ustalenia, wykonania lub obrony roszczeń z zakresu cyberbezpieczeństwa, własności intelektualnej, ochrony konsumentów lub innych roszczeń prawnych. Jest to zgodne z zaleceniem Komisji Europejskiej w sprawie zwalczania obrotu towarami podrobionymi, które zachęca podmioty świadczące usługi rejestracji nazw domen w UE do uznawania wszelkich osób fizycznych lub prawnych, które składają wniosek o prawo do informacji (ROI) na mocy	czy innego organu prowadzącego postępowanie.

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. IV

			dyrektywy 2004/48/WE w sprawie egzekwowania praw własności intelektualnej (IPRED), za uprawnione osoby ubiegające się o dostęp. ¹ Ponadto dostęp do danych WHOIS, zgodnie z motywem 112 preambuły, musi być bezpłatny, a dane te muszą być dostarczane na żądanie uprawnionego podmiotu ubiegającego się o dostęp bez zbędnej zwłoki. Pragniemy zwrócić uwagę na niedawną belgijską transpozycję, która obejmuje "każdą osobę w kontekście naruszeń praw własności intelektualnej lub praw pokrewnych" na liście osób uznawanych za wnioskodawców ubiegających się o prawnie uzasadniony dostęp do celów zapewnienia dostępu do danych rejestracyjnych nazw domen. W związku z tym z starą się zachęcać, aby krajowe transpozycje dyrektywy NIS2 w całej UE przyjmowały podobne podejście przy definiowaniu "wnioskodawców ubiegających się o prawnie uzasadniony dostęp", które umożliwia skuteczne monitorowanie i zwalczanie nielegalnej działalności online.	
91.	MPA	Uwaga	Rozwiązanie kwestii korzystania z usług proxy/privacy: W badaniu przeprowadzonym w 2021 r. przez Urząd Unii Europejskiej ds. Własności Intelektualnej (EUIPO) zauważono, że "znaczny odsetek nazw domen wykorzystywanych do prowadzenia nielegalnej lub szkodliwej działalności w Internecie jest rejestrowany za pośrednictwem usług ochrony prywatności lub usług proxy" oraz że od czasu wejścia w życie RODO uzasadnienie legalnego korzystania z usług ochrony prywatności lub usług proxy "zostało zakwestionowane". ³ Krajowa transpozycja dyrektywy NIS2 powinna zatem uwzględniać popularność usług proxy lub prywatności wśród tych, którzy prowadzą nielegalną i szkodliwą działalność online. W przypadku złożenia uzasadnionego wniosku o dostęp należy ujawnić podstawowe dane rzeczywistego klienta/użytkownika nazwy domeny, a nie tylko dane dostawcy usługi prywatności lub proxy, jeśli taka usługa prywatności lub proxy została wykorzystana w procesie rejestracji. W związku z tym rekomendujemy, aby państwa członkowskie, w tym Polska, wyraźnie włączyły następujący przepis do swojej implementacji art. 28: "Dostarczając dane w odpowiedzi na uzasadnione wnioski o dostęp, rejestry nazw TLD i podmioty świadczące usługi rejestracji nazw domen dostarczają dane rzeczywistego użytkownika nazwy domeny i nie mogą zamiast tego dostarczać danych dostawcy usług rejestracji prywatności lub serwerów proxy w zakresie rejestracji, które mogły zostać wykorzystane w procesie rejestracji nazwy domeny.". W związku z tym transpozycja obowiązków wynikających z art. 28 w zakresie weryfikacji dokładności danych WHOIS powinna mieć wyraźne zastosowanie do dostawców usług ochrony prywatności i usług proxy oraz odsprzedawców nazw domen, a także do rejestratorów i rejestrów nazw TLD. Jest to zgodne z art. 6 (22), który wyraźnie obejmuje dostawców usług w zakresie rejestracji prywatności lub serwerów proxy oraz odsprzedawców nazw domen jako przykłady "podmiotów świadczących usługi rejestracji nazw domen".	Uwaga wyjaśniona Z definicji rejestratora domen wynika, że obejmuje także usługi prywatności/proxy także nie jest zasadne dodawanie takiego przepisu.
92.	MPA	Uwaga	Rozwiązywanie nadużyć DNS na dużą skalę i im zapobieganie: Cyberprzestępcy często rejestrują wiele, a czasem nawet tysiące nazw domen w krótkim okresie czasu. Dotyczy to w szczególności phishingu, dystrybucji złośliwego oprogramowania i rozpowszechniania treści naruszających prawa autorskie. Zapewnienie, że wnioskodawca ubiegający się o prawnie	Uwaga nieuwzględniona Zdaniem projektodawcy to może być nieproporcjonalne rozwiązanie. Zwalczanie nadużyć jest ważne, ale

Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. IV

			uzasadniony dostęp jest w stanie uzyskać listę wszystkich nazw domen zarejestrowanych przy użyciu tych samych danych rejestrującego (odwrotne wyszukiwanie WHOIS) jest niezbędne, gdy podejrzewa się złożone i rozproszone nielegalne działania na taką skalę. W związku z tym rekomendujemy, taką transpozycję art. 28, która umożliwia, aby "w przypadku, gdy nazwa domeny jest powiązana z nieuczciwą lub nielegalną działalnością, zgodnie z domniemaniem uprawnionego podmiotu ubiegającego się o dostęp, rejestry nazw TLD i podmioty świadczące usługi rejestracji nazw domen muszą, na żądanie, dostarczyć wnioskodawca ubiegający się o prawnie uzasadniony dostęp listę wszystkich nazw domen, którymi administrują lub które zarejestrowały przy użyciu tych samych danych rejestrującego".	rejestry TLD nie powinny udzielać informacji ponad miarę.
93.	MPA	Uwaga	Osoby prawne: Dane WHOIS osób prawnych (co najmniej nazwa i roboczy/weryfikowany numer telefonu oraz roboczy/weryfikowany kontaktowy adres e-mail) muszą być publicznie dostępne zgodnie z art. 28 (4) w zw. z motywem 112.	Uwaga wyjaśniona Dane te będą dostępne zgodnie z art. 16a ust. 7 z wyłączeniem danych osobowych.
94.	MPA	Uwaga	Weryfikacja: Procedury weryfikacji danych WHOIS powinny być solidne i stale aktualizowane w celu odzwierciedlenia rozwoju technologii i procesów. Jak określono w motywie 111, procedury te powinny "przeciwdziałać powstawaniu nieprawidłowych danych rejestracyjnych i poprawiać je [...]" i powinny "odzwierciedlać najlepsze praktyki stosowane w branży [...]" oraz postępy poczynione w dziedzinie identyfikacji elektronicznej", jak też obejmować zarówno "kontrole ex ante przeprowadzane w momencie rejestracji, jak i kontrole ex post przeprowadzane po rejestracji". Chociaż rejestry nazw TLD mogą nie być w stanie zweryfikować danych WHOIS w momencie rejestracji, ponieważ początkowe gromadzenie danych jest zwykle podejmowane przez rejestratorów i/lub usługi prywatności/proxy, z pewnością mogą one podjąć procedury ex post w celu weryfikacji danych WHOIS. Rekomendujemy, aby wdrożenie krajowe wprowadziło obowiązkowe procedury weryfikacji ex post dla rejestrów nazw TLD. Ponadto powinny zostać wprowadzone konsekwencje za przekazanie nieprawidłowych, niedokładnych lub niekompletnych danych rejestracyjnych. Zdecydowanie popieramy wdrożenie przez Belgię4 tego punktu w transpozycji art. 28 w następujący sposób: "Jeśli dane rejestracyjne nazwy domeny wymienione w ust. 1(2) nazwy domeny są nieprawidłowe, niedokładne lub niekompletne, rejestry nazw domen najwyższego poziomu i podmioty świadczące usługi rejestracji nazw domen natychmiast blokują działanie tej nazwy domeny do czasu, gdy właściciel nazwy domeny poprawi dane rejestracyjne, tak aby stały się one prawidłowe, dokładne i kompletne. Jeśli rejestrujący nazwę domeny nie uczyni tego w terminie ustalonym przez rejestr nazw domen najwyższego poziomu lub podmiot świadczący usługi rejestracji nazw domen, nazwa domeny zostanie anulowana. Przeniesienie zablokowanej nazwy domeny do innego podmiotu świadczącego usługi rejestracji nazw domen jest zabroniony".	Uwaga wyjaśniona Zdaniem projektodawcy aktualizacja polityk weryfikacji wynika z obecnej propozycji przepisów (art. 16a ust. 5a), bowiem bez okresowej aktualizacji polityk nie jest możliwe wykonanie obowiązku posiadania rzetelnych danych dot. rejestracji domen. Zgodnie z propozycją przepisów procedury weryfikacji obejmują działania weryfikacyjne na etapie rejestracji nazwy domeny lub po takiej rejestracji ponadto są wyważone i proporcjonalne oraz prowadzą do zweryfikowania co najmniej jednego ze sposobów kontaktu. Z tego przepisu wynika więc, że procedury skutecznie zapewniać weryfikację danych. Procedura weryfikacji, która nie była aktualizowana nie realizuje celu.
95.	MPA	Uwaga	Thick WHOIS: Pojedynczy rejestr nazw TLD dla domen .com i .net, odpowiada za ponad połowę wszystkich zarejestrowanych nazw domen na świecie i ma umowy z ponad 2000 rejestratorami na całym świecie. Agencje rządowe i inni wnioskodawcy ubiegający się o	Uwaga nieuwzględniona Nie planuje się, aby przebudować Krajowy Rejestr Domen w Thick

Tabela uwag zgłoszonych w ramach konsultacji publicznych do *projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. IV*

			prawnie uzasadniony dostęp są obecnie zmuszeni do wysłедzenia odpowiedniego rejestratora w celu złożenia wniosku o dane WHOIS. Żmudny proces, który się z tym wiąże, a także fakt, że rejestrator może znajdować się w kraju, który nie jest współpracujący w zakresie takich wniosków, całkowicie podważa cel, jakim jest zwiększenie cyberbezpieczeństwa, a zamiast tego służy zapewnieniu osłony i ochrony nielegalnym podmiotom. W związku z tym istotne jest, aby ten rejestr, jak również wszystkie inne rejestry nazw TLD, utrzymywały kompletną, dokładną i niezależną bazę danych WHOIS dla wszystkich nazw domen, którymi administrują (zwaną "Thick WHOIS"), a dane te muszą obejmować dane rzeczywistego użytkownika nazwy domeny, a nie tylko dane dostawcy usług prywatności lub proxy, które mogły zostać wykorzystane w procesie rejestracji (patrz wyżej). Ten krytyczny wymóg zapewni, że organy ścigania i inni wnioskodawcy ubiegający się o prawnie uzasadniony dostęp będą mieli scentralizowane i pojedyncze źródło, z którego będą mogli uzyskać pełne i dokładne dane dotyczące dowolnej nazwy domeny zarządzanej przez rejestr nazw TLD.	WHOIS. Zdaniem projektodawcy wystarczające będą przepisy dot. udostępniania danych przez rejestratorów domen.

Tabela uwag zgłoszonych w ramach opiniowania do *projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw* (UC32)

Lp.	Zgłaszający uwagę	Jednostka redakcyjna	Treść uwagi	Stanowisko Ministra Cyfryzacji
UWAGI do projektu				
1.	Rzecznik Małych i Średnich Przedsiębiorców	Uwaga ogólna	W uzasadnieniu do Projektu wskazuje się, iż jego celem jest m.in. podniesienie poziomu odporności na cyberzagrożenia oraz poziomu ochrony informacji w sektorach: publicznym, militarnym i prywatnym. Projekt ma realizować te cele w odniesieniu do zapewnienia bezpieczeństwa łańcucha dostaw i utworzenia krajowego systemu certyfikacji cyberbezpieczeństwa oraz w konsekwencji wzmocnienia krajowego systemu cyberbezpieczeństwa jako całości. Zawarte w Projekcie regulacje mogą mieć istotny wpływ na zasady podejmowania, wykonywania i zakończenia działalności gospodarczej na terytorium Rzeczypospolitej Polskiej, gdyż mogą nakładać na przedsiębiorców w poszczególnych sektorach gospodarki obowiązki związane z zapewnieniem dbałości o cyberbezpieczeństwo. Skutkiem projektowanych przepisów może być konieczność poniesienia dodatkowych kosztów oraz wysiłku organizacyjnego - związanych z dostosowaniem się poszczególnych podmiotów krajowego systemu cyberbezpieczeństwa do wymogów wynikających z projektowanej ustawy. Odrębnym celem projektu jest konieczność wdrożenia do krajowego systemu prawa Dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii (NIS 2), która rozszerza krąg podmiotów objętych obowiązkami w zakresie cyberbezpieczeństwa, poszerza katalog sektorów objętych takimi obowiązkami (obok sektorów energii, transportu, zdrowia, bankowości, infrastruktury rynków finansowych, zaopatrzenia w wodę, infrastruktury cyfrowej) o sektory: ścieki, zarządzanie ICT, przestrzeń kosmiczna, poczta, produkcja, produkcja i dystrybucję chemikaliów, produkcja i dystrybucja żywności. Dyrektywa 2022/2555 ustanawia również nowy podział - na podmioty kluczowe i podmioty ważne. Należy zaznaczyć, iż wiele z proponowanych regulacji może bezpośrednio dotyczyć zasad, jak również kosztów oraz wysiłku organizacyjnego związanych z wykonywaniem działalności gospodarczej na terytorium Rzeczypospolitej Polskiej w szczególności przez mikroprzedsiębiorców, małych i średnich przedsiębiorców. Mając natomiast na względzie motyw leżący u podstaw proponowanych Projektem regulacji, w szczególności konieczność zapewnienia odpowiedniego poziomu cyberbezpieczeństwa - Rzecznik Małych i Średnich Przedsiębiorców zwraca uwagę na dostrzeżone wątpliwości lub zastrzeżenia, które są możliwe do zweryfikowania lub zmiany na obecnym etapie prac nad projektowanym aktem normatywnym.	Uwaga wyjaśniona Przedstawione stanowisko zostało przyjęte do wiadomości.

Tabela uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

2.	Rzecznik Małych i Średnich Przedsiębiorców	Uwaga ogólna	Poza wskazanymi powyżej zastrzeżeniami i postulatami zmian, Rzecznik Małych i Średnich Przedsiębiorców zwraca uwagę, iż: Projekt nie różnicuje obowiązków w zależności od wielkości, charakteru oraz realizowanych zadań - przez podmioty publiczne. Sytuacja taka może prowadzić do konieczności wdrażania niepotrzebnych lub nieadekwatnych rozwiązań organizacyjnych oraz ponoszenia kosztów nieznajdujących oparcia w zasadach gospodarowania środkami publicznymi i w konsekwencji pozostających w sprzeczności z regulacjami ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych.	Uwaga nieuwzględniona Od 2012 r. podmioty publiczne, bez względu na wielkość są obowiązane wdrożyć system zarządzania bezpieczeństwem informacji. Tym samym środki na ten system powinny być od tego czasu budżetowane.
3.	Rzecznik Małych i Średnich Przedsiębiorców	Uwaga ogólna	Reasumując, w świetle przytoczonych uwag i postulatów ujawnia się najistotniejsze zastrzeżenie do projektowanego aktu normatywnego - pominięcie zasady proporcjonalności. Planowane regulacje przewidują objęcie ich zakresem bardzo szerokiego kręgu podmiotów, w tym również mikroprzedsiębiorców małych i średnich przedsiębiorców przy jednoczesnym braku wystarczającego i adekwatnego miarkowania obowiązków w zależności o wielkości podmiotu. Należy wziąć pod uwagę, iż konieczność dostosowania do zmian wynikających z Projektu pociągać za sobą będzie: - bardzo duże koszty, - zmiany organizacyjne w funkcjonowaniu podmiotów. Niezbędne może być stworzenie lub wydzielenie nowych struktur, zatrudnienie dodatkowych specjalistów oraz zmiana lub wdrożenie nowych procedur. Skala kosztów wymaganych do poniesienia, zwłaszcza dla mniejszych podmiotów, stanowić może istotną barierę w wykonywaniu działalności gospodarczej na terytorium Rzeczypospolitej Polskiej, stąd potrzeba wniesienia do Projektu przynajmniej postulowanych w niniejszym piśmie zmian. Ponadto, działając na podstawie art. 12 ust. 1 oraz ust. 2 pkt 2 ustawy o Rzeczniku małych i średnich przedsiębiorców, załączam do niniejszej opinii wystąpienia organizacji przedsiębiorców skierowane do Rzecznika w przedmiocie uwag do przedmiotowego Projektu, wraz z prośbą o zajęcie merytorycznego stanowiska w odniesieniu do wszystkich podniesionych w nich zagadnień.	Uwaga wyjaśniona Co do zasady ustawie podlegają średnie przedsiębiorstwa z pewnymi wyjątkami, głównie wynikającymi z samej dyrektywy NIS 2. W obliczu obecnej sytuacji w cyberprzestrzeni konieczne jest nałożenie obowiązków z zakresu cyberbezpieczeństwa. Projekt przewiduje, że podmioty kluczowe i podmioty ważne będą wdrażać środki techniczne i organizacyjne proporcjonalne do wielkości podmiotu – uwzględniona została więc sytuacja podmiotów z sektora MŚP. Uwagi do załączonych stanowisk organizacji omówiono w tabeli z konsultacji publicznych.
4.	Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy	Uwaga ogólna	Obecnie trwają również prace nad ustawą o krajowym systemie certyfikacji cyberbezpieczeństwa, która służy stosowaniu rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno – komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie). Warto w projekcie nowelizacji ustawy o KSC zawrzeć	Uwaga wyjaśniona Należy zauważyć, że nie można odwoływać się w przepisach do projektów ustaw, w związku z czym nie można wprost odwołać się do przepisów projektu ustawy

Tabela uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

			spoiwo łączące oba te akty prawne. Po pierwsze, obie regulacje dotyczą zagadnień o tematyce związanej z cyberbezpieczeństwem, a podstawowy cel obu aktów jest zbliżony tj. określenie odpowiednio schematu krajowego systemu cyberbezpieczeństwa (ustawa o KSC) i krajowego systemu certyfikacji cyberbezpieczeństwa oraz zadań i obowiązków podmiotów wchodzących w skład tych systemów. Oba schematy uzupełniają się nawzajem tworząc, na poziomie krajowym, pełny schemat systemu cyberbezpieczeństwa. Po drugie, na poziomie unijnym akty prawne z zakresu prawa nowych technologii wzajemnie się uzupełniają tworząc jedną, zwartą całość. Wydaje się, że podobne podejście należy przyjąć w stosunku do ustawodawstwa krajowego wprowadzającego na grunt polski przepisy unijne.	o krajowym systemie certyfikacji cyberbezpieczeństwa, zwłaszcza, że oba projekty ciągle ulegają zmianom. Ustawa o krajowym systemie cyberbezpieczeństwa nawiązuje już do kwestii certyfikacji, np. dodawany art. 45 ust. 1 pkt 8.
5.	Narodowy Bank Polski	Uwaga ogólna	Na wstępie pragniemy wskazać, że projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (dalej jako „projekt ustawy”) w jego obecnym kształcie budzi daleko idące wątpliwości co do założeń znajdujących się po stronie projektodawcy. Trudno bowiem zgodzić się z przedstawionym w uzasadnieniu do przedmiotowego projektu podejściem, że pomimo identyfikowania konstytucyjnej niezależności Narodowego Banku Polskiego przez projektodawcę, jedyną kategorią ograniczeń w zakresie stosowania zaproponowanych regulacji są przepisy dotyczące wycofania produktów ICT, usług ICT lub procesów ICT pochodzących od dostawcy wysokiego ryzyka. Zaniepokojenie banku centralnego budzi fakt, że projekt ustawy w jego obecnym kształcie nie podlega konsultacji z Narodowym Bankiem Polskim oraz nie został skierowany do NBP w celu jego zaopiniowania po jego opublikowaniu w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji. Powyższe jest o tyle istotne, że projektowane zmiany dotyczące obowiązków NBP wynikających z ustawy dnia 5 lipca 2018 r. <i>o krajowym systemie cyberbezpieczeństwa</i> (dalej jako „ustawa o KSC”) są w naszej ocenie daleko idące. Narodowy Bank Polski zauważa, że mimo iż projekt ustawy przewiduje w niektórych aspektach wprowadzenie rozwiązań uwzględniających specyfikę banku centralnego, takich jak wyłączenie możliwości żądania wycofania przez bank centralny produktów, usług lub procesów ICT, co należy ocenić pozytywnie, to jednak proponowana regulacja nie zawiera podmiotowego wyłączenia przewidzianego dla banku centralnego, co jest niezgodne z intencją unijnego prawodawcy. Należy zauważyć, że wyłączenie takie zawarte jest w implementowanej do prawa polskiego dyrektywie Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r.	Uwaga częściowo uwzględniona Projekt zostanie skierowany do zaopiniowania przez Europejski Bank Centralny. Narodowy Bank Polski już obecnie jest podmiotem krajowego systemu cyberbezpieczeństwa co wynika z art. 4 pkt 9 ustawy. Jest m.in. zobowiązany do zarządzania incyidentem oraz zgłaszania incydentów w podmiocie publicznym do CSIRT GOV. Działalność Narodowego Banku Polskiego jest kluczowa dla stabilności polskiego systemu finansowego. Z tego powodu Narodowy Bank Polski powinien być elementem krajowego systemu cyberbezpieczeństwa.

Tabela uwag zgłoszonych w ramach opiniowania do *projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)*

		w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniającej rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającą dyrektywę (UE) 2016/1148 (dalej jako „dyrektywa NIS2”). Artykuł 6 pkt 35 przywołanej regulacji UE stanowi: „podmiot administracji publicznej” oznacza podmiot uznany za taki w danym państwie członkowskim zgodnie z prawem krajowym, <u>z wyłączeniem sądownictwa, parlamentów lub banków centralnych</u>. W naszej ocenie wyłączenie podmiotowe dla NBP powinno znaleźć się w opiniowanym projekcie ustawy w celu zachowania zgodności z implementowaną dyrektywą oraz właściwego zapewnienia niezależności banku centralnego. Informujemy dodatkowo, że Europejski Bank Centralny w dniu 11 kwietnia 2022 r. wydał opinię w sprawie wniosku dotyczącego dyrektywy Parlamentu Europejskiego i Rady w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, uchylającej dyrektywę (UE) 2016/1148¹⁾. W punkcie 1.2 opinii EBC stwierdził: „1.2 <u>EBC zauważa również, że w podejściu ogólnym do proponowanej dyrektywy Rada proponuje zmianę mającą na celu wyłączenie „podmiotów prowadzących działalność w obszarze sądownictwa, parlamentów lub banków centralnych” z zakresu zastosowania proponowanej dyrektywy.</u> EBC rozumie, że proponowana zmiana dotyczyłaby wszystkich podstawowych zadań i kompetencji Europejskiego Systemu Banków Centralnych (ESBC), określonych w art. 127 ust. 2 Traktatu oraz w art. 3 ust. 1 Statutu Europejskiego Systemu Banków Centralnych i Europejskiego Banku Centralnego (...), takich jak wspieranie sprawnego funkcjonowania systemów płatniczych. W związku z tym uznaje się, że będące własnością Eurosystemu i obsługiwane przez Eurosystem infrastruktury rynku finansowego, takie jak systemy TARGET2²⁾ i TARGET2-Securities, wchodzą w zakres proponowanego przez Radę wyłączenia banków centralnych z zakresu zastosowania proponowanej dyrektywy”. Przywołanych w powyższym fragmencie art. 127 ust. 2 Traktatu o funkcjonowaniu UE oraz art. 3 ust. 1 Statutu ESBC nie stosuje się do Państw Członkowskich objętych derogacją, niemniej przedmiotowa opinia EBC powinna być kierunkowo zastosowana do wszystkich banków centralnych UE. W związku z tym, postulujemy o dokonanie rewizji projektu w zakresie podejścia projektodawcy do statusu Narodowego Banku	

¹⁾ EUR-Lex: <https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52022AB0014>

²⁾ System TARGET2 w dniu 20 marca 2023 r. został zastąpiony przez system TARGET.

			Polskiego, dostosowując projekt ustawy do prawodawstwa zarówno krajowego jak i europejskiego. Pomimo wskazanych powyżej regulacji niezrozumiałe jest stanowisko projektodawcy znajdujące odzwierciedlenie w treści uzasadnienia projektu, zgodnie z którym „Projekt ustawy nie podlega przedstawieniu właściwym organom i instytucjom Unii Europejskiej, w tym Europejskiemu Bankowi Centralnemu, w celu uzyskania opinii, dokonania powiadomienia, konsultacji albo uzgodnienia.”, szczególnie w kontekście zobowiązań wynikających z udziału NBP w Europejskim Systemie Banków Centralnych. W przypadku opiniowanego projektu ustawy, właściwość EBC do wydania opinii wynika z art. 127 ust. 4 oraz art. 282 ust. 5 Traktatu o funkcjonowaniu Unii Europejskiej, jak również z art. 2 ust. 1 tiret trzecie, piąte i szóste decyzji 98/415/WE, gdyż projekt zawiera postanowienia odnoszące się do zadań NBP, tj. banku centralnego współtworzącego Europejski System Banków Centralnych. Zwracamy uwagę, że ewentualne niezastosowanie się polskich władz publicznych do obowiązku zasięgnięcia opinii EBC w trakcie niniejszego procesu legislacyjnego może przyczynić się do stwierdzenia naruszenia przepisów wspólnotowych, określających obowiązek konsultacji poszczególnych projektów aktów prawnych z organami UE. Należy ponadto wskazać, że konieczność pozyskania opinii Europejskiego Banku Centralnego w przypadku aktów implementujących przepisy dyrektywy NIS2 nie budzi zastrzeżeń innych zainteresowanych państw członkowskich UE, czego wyrazem jest wydana w dniu 13 maja br. opinia EBC (CON/2024/14) do projektu łotewskiej ustawy wprowadzającej dyrektywę NIS2 (Informācijas tehnoloģiju drošības likums, Latvijas Vēstnesis, 2010, 178)³⁾. Pragniemy również podkreślić, że Narodowy Bank Polski nałożone na niego (w związku z realizowaną w polskim systemie prawnym pozycją) zadania realizuje z poszanowaniem najwyższych standardów – w szczególności w zakresie bezpieczeństwa. NBP, pomimo braku takiego obowiązku, realizuje działania z zakresu dostosowania obowiązujących regulacji wewnętrznych do powszechnie uznanych standardów, m.in. takich jak normy z serii ISO 27000 czy 22301. Są to jednak działania o charakterze fakultatywnym względem otoczenia prawnego, w którym funkcjonuje NBP, co wpisuje się w konstytucyjną pozycję banku centralnego Rzeczypospolitej Polskiej.	

³⁾ <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52024AB0014>

Tabela uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

			Jakkolwiek kierunek działań proponowany przedmiotowym projektem, zmierzający do implementacji dyrektywy NIS2, zapewniający dostosowanie do nowych ram systemu zapewnienia cyberbezpieczeństwa w Unii Europejskiej poprzez zaproponowanie i wdrożenie odpowiednich i proporcjonalnych środków technicznych, operacyjnych i organizacyjnych w celu zarządzania ryzykiem dla bezpieczeństwa sieci i systemów informatycznych wykorzystywanych przez te podmioty do prowadzenia działalności lub świadczenia usług oraz w celu zapobiegania wpływowi incydentów na odbiorców ich usług lub na inne usługi bądź minimalizowania takiego wpływu - jest racjonalny, niemniej jego realizacja w stosunku do Narodowego Banku Polskiego budzi istotne zastrzeżenia. Wątpliwości dotyczące realnej niezależności banku centralnego budzą również projektowane przepisy odnoszące się do nadzoru i kontroli realizowanych w szczególności przez organy właściwe do spraw cyberbezpieczeństwa. W powyższe wpisują się również przepisy odnoszące się do odpowiedzialności w stosunku do kierownika podmiotu, a w szczególności w kontekście kar, które mogą być nakładane, a które mogą być realnym narzędziem nacisku, co stoi w oczywistej sprzeczności z samą ideą niezależności Narodowego Banku Polskiego jako banku centralnego Rzeczypospolitej Polskiej. Reasumując, w naszej ocenie realnie może dojść do materializacji naruszenia niezależności banku centralnego a tym samym do zachwiania fundamentów porządku prawa w Rzeczypospolitej Polskiej. Dodatkowo, abstrahując od aspektów merytorycznych przedmiotowego projektu ustawy, brak komunikacji projektodawcy z bankiem centralnym będącym podmiotem projektowanych rozwiązań nie wydaje się być w naszej ocenie dobrą praktyką i co najmniej poddaje w wątpliwość traktowanie Narodowego Banku Polskiego jako równorzędnego partnera w dyskusji o nowym kształcie przepisów ustanawiających ramy krajowego systemu cyberbezpieczeństwa.	
6.	Narodowy Bank Polski	Uwaga ogólna	Brak propozycji przepisów dodatkowych aktów prawnych w zakresie implementacji dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE (dyrektywa CER). Obecny brak propozycji przepisów dodatkowych aktów prawnych, które pozwoliłyby na jednolite podejście, co do wyłaniania usług, które mają kluczowe znaczenie dla utrzymania niezbędnych funkcji społecznych i gospodarczych państwa (w tym przypadku usług NBP), w rozumieniu dyrektywy CER, której implementacja	Uwaga wyjaśniona Projekt ustawy o zmianie ustawy o zarządzaniu kryzysowym oraz niektórych innych ustaw (UC47) ma wdrożyć dyrektywę Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę

Tabela uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

			pozostaje w gestii Rządowego Centrum Bezpieczeństwa, a w efekcie ma być powiązana z przedmiotową ustawą nie pozwala dokonać pełnej analizy potencjalnego wpływu wprowadzanych rozwiązań	Rady 2008/114/WE (Dz. Urz. UE L 333 z 27.12.2022 r. str. 164).
7.	Prezes Urzędu Komunikacji Elektronicznej	Art. 2 pkt 3b	Art. 1 pkt 2 lit. a w zakresie dotyczącym projektowanego art. 2 pkt 3b ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2023 r. poz. 913, z późn. zm.), zwanej dalej „ustawą o ksc” – przepisy projektowanej ustawy posługują się instytucją adresu do doręczeń elektronicznych, o którym mowa w art. 2 pkt 1 ustawy z dnia 18 listopada 2020 r. o doręczeniach elektronicznych. Wskazać należy, że np. przepis art. 7a ust. 3 zdanie drugie określa, iż zawiadomienie o wpisaniu do wykazu, o którym mowa w art. 7 ust. 1, przekazuje się na adres do doręczeń elektronicznych podmiotu (obligatoryjną konstrukcję przewidziano ponadto w art. 7b ust. 2, art. 53c ust. 3, art. 58 ust. 11 pkt 2). Podkreślić należy, że przepisy ustawy z dnia 18 listopada 2020 r. o doręczeniach elektronicznych w zakresie obowiązku posiadania adresu do doręczeń elektronicznych przez podmioty niepubliczne wciąż nie weszły w życie (np. art. 9 ust. 1 pkt 9 ustawy z dnia 18 listopada 2020 r. o doręczeniach elektronicznych, który dotyczy podmiotów niepublicznych wpisanych do Centralnej Ewidencji i Informacji o Działalności Gospodarczej) i w obrocie prawnym będziemy mieli do czynienia z podmiotami, które jeszcze przez ponad dwa lata nie będą zobligowane do posiadania adresu do doręczeń elektronicznych. W kontekście terminu implementacji dyrektywy NIS 2 (18 października 2024 r.) oraz miesięcznego vacatio legis projektowanych regulacji należy podnieść, że obowiązek przekazania określonych dokumentów na adres do doręczeń elektronicznych, o którym mowa w art. 2 pkt 1 ustawy z dnia 18 listopada 2020 r. o doręczeniach elektronicznych, będzie w przypadku pewnej grupy podmiotów niemożliwy do wykonania, gdyż nie będą one zobligowane do posiadania takiego adresu. Wydaje się, że problemu nie rozwiązuje projektowany przepis przejściowy art. 17, który obejmuje okres do czasu wdrożenia przez ministra właściwego do spraw informatyzacji rozwiązań technicznych niezbędnych do doręczania korespondencji z wykorzystaniem publicznej usługi rejestrowanego doręczenia elektronicznego lub publicznej usługi hybrydowej (zgodnie z art. 155 ust. 10 ustawy z dnia 18 listopada 2020 r. o doręczeniach elektronicznych, minister właściwy do spraw informatyzacji ogłosi komunikat określający termin wdrożenia przedmiotowych rozwiązań, który nie może być późniejszy niż 1 stycznia 2025 r.). Przepisu art. 17 nie będzie można zatem zastosować do okresu, jaki nastąpi po wskazanym wyżej wdrożeniu, natomiast np. podmioty niepubliczne wpisane do Centralnej Ewidencji i Informacji o Działalności	Uwaga uwzględniona Doręczanie będzie odbywało się w sposób zgodny z KPA.

Tabela uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

			Gospodarczej są obowiązane uzyskać wpis adresu do doręczeń elektronicznych do bazy adresów elektronicznych w terminie do dnia 30 września 2026 r.;	
8.	Prezes Urzędu Ochrony Danych Osobowych	Uwaga ogólna	Test prywatności Z projektowanego projektu ustawy, uzasadnienia ani dokumentów do niego dołączonych nie wynika, aby projektodawca przeprowadził test prywatności w procesie tworzenia prawa, w tym ocenę skutków dla ochrony danych, zgodnie z art. 25 ust. 1 ⁴⁾ i art. 35 rozporządzenia 2016/679 ⁵⁾ . Test ten, powinien być dokonany przez prawodawcę w razie konstruowania przepisów dotyczących przetwarzania, którego rodzaj, w szczególności z użyciem nowych technologii, ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych. Test prywatności, co do	Uwaga uwzględniona Test prywatności zostanie przeprowadzony, a jego wyniki zostaną zawarte w OSR do projektu.

⁴⁾ 7. Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze wynikające z przetwarzania, administrator - zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania - wdraża odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi niniejszego rozporządzenia oraz chronić prawa osób, których dane dotyczą.

⁵⁾ 1. Jeżeli dany rodzaj przetwarzania - w szczególności z użyciem nowych technologii - ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę. 2. Dokonując oceny skutków dla ochrony danych, administrator konsultuje się z inspektorem ochrony danych, jeżeli został on wyznaczony. 3. Ocena skutków dla ochrony danych, o której mowa w ust. 1, jest wymagana w szczególności w przypadku: a) systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną; b) przetwarzania na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1, lub danych osobowych dotyczących wyroków skazujących i czynów zabronionych, o czym mowa w art. 10; lub c) systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie. 4. Organ nadzorczy ustanawia i podaje do publicznej wiadomości wykaz rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków dla ochrony danych na mocy ust. 1. Organ nadzorczy przekazuje te wykazy Europejskiej Radzie Ochrony Danych, o której mowa w art. 68. 5. Organ nadzorczy może także ustanowić i podać do wiadomości publicznej wykaz rodzajów operacji przetwarzania niepodlegających wymogowi dokonania oceny skutków dla ochrony danych. Organ nadzorczy przekazuje te wykazy Europejskiej Radzie Ochrony Danych. 6. Jeżeli wykazy, o których mowa w ust. 4 i 5, obejmują czynności przetwarzania związane z oferowaniem towarów lub usług osobom, których dane dotyczą, lub z monitorowaniem ich zachowania w kilku państwach członkowskich lub mogące znacznie wpłynąć na swobodny przepływ danych osobowych w Unii, przed przyjęciem takich wykazów właściwy organ nadzorczy stosuje mechanizm spójności, o którym mowa w art. 63. 7. Ocena zawiera co najmniej: a) systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie - prawnie uzasadnionych interesów realizowanych przez administratora; b) ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów; c) ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą, o którym mowa w ust. 1; oraz d) środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie niniejszego rozporządzenia, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy. 8. Oceniając - w szczególności do celów oceny skutków dla ochrony danych - skutki operacji przetwarzania wykonywanych przez administratora lub podmiot przetwarzający, uwzględnia się przestrzeganie przez takiego administratora lub taki podmiot przetwarzający zatwierdzonych kodeksów postępowania, o których mowa w art. 40. 9. W stosownych przypadkach administrator zasięga opinii osób, których dane dotyczą, lub ich przedstawicieli w sprawie zamierzonego przetwarzania, bez uszczerbku dla ochrony interesów handlowych lub publicznych lub bezpieczeństwa operacji przetwarzania. 10. Ust. 1-7 nie mają zastosowania, jeżeli przetwarzanie na mocy art. 6 ust. 1 lit. c) lub e) ma podstawę prawną w prawie Unii lub w prawie państwa członkowskiego, któremu podlega administrator, i prawo takie reguluje daną operację przetwarzania lub zestaw operacji, a oceny skutków dla ochrony danych dokonano już w ramach oceny skutków regulacji w związku z przyjęciem tej podstawy prawnej - chyba że państwa członkowskie uznają za niezbędne, by przed podjęciem czynności przetwarzania dokonać oceny skutków dla ochrony danych. 11. W razie potrzeby, przynajmniej gdy zmienia się ryzyko wynikające z operacji przetwarzania, administrator dokonuje przeglądu, by stwierdzić, czy przetwarzanie odbywa się zgodnie z oceną skutków dla ochrony danych.

Tabela uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

			zasady, polega na przeprowadzeniu stosownych analiz i zadbania pod kątem różnorodnych kryteriów określonych w przepisach rozporządzenia 2016/679, by przepisy szczegółowe zawierały rozwiązania zapewniające wyczerpującą, przejrzystą, prawidłową, właściwie wpisaną w system prawny regulację zapewniającą stosowanie przepisów o ochronie danych osobowych (kształtowanie systemu ochrony danych osobowych). Ocena, czy projektowane przepisy są wystarczające z punktu widzenia zapewnienia skutecznej ochrony prawnej w świetle przepisów o ochronie danych osobowych, winna być dokonywana w oparciu o Wytyczne Grupy Roboczej Art. 29 dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko” do celów rozporządzenia 2016/679 (przyjęte w dniu 4 kwietnia 2017 r., ostatnio zmienione i przyjęte w dniu 4 października 2017 r.). Istotne informacje zawierające przykłady ogólnych ram oraz kryteria dopuszczalnej oceny skutków dla ochrony danych znaleźć można w załączniku 1 oraz załączniku 2 do Wytycznych. Wytyczne Grupy Roboczej art. 29 wskazują na konieczność wybrania metodyki dokonywania oceny skutków dla ochrony danych, która spełnia kryteria określone w załączniku 2 do Wytycznych. Przeprowadzenie testu prywatności wraz z oceną skutków dla ochrony danych i załączenie ich do projektu rozporządzenia przy zachowaniu wskazanej w Wytycznych systematyki może również wyeliminować ewentualne problemy i wątpliwości, które mogą mieć administratorzy po wejściu w życie projektowanych rozwiązań.	
9.	Prezes Urzędu Ochrony Danych Osobowych	Uwaga ogólna	Uwzględnienie zasad wynikających z art. 5 i 6 rozporządzenia 2016/679 Zgodne z prawem przetwarzanie danych wymaga, aby przepisy prawa skonstruowane były z uwzględnieniem zasad wskazanych w rozdziale II rozporządzenia 2016/679, w	Uwaga wyjaśniona W ocenie projektodawcy projektowane przepisy uwzględniają zasady wynikające z RODO. Określony został katalog danych, a ich przetwarzanie jest niezbędne do realizacji zadań wynikających z ustawy.

Tabela uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

			szczegółności tych wynikających z art. 5 ⁶⁾ i 6 ⁷⁾ . W art. 5 rozporządzenia 2016/679 wskazano na zasady dotyczące przetwarzania danych osobowych, natomiast w art. 6 określono warunki, jakie muszą być spełnione dla zgodnego z prawem przetwarzania. Należy zwrócić uwagę, że w przypadku omawianych poniżej przepisów szczególnie ważną przesłanką jest przesłanka wypełniania obowiązku prawnego ciążącego na administratorze (art. 6 ust. 1 lit. c rozporządzenia 2016/679). W takim przypadku prawodawca powinien pamiętać, że podstawa prawna takiego przetwarzania określona musi być w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator oraz przewidywać musi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą, być proporcjonalna do wyznaczonego celu, nie naruszać istoty prawa do ochrony danych oraz przewidywać odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.	
10.	Urząd Komisji Nadzoru Finansowego	Art. 2	W związku z postulatami wprowadzenia przepisów mających na celu uregulowanie relacji norm UKSC do rozporządzenia 2022/2554, w szczególności w kontekście zasady wyrażonej w art. 4 dyrektywy 2022/2555, zasadne jest dokonanie zmian w art.	Uwaga uwzględniona Definicje zostaną dodane z wyjątkiem incydentu związanego z ICT.

⁶⁾ 1. Dane osobowe muszą być: a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą ("zgodność z prawem, rzetelność i przejrzystość"); b) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 za niezgodne z pierwotnymi celami ("ograniczenie celu"); c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane ("minimalizacja danych"); d) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane ("prawidłowość"); e) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą ("ograniczenie przechowywania"); f) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych ("integralność i poufność"). 2. Administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie ("rozliczalność").

⁷⁾ 1. Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy - i w takim zakresie, w jakim - spełniony jest co najmniej jeden z poniższych warunków: a) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów; b) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy; c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze; d) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej; e) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi; f) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem. Akapit pierwszy lit. f) nie ma zastosowania do przetwarzania, którego dokonują organy publiczne w ramach realizacji swoich zadań.

Tabela uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

		2 UKSC. Należy postulować przede wszystkim dodanie do tego przepisu definicji następujących pojęć: – „incydent związany z ICT – incydent związany z technologiami informacyjno-komunikacyjnymi w rozumieniu art. 3 pkt 8 rozporządzenia 2022/2554”; – „podmiot finansowy – podmiot, o którym mowa w art. 18za ust. 1 ustawy z dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym (Dz. U. z 2024 r. poz. 135)”; – „poważny incydent związany z ICT – poważny incydent związany z technologiami informacyjno-komunikacyjnymi w rozumieniu art. 3 pkt 10 rozporządzenia 2022/2554”; – „rozporządzenie 2022/2554 – rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (Dz. Urz. UE L 333 z 27.12.2022, str. 1)”; – „właściwy organ w rozumieniu rozporządzenia 2022/2554 – Komisję Nadzoru Finansowego”; Definicja podmiotu finansowego następuje poprzez odesłanie do przepisów ustawy o nadzorze nad rynkiem finansowym, w której zawarte zostaną przepisy służące stosowaniu rozporządzenia 2022/2554 (projekt ustawy o zmianie niektórych ustaw w związku z zapewnieniem operacyjnej odporności cyfrowej sektora finansowego – UC11). Dodatkowo, w ocenie UKNF, art. 2 UKSC wymagać będzie także uzupełnienia o definicję rozporządzenia 2022/2554 oraz definicję właściwego organu w rozumieniu tego rozporządzenia, a także definicję incydentu związanego z ICT i poważnego incydentu związanego z ICT. Ze względu na równoległe toczące się prace nad ustawą służącą stosowaniu rozporządzenia 2022/2554 oraz nad nowelizacją UKSC, istotne będzie zapewnienie spójności pomiędzy przepisami obu ustaw w procesie legislacyjnym (jest to ważne również w kontekście faktu, że wprowadzenie do UKSC części z powyższych definicji zostało przewidziane w projekcie ustawy służącej stosowaniu rozporządzenia 2022/2554). Dodatkowo, w ocenie UKNF, w art. 2 UKSC warto również doprecyzować definicje „incydentu” oraz „poważnego incydentu”, tak aby wprost obejmowały one incydenty związane z ICT oraz poważne incydenty związane z ICT w rozumieniu rozporządzenia 2022/2554. Pozwoli to na rozstrzygnięcie, że omawiane terminy obejmują także incydenty związane z ICT oraz poważne incydenty związane z ICT,	W wyniku uwag MC do projektu ustawy służącej realizacji DORA regulacje odnoszące się do podmiotów finansowych zostaną określone w ustawie o nadzorze nad rynkiem finansowym. Natomiast regulacje KSC będą odnosiły się do podmiotów finansowych w zakresie polecenia zabezpieczającego, obowiązku wycofania sprzętu HRV oraz rekomendacji Pełnomocnika z art. 33 UKSC.

			co będzie miało istotne znaczenie dla stosowania przepisów ustawy dotyczących choćby zadań realizowanych przez CSIRT poziomu krajowego. Rozstrzygnięto to jednoznacznie, że CSIRT poziomu krajowego uprawnione będą przykładowo do sklasyfikowania poważnego incydentu związanego z ICT jako incydentu krytycznego, co wpisze się w obecne procedury współpracy w krajowym systemie cyberbezpieczeństwa. Dodatkowo, również CSIRT sektorowy w sektorze bankowym i infrastruktury rynków finansowych, pomimo przyjmowania zgłoszeń poważnych incydentów związanych z ICT w ramach przepisów rozporządzenia 2022/2554 przez właściwy organ na gruncie tego rozporządzenia, będzie m.in. uprawniony do wsparcia w obsłudze takich incydentów, tak jak w obecnym art. 44 UKSC (co samo w sobie wpisuje się dodatkowo w treść art. 22 ust. 1 rozporządzenia 2022/2554). W związku z powyższym postulowane jest przyjęcie przez definicje „incydentu” oraz „incydentu poważnego” następującej treści: – „incydent - zdarzenie, które ma lub może mieć niekorzystny wpływ na bezpieczeństwo systemów informacyjnych, w tym incydent związany z ICT”; – „incydent poważny - incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi przez podmiot kluczowy lub podmiot ważny, straty finansowe dla tego podmiotu lub wpływa na inne osoby fizyczne, osoby prawne, jednostki organizacyjnej nieposiadające osobowości prawnej poprzez wywołanie szkody materialnej lub niematerialnej, w tym poważny incydent związany z ICT”. UKNF dokonał przy tym kompleksowej analizy UKSC oraz projektu nowelizacji w zakresie przypadków użycia w/w terminów i proponowane podejście jest w ocenie UKNF optymalne dla zapewnienia, że w przypadkach, w których w ustawie mowa jest o incydencie lub incydencie poważnym, a dany przepis powinien znaleźć zastosowanie także do incydentów związanych z ICT lub poważnych incydentów związanych z ICT, to nie będzie wątpliwości co do takiej interpretacji przepisu. Będzie tak choćby w przypadku art. 26 ust. 1 UKSC (w którym mowa jest o zapewnianiu koordynacji incydentów przez CSIRT poziomu krajowego), art. 30 ust. 2 UKSC (zgodnie z którym CSIRT NASK priorytetowo traktuje zgłoszenia incydentów od podmiotów kluczowych i podmiotów ważnych), art. 44 ust. 1 pkt 2 UKSC (zgodnie z którym do zadań CSIRT sektorowych należy reagowanie na incydenty), czy też art. 49 ust. 6 UKSC (dotyczącego cyklicznego przekazywania do ENISA sprawozdania na temat m.in. incydentów i poważnych incydentów). Jednocześnie, dzięki treści projektowanego art. 8i UKSC w brzmieniu proponowanym w niniejszych uwagach, rozstrzygnięto zostanie, jakie przepisy nie	

Tabela uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

			będą miały zastosowania do podmiotów kluczowych i ważnych z sektora bankowego i infrastruktury rynków finansowych. Dotyczy to np. art. 8 ust. 1 pkt 2 UKSC (zgodnie z którym środki techniczne i organizacyjne wdrożone w systemie zarządzania bezpieczeństwem informacji powinny uwzględniać m.in. prawdopodobieństwo wystąpienia incydentów), art. 12 ust. 1 UKSC (w którym wskazano na elementy treści wczesnego ostrzeżenia o incydencie poważnym), czy art. 46 ust. 1 pkt 3 UKSC (zgodnie z którym system S46 powinien służyć do zgłaszania i obsługi incydentów). W niektórych przypadkach brak zastosowania danego przepisu, w którym pojawia się pojęcie „incydent” lub „incydent poważny”, do podmiotów kluczowych lub ważnych z sektora bankowego i infrastruktury rynków finansowych, będzie wynikać z samej treści danego przepisu. Jest tak choćby w przypadku art. 26 ust. 5 UKSC (który zgodnie z jego treścią dotyczy podmiotów podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych oraz przedsiębiorców realizujących zadania na rzecz Sił Zbrojnych) czy też art. 30 ust. 1 UKSC (którego treść odnosi się do podmiotów innych niż podmioty kluczowe lub ważne).	
11.	Narodowy Bank Polski	Art. 2 pkt 3c	Ad. art. 1 pkt 2 lit. a projektu ustawy w zakresie dodawanego pkt 3c: 3c) bezpieczeństwo systemów informacyjnych – odporność systemów informacyjnych na zdarzenia naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy. Proponujemy rozważyć, czy nie należałoby wskazać w tym punkcie „zdarzeń mających na celu naruszenie poufności, integralności” zamiast „naruszeń”. W naszej ocenie odporność, o której mowa w definicji bezpieczeństwa systemów informacyjnych, ma zapobiegać, aby do takiego naruszenia poufności, czy integralności nie doszło.	Uwaga nieuwzględniona Określenie celu może być w wielu przypadkach niemożliwe, poza tym część zdarzeń wpływających na system informacyjny nie jest celowa, np. awarie techniczne czy błędy ludzkie.
12.	Urząd Komisji Nadzoru Finansowego	Art.2	W projektowanej definicji podatności wskazano, że jest to właściwość produktu ICT lub usługi ICT, które mogą być wykorzystane przez cyberzagrożenie. W związku z użyciem liczby pojedynczej wyrazu „właściwość” proponujemy zmianę na „która może być wykorzystana”.	Uwaga uwzględniona
13.	Prezes Głównego Urzędu Statystycznego	Art. 2	Nowelizowana ustawa w ppkt „c” wprowadza pojęcie „dostawca sprzętu lub oprogramowania”, którym jest producent, upoważniony przedstawiciel, importer lub dystrybutor , w rozumieniu odpowiednio art. 2 pkt 3–6 rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 765/2008 z dnia 9 lipca 2008 r.	Uwaga wyjaśniona Jak wskazuje przytoczona definicja, aby być uznanym za producenta należy spełnić dwie przesłanki:

Tabela uwag zgłoszonych w ramach opiniowania do *projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)*

			ustanawiającego wymagania w zakresie akredytacji i uchylającego rozporządzenie (EWG) nr 339/93 (Dz. Urz. UE L 218 z 13.08.2008, str. 30, z późn. zm.)), produktu ICT, usługi ICT lub procesu ICT. Zgodnie z rozporządzeniem 765/2008 „producent” to każda osoba fizyczna lub prawna, która wytwarza produkt lub która zleca zaprojektowanie lub wytworzenie produktu i oferuje ten produkt pod własną nazwą lub znakiem towarowym. Brak jest jasności w zakresie roli i statusu podmiotu kluczowego lub powołanej przez podmiot kluczowy dedykowanej jednostki do obsługi IT, które we własnym zakresie prowadzą działania programistyczne, deweloperskie których skutkiem jest wytworzenie systemu informacyjnego, oprogramowania np. na użytek własny. Czy takie podmioty będą uznawane za „producentów” w rozumieniu Dyrektywy NIS 2 i będą podlegały wszystkim rygorom i obowiązkom producenta wynikającym z nowelizowanej ustawy.	1) wytworzenie produktu lub zlecenie jego wytworzenia czy zaprojektowania; 2) oferowanie produktu na rynku. W związku z tym, jeśli dany produkt, usługa, czy proces jest całkowicie wewnętrzny to dany podmiot nie jest producentem w rozumieniu tych przepisów.
14.	Prezes Głównego Urzędu Statystycznego	Art. 2	Nowelizowana ustawa w ppkt „c” wprowadza pojęcia: a) dostawca usług zarządzanych b) dostawca usług zarządzanych w zakresie cyberbezpieczeństwa W wielu sektorach i resortach administracji publicznej organ adm. publicznej powołał wyspecjalizowane podmioty pomocnicze świadczące usługi informatyczne, które obsługują część lub wszystkie jednostki budżetowe danego resortu, w tym realizują zadania związane z cyberbezpieczeństwem. W części przypadków wszystkie jednostki resortu funkcjonują i pracują w ramach jednej wspólnej sieci. W wielu tego rodzaju przypadkach systemy informatyczne, które są wykorzystywane przez jednostki, to systemy centralne, udostępnione zazwyczaj przez organ lub urząd go obsługujący (centralę). Zapisy budzą wątpliwości interpretacyjne w zakresie, czy tego rodzaju, powołane intencjonalnie w resorcie i wyspecjalizowane jednostki do obsługi resortu w zakresie zarządzania i utrzymania IT i realizacji zadań związanych z cyberbezpieczeństwem, należy uznać za a) dostawcę usług zarządzanych i/lub b) dostawcę usług zarządzanych w zakresie cyberbezpieczeństwa oraz czy podmioty te będą podlegały wszystkim rygorom i obowiązkom dostawców, wynikającym z nowelizowanej ustawy, w tym:	Uwaga wyjaśniona Zdaniem MC jednostki organizacyjne w administracji publicznej realizujące zadania w zakresie zarządzania ICT tudzież wsparcia w zakresie cyberbezpieczeństwa powinny mieć obowiązki z zakresu cyberbezpieczeństwa. Nie widzimy tutaj potrzeby ograniczania wymogów. Co do udostępniania informacji na stronie internetowej to dotyczy to informacji wymaganych przez dokument RFC 2350 co jest powszechnie przyjętym standardem.

Tabela uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

			1. dostawca usług zarządzanych w zakresie cyberbezpieczeństwa udostępnia na swojej stronie internetowej informacje na temat swojej działalności określone w art. 8g nowelizowanej ustawy; podmiot kluczowy zgłasza do rejestru podmiotów kluczowych informacje o zawarciu umowy z dostawcą usług zarządzanych w zakresie cyberbezpieczeństwa na realizację zadań, o których mowa w art. 8 i art. 11, wraz z danymi tego dostawcy zawierające nazwę (firmę) dostawcy, siedzibę, adres, numer telefonu, adres poczty elektronicznej;	
15.	Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy	Art. 2 pkt 10a	W art. 2 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2023 r. poz. 913 i 1703), zwanej dalej „ustawą o KSC”, zawarto słowniczek ustawowy. Należy zwrócić uwagę, że definicja organizacji badawczej, należącej do sektora badań naukowych, wynikająca z dodawanego pkt 10a w ww. artykule, nie wyłącza instytucji edukacyjnych, jak czyni to art. 6 pkt 41 dyrektywy 2022/2555. Taka propozycja brzmienia definicji, wobec włączenia instytutów badawczych i uczelni publicznych do sektora administracja publiczna jako podmiotów kluczowych, może budzić wątpliwości w przypadku niektórych podmiotów. Rekomendujemy zmianę brzmienia tego przepisu i jasne rozgraniczenie tych sektorów.	Uwaga uwzględniona Przed wszystkim w związku z uwzględnieniem uwagi z konsultacji publicznych uczelnie i organizacje badawcze będą tworzyć wspólny sektor. Ponadto uważamy, że uczelnie powinny być w krajowym systemie cyberbezpieczeństwa. Przy czym instytuty badawcze, które mogą być uznane za państwowe instytuty badawcze pozostawimy w sektorze podmiotów publicznych, z uwagi na możliwość realizacji zadań obronnych.
16.	Prezes Urzędu Komunikacji Elektronicznej	Art. 2	Art. 1 pkt 2 lit. e – w wyniku projektowanej propozycji nadania nowego brzmienia art. 2 pkt 8 ustawy o ksc, słowniczek ustawy o ksc przestanie obejmować pojęcie „incydent istotny”. W związku z tym należy zauważyć, że pomimo ww. projektowanej zmiany pojęcie to nadal będzie funkcjonować w nowelizowanej ustawie o ksc, m. in. w art. 26 ust. 3 pkt 6, 7 i 11, art. 29 i w art. 49 ust. 3 pkt 4, których to przepisów nie obejmuje projektowana nowelizacja. Podobny przykład braku konsekwencji terminologicznej odnosi się do wprowadzanego w art. 1 pkt 6 lit. a projektowanej ustawy pojęcia „podmioty kluczowe”, które ma zastąpić zawarte w art. 4 pkt 1 ustawy o ksc pojęcie „operatorzy usług kluczowych”. Należy bowiem wskazać, że projektowana nowelizacja nie obejmuje wszystkich przepisów ustawy o ksc, w których występuje pojęcie „operatorzy usług kluczowych”, w tym w tym np. art. 11 ust. 3, art. 15 ust. 6 oraz art. 49 ust. 1 pkt 5 i ust. 3 pkt 4 i 6. Kolejny przykład braku konsekwencji terminologicznej związany jest z zastąpieniem w art. 1 pkt 6 lit.	Uwaga uwzględniona, przepisy nowelizacji zostaną uzupełnione w niezbędnym zakresie

Tabela uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

			b (dotyczącym projektowanego art. 4 pkt 6 ustawy o ksc) pojęcia „sektorowe zespoły cyberbezpieczeństwa” pojęciem „CSIRT sektorowe”, która to zmiana nie została wprowadzona np. w art. 26 ust. 3 pkt 10 ustawy o ksc (w przepisie tym pozostało pojęcie „sektorowe zespoły cyberbezpieczeństwa”). W związku z powyższym projektowane przepisy wymagają weryfikacji w kontekście stosowanej terminologii;	
17.	Urząd Komisji Nadzoru Finansowego	Art. 2	Projektowana definicja potencjalnego zdarzenia dla cyberbezpieczeństwa pokrywa się z definicją incydentu, w zakresie w jakim obie definicje odnoszą się do zdarzenia, które może mieć niekorzystny wpływ na bezpieczeństwo systemów informacyjnych. W ocenie UKNF zakresy omawianych pojęć powinny być rozgraniczone.	Uwaga uwzględniona
18.	Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy	Art.. 2 pkt 20	Pojęcie „znaczące cyberzagrożenie”, które jest zdefiniowane w dodawanym art. 2 pkt 20 pojawia się następnie tylko raz w projekcie (w projektowanym art. 53 ust. 5 pkt 4). Zaproponowana definicja jest jednak niespójna z definicją cyberzagrożenia wynikającą z rozporządzenia 2018/881. Ponadto, wdrażany w art. 53 ust. 5 pkt 4 projektu ustawy art. 32 ust. 4 lit. e dyrektywy 2022/2555 odnosi się do poważnego, nie znaczącego, cyberzagrożenia. Tym samym, ze względu na występującą w systemie prawa definicję „cyberzagrożenia”, rekomendujemy rezygnację z tej definicji lub doprecyzowanie – np. w drodze rozporządzenia – progu, jaki cyberzagrożenie musi przekraczać, by móc zostać uznane za poważne.	Uwaga wyjaśniona Znaczące cyberzagrożenie pojawia się także przy art. 11 ust. 2a projektu co stanowi wdrożenie art. 23 ust. 2 NIS2. Znaczące cyberzagrożenie wdraża poważne cyberzagrożenie z NIS2. Definicja musi pozostać. Co do definiowania w rozporządzeniu – bardzo trudno jest zdefiniować progi dla znaczącego cyberzagrożenia. To musi pozostać klauzulą generalną.
19.	Prezes Głównego Urzędu Statystycznego	Art. 2a	W projektowanym art. 2a wskazuje się, że W przypadku podmiotu publicznego pod pojęciem usługi rozumie się także zadanie publiczne realizowane przez ten podmiot. W projekcie nie określono definicji czym jest zadanie publiczne od którego zależy, że podmiot podlega pod ustawę i jest uznany za podmiot kluczowy lub ważny. Zgodnie z Dyrektywą NIS 2, podmiot jest podmiotem administracji publicznej: (i) na poziomie rządu centralnego, zdefiniowanym przez państwo członkowskie, zgodnie z prawem krajowym; lub (ii) na poziomie regionalnym, zdefiniowanym przez państwo członkowskie zgodnie z prawem krajowym, który zgodnie z oceną opartą na analizie	Uwaga wyjaśniona Od wielu lat podmioty publiczne realizujące zadania publiczne przy wykorzystaniu systemów informacyjnych miały i mają obowiązek wdrożyć system zarządzania bezpieczeństwem informacji. Wynika to z rozporządzenia o Krajowym Ramach Interoperacyjności.

Tabela uwag zgłoszonych w ramach opiniowania do *projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)*

			ryzyka świadczy usługi, których zakłócenie mogłoby mieć znaczący wpływ na krytyczną działalność społeczną lub gospodarczą. Tym samym Dyrektywa na poziomie niższym definiuje ważność usługi tj. wskazuje, że chodzi o usługę, której zakłócenie mogłoby mieć znaczący wpływ na krytyczną działalność społeczną lub gospodarczą. Brak dookreślenia w ustawie czym jest zadanie publiczne powoduje, że ustawa znacząco rozszerza wymagania i definicje wynikające z NIS 2 i znacząco poszerza katalog podmiotów podlegających ustawie.	Projekt ustawy przejmuje te wymogi dot. SZBI dla podmiotów publicznych. Proponuje się opisanie zadania publicznego w uzasadnieniu do ustawy.
20.	Prezes Urzędu Ochrony Danych Osobowych	Art. 2a	W art. 1 pkt 3 projektu proponowane jest dodanie art. 2a KSC, zgodnie z którym w przypadku podmiotu publicznego pod pojęciem usługi rozumie się także zadanie publiczne realizowane przez ten podmiot. Kwestia ta ma znaczenie dla realizacji zadań publicznych i ich wykonywania przez podmioty publiczne z poszanowaniem cyberbezpieczeństwa, dla zachowania którego istotne jest także przetwarzanie danych osobowych zgodnie z obowiązującymi przepisami. Wpływa to także na bezpieczeństwo zasobów dotyczących informacji osobowych, a w szerszym kontekście ma znaczenie dla bezpieczeństwa państwa.	Uwaga wyjaśniona Rozumienie projektodawcy jest takie samo – wykonywanie zadań publicznych przy wykorzystaniu systemów informacyjnych musi być zabezpieczone przez odpowiednie wymagania cyberbezpieczeństwa.
21.	Krajowa Rada Radiofonii i Telewizji	Art. 5 ust. 1	W projektowanym przepisie art. 5 ust. 1 pkt 1 ustawy o krajowym systemie cyberbezpieczeństwa, wprowadzającym definicję podmiotu kluczowego, niezrozumiałe jest odesłanie do załącznika numer 2 do ustawy, odnoszącego się do podmiotów ważnych. Analogicznie, w projektowanym przepisie art. 5 ust. 2 pkt 1 ustawy, wprowadzającym definicję podmiotu ważnego, niezrozumiałe jest odesłanie do załącznika numer 1 do ustawy, odnoszącego się do podmiotów kluczowych. Niezrozumiałe jest także dlaczego w art. 5 ust. 1 pkt 1 powołując się na załączniki do ustawy zastosowano koniunkcję, a w art. 5 ust. 2 pkt 1 alternatywę.	Uwaga uwzględniona Przepisy zostaną stosownie zmienione, tj. w art. 5 ust. 1 pkt 1 pozostanie odesłanie tylko do zał. nr 1 do ustawy, a w ust. 2 – odesłanie do zał. nr 2.
22.	Prezes Urzędu Komunikacji Elektronicznej	Art. 5 ust. 1 i 2	Art. 1 pkt 8 i 11 w zakresie dotyczącym projektowanych art. 5 ust. 1 i 2 ustawy o ksc – analizując przepisy art. 3 dyrektywy NIS2 i załączników nr I oraz nr II oraz przepisy art. 5 projektu warto zauważyć, że zakres podmiotów uznanych za podmioty kluczowe, co w konsekwencji rzutować będzie na zakres podmiotów ważnych, będzie odmienny na gruncie dyrektywy i przepisów ustawy o ksc. Zgodnie bowiem m. in. z art. 3 ust. 1 lit. a dyrektywy NIS2 podmiotami kluczowymi są podmioty w rodzaju tych, o których mowa w załączniku I, przekraczające pułapy dla średnich przedsiębiorstw, określone w art. 2 ust. 1 załącznika do zalecenia 2003/361/WE. Projekt ustawy o ksc w art. 5 ust. 1 pkt 1 wskazuje natomiast, że podmiotem kluczowym jest również podmiot o analogicznej wielkości, ale wskazany także w załączniku nr 2 do ustawy. W konsekwencji przyjęcia odmiennej konstrukcji	Uwaga uwzględniona Odniesienie do zał. nr 2 przy podmiotach kluczowych zostanie usunięte.

Tabela uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

			przepisów kwalifikujących określone podmioty jako podmioty kluczowe albo podmioty ważne w przepisach projektowanej ustawy niż została określona w dyrektywie dojdzie do odmiennej oceny danego podmiotu w prawie krajowym. Celem przykładu należy przytoczyć kasus operatora pocztowego przekraczającego wymogi dla średniego przedsiębiorstwa, który na gruncie dyrektywy nie zostanie uznany za podmiot kluczowy (z uwagi na działalność prowadzoną w sektorze ważnym określonym w załączniku nr II dyrektywy), natomiast na podstawie wskazanego przepisu ustawy już tak.	
23.	Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy	Art. 41 i art. 41a	W stosunku do propozycji zmian w art. 41 i 41a rekomendujemy powrót do brzmienia odnoszącego się wyłącznie do sektorów: „Organami właściwymi do spraw cyberbezpieczeństwa są (...)”, a nie do podmiotów kluczowych/ważnych. W aktualnej propozycji brakuje wskazania organów właściwych dla podmiotów kluczowych w sektorach określonych w art. 41a (a zgodnie z proponowanym art. 5 ust. 1 pkt 1, podmiotami kluczowymi są większe niż średnie przedsiębiorstwa nie tylko z załącznika nr 1, ale i z załącznika nr 2 do ustawy). Analogicznie w art. 41 nie zawarto przepisów dotyczących organów właściwych dla podmiotów ważnych w sektorach określonych w tym przepisie. Powrót do poprzedniego brzmienia wprowadzenia do wyliczenia pozwoliłby na uniknięcie wątpliwości i zapewniłby większą jasność w zakresie organów właściwych.	Uwaga uwzględniona Przepis zostanie zmieniony.
24.	Prezes Urzędu Komunikacji Elektronicznej	Art. 5 i art. 7c w związku z art. 41 pkt 8a i art. 41a	Art. 1 pkt 8 i 11 w zakresie dotyczącym projektowanych art. 5 i art. 7c ustawy o ksc w związku z art. 1 pkt 40 i 41 w zakresie dotyczącym projektowanych art. 41 pkt 8a oraz art. 41a ustawy o ksc – należy wskazać, że przedsiębiorcy komunikacji elektronicznej będący mikro-, lub małym przedsiębiorcą, o którym mowa w art. 2 ust. 1 załącznika I do rozporządzenia 651/2014/UE, którzy nie zostaną uznani za podmioty kluczowe na podstawie art. 7c ust. 2 pkt 1, nie zostali objęci na gruncie ustawy o ksc właściwością organu właściwego do spraw cyberbezpieczeństwa. Zgodnie z projektowanymi przepisami Prezes Urzędu Komunikacji Elektronicznej będzie właściwy dla podmiotów kluczowych z sektora infrastruktury cyfrowej podsektora komunikacji elektronicznej z wyłączeniem podmiotów, o których mowa w art. 26 ust. 5, oraz dla podmiotów ważnych z sektora usług pocztowych. Przedsiębiorcy komunikacji elektronicznej, na podstawie art. 5 ust. 1 pkt 2, a także na podstawie art. 5 ust. 1 pkt 3 lit. f w związku z art. 7c ust. 2 pkt 1, zaliczeni zostaną do podmiotów kluczowych. Poza tym kręgiem znajdują się natomiast przedsiębiorcy komunikacji elektronicznej będący mikro-, lub małym przedsiębiorcą, o którym mowa w art. 2 ust. 1 załącznika I do rozporządzenia 651/2014/UE, którzy nie spełniają którejkolwiek z przesłanek określonych w art. 7c ust. 1 pkt 3, co spowoduje, że zgodnie z art. 5 ust. 2 pkt 3, będą traktowani jako podmioty ważne. Przepisy projektu nie przewidują	Uwaga uwzględniona Uwzględniając uwagi innych podmiotów – przepisy art. 41 zostaną przeredagowane, będą wskazywane OWCyber dla poszczególnych sektorów a nie dla podmiotów kluczowych/ważnych.

Tabela uwag zgłoszonych w ramach opiniowania do *projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)*

			natomiast dla tej grupy podmiotów ważnych organu właściwego do spraw cyberbezpieczeństwa. Analogiczna uwaga dotyczy podmiotów kluczowych z sektora usług pocztowych, którzy zostaną uznani za podmioty kluczowe na podstawie art. 5 ust. 1 pkt 1 ustawy o ksc. Podmiot wskazany w załączniku nr 1 i nr 2 do ustawy, który przewyższa wymogi dla średniego przedsiębiorstwa określone w art. 2 ust. 1 załącznika I do rozporządzenia 651/2014/UE, czyli we wskazanym przypadku operator pocztowy przewyższający te wymogi, jako podmiot kluczowy z sektora usług pocztowych nie zostanie objęty właściwością organu właściwego do spraw cyberbezpieczeństwa określonego w art. 41 oraz w art. 41a.	
25.	Prezes Urzędu Komunikacji Elektronicznej	Art. 7 i art. 7a	Art. 1 pkt 10 i 11 w zakresie dotyczącym projektowanych art. 7 i art. 7a ustawy o ksc – zaproponowane brzmienie art. 7 i art. 7a może wywoływać istotne wątpliwości w toku stosowania tych regulacji. Projektowany art. 7 określa normy dotyczące wykazu podmiotów kluczowych i podmiotów ważnych wpisywanych na wniosek oraz z urzędu (co sugeruje chociażby ust. 16). Przepisy te zostały jednak usystematyzowane w sposób utrudniający odkodowanie ich wzajemnej relacji. Przepis art. 7 ust. 6 stanowiący podstawę do wpisów z urzędu do wykazu, o którym mowa w art. 7 ust. 1, jest jednocześnie przepisem o charakterze <i>lex specialis</i> w stosunku do reguły określonej ust. 3 stanowiącej o wpisie do wykazu na wniosek. Nie jest natomiast jasne, w jakim trybie (tzn. na skutek jakiego zdarzenia) i w jakim terminie podmioty, o których mowa w art. 7 ust. 6, miałyby uzupełniać dane wpisane w wykazie (taki obowiązek statuuje ust. 7). Wskazane wątpliwości potęguje również systematyka art. 7, gdzie po przepisie ust. 3 dotyczącym wpisu na wniosek następuje regulacja o wpisie z urzędu (ust. 6 i 7), po czym ponownie mamy do czynienia z przepisami dotyczącymi wniosku. Nie jest również jasne, jak należy rozumieć przepisy art. 7a, które określają, że organ właściwy do spraw cyberbezpieczeństwa może wpisać podmiot do wykazu, o którym mowa w art. 7 ust. 1, jeżeli podmiot ten spełnia przesłanki uznania go za podmiot kluczowy albo podmiot ważny oraz podmiot ten nie złożył wniosku, o którym mowa w art. 7 ust. 3. Powstaje pytanie, jak w tym kontekście należy rozumieć przepis art. 7a ust. 2 stanowiący, że organ właściwy do spraw cyberbezpieczeństwa „wpisując” podmiot do wykazu korzysta z danych zawartych w rejestrach publicznych. Nie jest w konsekwencji wystarczająco klarowne, wobec projektowanej terminologii przepisu ust. 2, czy organ właściwy do spraw cyberbezpieczeństwa oceniając spełnienie przesłanki uznania danego podmiotu za podmiot kluczowy albo podmiot ważny (ust. 1) będzie ograniczony do korzystania z danych zawartych w rejestrach publicznych. Czy w sytuacji, gdy organ ten	Uwaga uwzględniona i wyjaśniona Przepisy dot. wykazu będą podlegały dodatkowej redakcji. Podmioty wpisane z urzędu do wykazu będą informowane o tym pismem MC – w praktyce zautomatyzowanym. Art. 7a dotyczy sytuacji gdy podmiot nie wpisał się do wykazu, chociaż powinien – OWCYber powinien mieć możliwość wpisania takiego podmiotu z urzędu do wykazu. Ale jest to inna sytuacja niż wpisywanie PT, DUZ, Podmiotów Krytycznych, podmiotów publicznych do wykazu - tutaj one już są znane organom i nie ma potrzeby, aby były zobligowane do samorejestracji, skoro już są ujęte w odpowiednich rejestrach.

Tabela uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

			poweźmie informację mogącą mieć wpływ na przedmiotową ocenę z innych źródeł (np. sprawozdania z działalności podmiotu) możliwe będzie skuteczne wpisanie danego podmiotu do wykazu, o którym mowa w art. 7 ust. 1? Kwestia ta jest o tyle istotna, że czynność wpisu do wykazu ma być „inną czynnością z zakresu administracji publicznej” (inny zakres środków ochrony praw niż w przypadku decyzji administracyjnej). Niezależnie od powyższego wydaje się, że na gruncie zmienianego art. 7 będziemy mieli do czynienia z dublowaniem się instytucji aktualizacji danych, o której mowa w ust. 17 i 19. Minister właściwy do spraw informatyzacji ma bowiem aktualizować dane zawarte we wpisach w wykazie, o którym mowa w ust. 1, co najmniej raz w roku, natomiast przedmiotowy obowiązek aktualizacji został jednocześnie nałożony na podmioty wpisane do tego wykazu w terminie 14 dni od dnia ich zmiany.	
26.	Rzecznik Małych i Średnich Przedsiębiorców	Art. 7	Wg kolejności zmienianych, lub dodawanych Projektem przepisów: Proponowana treść art. 1 pkt 10 Projektu (nadający nowe brzmienie art. 7 ustawy zmienianej), który określa wykaz podmiotów kluczowych i podmiotów ważnych (dalej Wykaz) oraz procedurę wpisu do tego Wykazu - wymaga zdaniem Rzecznika ponownego rozważenia. Projektowany art. 7 ust. 3 ustawy zmienianej nakłada na podmioty kluczowe i podmioty ważne obowiązek złożenia wniosku o wpis do Wykazu w terminie 2 miesiące od dnia spełnienia określonych wymogów. Zakres oraz treść informacji koniecznych do zawarcia we wniosku o wpis do Wykazu określa projektowany art. 7 ust. 2. Niektóre z tych informacji wymagają podjęcia szeregu czynności formalnych i faktycznych - jak np. ustanowienie w wewnętrznej strukturze osób do kontaktu z podmiotami krajowego systemu cyberbezpieczeństwa. Wobec powyższego zasadny jest postulat, aby: – dla podmiotów kluczowych i podmiotów ważnych będących mikroprzedsiębiorcami i małymi przedsiębiorcami wpis do Wykazu powinien być fakultatywny, z zastrzeżeniem sytuacji określonej w art. 1 pkt 11 Projektu (dodający do ustawy zmienianej art. 7a i kolejne, czyli wpis z urzędu dokonany przez organ właściwy), – termin na złożenie wniosku o wpis do Wykazu (określony w nowej treści art. 7 ust.3 ustawy zmienianej) powinien być dłuższy i wynosić co najmniej 3 miesiące, – termin na uzupełnienie brakujących danych, określony w projektowanym art. 7 ust. 16 również powinien być dłuższy i wynosić co najmniej 1 miesiąc,	Uwaga częściowo uwzględniona Dla mikroprzedsiębiorców zostanie wprowadzony wymóg podania 1 osoby do kontaktów. Termin na wpis do wykazu zostanie wydłużony do 3 miesięcy.

Tabela uwag zgłoszonych w ramach opiniowania do *projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw* (UC32)

			– w odniesieniu do projektowanego art. 7 ust. 2 pkt 11 (dane gromadzone w wykazie) określającego wymóg podania danych co najmniej dwóch osób do kontaktu z podmiotami krajowego systemu cyberbezpieczeństwa - dla podmiotów będących mikroprzedsiębiorcami lub małymi przedsiębiorcami - jedna taka osoba. Uzasadnienie: Potrzeba zmiany postrzegania znaczenia cyberbezpieczeństwa jest istotna, jednak projektodawcy powinni mieć na względzie, iż planowane do wdrożenia regulacje dotyczyć będą wielu podmiotów z nowych sektorów, które do tej pory nie były objęte tego typu obowiązkami, w tym podmiotów spoza dziedzin IT/ICT. Ponadto, zgodnie z art. 1 pkt 8 Projektu (nadający nowe brzmienie art. 5 ust 1 pkt 3 oraz art. 5 ust. 2 pkt 2-4) regulacje zawarte w Projekcie mogą dotyczyć podmiotów z różnych sektorów niezależnie od ich wielkości, również mikroprzedsiębiorców, małych przedsiębiorców. Niektóre z tych podmiotów będą musiały wdrożyć dodatkowe, nowe dla nich procedury i wyznaczyć w ramach istniejących struktur nowe osoby lub zespoły osób do realizacji zadań z zakresu cyberbezpieczeństwa. Obowiązki nałożone Projektem, dla mniejszych podmiotów zwłaszcza mikroprzedsiębiorców - mogą stanowić duże wyzwanie organizacyjne oraz finansowe i w takim kontekście przeszkodę w wykonywaniu działalności gospodarczej na terytorium Rzeczypospolitej. Proponowane zmiany mogą stanowić istotne ułatwienie dla podmiotów objętych nowymi regulacjami przy jednoczesnym braku negatywnego wpływu na realizację założonych celów nowelizacji.	

Tabela uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

27.	Prezes Urzędu Ochrony Danych Osobowych	Art. 7	Art. 1 pkt 10 projektu zawiera propozycję art. 7 KSC, w którym określono obowiązek ministra właściwego do spraw informatyzacji prowadzenia wykazu podmiotów kluczowych i ważnych oraz określono zawartość tego wykazu. Ze względu na to, że w wykazie tym będą przetwarzane dane osobowe, przepis ten wymaga uzupełnienia o wskazanie celu prowadzenia tego wykazu i bezpośredniego powiązania niezbędności przetwarzania danych osobowych z takim celem. Wyjaśnienia wymaga również niezbędność uczynienia danych z projektowanego ust. 2 pkt. 11 tego artykułu, obejmujących imię i nazwisko, numer telefonu oraz adres poczty elektronicznej co najmniej dwóch osób do kontaktu z podmiotami systemu cyberbezpieczeństwa, jawnymi i publicznie dostępnymi. Kwestia niezbędności upublicznienia tych danych istotna jest nie tylko z punktu widzenia ochrony danych osobowych, ale także ze względów cyberbezpieczeństwa. Ma to znaczenie również z tego powodu, że ustawa nie precyzuje czy wymagany numer telefonu i adres poczty elektronicznej osób do kontaktu, mają być danymi służbowymi czy prywatnymi.	Uwaga częściowo uwzględniona Wykaz podmiotów kluczowych i podmiotów ważnych nie będzie dostępny szeroko. Wymagany numer telefonu i adres poczty elektronicznej powinien być służbowy – przepis zostanie uzupełniony. Przepis zostanie uzupełniony o cel prowadzenia wykazu. Celem prowadzenia wykazu jest zapewnienie możliwości skutecznej komunikacji między zespołami CSIRT poziomu krajowego, zespołami CSIRT sektorowymi a podmiotami kluczowymi i podmiotami ważnymi.
28.	Najwyższa Izba Kontroli	Art. 7	W art. 7 ust. 22 nowelizowanej ustawy wśród podmiotów którym udostępnia się dane, o których mowa w ust. 2, w zakresie niezbędnym do realizacji ich ustawowych zadań, nie wskazano Najwyższej Izby Kontroli co może w przyszłości utrudniać pozyskiwanie przez NIK danych zawartych w rejestrze prowadzonym przez ministra właściwego ds. informatyzacji, a tym samym może mieć negatywny wpływ na przygotowanie i przeprowadzanie kontroli w tym zakresie.	Uwaga uwzględniona NIK został dodany do podmiotów uprawnionych do żądania informacji z wykazu podmiotów kluczowych i podmiotów ważnych.
29.	Narodowy Bank Polski	Art. 7	Ad art. 1 pkt 10 projektu ustawy w zakresie zmiany brzmienia art. 7 ust. 1 i 2: 1. Minister właściwy do spraw informatyzacji prowadzi wykaz podmiotów kluczowych i podmiotów ważnych. 2. Wykaz, o którym mowa w ust. 1, zawiera: (...) 22) „umieść w wykazie”; 23) datę wpisu do wykazu; 24) tytuł prawnym wpisany do wykazu, o którym mowa w ust. 1; 25) datę wykreślenia z wykazu, o którym mowa w ust. 1. Proponujemy uporządkować zawartość przedmiotowego dokumentu i doprecyzować użycie wyrazu „wykaz”. W punktach 22-23 jest ono przytoczone samodzielnie jako „wykaz”, w pkt 24-25 zastąpione jest wyrażeniem „wykaz, o którym mowa w ust. 1”.	Uwaga uwzględniona W ustępie pierwszym zostanie wprowadzony skrót „zwany dalej „wykazem””.

Tabela uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

30.	Urząd Komisji Nadzoru Finansowego	Art. 7 ust. 2 pkt 1, 3 i 13	W projektowanym art. 7 ust. 2 pkt 1 UKSC należy w ocenie UKNF rozważyć wskazanie także na imię i nazwisko (w przypadku osób fizycznych), zaś w pkt 3 również na adres (w przypadku osób fizycznych). Dodatkowo projektowany art. 7 ust. 2 pkt 13 UKSC powinien zostać w ocenie UKNF uzupełniony o możliwość wskazania w deklaracji na przekroczenie wymogów dla średniego przedsiębiorstwa. Również terminologia w tym przepisie, jak i w innych przepisach ustawy odwołujących się do mikroprzedsiębiorcy, małego przedsiębiorcy czy średniego przedsiębiorcy, powinna zostać w ocenie UKNF dostosowana do terminologii załącznika I do rozporządzenia 651/2014, z uwagi na jego stosowanie do ustalania statusu MŚP podmiotów kluczowych lub ważnych (rozporządzenie to posługuje się terminami „mikroprzedsiębiorstwo”, „małe przedsiębiorstwo” oraz „średnie przedsiębiorstwo”). W związku z powyższym omawiany przepis powinien w ocenie UKNF przyjąć brzmienie: „13) deklarację podmiotu kluczowego lub podmiotu ważnego, czy spełnia kryteria mikroprzedsiębiorstwa, małego przedsiębiorstwa, średniego przedsiębiorstwa lub przekracza wymogi dla średniego przedsiębiorstwa;”.	Uwaga uwzględniona W przypadku firmy nie ma konieczności wskazywania imienia i nazwiska, ponieważ zgodnie z kodeksem cywilnym firmą osoby fizycznej jest jej imię i nazwisko. Przepis zostanie uzupełniony w zakresie deklaracji MŚP.
31.	Urząd Komisji Nadzoru Finansowego	Art. 7	W związku z koniecznością ustalania statusu MŚP podmiotów finansowych na gruncie rozporządzenia 2022/2554, UKNF zgłosiło do projektu ustawy służącej stosowaniu tego rozporządzenia (projekt ustawy o zmianie niektórych ustaw w związku z zapewnieniem operacyjnej odporności cyfrowej sektora finansowego – UC11) uwagi dotyczące składania do KNF przez podmioty finansowe oświadczeń w omawianym zakresie. W przypadku uwzględnienia omawianych uwag, zasadne może być takie ukształtowanie przepisów UKSC, aby podmiot kluczowy lub ważny, który złożył już w/w oświadczenie do KNF jako właściwego organu w ramach rozporządzenia 2022/2554, mógł nie składać deklaracji z projektowanego art. 7 ust. 2 pkt 13 UKSC. Dane w tym zakresie byłyby zaś uzupełniane przez organ właściwy do spraw cyberbezpieczeństwa. Rozwiązanie takie miałoby na celu unikanie powielania podobnych obowiązków regulacyjnych. Ze względu jednak na toczące się równoległe prace na ustawą implementującą dyrektywę 2022/2555 oraz ustawą służącą stosowaniu rozporządzenia 2022/2554, realizacja omawianego postulatu musiałaby nastąpić w ramach skoordynowania prac nad tymi projektami.	Uwaga uwzględniona Prace nad projektami będą skoordynowane tak aby dążyć do uspoźnienia przepisów.
32.	Urząd Komisji Nadzoru Finansowego	Art. 7	W projektowanym art. 7 ust. 2 pkt 19 UKSC użycie słowa „właściwy” wydaje się zbędne.	Uwaga uwzględniona

Tabela uwag zgłoszonych w ramach opiniowania do *projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)*

33.	Urząd Komisji Nadzoru Finansowego	Art.7	W projektowanym art. 7 ust. 2 pkt 25 UKSC wskazano na datę wykreślenia podmiotu kluczowego lub ważnego z wykazu. W związku z tym, jak i w kontekście całego projektowanego art. 7 ust. 2 UKSC, powstaje wątpliwość, czy przewidziane jest przetwarzanie w wykazie wpisów historycznych, np. dotyczących zmian wpisów wraz z datami ich dokonywania. Jeśli tak, to w ocenie UKNF przepisy nowelizacji mogą wymagać doprecyzowania w tym zakresie.	Uwaga uwzględniona Wprowadzono odpowiedni przepis.
34.	Prezes Głównego Urzędu Statystycznego	art. 7 ust. 3 i 6	Art. 7 ust. 3 projektu ustawy (o krajowym systemie cyberbezpieczeństwa) brzmi: „3. Podmiot kluczowy i podmiot ważny składa wniosek o wpis w wykazie, o którym mowa w ust. 1, w terminie 2 miesięcy od dnia spełnienia wymogów, o których mowa w art. 5 ust. 1 lub ust. 2.” Natomiast art. 7 ust. 6 projektu ustawy (o krajowym systemie cyberbezpieczeństwa) brzmi „6. W przypadku: 1) <i>przedsiębiorców telekomunikacyjnych,</i> 2) <i>dostawców usług zaufania,</i> 3) <i>podmiotów publicznych,</i> 4) <i>podmiotów krytycznych</i> – <i>minister właściwy do spraw informatyzacji wpisuje dane, o których mowa w ust. 2, do wykazu, o którym mowa w ust. 1, dotyczące tych podmiotów w oparciu o dane zawarte w rejestrach publicznych lub przekazane przez właściwe organy nadzorcze.</i> ” Obecnie projektowane zapisy budzą wątpliwości interpretacyjne. Zapisy te są niejasne i wprowadzają wzajemne wykluczenie. Przepis powinien jasno określać czy wpisy do rejestru podmiotów kluczowych i ważnych, które są podmiotami publicznym będzie miał miejsce również na wniosek, czy w ramach działania „z urzędu”.	Uwaga uwzględniona Regułą jest samorejestracja podmiotów. Przepis ustępu 6 dotyczy wyjątku od tej samorejestracji, ponieważ te podmioty zostały już ujęte we właściwych rejestrach i nie ma potrzeby, aby musiały się podwójnie rejestrować. Przepis zostanie wyodrębniony do odrębnej jednostki redakcyjnej.
35.	Rzecznik Praw Obywatelskich	Art. 7 ust. 4	W art. 7 ust. 4 wprowadzone zostaje blankietowe wyłączenie dostępu do informacji publicznej do wykazu podmiotów kluczowych i ważnych prowadzonych przez ministra ds. informatyzacji. Takie blankietowe wyłączenie jest naruszeniem istoty prawa do informacji publicznej (art. 31 ust. 3 zd. 2 Konstytucji). Dostęp do informacji publicznej można ograniczyć, ale ustawa nie powinna z góry określać, że pewne informacje nigdy nie podlegają udostępnieniu, bez względu na okoliczności indywidualne.	Uwaga częściowo uwzględniona Wyłączenie ustawy o dostępie do informacji publicznej ma na celu ochronę danych podmiotów zgromadzonych w wykazie. Wykaz będzie też zawierał dane osobowe jak np. dane osób kontaktowych. Upublicznienie wykazu ułatwiłoby hakywistom czy grupom APT przeprowadzenie rekonesansu

Tabela uwag zgłoszonych w ramach opiniowania do *projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)*

				przed atakiem. Stąd też w interesie podmiotów kluczowych i podmiotów ważnych jest to, aby wykaz co do zasady nie był dostępny publicznie. Jednakże możliwe jest opublikowanie danych statystycznych o liczbie podmiotów znajdujących się w wykazie w podziale na sektory. W tym zakresie minister właściwy do spraw informatyzacji zostanie obowiązany do publikacji tych danych.
36.	Urząd Komisji Nadzoru Finansowego	Art. 7 ust. 13	W projektowanym art. 7 ust. 13 UKSC wskazano, że wnioskiem niepoprawnym jest m.in. wniosek złożony przez osobę, wobec której prawomocnie orzeczono zakaz prowadzenia wszelkiej działalności gospodarczej. W ocenie UKNF można rozważyć w tym zakresie dodatkowe wskazanie również na zakaz prowadzenia działalności gospodarczej tożsamej z przedmiotem działalności podmiotu kluczowego lub ważnego, którego dotyczy wniosek. Wniosek złożony przez osobę z takim zakazem w świetle obecnego sformułowania przepisów byłby poprawny – nie jest to bowiem zakaz wszelkiej działalności gospodarczej (chyba, że przepis ma na celu uniemożliwienie złożenia wniosku przez osobę z jakimkolwiek zakazem prowadzenia działalności gospodarczej – wtedy słowo „wszelkiej” byłoby jednak zbędne, jako ograniczające zakres zastosowania przepisu). Jednocześnie, zakres zastosowania projektowanego art. 7 ust. 13 pkt 3 UKSC należałoby w ocenie UKNF zawęzić do wniosków o wpis – poprawne będą bowiem wnioski o zmianę wpisu lub wykreślenie jeśli dotyczą podmiotu już wpisanego do wykazu. W tym celu przed słowem „dotyczący” można byłoby dodać sformułowanie „o wpis do wykazu”.	Uwaga wyjaśniona Zrezygnowano w ogóle z odnoszenia się przy wniosku niepoprawnym do sprawdzania czy został on złożony przez osobę, wobec której prawomocnie orzeczono zakaz prowadzenia działalności gospodarczej. Taka weryfikacja jest trudna do przeprowadzenia. Tymczasem wniosek składa się pod rygorem odpowiedzialności karnej za złożenie fałszywego oświadczenia, co powinno zabezpieczyć prawidłowość wniosku.
37.	Prezes Urzędu Ochrony Danych Osobowych	Art. 7 ust. 21 i 22	W projektowanym art. 7 ust. 21 i 22 KSC, wprowadzanym art. 1 pkt 10 projektu, minister właściwy do spraw informatyzacji udostępnia dane, o których mowa w ust. 2 tego artykułu, wskazanym podmiotom. Wśród przekazywanych danych znajdują	Uwaga uwzględniona Informacje te będą udostępniane za pomocą systemu S46, co zapewni

Tabela uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

			się również dane osobowe, w związku z czym ustawa powinna wskazywać sposób udostępniania danych innym organom oraz w sposób przejrzysty i precyzyjny określać tryb udostępniania danych.	odpowiedni poziom bezpieczeństwa.
38.	Prezes Urzędu Transportu Kolejowego	Art. 7	Prezes UTK wykonujący zadania krajowej władzy bezpieczeństwa kolejowego (vide: art. 10 ust. 1 ustawy z dnia 28 marca 2003 r. o transporcie kolejowym) powinien posiadać dostęp do odpowiedniej wiedzy o podmiotach kluczowych i ważnych w zakresie podsektora kolejowego. Jest to wiedza niezbędna do realizacji ustawowych zadań tego organu, w szczególności w obszarze bezpieczeństwa ruchu kolejowego oraz nadzoru technicznego nad eksploatacją i utrzymaniem infrastruktury kolejowej oraz pojazdów kolejowych. Proponuje się w zmienianym art. 7 w ust. 22 w pkt 15 kropkę zastąpić średnikiem i dodać pkt 16 w brzmieniu: „16) Prezesowi Urzędu Transportu Kolejowego”.	Uwaga uwzględniona
39.	Prezes Urzędu Ochrony Danych Osobowych	Art. 7a ust. 2 art. 7b ust. 1	W art. 1 pkt 11 projektu proponowane jest dodanie art. 7a ust. 2 KSC, zezwalającego na korzystanie z danych zawartych w rejestrach publicznych przez organ właściwy do spraw cyberbezpieczeństwa przy wpisywaniu podmiotu do wykazu. Rejestry publiczne prowadzone są w konkretnych, wskazanych w przepisach prawa celach, w których też przetwarzane są dane osobowe w nich zgromadzone. Pozyskiwanie przez organ publiczny danych z innych baz danych powinno odbywać się z poszanowaniem zasad i gwarancji wynikających z rozporządzenia 2016/679⁸⁾. Zgodnie z motywem 31 rozporządzenia 2016/679 żądanie ujawnienia danych osobowych, z którym występują organy publiczne, powinno zawsze mieć formę pisemną, być uzasadnione, mieć charakter wyjątkowy, nie powinno dotyczyć całego zbioru danych ani prowadzić do połączenia zbiorów danych. Z tych względów w przepisach określone powinny być procedury, formy, zakres i tryb udostępniania danych osobowych. Określenia wymaga również w jaki sposób organ przetwarzać będzie informacje. Analogiczna uwaga odnosi się do projektowanego art. 7b ust. 1, przewidującego weryfikację danych za pomocą danych zawartych w rejestrach publicznych lub innych powszechnie dostępnych źródłach informacji. Zmiany w funkcjonowaniu istniejących rejestrów publicznych powinny być poprzedzone analizą przepisów krajowych kształtujących zasady ich prowadzenia, udostępniania z nich danych, trybu	Uwaga wyjaśniona Z rejestrów publicznych potrzebne są dane dotyczące rodzaju działalności podmiotu (ew. informacja o wpisie do rejestru działalności regulowanej czy uzyskaniu koncesji), dane o przychodzie lub obrocie oraz liczba pracowników. Te informacje łącznie dają obraz tego czy podmiot wchodzi w zakres ustawy czy nie. Przepis zostanie doprecyzowany w tym zakresie – wskazane zostanie, że chodzi o dane zawarte w publicznie dostępnych rejestrach publicznych.

⁸⁾ Wyrok TSUE w sprawie C-201/14 z dnia 1 października 2014 r.(wniosek o wydanie orzeczenia w trybie prejudycjalnym złożony przez Curtea de Apel Cluj - Rumunia) Smaranda Bara i in./Casa Națională de Asigurări de Sănătate, Președintele Casei Naționale de Asigurări de Sănătate, Agenția Națională de Administrare Fiscală (ANAF).

Tabela uwag zgłoszonych w ramach opiniowania do *projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)*

			udostępniania, ewentualnie przeglądem tych przepisów pod kątem enumeratywnie wskazanych w nich podmiotów, które mogą mieć dostęp do danych zawartych w takich rejestrach. Gdyby taki test prywatności został przeprowadzony, projektodawca mógłby horyzontalnie ocenić istniejące prawodawstwo, tak aby nie obniżać gwarancji ochrony danych osobowych wynikających z aktualnie obowiązujących przepisów prawa i cel jakim jest zadbanie o cyberbezpieczeństwo realizowany byłby przez wykonawców norm z poszanowaniem także praw podmiotów danych. Być może zatem należałoby zmienić dodatkowo przepisy krajowe, a nie tworzyć ogólną normę blankietową, z której nie wynika na jakich innych zasadach niż dotychczas obowiązujące miałyby być udostępniane dane z rejestrów publicznych.	
40.	Rzecznik Małych i Średnich Przedsiębiorców	Art. 7a i art. 7c	Proponowana treść art. 1 pkt 11 Projektu (dodający do ustawy zmienianej art. 7a - 7c), który określa procedurę wpisu z urzędu do Wykazu przez organ właściwy. Procedura ta nie daje podmiotowi, który może zostać wpisany do Wykazu z urzędu - żadnej możliwości wzruszenia decyzji wydanej w tym zakresie przez organ właściwy. Postulat: – zmiana treści art. 1 pkt 11 Projektu w zakresie odnoszącym się w szczególności do dodawanego art. 7c ust. 4-6 przez jednoznaczne wskazanie drogi odwoławczej dla podmiotu, wobec którego organ właściwy wydaje decyzję o wpisie do Wykazu, – zmiana treści art. 1 pkt 11 Projektu w odniesieniu do dodawanego art. 7c ust. 3 pkt 2, przez wydłużenie terminu na uzupełnienie brakujących danych do co najmniej 1 miesiąca, – zmiana treści art. 1 pkt 11 Projektu w odniesieniu do dodawanego art. 7c ust. 6 pkt 1, przez wydłużenie okresu na dostosowanie do 12 miesięcy, – zmiana treści art. 1 pkt 11 Projektu w odniesieniu do dodawanego art. 7c ust. 6 pkt 2, przez wydłużenie terminu na przeprowadzenie audytu do 24 miesięcy. Uzasadnienie: Wpis z urzędu do Wykazu ma dla podmiotu, którego dotyczy daleko idące konsekwencje w wymiarze organizacyjnym i finansowym, z tego powodu konieczne jest, aby podmiot, którego dotyczy decyzja o wpisie do Wykazu posiadał możliwość wzruszenia wydanej decyzji. Uzasadnienie Projektu⁶ zawiera wyjaśnienie, iż podmiot będzie miał możliwość ochrony swoich praw, jednak nie wskazuje ono precyzyjnie przysługującej drogi odwoławczej, z której można skorzystać. Ponadto po	Uwaga częściowo uwzględniona Termin na uzupełnienie brakujących danych wyniesie 2 mies. Termin na dostosowanie się do wymogów ustawy wyniesie 6 miesięcy, a na pierwszy audyt 24 miesiące.

Tabela uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

			zakończeniu prac nad Projektem, objęte nim zmiany będą funkcjonować w obrocie prawnym bez uzasadnienia, dlatego ważne jest, aby planowane do wprowadzenia regulacje nie pozostawiały wątpliwości interpretacyjnych w tak istotnym zakresie. W odniesieniu do terminów określonych w projektowanych art. 7c ust. 3 pkt 2 oraz art. 7c ust. 6 pkt 1 Należy wziąć pod uwagę, iż wpis z urzędu do Wykazu - może dotyczyć mniejszych podmiotów oraz podmiotów, które nie przewidywały, iż będą podlegać omawianym regulacjom - z tego powodu może nie być możliwe uzupełnienie treści niektórych informacji w terminie 14 dni oraz osiągnięcie pełnej zgodności z wymogami rozdziału ustawy zmienianej w ciągu 6 miesięcy. Postulowane wydłużenie tych terminów do odpowiednio 30 dni oraz 12 miesięcy daje podmiotom zobowiązany szansę na wdrożenie przemyślanych zmian organizacyjnych i uniknięcie dotkliwych kar. Mając na względzie żądane art. 7c ust. 6 pkt 2 przeprowadzenie audytu bezpieczeństwa przez podmiot, który został wpisany do Wykazu z urzędu, zasadne jest, aby podmiot taki nie był w gorszym położeniu niż inne podmioty kluczowe i podmioty ważne, dlatego postulat 24 miesięcy na przeprowadzenie audytu bezpieczeństwa jest zgodny z regulacją zawartą w art. 1 pkt 20 lit. a) Projektu (art. 15 ust 1 ustawy zmienianej).	
41.	Krajowa Rada Radiofonii i Telewizji	Art. 7c ust. 1 i 2	Ponadto, kwestię terminologii – zasadniczą dla ustalenia zakresu podmiotowego projektowanych regulacji, dodatkowo komplikują przepisy projektowanego art. 7c ust. 1 i 2 ustawy.	Uwaga wyjaśniona Uwaga jest bardzo ogólnikowa i nie jest jasna intencja KRRIT.
42.	Urząd Komisji Nadzoru Finansowego	Art. 7c ust. 1 pkt 3 lit. b	W kontekście projektowanego art. 7c ust. 1 pkt 3 lit. b) UKSC należy zwrócić uwagę, że w art. 2 ust. 2 lit. c) dyrektywy 2022/2555 obok porządku publicznego oraz bezpieczeństwa publicznego wymieniono także zdrowie publiczne.	Uwaga uwzględniona Przepis zostanie uzupełniony o zdrowie publiczne.
43.	Urząd Komisji Nadzoru Finansowego	Rozdział 3	W projekcie brakuje przepisu zmieniającego tytuł rozdziału 3 ustawy na „Obowiązki podmiotów kluczowych i podmiotów ważnych”.	Uwaga uwzględniona
44.	Prezes Urzędu Komunikacji Elektronicznej	Art. 8	Art. 1 pkt 12 w zakresie dotyczącym projektowanego art. 8 ustawy o ksc – mając na uwadze brzmienie niniejszego przepisu proponuje się uzupełnić projektowaną ustawę o dodatkową regulację, na podstawie której kierownik podmiotu kluczowego lub podmiotu ważnego będzie mógł powierzyć podmiotowi zewnętrznemu (tj. działającemu poza strukturą organizacyjną podmiotu kluczowego lub podmiotu ważnego) realizację wymagań, o których mowa w projektowanym art. 8 ustawy o ksc, z zastrzeżeniem, iż:	Uwaga nieuwzględniona Z uwagi na transgraniczność usług społeczeństwa informacyjnego te wymogi mogą być niemożliwe do spełnienia. Bywa tak, że są manager security services providers, którzy mają swoje centra przetwarzania danych w kilku państwach, a nawet

Tabela uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

			– podmiot zewnętrzny dysponuje zdolnościami technicznymi i organizacyjnymi niezbędnymi do realizacji ww. wymagań, – infrastruktura podmiotu zewnętrznego, wykorzystywana do realizacji ww. wymagań, znajduje się na terytorium Unii Europejskiej, – dane przetwarzane w związku z realizacją ww. wymagań powinny być dostępne na terytorium Rzeczypospolitej Polskiej, – umowa zawarta przez kierownika podmiotu kluczowego lub podmiotu ważnego z podmiotem zewnętrznym będzie zawierać wymóg, zgodnie z którym świadczenie usług na rzecz podmiotu kluczowego lub podmiotu ważnego będzie podlegać regulacjom prawa Rzeczypospolitej Polskiej. Niniejsza propozycja jest zgodna z wymaganiami określonymi na potrzeby aukcji 5G, które uzyskały w dniu 23 marca 2023 r. pozytywną opinię Kolegium do Spraw Cyberbezpieczeństwa.	na kilku kontynentach. Wprowadzenie takich wymogów znacznie ograniczyłoby liczbę takich dostawców.
45.	Prezes Urzędu Ochrony Danych Osobowych	Art. 8 ust. 1	W art. 8 ust. 1 KSC (określonym w art. 1 pkt 12 projektu) prawodawca wyznaczył podmiot kluczowy lub podmiot ważny do wdrażania systemu zarządzania bezpieczeństwem informacji w procesach wpływających na świadczenie usług przez ten podmiot. Należy zauważyć, że podmiot kluczowy oraz podmiot ważny jako takie są związane także przepisami rozporządzenia 2016/679 i z tego względu obowiązane są do stosowania m.in. analizy ryzyka, oceny skutków dla ochrony danych, domyślnej ochrony danych, bezpieczeństwa danych i obsługi naruszeń ochrony danych osobowych, a więc do stosowania rozwiązań systemowych wynikających z obowiązków nałożonych na administratora, określonych przepisami rozdziału IV rozporządzenia 2016/679. Kwestia ta odnosi się zasadniczo do ogólnych obowiązków podmiotu kluczowego oraz podmiotu ważnego, jak i do obowiązków szczegółowych wynikających z projektowanego art. 8 ust. 1 oraz 4 KSC.	Uwaga wyjaśniona Obowiązki z projektowanego art. 8 nie zagrażają wykonywaniu obowiązków wynikających z RODO – wręcz przeciwnie są one komplementarne.
46.	Polski Komitet Normalizacyjny	Art.8 ust 2	Niewłaściwy numer normy, prawidłowy numer to PN EN ISO 22301	Uwaga wyjaśniona Pod wpływem różnych uwag zrezygnowano z koncepcji mapowania.
47.	Urząd Dozoru Technicznego	Art. 8 ust. 2	W zmienianym art. 8 ust. 2 ustawy proponuje się, aby jednostka redakcyjna otrzymała następujące brzmienie: <i>„2. Wymagania, o których mowa w ust. 1, uznaje się za spełnione, gdy podmiot kluczowy i podmiot ważny zapewnia system zarządzania bezpieczeństwem informacji</i>	Uwaga wyjaśniona Pod wpływem różnych uwag zrezygnowano z koncepcji mapowania.

Tabela uwag zgłoszonych w ramach opiniowania do *projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)*

			<i>certyfikowany przez akredytowaną jednostkę, zgodny z wymaganiami określonymi w Polskiej Normie PN-EN ISO/IEC 27001 oraz PN-EN ISO 22301”.</i> Gwarancją prawidłowego wykonywania zadań z zakresu cyberbezpieczeństwa jest wskazanie, że spełnienie wymagań, o których mowa w ust. 1 zostanie potwierdzone poprzez certyfikację uzyskaną od akredytowanej jednostki. Zapewnienie systemu zarządzania bezpieczeństwem informacji jest możliwe po dokonaniu oceny przez niezależną trzecią stronę – akredytowaną jednostkę certyfikującą. Certyfikowany system zarządzania potwierdza, że organizacja działa w sposób zorganizowany i strategiczny w celu poprawy bezpieczeństwa, potwierdza spełnienie określonych wymagań wskazanych standardów, wpływa na minimalizację ryzyka, zapewnia właściwy pomiar, poprawne dokumentowanie oraz raportowanie poprzez ciągły nadzór akredytowanej jednostki nad udzieloną certyfikacją. Natomiast akredytacja potwierdza uznanie i potwierdzenie kompetencji technicznych danej jednostki (organizacji) do przeprowadzania działań certyfikacji, zaświadcza o działaniu wedle uczciwej praktyki rynkowej oraz potwierdza kompetencje jednostki certyfikującej. Ponadto proces akredytacji eliminuje jednostki będące jednocześnie firmami wdrażającymi systemy zarządzania. Proces certyfikacji wdrażanego przez tę samą jednostkę systemu zarządzania wyklucza zastosowanie kryterium bezstronności. Akredytowane jednostki zapewniają powtarzalność i równe traktowanie certyfikowanych podmiotów i nie są narażone na ryzyko podejmowania decyzji w trakcie procesu certyfikacji wynikające z kryterium przychodowego. Pozostawienie brzmienia projektu przepisu w brzmieniu zaproponowanym przez projektodawcę w zasadzie pozostawia obowiązek wykazania spełnienia wymagań z ust. 1 na podmiocie kluczowym/podmiocie ważnym bez udziału niezależnej strony trzeciej.	
48.	Urząd Komisji Nadzoru Finansowego	Art. 8 ust. 2	W kontekście wskazania w projektowanym art. 8 ust. 2 UKSC na Polskie Normy PN-EN ISO/IEC 27001 oraz PN-EN ISO/IEC 22301 powstaje wątpliwość, jakie normy miałyby w tym zakresie zastosowanie w przypadku ich wycofania. W ocenie UKNF można rozważyć wskazanie w tym przepisie podobne jak w projektowanym art. 10 ust. 3 pkt 1 UKSC, tj. odniesienie również do normy równoważnej.	Uwaga wyjaśniona Pod wpływem różnych uwag zrezygnowano z koncepcji mapowania.
49.	Polski Komitet Normalizacyjny	Art.8 ust 3	<i>Minister właściwy do spraw informatyzacji może udostępnić w Biuletynie Informacji Publicznej na swojej stronie podmiotowej mapowanie wymogów Polskich Norm,</i>	Uwaga wyjaśniona

Tabela uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

			<i>o których mowa w ust. 2, na obowiązki wynikające z ustawy oraz z przepisów wydanych na podstawie art. 8a.</i> Zdaniem PKN powyższy zapis jest niejasny. Czy oznacza on wprowadzenie pewnych norm do obowiązkowego stosowania poprzez opublikowanie informacji o tym w BIP? Byłoby to sprzeczne z zasadą dobrowolności stosowania norm zapisaną w art. 5 ust. 3 ustawy o normalizacji z dnia 12 września 2002 r. (t.j. Dz. U. z 2015 r. poz. 1483).	Mapowanie Polskich Norm na obowiązki ma być jedynie działaniem dodatkowym, które ma pomóc przedsiębiorcom w realizacji obowiązków nałożonych niniejszą ustawą. Dzięki temu będą oni wykorzystywać normy w celu realizacji swoich ustawowych obowiązków. Nie oznacza to jednak obowiązku stosowania tych norm w związku z czym nie jest to sprzeczne z art. 5 ust. 3 ustawy z dnia 12 września 2002 r. o normalizacji
50.	Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy	Art. 8 ust. 4	W zakresie proponowanego brzmienia art. 8 ust. 4 warto rozważyć usunięcie we wprowadzeniu do wyliczenia odesłania do „lit. c”, a pozostawienie odesłania do środków, o których mowa w ust. 1 pkt 2. Uwzględnianie podatności, ogólnej jakości produktów, usług i procesów ICT oraz wyników skoordynowanej oceny bezpieczeństwa przez podmiot nie powinno się ograniczać tylko do środków technicznych i organizacyjnych w zakresie bezpieczeństwa fizycznego i środowiskowego, uwzględniającego kontrolę dostępu, a raczej do wszystkich środków technicznych i organizacyjnych w systemie zarządzania bezpieczeństwem informacji.	Uwaga uwzględniona Przepis zostanie zmieniony.
51.	Urząd Komisji Nadzoru Finansowego	Art. 8a	Ze względu na zastosowanie do podmiotów z sektora bankowego i infrastruktury rynków finansowych przepisów rozporządzenia 2022/2554 oraz aktów wykonawczych do tego rozporządzenia w zakresie wymogów dotyczących zarządzania ryzykiem w cyberbezpieczeństwie, w tym wymogów dotyczących bezpieczeństwa sieci i systemów informatycznych, postuluje się wyłączenie możliwości wydania rozporządzenia, o którym mowa w projektowanym art. 8a UKSC, w stosunku do działalności wykonywanej przez podmioty kluczowe lub ważne tego sektora.	Uwaga uwzględniona Przepis zostanie zmieniony.
52.	Rzecznik Małych i Średnich Przedsiębiorców	Art. 8a	W odniesieniu do art. 1 pkt 13 Projektu (dodający do ustawy zmienianej art. 8a-8i), który w art. 8a nadaje Radzie Ministrów uprawnienie do wydania rozporządzenia określającego szczegółowe wymagania systemu zarządzania bezpieczeństwem informacji, o którym mowa w zmienianym art. 8 - za zasadny należy uznać postulat,	Uwaga wyjaśniona Decyzja o wydaniu rozporządzenia powinna podlegać wcześniej analizie czy jest zasadne

Tabela uwag zgłoszonych w ramach opiniowania do *projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)*

			aby Rada Ministrów została zobligowana do wydania takiego rozporządzenia, wobec czego proponuje się następujące brzmienie tego przepisu: <i>„Art. 8a. Rada Ministrów <u>określi</u>, w drodze rozporządzenia, odrębnie dla danego rodzaju działalności wykonywanej przez podmioty kluczowe lub podmioty ważne szczegółowe wymagania dla systemu zarządzania bezpieczeństwem informacji, o którym mowa w art. 8 ust. 1, biorąc pod uwagę rekomendacje międzynarodowe o charakterze specjalistycznym, w tym rekomendacje Agencji Unii Europejskiej do spraw Cyberbezpieczeństwa, zwanej dalej „ENISA”, skalę działalności wykonywanej przez te podmioty, ich wielkość w rozumieniu Załącznika I do rozporządzenia Komisji (UE) nr 651/2014 z dnia 17 czerwca 2014 r. uznającego niektóre rodzaje pomocy za zgodne z rynkiem wewnętrznym w zastosowaniu art. 107 i 108 Traktatu⁷⁾ oraz potrzebę podejmowania przez te podmioty działań zapewniających cyberbezpieczeństwo.”</i>(zmiany podkreślone) Uzasadnienie: Zasady oraz wytyczne określające system zarządzania bezpieczeństwem informacji w procesach wpływających na świadczenie usług, który podmioty kluczowe oraz podmioty ważne zobowiązane będą wdrożyć, są bardzo istotne, a związany z tym wysiłek organizacyjny i finansowy adekwatnie duży. Z tego powodu zasadne jest, aby organ uprawniony taki akt wykonawczy wydał. Akt ten powinien również określać standardy systemu z uwzględnieniem wielkości podmiotu. Podmioty zobowiązane do wdrożenia systemu powinny mieć na wypełnienie tego obowiązku co najmniej 12 miesięcy od daty publikacji przedmiotowego rozporządzenia, zatem wejście w życie zmienianego przepisu art. 8 powinno nastąpić w proponowanym czasie po publikacji w dzienniku ustaw tego rozporządzenia,	doprecyzowanie wymogów systemu zarządzania bezpieczeństwem informacji. Planowane jest wydawanie rozporządzeń dostosowane do wielkości podmiotów. Vacatio legis takiego rozporządzenia powinno być dostosowane do charakteru obowiązków zgodnie z art. 2 Konstytucji.
53.	Prezes Głównego Urzędu Statystycznego	Art. 8c	Proponowany art. 8c projektu ustawy (o krajowym systemie cyberbezpieczeństwa) powinien jasno określać rodzaj i zakres odpowiedzialności Kierownika podmiotu kluczowego lub podmiotu ważnego. Kary finansowe zostały wskazane w art. 73a i następne. Jeżeli zapisy dot. odpowiedzialności kierownika mają pozostać w art. 8c to należy dookreślić jaki jest to rodzaj odpowiedzialności i wskazać odwołanie do art. 73a i następnych. Ewentualnie należy zapisy art. 8c przenieść do art. 73a.	Uwaga uwzględniona Przepis art. 73a został doprecyzowany o odpowiedzialność za niewykonanie obowiązków, o których mowa w art. 15. Pozostałe obowiązki zostały już przewidziane w przepisie i pokrywają się z odpowiedzialnością kierownika podmiotu określoną na podstawie art. 8c ust. 1. Różnica w odwołaniu

Tabela uwag zgłoszonych w ramach opiniowania do *projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)*

				wynika z konieczności zapewnienia najwyższej precyzji przy określaniu przepisów o charakterze represyjnym (przepis o karze pieniężnej). Z tego względu zdecydowano się szczegółowo wskazać ustępy przy właściwych artykułach – wśród nich wskazane są obowiązki podmiotów, za które odpowiada również kierownik. Odwołanie przy sankcji karnej do całości przepisu byłoby nieprecyzyjne z uwagi na to, że przepisy te mają niekiedy charakter techniczny lub odnoszą się do uprawnień i obowiązków ministra właściwego do spraw informatyzacji czy innych organów właściwych do spraw cyberbezpieczeństwa.
54.	Prezes Urzędu Komunikacji Elektronicznej	Art. 8e	Art. 1 pkt 13 w zakresie dotyczącym projektowanego art. 8e ustawy o ksc – w odniesieniu do projektowanego przepisu proponuje się rozważyć, aby obowiązek przechodzenia szkolenia, o którym mowa w tym przepisie, dotyczył nie tylko kierownika podmiotu kluczowego lub podmiotu ważnego, ale również osoby, której została powierzona realizacja części obowiązków kierownika podmiotu kluczowego lub podmiotu ważnego, w tym np. obowiązek wynikający z art. 8 ust. 1 pkt 2 lit. b projektowanej ustawy o ksc polegający na zapewnieniu utrzymania i bezpiecznej eksploatacji systemu informacyjnego;	Uwaga uwzględniona Wprowadzony zostanie obowiązek szkoleń dla osób realizujących zadania kierownika podmiotu – ale to nie będzie zwalniało samego kierownika ze szkolenia.
55.	Prezes Urzędu Ochrony Danych Osobowych	Art. 8f ust.2	Art. 1 pkt 13 projektu wprowadza propozycję dodania art. 8f ust. 2 KSC, dotyczącego weryfikacji niekaralności osób dokonywanej przez podmiot kluczowy i podmiot ważny. Tak istotna kwestia nie może być uregulowana tak lakonicznym, wręcz blankietowym przepisem. Wyjaśnienia wymaga co oznacza sformułowanie „weryfikacja niekaralności”, w szczególności w zakresie informacji, jakie będą przetwarzane oraz trybu tej weryfikacji. Nie jest jasne czy wystarczające dla wypełnienia obowiązku wynikającego z przepisu będzie jedynie ustalenie braku przesłanki ukarania, a jeśli tak, to czy chodzi o ukaranie za wszelkie przestępstwa i	Uwaga uwzględniona Przepis zostanie poprawiony.

Tabela uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

			wykroczenia, czy też tylko za określone ich typy. Weryfikacja taka będzie się wiązać z przetwarzaniem danych objętych szczególnym reżimem przetwarzania dotyczącym wyroków skazujących i czynów zabronionych lub powiązanych środków bezpieczeństwa (art. 10 rozporządzenia 2016/679) ⁹⁾ . Przetwarzanie tej kategorii danych wymaga z kolei szczególnych rozwiązań w przepisach, z uwzględnieniem warunków z art. 10 rozporządzenia 2016/679.	
56.	Urząd Komisji Nadzoru Finansowego	Art. 8h	W świetle projektowanego art. 8h UKSC należy w ocenie UKNF postulować wskazanie w ustawie na uprawnienie udziału CSIRT (zarówno poziomu krajowego, jak i sektorowych), w mechanizmach wymiany informacji na temat cyberbezpieczeństwa podmiotów kluczowych lub ważnych (tak, aby warunki udziału organów publicznych w takich mechanizmach nie mogły wykluczyć takiego uprawnienia). Dane przetwarzane w ramach tego rodzaju mechanizmów mogą być bowiem cennym źródłem informacji dla zespołów CSIRT, umożliwiając im osiągnięcie jeszcze większej świadomości sytuacyjnej m.in. w obszarze bieżących cyberzagrożeń. Postulat ten znajduje swoje uzasadnienie również w treści art. 29 ust. 3 zdanie trzecie i czwarte dyrektywy 2022/2555, w których wskazano, że „Określając szczegóły udziału organów publicznych w tych mechanizmach, państwa członkowskie mogą ustalać warunki udostępniania informacji przez właściwe organy lub CSIRT. Państwa członkowskie oferują pomoc w stosowaniu takich mechanizmów zgodnie ze swoją polityką, o której mowa w art. 7 ust. 2 lit. h).”.	Uwaga uwzględniona
57.	Prezes Urzędu Ochrony Danych Osobowych	Art. 8h	Proponowany art. 8h ust. 1 KSC (wprowadzany w art. 1 pkt 13 projektu) dotyczący wymiany informacji dotyczących cyberbezpieczeństwa między podmiotami kluczowymi i podmiotami ważnymi wymaga uzupełnienia o wskazanie, że wymianie takiej nie będą podlegały dane osobowe. W proponowanym ust. 5 tego artykułu dotyczącym zawarcia porozumienia w sprawie wymiany informacji między podmiotami kluczowymi, podmiotami ważnymi, CSIRT sektorowymi lub innymi podmiotami, należy podkreślić, że o ile wśród wymienianych informacji znajdowałyby się dane osobowe, to ich wymiana może odbywać się tylko na podstawie przepisów prawa, uwzględniających wymagania określone w art. 6 ust. 3	Uwaga uwzględniona W systemie S46 nie będą wymieniane dane osobowe w zakresie art. 8h. Nie można wykluczyć, że wymianie będą podlegały dane osobowe w ramach porozumień z ust. 5. Sama dyrektywa NIS2 wskazuje, że można wymieniać się informacjami o grupach przestępczych.

⁹⁾ Przetwarzania danych osobowych dotyczących wyroków skazujących oraz czynów zabronionych lub powiązanych środków bezpieczeństwa na podstawie art. 6 ust. 1 wolno dokonywać wyłącznie pod nadzorem władz publicznych lub jeżeli przetwarzanie jest dozwolone prawem Unii lub prawem państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw i wolności osób, których dane dotyczą. Wszelkie kompletne rejestry wyroków skazujących są prowadzone wyłącznie pod nadzorem władz publicznych.

Tabela uwag zgłoszonych w ramach opiniowania do *projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)*

			rozporządzenia 2016/679, a nie w drodze porozumienia kształtującego w sposób dowolny zasady przetwarzania danych.	Informacje o tym kto zidentyfikował podatności, albo kto stworzył oprogramowanie ransomware, nawet jeżeli kryłby się tylko pod pseudonimem. Co istotne przepis ten zostanie doprecyzowany – wymiana informacji będzie miała charakter fakultatywny, tak jak stanowi dyrektywa NIS2. Dlatego nie znajdzie tutaj zastosowania art. 6 ust. 1 lit. c oraz e rozporządzenia 2016/679. W opinii MC potencjalnie może tutaj zaistnieć przetwarzanie danych osobowych (np. pseudonim hakerów, adres email, z którego hakerzy wysyłają fałszywe wiadomości email, adresy IP) na podstawie art. 6 ust. 1 lit. f – prawnie uzasadnionym interesem będzie konieczność zapewnienia bezpieczeństwa systemów informacyjnych danego podmiotu.
58.	Urząd Komisji Nadzoru Finansowego	Art. 8i	UKNF kierunkowo akceptuje rozwiązanie przyjęte w projektowanym art. 8i ustawy o krajowym systemie cyberbezpieczeństwa (dalej jako „UKSC”). Przepis ten stanowi realizację zasady wynikającej z art. 4 dyrektywy 2022/2555, zgodnie z którą rozporządzenie 2022/2554, jako sektorowy akt prawny Unii, stanowić będzie <i>lex specialis</i> w stosunku do wymogów w/w dyrektywy związanych ze środkami zarządzania ryzykiem w cyberbezpieczeństwie lub zgłaszania poważnych incydentów oraz powiązanych z nimi przepisów dotyczących egzekwowania, w przypadku podmiotów kluczowych lub ważnych będących podmiotami finansowymi. W ocenie UKNF zasadne jest jednak doprecyzowanie zakresu obowiązków wynikających z UKSC, które będą miały zastosowanie do podmiotów kluczowych lub ważnych z sektora bankowego i infrastruktury rynków finansowych. Zwiększy to przede wszystkim poziom pewności prawa z perspektywy takich podmiotów, poprzez jasne określenie obowiązków wynikających z UKSC, które będą one realizować.	Uwaga uwzględniona Przepis zostanie dodany przy czym dostosowano go do numeracji.

			Pośrednio posłuży to również np. doprecyzowaniu zakresu zadań organu właściwego ds. cyberbezpieczeństwa w omawianym sektorze (z uwagi na korelację zakresu nadzoru oraz nakładanych kar pieniężnych, z zakresem obowiązków ciążących na podmiotach kluczowych lub ważnych tego sektora). W związku z powyższym UKNF postuluje nadanie projektowanemu art. 8i UKSC następującego brzmienia: „Art. 8i. 1. Do podmiotów kluczowych i podmiotów ważnych z sektora bankowego i infrastruktury rynków finansowych nie stosuje się przepisów ustawy dotyczących środków zarządzania ryzykiem w cyberbezpieczeństwie lub zgłaszania poważnych incydentów, z wyjątkiem art. 3a, art. 5 ust. 1-3, art. 7-7c, art. 8 ust. 1 pkt 1 i 6, art. 8h, art. 9, art. 11 ust. 1 pkt 5 i 6, art. 13, art. 15, art. 16, art. 26a ust. 2-4, art. 32, art. 33 ust. 5, 7 oraz 8, art. 36a, art. 36b, art. 37, art. 43, art. 46 ust. 1 pkt 1, 2, 4-7 oraz ust. 4-6, art. 67a ust. 4, art. 67c, art. 67d, art. 67g, art. 67h oraz art. 67i. 2. Do podmiotów kluczowych i podmiotów ważnych z sektora bankowego i infrastruktury rynków finansowych odpowiednio stosuje się art. 8 ust. 2, art. 8c, art. 8d, art. 8e, art. 8f, art. 12 ust. 7 oraz art. 31 ust. 1 ustawy. 3. Przepisy rozdziałów 11 i 14 ustawy stosuje się do podmiotów, o których mowa w ust. 1, w zakresie art. 3a, art. 5 ust. 1-3, art. 7-7c, art. 8 ust. 1 pkt 1 i 6, art. 8h, art. 9, art. 11 ust. 1 pkt 5 i 6, art. 13, art. 15, art. 16, art. 26a ust. 2-4, art. 32, art. 33 ust. 5, 7 oraz 8, art. 36a, art. 36b, art. 37, art. 43, art. 46 ust. 1 pkt 1, 2, 4-7 oraz ust. 4-6, art. 67a ust. 4, art. 67c, art. 67d, art. 67g, art. 67h oraz art. 67i ustawy oraz stosowanych odpowiednio art. 8 ust. 2, art. 8c, art. 8d, art. 8e, art. 8f, art. 12 ust. 7 oraz art. 31 ust. 1 ustawy.”. Zakres wskazanych powyżej przepisów określony został na podstawie analizy treści UKSC oraz opiniowanej nowelizacji w kontekście wymogów płynących z rozporządzenia 2022/2554 i odpowiada on w ocenie UKNF zakresowi wyłączenia, jakie wynika z zasady dotyczącej statusu rozporządzenia 2022/2554 jako <i>lex specialis</i> wobec dyrektywy 2022/2555. Dodatkowo należy mieć przy tym na uwadze wskazanie w motywie 18 rozporządzenia 2022/2554, że pomimo stosowania powyższej zasady, podmioty kluczowe i ważne będące podmiotami finansowymi powinny pozostać częścią „ekosystemu” dyrektywy 2022/2555. Odzwierciedlają to także inne przepisy rozporządzenia 2022/2554, jak np. jego art. 22 ust. 1, przewidujący możliwość udzielania wsparcia przez zespoły CSIRT na rzecz podmiotów finansowych. Wyznaczony powyżej zakres obowiązków mających zastosowanie do podmiotów kluczowych i ważnych w sektorze bankowym i infrastruktury rynków finansowych	

			ma także na celu zachowanie spójnego podejścia z treścią art. 1 ust. 3 rozporządzenia 2022/2554, w którym podkreślono, że rozporządzenie to pozostaje bez uszczerbku dla odpowiedzialności państw członkowskich w zakresie podstawowych funkcji państwa dotyczących bezpieczeństwa publicznego, obronności i bezpieczeństwa narodowego. Przepisy mające na celu ochronę bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego zawarte są zaś w projektowanej nowelizacji UKSC, czego przykładem może być regulacja dotycząca dostawcy wysokiego ryzyka. Dodatkowo, wskazane powyżej w opiniowanym art. 8i UKSC przepisy obejmują również dodatkowe uprawnienia podmiotów kluczowych lub ważnych, jak choćby projektowany art. 3a UKSC (umożliwiający podmiotom kluczowym lub ważnym podejmowanie działań w ramach obsługi incydentów, polegających w szczególności na wykrywaniu źródła lub dokonywania analizy ruchu sieciowego powodujących wystąpienie incydentu zakłócającego świadczenie przez ten podmiot usług), czy też dotyczących kwestii określenia podmiotów kluczowych lub ważnych w sektorze bankowym i infrastruktury rynków finansowych (np. art. 5 czy art. 7 UKSC). Proponuje się także dodanie nowego ust. 2 w omawianym przepisie, aby wskazać na odpowiednie stosowanie określonych przepisów UKSC do podmiotów kluczowych lub ważnych w sektorze bankowym i infrastruktury rynków finansowych. Chodzi przede wszystkim o przypadki, gdy dany wymieniony w dodawanym ust. 2 przepis, z racji zakresu katalogu ujętego w projektowanym art. 8i ust. 1 UKSC, znajdzie zastosowanie do w/w podmiotów jedynie w części, a nie w pełnym zakresie/wprost. Przykładowo, art. 8c UKSC wymieniony w katalogu z ust. 2, znajdzie zastosowanie jedynie w części dotyczącej art. 7, art. 8 ust. 1 pkt 1 i 6, art. 8h, art. 9, art. 11 ust. 1 pkt 5 i 6, art. 13 oraz art. 15 (te przepisy znalazłyby bowiem zastosowanie do podmiotów kluczowych lub ważnych w sektorze bankowym i infrastruktury rynków finansowych), a nie znajdzie zastosowania w pozostałym zakresie, z uwagi na brak zastosowania pozostałych wymienionych w nim przepisów do w/w podmiotów. Jako inny przykład można wskazać także na odesłanie do art. 12 ust. 7 UKSC – jego odpowiednie stosowanie ma na celu umożliwienie uzyskania informacji przez CSIRT poziomu krajowego od podmiotów kluczowych lub ważnych w sektorze bankowym i infrastruktury rynków finansowych, ale potrzebna jest modyfikacja jego stosowania, gdyż przepis ten nie odnosi się do wstępnego powiadomienia i zgłoszeń, o których mowa w art. 19 ust. 4 rozporządzenia 2022/2554, a zastosowana jest w nim terminologia odpowiadająca dyrektywie 2022/2555. Podobnie jeżeli chodzi np. o katalog kar pieniężnych mających zastosowanie do podmiotów kluczowych lub ważnych w sektorze bankowym i infrastruktury rynków finansowych – do podmiotów	

Tabela uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

			tych znalazłyby zastosowanie jedynie te przepisy rozdziału 14 ustawy, które sankcjonują naruszenia obowiązków wymienionych w projektowanym art. 8i UKSC, w brzmieniu zaproponowanym powyżej. Rolę w tym zakresie, jak i w zakresie nadzoru, pełni proponowany ust. 3.	
59.	Narodowy Bank Polski	Art. 8i	Ad. art. 1 pkt 13 projektu ustawy w zakresie dodawanego art. 8i: „8i. Podmioty kluczowe i podmioty ważne z sektora bankowość i infrastruktura rynków finansowych nie stosują przepisów niniejszego rozdziału w zakresie w jakim mają obowiązek stosować rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016r1011 (Dz. Urz. UE L 333 z 27.12.2022, str. 1).”. Biorąc pod uwagę specyfikę sektora oraz skalę działalności (wielkość) podmiotów uznanych za podmioty kluczowe i ważne, proponujemy doprecyzować art. 8i, dotyczący podmiotów z sektora bankowości i infrastruktury, o zasadę proporcjonalności.	Uwaga wyjaśniona Przepis zostanie zmieniony zgodnie z propozycją UKNF.
60.	Urząd Komisji Nadzoru Finansowego	Art. 9 pkt 1	W ocenie UKNF osoby, o których mowa w zmienianym art. 9 pkt 1 UKSC powinny być odpowiedzialne za utrzymywanie kontaktów z innymi podmiotami krajowego systemu cyberbezpieczeństwa (np. organami właściwymi ds. cyberbezpieczeństwa), a nie wyłącznie z innymi podmiotami kluczowymi lub ważnymi. Wyznaczenie tego rodzaju osób kontaktowych w organizacji korzystnie wpłynie na sprawny kontakt podmiotów kluczowych lub ważnych w szczególności z organami właściwymi ds. cyberbezpieczeństwa, przede wszystkim w sytuacjach, gdy występuje potrzeba szybkiego, roboczego kontaktu z podmiotem. W ocenie UKNF za wnioskiem takim przemawiają doświadczenia stosowania dotychczasowego art. 9 ust. 1 pkt 1 UKSC zgodnie z którym operator usługi kluczowej wyznacza osobę odpowiedzialną za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa. Proponowana przez UKNF zmiana będzie także spójna z projektowanym art. 7 ust. 2 pkt 11 UKSC, w którym wskazano na dane co najmniej 2 osób do kontaktu z podmiotami krajowego systemu cyberbezpieczeństwa zawierające imię i nazwisko, numer telefonu oraz adres poczty elektronicznej.	Uwaga uwzględniona
61.	Prezes Urzędu Komunikacji Elektronicznej	Art. 9 pkt 3	Art. 1 pkt 14 w zakresie dotyczącym projektowanego art. 9 pkt 3 ustawy o ksc – z projektowanego art. 9 pkt 3 ustawy o ksc wynika, że podmiot kluczowy i podmiot ważny po uzyskaniu wpisu do wykazu podmiotów kluczowych i podmiotów ważnych	Uwaga wyjaśniona Podmiot kluczowy/podmiot ważny otrzyma dostęp do systemu w

Tabela uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

			uzyska dostęp do systemu teleinformatycznego, o którym mowa w art. 46 ust. 1 ustawy o ksc. Zatem każdy z tych podmiotów - bez względu na jego wielkość i państwo pochodzenia - niejako automatycznie uzyska pełny dostęp do informacji zawartych w tym systemie. Co więcej przepisy ustawy nakładają na ww. podmioty obowiązek korzystania z systemu w celu realizacji obowiązków z zakresu cyberbezpieczeństwa pod rygorem kary (por. np. projektowany art. 73 ust. 1 pkt 18 ustawy o ksc). Wydaje się, że takie ukształtowanie projektowanej regulacji może mieć negatywny wpływ nie tylko na bezpieczeństwo systemu, o którym mowa w art. 46 ust. 1 ustawy o ksc i innych systemów z nim współpracujących, ale także na obronność i bezpieczeństwo państwa. Wobec powyższego proponuje się ewentualne rozważenie wprowadzenia zmian mających na celu zróżnicowanie poziomu dostępu do funkcjonalności systemu, o którym mowa w art. 46 ust. 1 ustawy o ksc, dla poszczególnych jego użytkowników.	zakresie w jakim jest niezbędny do realizacji obowiązków. Nie oznacza to, że podmiot kluczowy/ważny otrzyma dostęp do wszystkich informacji zgromadzonych w systemie.
62.	Rzecznik Małych i Średnich Przedsiębiorców	Art. 9 i art. 10	Proponowana treść art. 1 pkt 14 Projektu (nadający nowe brzmienie art. 9 i 10 ustawy zmienianej), w odniesieniu do zmienianego art. 9 pkt 1 określającego wymóg podania danych co najmniej dwóch osób do kontaktu z podmiotami krajowego systemu cyberbezpieczeństwa - adekwatnie do postulatu zmiany wyrażonego wcześniej w pkt 1 lit d) - dla podmiotów będących mikroprzedsiębiorcami lub małymi przedsiębiorcami - wyznaczenie jednej takiej osoby.	Uwaga uwzględniona
63.	Prezes Urzędu Komunikacji Elektronicznej	Art. 11 ust. 1 pkt 4b	Art. 1 pkt 15 lit. a tiret czwarte w zakresie dotyczącym projektowanego art. 11 ust. 1 pkt 4b ustawy o ksc – niejasne jest jaki okres czasu ma obejmować „sprawozdanie okresowe”, o którym mowa w tym przepisie.	Uwaga nieuwzględniona Należy zauważyć, że „sprawozdanie okresowe” będzie przekazywane na wniosek CSiRT sektorowego, w którym zostaną określone szczegółowe informacje dotyczące obsługi incydentu. Ponadto część informacji dot. incydentu będzie wskazana w wstępnym ostrzeżeniu, więc można założyć, że sprawozdanie będzie zawierało uzupełnienie tych informacji, np. czas trwania incydentu.

Tabela uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

64.	Prezes Urzędu Komunikacji Elektronicznej	Art. 11 ust. 1 pkt 4b i 4c, art. 12b	Art. 1 pkt 15 lit. a tiret czwarte (w zakresie dotyczącym dodawanych w art. 11 ust. 1 ustawy o ksc pkt 4b i 4c), art. 1 pkt 15 lit. c oraz art. 1 pkt 17 (w zakresie dotyczącym dodawanego art. 12b) – należy zauważyć, że w ww. projektowanych przepisach jest mowa odpowiednio o: „sprawozdaniu okresowym z obsługi incydentu poważnego”, „sprawozdaniu końcowym z obsługi incydentu poważnego”, „sprawozdaniach okresowych”, „sprawozdaniach końcowych”, „sprawozdaniu z postępu obsługi incydentu poważnego” oraz o „sprawozdaniu okresowym z postępu obsługi incydentu poważnego”. W związku z tym proponuje się ujednolicić projektowaną terminologię w niniejszym zakresie.	Uwaga uwzględniona Zostanie doprecyzowany przepis art. 11 ust. 2 oraz art. 12b ust. 1.
65.	Prezes Urzędu Komunikacji Elektronicznej	Art. 11 ust. 2b	Art. 1 pkt 15 lit. d w zakresie dotyczącym dodawanego w art. 11 ustawy o ksc ust. 2b – w ramach projektowanego przepisu niejasne jest, o jakich usługach jest w nim mowa i przez kogo świadczonych. Jednocześnie z projektowanego przepisu nie wynika, czy zawarty w nim obowiązek informacyjny ma być realizowany przez podmiot kluczowy i podmiot ważny wobec wszystkich swoich użytkowników, czy może jedynie wobec tych spośród swoich użytkowników, którzy korzystają z usługi, na którą ma niekorzystny wpływ incydent poważny.	Uwaga uwzględniona Przepis został przeredagowany. Uzasadnienie zostanie uzupełnione w tym zakresie.
66.	Narodowy Bank Polski	Art. 11 ust. 1 pkt 4	Art. 1 pkt 15 projektu ustawy w zakresie zmiany brzmienia art. 11 pkt 4: 4) zgłasza wczesne ostrzeżenie o incydencie poważnym niezwłocznie, nie później niż w ciągu 24 godzin od momentu jego wykrycia, do właściwych CIRT i CIIR;”. Biorąc pod uwagę, że w dalszej części tego punktu uszczegóławia się treść przepisu o fragment „niezwłocznie, nie później niż w ciągu 24 godzin”, proponujemy wykreślenie z przedmiotowego punktu wyrazu „wczesne” albo doprecyzowanie, co rozumie się przez „wczesne ostrzeżenie o incydencie”.	Uwaga nieuwzględniona Pojęcie „wczesne ostrzeżenie” występuje w NIS2, co więcej dyrektywa ta określa co jest elementem „wczesnego ostrzeżenia”.
67.	Urząd Komisji Nadzoru Finansowego	Art. 11 ust. 4	W zmienianym art. 11 ust. 4 UKSC powinno nastąpić usunięcie słowa „kluczowej” w końcowej części tego przepisu (tj. we fragmencie „– kierując się potrzebą zapewnienia ochrony przed zagrożeniem życia lub zdrowia ludzi, znacznymi stratami majątkowymi oraz obniżeniem jakości świadczonej usługi kluczowej.”).	Uwaga uwzględniona Przepis został zmieniony.
68.	Naukowa i Akademicka Sieć Komputerowa – Państwowy	Art. 12 ust. 1 pkt 5	W nowelizowanym art. 12 ust. 1 pkt 5 warto doprecyzować, że wskazanie to powinno dotyczyć nie tego, czy incydent poważny wyczerpuje znamiona przestępstwa, gdyż podmiot zgłaszający może nie umieć tego ocenić, nawet posiadając pełną wiedzę w zakresie incydentu poważnego. Rekomendujemy rozważenie uzupełnienia tego	Uwaga uwzględniona Przepis został przeredagowany: „wskazanie czy incydent poważny został wywołany działaniem

Tabela uwag zgłoszonych w ramach opiniowania do *projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)*

	Instytut Badawczy		przepisu w następujący sposób: „wskazanie, czy incydent poważny może wyczerpywać znamiona przestępstwa”.	bezpawnym lub działaniem w złej wierze”. Takie brzmienie zapewnia spójność z dyrektywą NIS2.
69.	Narodowy Bank Polski	Art. 12 ust. 1	Ad art. 1 pkt 16 projektu ustawy w zakresie zmiany brzmienia art. 12 ust. 1: 1. Wczesne ostrzeżenie, o którym mowa w art. 11 ust. 1 pkt 4, zawiera: (...) wskazanie czy incydent poważny wyczerpuje znamiona przestępstwa. Zgłaszamy wątpliwość, czy na etapie przesyłania ostrzeżenia możliwe będzie jednoznaczne wskazanie, czy incydent poważny będzie wyczerpywał znamiona przestępstwa, oraz kto i na jakiej podstawie prawnej będzie decydował o klasyfikacji incydentu jako przestępstwo. Sugerujemy zweryfikować, czy instytucja wysyłająca wczesne ostrzeżenie będzie posiadała odpowiednie informacje i uprawnienia w przedmiotowym zakresie.	Uwaga uwzględniona Przepis został przeredagowany: „wskazanie czy incydent poważny został wywołany działaniem bezpawnym lub działaniem w złym zamiarze”. Takie brzmienie zapewnia spójność z dyrektywą NIS2.
70.	Prezes Urzędu Komunikacji Elektronicznej	Art. 12 ust. 2	Art. 1 pkt 16 w zakresie dotyczącym projektowanego art. 12 ust. 2 ustawy o ksc – zgodnie z niniejszym przepisem zgłaszane przez podmiot kluczowy i podmiot ważny wczesne ostrzeżenie o incydencie poważnym może zawierać skierowany do CSIRT sektorowego wniosek m. in. o wsparcie techniczne przy obsłudze incydentu. W związku z tym należy podkreślić, że zakres ww. „wsparcia technicznego” na gruncie projektowanego przepisu jest niejasny, a tym samym budzi on poważne wątpliwości interpretacyjne, tj. na czym owo wsparcie techniczne miałyby polegać? Jednocześnie nasuwa się wątpliwość – jeżeli wsparcie to miałyby być związane np. z zaangażowaniem środków rzeczowych lub osobowych po stronie CSIRT sektorowego (koszty), czy nie powinno to znaleźć odzwierciedlenia w OSR dla projektowanej ustawy?	Uwaga nieuwzględniona Udzielanie wsparcia jest jednym z zadań CSIRT wskazanych w dyrektywie NIS2 dlatego nie możemy wyłączyć tego obowiązku. Należy podkreślić, że już obecnie jednym z zadań sektorowych zespołów ds. cyberbezpieczeństwa jest wspieranie operatorów usług kluczowych w wykonywaniu ich obowiązków w tym w obsłudze incydentów. Proponuje się doprecyzowanie tego określenia przez dodanie wyrazu „dodatkowego”, w związku z tym we wczesnym ostrzeżeniu podmiot kluczowy i ważny będzie mógł wystąpić o „dodatkowe wsparcie techniczne” – to doprecyzowanie jest zgodne z art. 23 ust. 5 NIS2,

Tabela uwag zgłoszonych w ramach opiniowania do *projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)*

				który mówi właśnie o „dodatkowym wsparciu”.
71.	Prezes Urzędu Komunikacji Elektronicznej	Art. 12 ust. 3 pkt 1 lit. b art. 35 ust. 2 pkt 1 lit. a oraz art. 53 ust. 10 pkt 4	Art. 1 pkt 16 (w zakresie dotyczącym projektowanego art. 12 ust. 3 pkt 1 lit. b ustawy o ksc), art. 1 pkt 33 lit. b (dotyczący zmian wprowadzanych w art. 35 ust. 2 pkt 1 lit. a ustawy o ksc) oraz art. 1 pkt 56 (w zakresie projektowanego art. 53 ust. 10 pkt 4 ustawy o ksc) – w ww. przepisach jest odpowiednio mowa o: „liczbie użytkowników usługi, na których incydent poważny miał wpływ”, „liczbie użytkowników, których dotyczy incydent” oraz o „liczbie użytkowników, których dotyka incydent”. Należy zatem wskazać na brak jednolitości redakcyjnej w sposobie posługiwania się pojęciem „użytkownik” w kontekście zaistniałego incydentu, co w konsekwencji może powodować wątpliwości interpretacyjne, np. czy jest tu mowa o liczbie użytkowników, którzy podjęli faktyczną, nieudaną (z powodu incydentu) próbę skorzystania z usługi, czy może o liczbie użytkowników, którzy jedynie potencjalnie mogliby usiłować skorzystać z usługi w czasie wystąpienia incydentu. W związku z tym proponuje się ujednolicić terminologię w powyższym akresie w sposób, który pozwoli na jednoznaczne oszacowanie liczby użytkowników dotkniętych skutkami incydentu.	Uwaga uwzględniona Terminologia zostanie uspoźniona.
72.	Prezes Głównego Urzędu Statystycznego	Art. 15	Obecnie projektowane zapisy art. 15 ust. 1 przy uwzględnieniu projektowanego zapisu dot. pojęcia systemu informacyjnego oraz projektowanego art. 2a i art. 32 NIS 2 budzą wątpliwości interpretacyjne w jakim zakresie i w stosunku do jakich i ilu systemów informacyjnych podmiot publiczny zobowiązany będzie przeprowadzić audyt bezpieczeństwa raz na 2 lata. Przepis nie wskazuje, że dobór systemów do audytów ma być zrealizowany w oparciu o analizę ryzyka – co zdaje się wynikać z NIS 2. Podmioty publiczne realizują szereg zadań publicznych (usług) i wykorzystują wiele systemów informatycznych. W przypadku takiego podmiotu jak Prezes GUS i jednostki służb statystyki publicznej ilość systemów informacyjnych wykorzystywanych do realizacji wielu zadań publicznych jest bardzo duża i liczona jest w setkach, a nie dziesiątkach. Podobną sytuację będą miały również inne podmioty publiczne o podobnej strukturze centrali i jednostek podległych, np. Państwowa Inspekcja Pracy, Sanepid, ZUS. Nie jest możliwym, aby w perspektywie raz na dwa lata przeprowadzić audyt wszystkich systemów informacyjnych – a taki wniosek płynie z literalnej interpretacji projektowanego przepisu.	Uwaga częściowo uwzględniona i w pozostałym zakresie wyjaśniona Zmieniono brzmienie przepisu doprecyzowując, że organ właściwy do spraw cyberbezpieczeństwa zlecając przeprowadzenie audytu będzie mógł wskazać zakres tego audytu. Wskazanie zakresu wykluczy konieczność przeprowadzenia audytu bezpieczeństwa wszystkich systemów informacyjnych. Co do audytów wynikających z rozporządzenia w sprawie Krajowych Ram Interoperacyjności należy wskazać, że przepis ten zostanie uchylony.

Tabela uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

			Dodatkowo zgodnie z nadal jeszcze obowiązującym rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (które ma być zmienione do 23 maja 2024) Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań (...) zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok. Co prawda w art. 15 ust. 6 dotychczasowej ustawy o KSC wskazano, że 6. Operator usługi kluczowej, u którego w danym roku w stosunku do systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej został przeprowadzony przez osoby spełniające warunki określone w ust. 2 pkt 2 audyt wewnętrzny w zakresie bezpieczeństwa informacji, o którym mowa w przepisach wydanych na podstawie art. 18 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, nie ma obowiązku przeprowadzania audytu przez 2 lata – niemniej przepisy nowej ustawy o KSC powinny wskazać zależności między prowadzeniem obu rodzajów audytów oraz należy uspoźnić te zapisy, tak aby podmioty publiczne nie były podwójnie zobowiązane do prowadzenia różnego zakresu audytów bezpieczeństwa informacji dot. systemów informacyjnych, co do których to audytów są różne wymagania w zakresie podmiotów, które mogą je prowadzić lub zakresu i podstaw przeprowadzenia audytów.	
73.	Rzecznik Małych i Średnich Przedsiębiorców	Art. 15	Treść art. 1 pkt 20 Projektu (nadający nowe brzmienie art. 15 ustawy zmienianej), w odniesieniu do zmienianego art. 15 ust. 1 nakładającego na podmioty kluczowe oraz podmioty ważne obowiązek audytu systemu bezpieczeństwa, na własny koszt, co najmniej raz na 2 lata - mając na względzie obowiązki związane z wdrożeniem systemu zarządzania bezpieczeństwem informacji (art. 1 pkt 12 Projektu), obowiązek wymiany informacji, o którym mowa w dodawanym art. 8h - powinien w odniesieniu do podmiotów kluczowych oraz podmiotów ważnych będących mikroprzedsiębiorcami lub małymi przedsiębiorcami być wykonywany z częstotliwością raz na 3 lata. Uzasadnienie: Postulat niniejszy uzasadniają koszty przeprowadzenia audytu bezpieczeństwa, które dla mniejszych podmiotów mogą stanowić bardzo duże obciążenie. Wykonanie niniejszego wymogu w okresie 3 lat zapewni realizację celów Projektu a jednocześnie	Uwaga wyjaśniona Zostanie wprowadzona fakultatywna wymiana informacji.

Tabela uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

			nie będzie stanowił przeszkody w wykonywaniu działalności gospodarczej dla mniejszych i słabszych ekonomicznie podmiotów.	
74.	Polski Komitet Normalizacyjny	Art. 15 i art. 16	Artykuły 15, 16 projektu ustawy dotyczą zasad przeprowadzenia audytów bezpieczeństwa. W ocenie KT 182 ds. Ochrony Informacji w Systemach Teleinformatycznych w przepisach brakuje wskazania jakichkolwiek kryteriów, zgodnie z którymi powinien zostać przeprowadzony audyt bezpieczeństwa. Sugerujemy doprecyzowanie kryteriów przeprowadzania audytów.	Uwaga wyjaśniona Zakres audytu będzie mógł być wskazany przez organ właściwy do spraw cyberbezpieczeństwa w przypadku zlecenia audytu doraźnego. Jeśli natomiast chodzi o kryteria to zostanie to dookreślone w nowym szablonie audytu.
75.	Rzecznik Małych i Średnich Przedsiębiorców	Art. 15	Treść art. 1 pkt 20 Projektu (nadający nowe brzmienie art. 15 ustawy zmienianej), w odniesieniu do zmienianego art. 15 ust. 1 nakładającego na podmioty kluczowe oraz podmioty ważne obowiązek audytu systemu bezpieczeństwa, na własny koszt, co najmniej raz na 2 lata – mając na względzie obowiązki związane z wdrożeniem systemu zarządzania bezpieczeństwem informacji (art. 1 pkt 12 Projektu), obowiązek wymiany informacji, o którym mowa w dodawanym art. 8h – powinien w odniesieniu do podmiotów kluczowych oraz podmiotów ważnych będących mikroprzedsiębiorcami lub małymi przedsiębiorcami być wykonywany z częstotliwością raz na 3 lata. Uzasadnienie: Postulat niniejszy uzasadniają koszty przeprowadzenia audytu bezpieczeństwa, które dla mniejszych podmiotów mogą stanowić bardzo duże obciążenie. Wykonanie niniejszego wymogu w okresie 3 lat zapewni realizację celów projektu a jednocześnie nie będzie stanowił przeszkody w wykonywaniu działalności gospodarczej dla mniejszych i słabszych ekonomicznie podmiotów.	Uwaga uwzględniona Podmioty ważne zostały wyłączone z obowiązku dokonywania audytów regularnych, a podmioty kluczowe zobowiązane będą do audytów co 3 lata.
76.	Prezes Urzędu Ochrony Danych Osobowych	Art. 15	W proponowanym art. 15 KSC (wprowadzanym w art. 1 pkt 20 projektu) przewidziano obowiązek podmiotu kluczowego lub podmiotu ważnego co do zapewnienia przeprowadzenia audytu bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi. Pamiętać należy, iż realizacja tego obowiązku nie zwalnia administratora, wykonawcy norm ustawy o KRC, z obowiązków wynikających z rozporządzenia 2016/679 w zakresie realizacji zasady poufności i integralności (art. 5 ust. 1 lit f) i konieczności wdrożenia odpowiednich	Uwaga uwzględniona Kwestia ta zostanie omówiona w uzasadnieniu.

Tabela uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

			środków technicznych i organizacyjnych z uwzględnieniem analizy ryzyka (art. 25, art. 35 i in.).	
77.	Prezes Urzędu Ochrony Danych Osobowych	Art. 16a ust. 4	W art. 16a ust. 4 KSC (wprowadzanym w art. 1 pkt 22 projektu) wskazano na „bazy danych” dotyczące rejestracji nazw domen. Prawodawca zdaje się używać pojęcia „rejestru” oraz „bazy danych” jako synonimów. Rejestr publiczny został zdefiniowany w art. 3 pkt. 5 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2023 r. poz. 57).¹⁰⁾ Baza danych została natomiast zdefiniowana w art. 2 ust. 1 pkt 1 ustawy z dnia 27 lipca 2001 r. o ochronie baz danych (Dz. U. z 2021 r. poz. 386)¹¹⁾. Ze wskazanych definicji, w ocenie organu nadzorczego, wynika, że rozwiązanie proponowane przez prawodawcę odpowiada wymogom rejestru publicznego, przy czym to projektodawca powinien dokonać ostatecznej oceny powyższego. W przypadku przyjmowania rozwiązań dedykowanych budowie rejestru publicznego, prawodawca musi dokładnie określić zasady jego prowadzenia w związku z przetwarzaniem danych osobowych (zakres danych, okresy retencji, model udostępnienia danych, bezpieczeństwo danych itd.) oraz dokładnie zidentyfikować wszystkie cele, dla których realizacji przetwarzanie danych będzie konieczne i niezbędne, co pozwoli na ustalenie także zakresu tych danych. Prawodawca zobowiązany jest do tego na mocy art. 6 ust. 3 rozporządzenia 2016/679. Ponadto należy zauważyć, iż prawodawca skonstruował przepis w sposób wskazujący jakoby to rejestry nazw domen najwyższego poziomu wdrażały polityki i procedury weryfikacji. Rejestry nie stanowią podmiotu prawa i nie mogą wdrażać polityk ani procedur. Prawa i obowiązki w tym zakresie powinny być przypisane skonkretyzowanym podmiotom lub osobom.	Uwaga wyjaśniona Rejestr nazw domen nie jest rejestrem publicznym w rozumieniu ustawy o informatyzacji. Rejestr nazw domen jest podmiotem prawa - w Polsce jest nim NASK-PIB. Określenie „rejestr” jest powszechnie używane na całym świecie dla rejestrów domen najwyższego poziomu w systemie DNS (np. ang. „registry”, fr. „le registre”, niem. „registriert”) i zostało usankcjonowane w przepisach NIS 2. Dyrektywa wprowadza zarówno definicję tego podmiotu, jak i obowiązki dla rejestrów domen najwyższego poziomu. Zakres zbieranych danych i obowiązek ich przetwarzania został ustalony zgodnie z dyrektywą NIS2. Stosunek, jaki łączy abonenta domeny-rejestratora-rejestr nazw domen, ma charakter cywilnoprawny.

¹⁰⁾ Rejestr, ewidencję, wykaz, listę, spis albo inną formę ewidencji, służące do realizacji zadań publicznych, prowadzone przez podmiot publiczny na podstawie odrębnych przepisów ustawowych.

¹¹⁾ Baza danych oznacza zbiór danych lub jakichkolwiek innych materiałów i elementów zgromadzonych według określonej systematyki lub metody, indywidualnie dostępnych w jakikolwiek sposób, w tym środkami elektronicznymi, wymagający istotnego, co do jakości lub ilości, nakładu inwestycyjnego w celu sporządzenia, weryfikacji lub prezentacji jego zawartości.

Tabela uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

78.	Prezes Urzędu Ochrony Danych Osobowych	Art. 16a ust. 5 pkt 1 i 4	Procedury weryfikacji danych, o których mowa w art. 16a ust. 5 pkt 1 i 4 KSC powinny wskazywać obowiązki organów, a nie jedynie „możliwość” ich wykonywania. Z uwzględnieniem konstytucyjnej zasady legalizmu (art. 7 Konstytucji RP) oraz warunków określonych w art. 6 ust. 3 w zw. z art. 6 ust. 1 lit. c i lit. e rozporządzenia 2016/679 prawodawca powinien doprecyzować warunki podejmowania działań wskazanych w ust. 1 i 4, jakie mają być przestrzegane przez podmioty świadczące usługi rejestracji nazw domen. Wyjaśnienia wymaga czy w procesie weryfikacji dochodzi do zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach, o którym mowa w art. 22¹²⁾ rozporządzenia 2016/679 – tj. do takiego sposobu przetwarzania danych osobowych, który wywołuje wobec osoby fizycznej skutki prawne lub w podobny sposób istotnie na nią wpływa. Jeśli miałyby to mieć miejsce, to powinny być spełnione warunki wskazane w ww. przepisie. Jako przykład rozwiązań w tym zakresie można wskazać uregulowania zawarte w ustawie z dnia 29 sierpnia 1997 r.– Prawo bankowe (Dz. U. z 2023 r. poz.	Uwaga uwzględniona Usunięte zostanie wskazanie „możliwości”. W procesie rejestracji nie dochodzi do zautomatyzowanego podejmowania decyzji, w indywidualnych przypadkach, o którym mowa w art. 22¹³⁾ rozporządzenia 2016/679.

¹²⁾ Art. 22. 1. Osoba, której dane dotyczą, ma prawo do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa.

2. Ust. 1 nie ma zastosowania, jeżeli ta decyzja:

a) jest niezbędna do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a administratorem;

b) jest dozwolona prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator i które przewiduje właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą; lub

c) opiera się na wyraźnej zgodzie osoby, której dane dotyczą.

3. W przypadkach, o których mowa w ust. 2 lit. a) i c), administrator wdraża właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą, a co najmniej prawa do uzyskania interwencji ludzkiej ze strony administratora, do wyrażenia własnego stanowiska i do zakwestionowania tej decyzji.

4. Decyzje, o których mowa w ust. 2, nie mogą opierać się na szczególnych kategoriach danych osobowych, o których mowa w art. 9 ust. 1, chyba że zastosowanie ma art. 9 ust. 2 lit. a) lub g) i istnieją właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą.

¹³⁾ Art. 22. 1. Osoba, której dane dotyczą, ma prawo do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa.

2. Ust. 1 nie ma zastosowania, jeżeli ta decyzja:

a) jest niezbędna do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a administratorem;

b) jest dozwolona prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator i które przewiduje właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą; lub

c) opiera się na wyraźnej zgodzie osoby, której dane dotyczą.

3. W przypadkach, o których mowa w ust. 2 lit. a) i c), administrator wdraża właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą, a co najmniej prawa do uzyskania interwencji ludzkiej ze strony administratora, do wyrażenia własnego stanowiska i do zakwestionowania tej decyzji.

4. Decyzje, o których mowa w ust. 2, nie mogą opierać się na szczególnych kategoriach danych osobowych, o których mowa w art. 9 ust. 1, chyba że zastosowanie ma art. 9 ust. 2 lit. a) lub g) i istnieją właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą.

Tabela uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

			2488 ze zm.) oraz ustawie z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej (Dz. U. z 2023 r. poz. 656 ze zm.).	
79.	Prezes Urzędu Ochrony Danych Osobowych	Art. 16a ust. 9	W projektowanym art. 16a ust. 9 KSC wskazano na obowiązek uzyskania zgody w przypadku podawania danych. Konstrukcja przepisu jest nieprzejrzysta i nie wskazuje również celu, na jaki zgoda ma być wyrażona, jak i samego celu regulacji, który prawodawca chce osiągnąć, co sprzeczne jest z zasadą legalizmu, rzetelności i przejrzystości (art. 5 ust. 1 lit. a rozporządzenia 2016/679). Aby zgoda na przetwarzanie danych była skutecznie wyrażona musi spełniać warunki wyrażenia zgody z art. 7 rozporządzenia 2016/679 ¹⁴⁾ . Poza tym prawodawca rozstrzygając o przyjęciu takiego rozwiązania powinien wziąć pod uwagę, że zgoda może być w każdym czasie odwołana, zgodnie uprawnieniem osoby, której dane dotyczą wskazanym w art. 7 ust. 3 rozporządzenia 2016/679. Prawodawca powinien również określić jakie konsekwencje będzie nieść za sobą odwołanie zgody. Należy pamiętać, że o ile zgoda ma być jedyną podstawą przetwarzania danych to staje się ona przesłanką legalizującą, ale wyłącznie dla administratora, który dla realizacji swoich celów przetwarzania danych ją pozyskuje. Pozostaje zatem pytanie, przy tak skonstruowanym przepisie, o podstawy przetwarzania danych przez kolejnych administratorów.	Uwaga wyjaśniona Projektowany art. 16a ust. 9 dotyczy wyłącznie zgody osoby, której dane dotyczą, na publikowanie jej danych dotyczących rejestracji domeny. Obowiązek publikacji wynika z dyrektywy NIS 2 oraz projektowanego ust. 7. Publikacja musi następować zgodnie z przepisami RODO. Część abonentów, z różnych względów, oczekuje podawania ich danych do publicznej wiadomości. Taka możliwość wymaga podstawy prawnej w postaci zgody, co reguluje ust. 9.
80.	Rzecznik Praw Obywatelskich	Art. 16b ust. 1	W art. 16b ust. 1 przyznaje się sądom, prokuraturze, policji i innym służbom mundurowym praktycznie nieograniczony wgląd do rejestru nazw domen najwyższego poziomu, co stanowi ingerencję w prawo do prywatności i prawo do ochrony danych osobowych. Przesłanka uzyskania wglądu jest ogólnikowa (związek z toczącym się postępowaniem) i w praktyce ta kompetencja będzie mogła być łatwo nadużywana.	Uwaga wyjaśniona Kwestie te wynikają bezpośrednio z dyrektywy NIS2.

¹⁴⁾ Art. 7. 1. Jeżeli przetwarzanie odbywa się na podstawie zgody, administrator musi być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych. 2. Jeżeli osoba, której dane dotyczą, wyraża zgodę w pisemnym oświadczeniu, które dotyczy także innych kwestii, zapytanie o zgodę musi zostać przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem. Część takiego oświadczenia osoby, której dane dotyczą, stanowiąca naruszenie niniejszego rozporządzenia nie jest wiążąca. 3. Osoba, której dane dotyczą, ma prawo w dowolnym momencie wycofać zgodę. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem. Osoba, której dane dotyczą, jest o tym informowana, zanim wyrazi zgodę. Wycofanie zgody musi być równie łatwe jak jej wyrażenie. 4. Oceniając, czy zgodę wyrażono dobrowolnie, w jak największym stopniu uwzględnia się, czy między innymi od zgody na przetwarzanie danych nie jest uzależnione wykonanie umowy, w tym świadczenie usługi, jeśli przetwarzanie danych osobowych nie jest niezbędne do wykonania tej umowy.

Tabela uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

81.	Prezes Urzędu Ochrony Danych Osobowych	Art. 16b	W projektowanym art. 16b KSC (określonym w art. 1 pkt 22 projektu), dotyczącym udzielania dostępu do rejestru nazw domen najwyższego poziomu na żądanie sądu, prokuratora lub policji oraz innych upoważnionych organów w postępowaniu karnym, rozważenia przez prawodawcę wymaga czy takie sformułowanie przepisu nie jest nazbyt blankietowe, zwłaszcza, jeśli chodzi o kwestię „udzielenia dostępu”. Wyjaśnienia i doprecyzowanie wymaga na czym to „udzielenie dostępu miałyby polegać” oraz jak dokładnie ma ono wyglądać, tym bardziej, że jest to regulacja wiążąca podmioty publiczne, obowiązane do działania na podstawie i w granicach prawa (art. 7 Konstytucji RP ¹⁵⁾).	Uwaga uwzględniona Przepis zostanie doprecyzowany - podmiot żądający dostępu będzie zobowiązany wskazać jakie konkretne dane są potrzebne i w jaki celu.
82.	Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy	Art. 23	Art. 23 ust. 2 i 3 proponujemy nadać brzmienie: „2. CSIRT MON, CSIRT NASK lub CSIRT GOV może wystąpić do organu właściwego do spraw cyberbezpieczeństwa z wnioskiem o wezwanie podmiotu kluczowego lub podmiotu ważnego, aby w wyznaczonym terminie usunął podatności, które doprowadziły lub mogłyby doprowadzić do incydentu poważnego lub krytycznego. 3. CSIRT MON, CSIRT NASK lub CSIRT GOV może wystąpić bezpośrednio do podmiotu kluczowego lub podmiotu ważnego o udostępnienie informacji technicznych związanych z incydem, które będą niezbędne do przeprowadzenia analizy lub koordynacji obsługi takiego incydentu.”.	Uwaga uwzględniona Przepis zostanie zmieniony.
83.	Prezes Urzędu Ochrony Danych Osobowych	Art. 26 ust. 2b	Art. 26 ust. 2b KSC (wprowadzanym w art. 1 pkt 26 projektu) odnosi się do zgody na wsparcie w obsłudze incydentów. Wątpliwości organu nadzorczego budzą skutki takiego uregulowania dla ochrony danych. Niejasny jest bowiem status w rozumieniu rozporządzenia 2016/679 podmiotu wspierającego, który przejmowałby zadania do realizacji i tym samym przetwarzał dane osobowe. Taka regulacja nie sprzyja jednoznacznemu ustaleniu kto w takiej sytuacji będzie adresatem praw i obowiązków wynikających z rozporządzenia 2016/679. Jest to istotne, szczególnie z punktu widzenia wytycznych EROD dotyczących pojęć administratora i podmiotu przetwarzającego zawartych w rozporządzeniu 2016/679 ¹⁶ .	Uwaga wyjaśniona Administratorem danych pozostaje podmiot u którego wystąpił incydent. Otrzymanie wsparcie nie zmienia obowiązków podmiotu wynikających z przepisów prawa, w tym z rozporządzenia 2016/679. Podmiot wspierający nie przejmuje na siebie żadnych obowiązków podmiotu udzielającego wsparcie.
84.	Prezes Urzędu Komunikacji Elektronicznej	Art. 26 ust. 3 pkt 18	Art. 1 pkt 26 lit. c tiret piąte w zakresie dotyczącym projektowanego art. 26 ust. 3 pkt 18 ustawy o ksc – w ramach projektowanego przepisu niejasne jest co należy	Uwaga wyjaśniona Chodzi o stowarzyszenia, luźne grupy, ISAC itd.

¹⁵⁾ Organy władzy publicznej działają na podstawie i w granicach prawa.

¹⁶⁾ Wytyczne EROD dotyczące pojęć administratora i podmiotu przetwarzającego zawartych w RODO, wersja 2.0, przyjęta 7 lipca 2021 r. [źródło: https://www.edpb.europa.eu/system/files/2023-10/edpb_guidelines_202007_controllerprocessor_final_pl.pdf].

Tabela uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

			rozumieć przez „sektorowe i międzysektorowe społeczności” podmiotów kluczowych i podmiotów ważnych.	
85.	Prezes Urzędu Ochrony Danych Osobowych	Art. 26 ust. 3 pkt 19	W proponowanym art. 26 ust. 3 pkt. 19 KSC (wprowadzanym w art. 1 pkt 26 projektu) dotyczącym współpracy z krajowymi zespołami reagowania na incydenty bezpieczeństwa komputerowego państw trzecich, w ramach której mogą wymieniać informacje, wskazano również na możliwość wymiany danych osobowych „zgodnie z unijnymi przepisami o ochronie danych osobowych”. Tego rodzaju regulacja jest zbędna ze względu na jej zbytnią ogólność a tym samym blankietowość – przepis prawa krajowego powinien wskazywać w jakim trybie, celu i na jakiej podstawie prawnej wymiana danych ma być dokonywana, co jest istotne dla poszanowania konstytucyjnej zasady legalizmu oraz wynikającej z rozporządzenia 2016/679 zasady zgodności z prawem, rzetelności i przejrzystości (art. 5 ust. 1 lit. a rozporządzenia 2016/679). Pamiętać należy, iż unijne przepisy o ochronie danych osobowych nakazują spełnienie określonych warunków przy tworzeniu podstawy prawnej dla przetwarzania danych osobowych, w tym udostępniania danych osobowych pomiędzy administratorami, a ich uszczegółowienie powinno następować w ustawie (art. 6 ust. 3 rozporządzenia 2016/679).	Uwaga uwzględniona Przepis, w zakresie w jakim dotyczy wymiany informacji, zostanie usunięty.
86.	Urząd Komisji Nadzoru Finansowego	Art. 26	W art. 26 UKSC postuluje się dodanie nowego ust. 13-15 o następującym brzmieniu: „13. Przepisy ust. 2 i 3 stosuje się odpowiednio do zadań realizowanych przez CSIRT NASK lub CSIRT GOV w sektorze bankowym i infrastruktury rynków finansowych, w szczególności w zakresie poważnych incydentów związanych z ICT zgłaszanych przez podmioty kluczowe lub podmioty ważne z tego sektora. 14. CSIRT NASK lub CSIRT GOV może również realizować swoje zadania w odniesieniu do podmiotów finansowych niebędących podmiotami kluczowymi lub podmiotami ważnymi, gdy nie stanowi to dla tego zespołu nieproporcjonalnego czy nadmiernego obciążenia, z uwzględnieniem priorytetowego traktowania poważnych incydentów związanych z ICT zgłaszanych przez podmioty finansowe będące podmiotami kluczowymi lub podmiotami ważnymi, oraz z zastrzeżeniem odpowiedniego stosowania ust. 2 i 3 do realizacji zadań przez CSIRT NASK lub CSIRT GOV. 15. CSIRT NASK lub CSIRT GOV współpracują i wymieniają informacje z właściwym organem w rozumieniu rozporządzenia 2022/2554 gdy jest to niezbędne	Uwaga uwzględniona Przepis zostanie dodany.

			dla realizacji zadań CSIRT NASK lub CSIRT GOV bądź realizacji zadań tego właściwego organu.”. Podobnie jak w przypadku wpływu zasady z art. 4 dyrektywy 2022/2555 w kontekście środków zarządzania ryzykiem w cyberbezpieczeństwie na zadania organu właściwego do spraw cyberbezpieczeństwa dla sektora bankowego i infrastruktury rynków finansowych oraz CSIRT sektorowego dla tego sektora, tak i w przypadku CSIRT NASK i CSIRT GOV doprecyzowaniu powinien ulec zakres zadań tych zespołów w związku z zastosowaniem do podmiotów finansowych rozporządzenia 2022/2554 w odniesieniu do incydentów związanych z ICT. Różnice w podejściu do realizowania omawianych zadań mogą wynikać m.in. z faktu, że zgłoszenia poważnych incydentów związanych z ICT kierowane są przez podmioty finansowe (w tym będące podmiotami kluczowymi lub ważnymi) do właściwego organu z rozporządzenia 2022/2554, stosuje się do nich inne zasady klasyfikacji, mają one inną treść, stosuje się do nich odrębne formularze ustalone w przepisach wykonawczych do rozporządzenia 2022/2554, itd. Dodawany ust. 14 ma zaś na celu skorelowanie zakresu zadań CSIRT NASK lub CSIRT GOV z postulowanym rozwiązaniem obejmującym m.in. możliwość przekazania do CSIRT poziomu krajowego, przez CSIRT sektorowy ustanowiony w sektorze bankowym i infrastruktury rynków finansowych, zgłoszenia poważnego incydentu związanego z ICT pochodzącego od podmiotu finansowego niebędącego podmiotem kluczowym lub ważnym (rozwiązanie takie zostało zaproponowane w projekcie ustawy o zmianie niektórych ustaw w związku z zapewnieniem peracyjnej odporności cyfrowej sektora finansowego – UC11, co dodatkowo uzasadnia skorelowanie prac legislacyjnych nad oboma projektami). Jednocześnie w w/w przepisie przewidziano przesłanki, które mają zapewnić priorytetowe traktowanie podmiotów objętych zakresem dyrektywy 2022/2555, które wzorowane są na art. 30 ust. 3 UKSC. Zaproponowane podejście koresponduje z art. 22 ust. 1 rozporządzenia 2022/2554. Dodawany ust. 15 stanowi zaś odzwierciedlanie art. 47 ust. 2 rozporządzenia 2022/2554, zgodnie z którym „W stosownych przypadkach właściwe organy mogą konsultować się i wymieniać informacje z pojedynczymi punktami kontaktowymi i CSIRT wyznaczonymi lub ustanowionymi zgodnie z dyrektywą (UE) 2022/2555.”. Jednocześnie, dla uniknięcia wątpliwości w kontekście zakresu pojęcia „poważny incydent”, a tym samym np. zakresu zadań CSIRT poziomu krajowego w odniesieniu do poważnych incydentów związanych z ICT, postulowane są także zmiany w definicjach, które omówione zostały w ramach uwagi nr 1 powyżej.	

Tabela uwag zgłoszonych w ramach opiniowania do *projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)*

87.	Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy	Art. 26 ust. 2a	W projektowanym art. 26 ust. 2a zaproponowano przepisy, zgodnie z którymi Pełnomocnik może zlecić zapewnienie wsparcia w obsłudze incydentów wymienionym podmiotom – CSIRT MON, CSIRT NASK, CSIRT GOV. W przypadku CSIRT MON oraz CSIRT GOV, projektodawca przewidział konieczność udzielenia zgody przez Ministra Obrony Narodowej (w przypadku CSIRT MON) oraz Szefa Agencji Bezpieczeństwa Wewnętrznego (w przypadku CSIRT GOV). Analogicznie, taki sam sposób postępowania powinien dotyczyć CSIRT NASK. Biorąc to pod uwagę zwracamy się z prośbą o dodanie w art. 26 ust. 2a pkt 2 obowiązku wyrażenia zgody przez dyrektora NASK-PIB, czyli jednostki, w której prowadzony jest CSIRT NASK. Pozwoli to uspołnić rozwiązanie z pkt 1 i 3 z pkt 2.	Uwaga nieuwzględniona Zasadą wynikającą z ustawy o Radzie Ministrów czy ustawy o działach administracji rządowej jest to, że minister nadzorujący może kierować do jednostek podległych i nadzorowanych wiążące wytyczne i polecenia. Pełnomocnik Rządu do spraw cyberbezpieczeństwa będzie ministrem lub wiceministrem cyfryzacji a minister cyfryzacji nadzoruje NASK-PIB.
88.	Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy	Art. 26 ust. 3 pkt 2	W art. 26 ust. 3 pkt 2 rekomendujemy powrót do poprzedniego brzmienia tego przepisu lub takie jego sformułowanie, aby jego treść była bliższa art. 11 ust. 3 lit d dyrektywy 2022/2555. Aktualna propozycja brzmienia tego przepisu sugeruje zapewnienie <u>każdemu konkretnemu podmiotowi krajowego systemu cyberbezpieczeństwa</u> dynamicznej analizy ryzyka, co w rzeczywistości może być niewykonalne. Dodatkowo, proponujemy odpowiednie doprecyzowanie zaproponowanego brzmienia art. 53b ust. 1 ustawy o KSC.	Uwaga uwzględniona Zmieniono brzmienie przedmiotowego przepisu.
89.	Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy	Art. 26 ust. 3 pkt 16	Należy pamiętać, że Komisja Europejska pełni w sieci CSIRT rolę obserwatora, a nie pełnoprawnego członka, zaś ENISA zapewnia w tym zakresie wyłącznie sekretariat (por. art. 15 ust. 2 dyrektywy 2022/2555). Tym samym wnosimy o wykreślenie tych organów z art. 26 ust. 3 pkt 16.	Uwaga częściowo uwzględniona Usunięto odwołanie do ENISY. Komisja uczestniczy w sieci w roli obserwatora, a więc nie ma potrzeby wykreślenia jej z przedmiotowego przepisu.
90.	Prezes Urzędu Ochrony Danych Osobowych	Art. 26 ust. 3 pkt 17	Podobne zastrzeżenia budzi rozwiązanie proponowane w art. 26 ust. 3 pkt 17 KSC (wprowadzanym art. 1 ust. 26 projektu), dotyczącym gromadzenia i analizowania danych na potrzeby postępowań karnych. Wyjaśnienia wymaga na czym polegać ma wskazana w przepisie „analiza”, w jaki sposób ma być ona dokonywana (w tym czy nie będzie dochodziło do zautomatyzowanego podejmowania decyzji, a jeśli tak to czy zostaną spełnione warunki z art. 22 rozporządzenia 2016/679) ¹²⁾ . Ponadto należy zwrócić uwagę, że do zadań CSIRT MON, CSIRT NASK i CSIRT GOV nie należy prowadzenie postępowań karnych, a taki wniosek wynika z literalnej interpretacji przepisu zawartego w proponowanym art. 26 ust. 3 pkt. 17 KSC. Wskazane podmioty mogą ewentualnie udostępniać dane organom prowadzącym takie postępowania, co również powinno być szczegółowo uregulowane w przepisach prawa.	Uwaga wyjaśniona Przepis ten precyzuje już dotychczasową działalność zespołów CSIRT związaną z analizą powłamaniami i udzielaniem wsparcia podmiotom dotkniętym incydentami. Te dane są następnie przekazywane do organów ścigania, które prowadzą postępowanie karne.

Tabela uwag zgłoszonych w ramach opiniowania do *projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)*

				W ramach tej analizy nie będzie dochodziło do zautomatyzowanego podejmowania decyzji.
91.	Prezes Urzędu Ochrony Danych Osobowych	Art. 26a ust. 4	Podobnie względ na ww. zasady wymaga przyjęcia stosownego brzmienia dodawanego art. 26a ust. 4 KSC, o którym mowa w art. 1 pkt 27 projektu, dotyczącego działań CSIRT NASK zapewniającego formularz do dokonywania zgłoszeń podatności. W ust. 5 pkt. 2 tego artykułu CSIRT NASK koordynuje komunikację między osobową fizyczną lub prawną zgłaszającą podatność a producentem lub dostawcą potencjalnie podatnych produktów ICT lub usług ICT. Wyjaśnienia i doprecyzowania wymaga jakim przepisom powszechnie obowiązującym będzie podlegać obsługa wnoszonych zgłoszeń oraz komunikacja między podmiotami, a także jakie dane osobowe będą przetwarzane, w jaki sposób oraz przez jaki okres czasu.	Uwaga wyjaśniona Przetwarzanie danych w tym zakresie podlega ogólnym zasadom. CSIRT NASK będzie przetwarzał dane osób, które dobrowolnie je przekazały w związku ze zgłoszeniem podatności. Dane osobowe tych osób nie będą bez ich zgody przekazywane dalej, a ich przetwarzanie będzie odbywać się tylko w związku z realizacją ustawowego obowiązku obsługi zgłoszenia. W zakresie zasad przetwarzania danych osobowych zastosowanie będą miały przepisy rozdziału 7 ustawy o krajowym systemie cyberbezpieczeństwa.
92.	Prezes Urzędu Ochrony Danych Osobowych	Art. 31 ust. 2	W zmienianym art. 31 ust. 2 KSC (wskazanym w art. 1 pkt 30 projektu) wskazano, że CSIRT NASK określi sposób dokonywania zgłoszeń, o których mowa w art. 30 ust. 1 KSC. Wśród danych, które należy podać przy zgłaszaniu incydentu do CSIRT NASK, zgodnie z art. 30 KSC, mogą znajdować się dane osobowe. W takim przypadku sposób dokonywania zgłoszeń powinien być precyzyjnie określony w przepisach ustawy, która wskazywać powinna również na sposób przetwarzania danych, podmioty uprawnione do ich przetwarzania oraz okres ich przechowywania.	Uwaga wyjaśniona Zakres przetwarzanych danych oraz inne kwestie związane z nimi zostały określone w obecnie obowiązujących przepisach ustawy w związku z czym nie jest konieczne uzupełnienie projektu w tym zakresie. Podstawowy sposób przekazywania zgłoszeń został określony w przepisach będzie on odbywał się za pomocą systemu, o którym mowa w art. 46 ustawy o krajowym systemie cyberbezpieczeństwa. Art. 31 reguluje jedynie sytuacje gdy z jakiegoś powodu nie będzie możliwy dostęp do tego systemu, a

Tabela uwag zgłoszonych w ramach opiniowania do *projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)*

				więc sytuacje nadzwyczajną i tymczasową. Dlatego, nie jest możliwe określenie na etapie projektowania przepisów w jaki sposób to przekazywanie będzie się odbywać. Każdorazowo będą to określać zainteresowane podmioty biorąc pod uwagę zapewnienie efektywności wykonywanych zadań. W zakresie zasad przetwarzania danych osobowych zastosowanie będą miały przepisy rozdziału 7 ustawy o krajowym systemie cyberbezpieczeństwa.
93.	Prezes Urzędu Ochrony Danych Osobowych	Art. 33 ust. 1b	Proponowany art. 33 ust. 1b KSC (wskazany w art. 1 pkt 31 projektu) stanowi o uprawnieniu CSIRT MON, CSIRT NASK i CSIRT GOV do m.in. dostępu do przetwarzanych danych oraz do odtworzenia algorytmu przetwarzania danych w celu przeprowadzenia badań urządzenia informatycznego lub oprogramowania. Przepisy powinny określać na czym dokładnie polega przetwarzanie danych osobowych związanych z tak ogólnie określonym działaniem opisanym jako „dostęp do danych osobowych”. Nie jest także jasne czy w przypadku odtwarzania algorytmu przetwarzania danych, wśród których mogą znajdować się dane osobowe, dochodzi do zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach mających wpływ na jednostkę. Kwestia ta wymaga zatem wyjaśnienia, ewentualnie projektodawca powinien w przepisach prawa uczynić zadość wymogom stawianym zautomatyzowanemu przetwarzaniu wyrażonym w art. 22 rozporządzenia 2016/679.	Uwaga wyjaśniona W ramach opisywanego obowiązku nie dojdzie do zautomatyzowanego podejmowania decyzji. Ponadto czynności badania mają zapewnić bezpieczeństwo narodowe i w związku z tym nie stosuje się tutaj przepisów RODO.
94.	Prezes Urzędu Komunikacji Elektronicznej	Art. 34	Art. 1 pkt 32 dotyczący zmian wprowadzanych w art. 34 ustawy o ksc – proponuje się rozszerzyć zakres projektowanych zmian wprowadzanych w art. 34 ustawy o ksc o zmiany w ustępie 2 tego przepisu polegające na uzupełnieniu zawartego w nim katalogu CSIRT, tj.: CSIRT MON, CSIRT NASK, CSIRT GOV, także o CSIRT sektorowe. Projektowany przepis art. 44 ust. 1b pkt 2 ustawy o ksc stanowi bowiem, iż CSIRT sektorowy może koordynować, w ramach sektora lub podsektora, obsługę incydentów w uzgodnieniu z podmiotami kluczowymi lub podmiotami ważnymi. Zasadnym jest zatem, aby także CSIRT sektorowy, w ramach koordynowania obsługi	Uwaga uwzględniona

Tabela uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

			incydentu, który doprowadził do naruszenia ochrony danych osobowych, współpracował z organem właściwym do spraw ochrony danych osobowych.	
95.	Prezes Urzędu Ochrony Danych Osobowych	Art. 35 ust. 1	Proponowany art. 35 ust. 1 KSC (wprowadzany w art. 1 pkt 33 projektu) dotyczy przekazywania przez CSIRT MON, CSIRT NASK i CSIRT GOV między sobą informacji o incydencie krytycznym lub incydencie w cyberbezpieczeństwie na dużą skalę oraz informowania o nim Rządowego Centrum Bezpieczeństwa oraz właściwego CSIRT sektorowego. O ile wśród wymienianych informacji znajdować się będą dane osobowe, tryb wymiany informacji powinien być precyzyjnie określony oraz zgodny z zasadami wynikającymi z art. 5 rozporządzenia 2016/679, w szczególności w świetle zgodności z zasadą legalizmu, przejrzystości i rzetelności oraz zasadą rozliczalności (art. 5 ust. 2 rozporządzenia 2016/679).	Uwaga uwzględniona Doprecyzowano kwestię przekazywania danych osobowych. W zakresie zasad przetwarzania danych osobowych zastosowanie będą miały przepisy rozdziału 7 ustawy o krajowym systemie cyberbezpieczeństwa.
96.	Krajowa Rada Radiofonii i Telewizji	Art. 36a ust. 3 pkt 2	Projektowany przepis art. 36a ust. 3 pkt 2) ustawy powinien otrzymać następującą treść: „akredytowanych na podstawie art. 48 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2024 r. poz. 632).”.	Uwaga uwzględniona
97.	Prezes Urzędu Komunikacji Elektronicznej	Art. 36a ust. 6 ustawy o ksc	Art. 1 pkt 35 w zakresie dotyczącym projektowanego art. 36a ust. 6 ustawy o ksc – w odniesieniu do zdania pierwszego niniejszego przepisu przewidującego możliwość przeprowadzenia oceny bezpieczeństwa systemu informacyjnego podmiotu kluczowego lub podmiotu ważnego może pojawić się wątpliwość, czy chodzi w nim o zgodę CSIRT MON, CSIRT NASK lub CSIRT GOV właściwego dla danego podmiotu kluczowego lub podmiotu ważnego. Proponuje się zatem rozważenie doprecyzowania projektowanego przepisu w niniejszym zakresie.	Uwaga uwzględniona Chodzi o zgodę CSIRT – przepis zostanie przeredagowany, aby było to jasne.
98.	Najwyższa Izba Kontroli	Art. 36b	Stosownie do art. 36b ust. 1 ocena bezpieczeństwa systemu informacyjnego może być przeprowadzona również bez zgody podmiotu ksc na zlecenie organu właściwego ds. cyberbezpieczeństwa. Może to kolidować z autonomią NIK w szczególności poprzez narażenie na nieuprawnione udostępnienie informacji objętych tajemnicą kontrolerską. Izba zgłasza wprowadzenie do przepisu odpowiedniego zastrzeżenia, podobnie jak w pkt. 4.	Uwaga uwzględniona Wprowadzony zostanie wymóg zgody NIK na przeprowadzenie oceny bezpieczeństwa.
99.	Najwyższa Izba Kontroli	Art. 36b	Stosownie do art. 36b ust. 7 komisja powołana do zniszczenia informacji uzyskanych podczas przeprowadzania oceny bezpieczeństwa systemu informacyjnego składa się z trzech osób powołanych przez osobę kierującą zespołem CSIRT spośród pracowników, funkcjonariuszy lub żołnierzy realizujących zadania odpowiednio w	Uwaga nieuwzględniona Ze względu na konieczność zapewnienia ochrony działania zespołów CSIRT nie przewiduje się

Tabela uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

			CSIRT MON, CSIRT NASK, CSIRT GOV albo CSIRT sektorowym. W przypadku badania bezpieczeństwa systemu informacyjnego NIK, Izba zgłasza rozszerzenie składu komisji o swojego przedstawiciela.	możliwości rozszerzania komisji o przedstawiciela podmiotu, którego system podlegał badaniu.
100.	Prezes Urzędu Komunikacji Elektronicznej	Art. 37 ust. 2	Art. 1 pkt 36 lit. b dotyczący zmian wprowadzanych w art. 37 ust. 2 ustawy o ksc – zawarte w tym przepisie uprawnienie do publikowania informacji o incydentach poważnych, w sytuacji gdy jest to niezbędne, aby zapobiec wystąpieniu incydentu albo zapewnić obsługę incydentu proponuje się rozszerzyć na CSIRT sektorowe, które - stosownie do projektowanego brzmienia art. 44 ust. 1b pkt 2 ustawy o ksc - mogą koordynować obsługę incydentów w ramach sektora lub podsektora. Informacje te CSIRT sektorowe mogłyby publikować np. na stronie podmiotowej Biuletynu Informacji Publicznej organu właściwego do spraw cyberbezpieczeństwa zapewniającego funkcjonowanie danego CSIRT.	Uwaga uwzględniona
101.	Najwyższa Izba Kontroli	Art. 39	Stosownie do art. 39 ust. 10 nowelizowanej ustawy dane, o których mowa w ust. 4, są usuwane lub anonimizowane przez ministra właściwego do spraw informatyzacji, dyrektora Rządowego Centrum Bezpieczeństwa, Pełnomocnika oraz organy właściwe do spraw cyberbezpieczeństwa niezwłocznie po stwierdzeniu, że nie są niezbędne do realizacji zadań wynikających z niniejszej ustawy. Termin usunięcia lub anonimizacji jest zatem niedookreślony i uznaniowy, Izba zgłasza wprowadzenie maksymalnego czasu na usunięcie lub anonimizację tych danych.	Uwaga uwzględniona Będzie wskazany termin 5 lat.
102.	Prezes Urzędu Komunikacji Elektronicznej	Art. 39 ust. 10	Art. 1 pkt 37 lit. h dotyczący projektowanego art. 39 ust. 10 ustawy o ksc – proponuje się rozważyć dodanie przepisu zawierającego upoważnienie ustawowe do wydania rozporządzenia określającego sposób usuwania i anonimizowania danych, o których mowa w art. 39 ust. 4 ustawy o ksc.	Uwaga nieuwzględniona Zrezygnowano z narzucania grupie różnorodnych podmiotów sposobu, w jaki mają usuwać i anonimizować przetwarzane dane. W ocenie projektodawcy są to czynności techniczne, które powinny być rozstrzygnięte na poziomie danej jednostki.
103.	Krajowa Rada Radiofonii i Telewizji	Art. 39 ust. 6a	W związku z projektowanym przepisem art. 39 ust. 6a ustawy zasadne wydaje się uregulowanie sposobu realizacji obowiązku określonego w art. 13 ust. 1 i 2 oraz art. 14 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).	Uwaga uwzględniona Przepis zostanie doprecyzowany, wskazane zostaną kategorie danych osobowych, które będą przetwarzane przy uwierzytelnianiu do systemu S46.

Tabela uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

104.	Prezes Urzędu Ochrony Danych Osobowych	Art. 39 ust. 6a	W projekcie proponuje się dodanie w KSC art. 39 ust. 6a (w art. 1 pkt 37 projektu), zgodnie z którym minister właściwy do spraw informatyzacji przetwarza dane osobowe w celu uwierzytelnienia osób fizycznych korzystających z systemu teleinformatycznego. Sformułowanie przepisu w taki sposób jest zbyt ogólne i blankietowe – brakuje bowiem określenia zakresu weryfikowanych danych oraz źródła ich pochodzenia, jak również sposobu weryfikacji. Ponadto minister właściwy do spraw informatyzacji jest administratorem systemu, o którym mowa w art. 46 ust. 1 KSC. Przepisy powinny więc określać w jakim zakresie odpowiada on za przetwarzanie danych zawartych w tym systemie. Regulacji prawnej powinno także podlegać przetwarzanie danych osobowych, o ile przy prowadzeniu systemu w celach innych niż uwierzytelnienie osób korzystających z systemu ono następuje.	Uwaga uwzględniona Przepis zostanie doprecyzowany, wskazane zostaną kategorie danych osobowych, które będą przetwarzane przy uwierzytelnianiu do systemu S46.
105.	Urząd Komisji Nadzoru Finansowego	Art. 39 ust. 7	W związku ze zmianą terminologii w projekcie ustawy w zakresie nazewnictwa sektorowych zespołów cyberbezpieczeństwa, również w art. 39 ust. 7 UKSC termin „sektorowe zespoły cyberbezpieczeństwa” powinien zostać zastąpiony przez termin „CSIRT sektorowe”.	Uwaga uwzględniona
106.	Prezes Urzędu Ochrony Danych Osobowych	Art. 39 ust. 8	Projektowany art. 39 ust. 8 KSC przewiduje wyłączenia realizacji wskazanych obowiązków wynikających z rozporządzenia 2016/679. Przepisów tego aktu nie można całkowicie wyłączyć, ale można je ograniczyć, na co wskazuje art. 23 rozporządzenia 2016/679. Tylko zatem po spełnieniu warunków wynikających z tego przepisu można ograniczyć określone prawa i obowiązki w celach wskazanych w art. 23 ust. 1 ¹⁷⁾ i z uwzględnieniem wytycznych Europejskiej Rady Ochrony Danych w sprawie ograniczeń na podstawie art. 23 rozporządzenia 2016/679 ¹⁸⁾ . Kwestia wyłączenia praw i obowiązków wynikających z rozporządzenia 2016/679 jest	Uwaga wyjaśniona Wskazać należy, że należy tutaj ostrożnie realizować obowiązki z RODO – udostępnianie informacji hakerom o ich danych osobowych czy uwzględnianie prawa do zapomnienia w tym przypadku

¹⁷⁾ Prawo Unii lub prawo państwa członkowskiego, któremu podlegają administrator danych lub podmiot przetwarzający, może aktem prawnym ograniczyć zakres obowiązków i praw przewidzianych w art. 12-22 i w art. 34, a także w art. 5 - o ile jego przepisy odpowiadają prawom i obowiązkom przewidzianym w art. 12-22 - jeżeli ograniczenie takie nie narusza istoty podstawowych praw i wolności oraz jest w demokratycznym społeczeństwie środkiem niezbędnym i proporcjonalnym, służącym: a) bezpieczeństwu narodowemu; b) obronie; c) bezpieczeństwu publicznemu; d) zapobieganiu przestępczości, prowadzeniu postępowań przygotowawczych, wykrywaniu lub ściganiu czynów zabronionych lub wykonywaniu kar, w tym ochronie przed zagrożeniami dla bezpieczeństwa publicznego i zapobieganiu takim zagrożeniom; e) innym ważnym celom leżącym w ogólnym interesie publicznym Unii lub państwa członkowskiego, w szczególności ważnemu interesowi gospodarczemu lub finansowemu Unii lub państwa członkowskiego, w tym kwestiom pieniężnym, budżetowym i podatkowym, zdrowiu publicznemu i zabezpieczeniu społecznemu; f) ochronie niezależności sądów i postępowania sądowego; g) zapobieganiu naruszeniom zasad etyki w zawodach regulowanych, prowadzeniu postępowań w takich sprawach, ich wykrywaniu oraz ściganiu; h) funkcjom kontrolnym, inspekcyjnym lub regulacyjnym związanym, nawet sporadycznie, ze sprawowaniem władzy publicznej w przypadkach, o których mowa w lit. a) - e) oraz g); i) ochronie osoby, której dane dotyczą, lub praw i wolności innych osób; j) egzekucji roszczeń cywilnoprawnych.

¹⁸⁾ Wytyczne EROD 10/2020 w sprawie ograniczeń na podstawie art. 23 RODO, wersja 2.1, przyjęte 13 października 2021 r. [źródło: https://www.edpb.europa.eu/system/files/2023-07/edpb_guidelines_202010_art23_adopted_afterpublicconsultation_pl.pdf]

Tabela uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

			przedmiotem licznych rozstrzygnięć TSUE, które należy także wziąć pod uwagę celem zachowania balansu pomiędzy prawem do prywatności a potrzebą zapewnienia bezpieczeństwa ¹⁹⁾ . Prawodawca powinien również wskazać co oznacza niemożliwość realizacji zadań przez CSIRT NASK, CSIRT MON i CSIRT sektorowych, w wyniku której zastosowania nie znajdowałyby niektóre przepisy rozporządzenia 2016/679.	może negować cel w postaci skutecznej reakcji na incydent. Przepis zostanie zmieniony, aby uczynić zadość wymaganiom z art. 23 RODO.
107.	Prezes Urzędu Ochrony Danych Osobowych	Art. 39 ust. 10	W proponowanym art. 39 ust. 10 KSC (wprowadzanym w art. 1 pkt 37 lit. h projektu) dotyczącym anonimizowania lub usuwania danych wątpliwości organu nadzorczego budzi zastosowane rozróżnienie. W rozumieniu przepisów rozporządzenia 2016/679 anonimizacja danych oraz ich usunięcie stanowią pojęcia tożsame. Nie jest jasnym dlaczego projektodawca różnicuje te pojęcia.	Uwaga uwzględniona Pojęcia zostaną ujednolicone.
108.	Prezes Urzędu Ochrony Danych Osobowych	Art. 39a ust. 1	Poważne wątpliwości organu nadzorczego budzi proponowany art. 39a ust. 1 KSC (wskazany w art. 1 pkt 38 projektu), zgodnie z którym ministrowi właściwemu do spraw informatyzacji zezwala się na wykorzystywanie danych uzyskanych na podstawie art. 26 ust. 1 ustawy o krajowym systemie cyberbezpieczeństwa, w tym danych wrażliwych, na tworzenie i udostępnianie usługi online polegającej na możliwości sprawdzenia przez użytkownika czy jego dane zostały upublicznione w sieci internet w sposób nieuprawniony. Ustawa określać powinna sposób działania usługi, jeżeli w jej ramach przetwarzane mają być dane osobowe oraz jakie dane mają być przetwarzane. Należy podkreślić, że dane osobowe uzyskiwane są w konkretnym celu i dla wykonania tego celu powinny być przetwarzane. Dalsze przetwarzanie tych danych w celu innym niż pierwotny jest możliwe, ale jedynie po spełnieniu warunków określonych w art. 13 ust. 3 rozporządzenia 2016/679 ²⁰⁾ . Dodatkowo, w przypadku danych szczególnych kategorii, wskazanych w art. 9 ust. 1 ²¹⁾ i 10 rozporządzenia 2016/679, ich przetwarzanie jest co do zasady zabronione. Przetwarzanie takich danych jest możliwe tylko przy spełnieniu jednego z warunków wskazanych w art. 9	Uwaga uwzględniona Przepis został zmieniony w ten sposób, że stanowić będzie art. 26c jako zadanie CSIRT NASK, a uzupełniać go będzie art. 39 w zmienionym brzmieniu. Doprecyzowano również uzasadnienie w tym zakresie.

¹⁹⁾ Np. wyrok TSUE z dnia 10 grudnia 2022 r. w sprawie C-620/19, wyrok TSUE z dnia 22 lutego 2022 r. w sprawie C-175/20.

²⁰⁾ Jeżeli administrator planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym dane osobowe zostały zebrane, przed takim dalszym przetwarzaniem informuje on osobę, której dane dotyczą, o tym innym celu oraz udziela jej wszelkich innych stosownych informacji, o których mowa w ust. 2.

²¹⁾ Zabrania się przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby.

Tabela uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

			ust. 2 ²²⁾ (w odniesieniu do danych, o których mowa w art. 9 ust. 1) lub gdy dokonywane jest pod nadzorem władz publicznych lub jeżeli dozwolone jest prawem Unii lub prawem państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw i wolności osób, których dane dotyczą (w odniesieniu do danych, o których mowa w art. 10 rozporządzenia 2016/679). Przetwarzanie danych szczególnych kategorii może więc odbywać się wyłącznie w przypadku ścisłego określenia zasad takiego przetwarzania w przepisach prawa, z uwzględnieniem retencji danych. We wskazanym przepisie mowa jest natomiast o „możliwości” wykorzystania danych. Organy publiczne działają wyłącznie na podstawie i w granicach prawa (art. 7 Konstytucji RP), przepis powinien więc określać „obowiązki” organu, a nie jego działania fakultatywne („możliwe”). Ponadto brak jest dookreślenia w przepisach sposobów przetwarzania danych osobowych dla realizacji „tworzenia i udostępniania usługi online”. Jeżeli celem prawodawcy jest wprowadzenie systemu teleinformatycznego i wprowadzenie przy jego pomocy realizacji nowego zadania to takie działanie, z uwagi na kształtowanie nowych procesów przetwarzania danych, poprzedzone musi być wykonaniem testu prywatności przeprowadzonym w związku z projektowaniem przedmiotowych regulacji i ustaleniem sposobów przetwarzania danych. Prawodawca powinien zadbać także o to, aby realizacja usługi odbywała się	

²²⁾ Ust. 1 nie ma zastosowania, jeżeli spełniony jest jeden z poniższych warunków: a) osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach, chyba że prawo Unii lub prawo państwa członkowskiego przewidują, iż osoba, której dane dotyczą, nie może uchylić zakazu, o którym mowa w ust. 1; b) przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii lub prawem państwa członkowskiego, lub porozumieniem zbiorowym na mocy prawa państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą; c) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody; d) przetwarzanie dokonuje się w ramach uprawnionej działalności prowadzonej z zachowaniem odpowiednich zabezpieczeń przez fundację, stowarzyszenie lub inny niezarobkowy podmiot o celach politycznych, światopoglądowych, religijnych lub związkowych, pod warunkiem że przetwarzanie dotyczy wyłącznie członków lub byłych członków tego podmiotu lub osób utrzymujących z nim stałe kontakty w związku z jego celami oraz że dane osobowe nie są ujawniane poza tym podmiotem bez zgody osób, których dane dotyczą; e) przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą; f) przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy; g) przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą; h) przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa państwa członkowskiego lub zgodnie z umową z pracownikiem służby zdrowia i z zastrzeżeniem warunków i zabezpieczeń, o których mowa w ust. 3; i) przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa Unii lub prawa państwa członkowskiego, które przewidują odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową; j) przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie, konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.

Tabela uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

			z poszanowaniem zasady poufności i integralności. Wyjaśnienia wymaga również, czy funkcjonowanie takiej „usługi online” nie doprowadzi do gromadzenia danych osobowych. A jeśli tak, to jaka będzie podstawa przetwarzania danych, zważywszy na fragmentaryczność regulacji i brak oceny skutków, kto będzie odpowiedzialny za bezpieczeństwo zgromadzonych danych, nadanie upoważnień dostępowych, zgłaszanie naruszeń, itd. W ust. 2 tego artykułu wskazano, że realizację usługi online minister właściwy do spraw informatyzacji może powierzyć jednostce mu podległej lub przez niego nadzorowanej. Wyjaśnienia wymaga status tego podmiotu na gruncie rozporządzenia 2016/679. Jeśli będzie on podmiotem przetwarzającym, to projektodawca powinien określić zakres jego odpowiedzialności poprzez stworzenie odpowiedniego instrumentu prawnego, zgodnie z wymogami wynikającymi z art. 28 rozporządzenia 2016/679.	
109.	Prezes Urzędu Ochrony Danych Osobowych	Art. 39a ust. 2	Ponadto w art. 39a ust. 2 KSC wskazano, że szczegółowe warunki realizacji usługi online określi umowa pomiędzy ministrem właściwym do spraw informatyzacji a jednostką mu podległą lub przez niego nadzorowaną. W przypadku przetwarzania danych osobowych, w tym danych szczególnych kategorii, szczegółowe warunki funkcjonowania usługi online, powinny być określone w przepisach powszechnie obowiązujących rangi ustawowej, skoro regulowane mają być prawa i obowiązki dotyczące przetwarzania danych osobowych. Umowa zawarta pomiędzy podmiotami publicznymi może jedynie dookreślać warunki techniczno-organizacyjne, a nie kształtować kluczowych procesów związanych z nadawaniem statusu administratora i kształtujących granice jego odpowiedzialności.	Uwaga wyjaśniona Na skutek wprowadzonych zmian w przepisie uwaga stała się bezprzedmiotowa.
110.	Prezes Urzędu Ochrony Danych Osobowych	Art. 42 ust. 10	W art. 1 pkt 42 proponowana jest zmiana art. 42 ust. 10 KSC, dzięki której organ właściwy do spraw cyberbezpieczeństwa będzie mógł przetwarzać m.in. dane osobowe dotyczące podmiotów kluczowych i podmiotów ważnych. Wskazany przepis jest sformułowany w sposób blankietowy i wymaga doprecyzowania - wszystkie sytuacje wymagające niezbędności przetwarzania danych osobowych powinny wynikać wprost z przepisów ustawy o KSC lub ewentualnie innych norm o charakterze powszechnie obowiązującym, co wynika z zasady proporcjonalności i przejrzystości.	Uwaga uwzględniona Przepis zostanie doprecyzowany, że takie dane są przetwarzane w ramach postępowań kontrolnych.
111.	Urząd Komisji Nadzoru Finansowego	Art. 42	Postuluje się dodanie w 42 UKSC nowego ust. 10 doprecyzującego, że organ właściwy do spraw cyberbezpieczeństwa dla sektora bankowego i infrastruktury	Uwaga uwzględniona

			rynków finansowych realizuje swoje zadania z uwzględnieniem zakresu zastosowania ustawy do podmiotów finansowych. Omawiana zmiana ma na celu doprecyzowanie zakresu zadań organu właściwego do spraw cyberbezpieczeństwa dla sektora bankowego i infrastruktury rynków finansowych do skutków płynących z zastosowania art. 4 dyrektywy 2022/2555, tj. braku zastosowania do podmiotów finansowych środków zarządzania ryzykiem w cyberbezpieczeństwie implementujących dyrektywę 2022/2555. Dotyczy to także braku zastosowania w odpowiednim zakresie przepisów dotyczących nadzoru i egzekwowania przepisów. Propozycja ta uwzględnia również postulat stosowania do podmiotów finansowych (z wyłączeniem podmiotów finansowych niebędących podmiotami kluczowymi lub ważnymi stosujących uproszczone ramy zarządzania ryzykiem związanym z ICT), przepisów dotyczących polecenia zabezpieczającego oraz dostawcy wysokiego ryzyka, w tym co do nadzoru sprawowanego w tym zakresie przez organ właściwy do spraw cyberbezpieczeństwa, co z kolei stanowi rozszerzenie zakresu jego zadań poza podmioty wymienione w załączniku nr 1 do UKSC. Postulowany przepis mógłby przyjąć następujące brzmienie: „10. Organ właściwy do spraw cyberbezpieczeństwa dla sektora bankowego i infrastruktury rynków finansowych realizuje swoje zadania z uwzględnieniem zakresu zastosowania ustawy do podmiotów finansowych.”. Dodatkowo, w art. 41 UKSC postuluje się oznaczenie jego dotychczasowej treści jako ust. 1 i dodanie ust. 2 w brzmieniu: „Organ właściwy do spraw cyberbezpieczeństwa, o którym mowa w ust. 1, współpracuje oraz wymienia informacje i dokumenty z właściwym organem w rozumieniu rozporządzenia 2022/2554, w zakresie niezbędnym do wykonywania przez ten organ obowiązków wynikających z rozporządzenia 2022/2554.”. W art. 42 UKSC postuluje się zaś dodanie nowego ust. 11, o następującym brzmieniu: „W ramach współpracy przewidzianej w art. 41 ust. 2 organ właściwy do spraw cyberbezpieczeństwa w szczególności udziela informacji oraz wszelkich istotnych zaleceń technicznych i pomocy technicznej, w przypadku gdy zwróci się o nie właściwy organ w rozumieniu rozporządzenia 2022/2554 w związku z realizowanymi przez ten organ obowiązkami wynikającymi z rozporządzenia 2022/2554 mającymi związek z podmiotem kluczowym lub podmiotem ważnym, a który zgodnie z rozporządzeniem 2022/2554 został wyznaczony jako kluczowy zewnętrzny dostawca	

Tabela uwag zgłoszonych w ramach opiniowania do *projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)*

			usług ICT, a także współpracuje z nim w sposób umożliwiający skuteczną i szybką koordynację działań nadzorczych, w tym na potrzeby prowadzenia kontroli.”. Propozycje dotyczące art. 41 ust. 2 oraz art. 42 ust. 11 UKSC odzwierciedlają treść art. 47 ust. 3 i 4 rozporządzenia 2022/2554. Wprowadzenie omawianych przepisów jest w ocenie UKNF uzasadnione również względami zapewnienia sprawnej współpracy z innymi organami właściwymi ds. cyberbezpieczeństwa, w szczególności w kontekście działań mających wpływ na kluczowych zewnętrznych dostawców usług ICT będących podmiotami kluczowymi lub ważnymi w rozumieniu dyrektywy 2022/2555.	
112.	Prezes Urzędu Transportu Kolejowego	Art. 41	Prezes UTK jest centralnym organem administracji rządowej niezależnym od ministra właściwego do spraw transportu. Jako regulator i organ nadzorujący bezpieczeństwo transportu kolejowego, Prezes UTK dysponuje specjalistyczną wiedzą na temat funkcjonowania tego rynku. To pozwala na pełne zrozumienie specyficznych zagrożeń i potrzeb związanych z cyberbezpieczeństwem, które jest nieodłącznym elementem bezpieczeństwa infrastruktury kolejowej i przewozów kolejowych. Obecnie Prezes UTK nie posiada żadnych kompetencji w zakresie cyberbezpieczeństwa. Włączenie cyberbezpieczeństwa do istniejących ram regulacyjnych i nadzorczych Prezesa UTK pozwoli na bardziej holistyczne podejście do zarządzania ryzykiem w transporcie kolejowym. Prezes UTK ma bowiem doświadczenie w monitorowaniu przestrzegania przepisów prawnych i norm bezpieczeństwa oraz certyfikacji w sektorze kolejowym. Prezes UTK mógłby wdrożyć procedury oceny zgodności i audyty bezpieczeństwa w zakresie zgodności z krajowym systemem cyberbezpieczeństwa jako część standardowych procedur audytowych realizowanych wobec przewoźników, zarządców infrastruktury oraz inne podmioty kolejowe. Rozszerzenie zadań tego organu o cyberbezpieczeństwo w podsektorze transportu kolejowego może wpłynąć na efektywniejsze egzekwowanie przepisów dotyczących ochrony infrastruktury cyfrowej w kolejnictwie Proponuje się w zmienianym art. 41 nadać następujące brzmienie pkt 2: „2) dla sektora transportu z wyłączeniem podsektora transportu wodnego oraz podsektora transportu kolejowego – minister właściwy do spraw transportu;” oraz po pkt 2 dodać pkt 2a w brzmieniu:	Uwaga nieuwzględniona Minister Infrastruktury (MI) jest organem właściwym ds. cyberbezpieczeństwa dla sektora transportu, w tym podsektora transportu kolejowego od 2018 r. - zadania organu właściwego są realizowane przez MI już od dłuższego czasu, w związku z czym MI nie tylko zbudowało i posiada wiedzę i kompetencje dziedzinowe, ale także przeniesienie zadań dla tego podsektora do UTK jako organu właściwego doprowadziłoby do nieproporcjonalnego rozdziału obowiązków nadzorczych pomiędzy podsektor kolejowy i pozostałe podsektory w sektorze transportu. Postulat ustanowienia UTK jako organu właściwego ds. cyberbezpieczeństwa jest tym bardziej nieuzasadniony, gdy weźmie się pod uwagę, że UTK nie jest jednostką podległą i nadzorowaną przez MI.

Tabela uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

			„2a) dla podsektora transportu kolejowego – Prezes Urzędu Transportu Kolejowego;”.	Wyłączenie podsektora kolejowego spod właściwości MI oddziałuje negatywnie nie tylko w kontekście wyżej przedstawionych argumentów, ponieważ taka sytuacja rodziłaby konieczność dokonania szeregu zmian: czy to w przestrzeni prawnej, czy w zakresie współpracy w obszarze sektora transportu, czy chociażby wymiany informacji.
113.	Prezes Urzędu Transportu Kolejowego	Art. 42 ust. 9	Niniejsza uwaga wiąże się z uwagą nr 2 powyżej, której konsekwencją jest konieczność zapewnienia możliwości finansowania zadań Prezesa UTK jako organu właściwego do spraw cyberbezpieczeństwa dla podmiotów kluczowych. W zmienianym art. 42 proponuje się następujące brzmienie dodawanego ust. 9: „9. Komisja Nadzoru Finansowego oraz Prezes Urzędu Transportu Kolejowego otrzymują dotację celową na realizację swoich zadań ustawowych z części budżetowej, której dysponentem jest Szef Kancelarii Prezesa Rady Ministrów”.	Uwaga nieuwzględniona w zw. z nieuwzględnieniem uwagi UTK do art. 41.
114.	Prezes Urzędu Komunikacji Elektronicznej	Art. 41 pkt 8a	Art. 1 pkt 40 lit. b dotyczący projektowanego art. 41 pkt 8a ustawy o ksc – w brzmieniu projektowanego art. 41 pkt 8a ustawy o ksc oznaczenie jednostki redakcyjnej: „8)” należy zastąpić oznaczeniem: „8a)”.	Uwaga uwzględniona
115.	Prezes Urzędu Ochrony Danych Osobowych	Art. 43 ust. 2	W proponowanym art. 43 ust. 2 KSC (wprowadzanym w art. 1 pkt 43 projektu), stanowiącym o możliwości zwracania się przez organ właściwy do spraw cyberbezpieczeństwa do innych organów administracji publicznej o przekazanie informacji umożliwiających ocenę podmiotu jako kluczowego lub ważnego, o ile wśród przekazywanych informacji byłyby dane osobowe, przekazywanie tych informacji przez organ publiczny powinno odbywać się na podstawie przepisów dokładnie określających procedurę oraz formę zarówno zwracania się o przekazanie informacji, jak i ich udostępniania. Przepisy określać powinny również kiedy organ może występować o przekazanie takich informacji oraz jaki zakres informacji może być mu udostępniony.	Uwaga wyjaśniona Wśród informacji przekazywanych na podstawie tego przepisu nie będzie danych osobowych.
116.	Naukowa i Akademicka Sieć Komputerowa –	Art. 44	W kontekście proponowanego brzmienia art. 44 ust. 1, rekomendujemy rozszerzyć wynikające z niego zadania CSIRT sektorowego na zadania, które planowane są do	Uwaga uwzględniona

Tabela uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

	Państwowy Instytut Badawczy		dodania w nowelizacji, w szczególności przyjmowanie zgłoszeń o potencjalnych zdarzeniach dla cyberbezpieczeństwa oraz wczesnych ostrzeżeń.	
117.	Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy	Art. 44	W odniesieniu do art. 44 ust. 1a warto rozważyć wprowadzenie obowiązku przekazania przez CSIRT sektorowy do właściwego CSIRT poziomu krajowego nie tylko wczesnego ostrzeżenia, ale również samego zgłoszenia incydentu (tj. art. 11 ust. 1 pkt 4 i 4a). Ponadto, proponujemy również objęcie obowiązkiem niezwłocznego przekazania do CSIRT poziomu krajowego sprawozdań, o których mowa w art. 11 ust. 1 pkt 4b i 4c. Dodatkowo, w tym zakresie, prosimy o rozważenie wprowadzenia obowiązku przekazywania incydentu poważnego jednocześnie – w Systemie S46 – do CSIRT poziomu krajowego i CSIRT sektorowego. Takie rozwiązanie odpowie na praktyczny problem związany z czasem przekazania zgłoszenia przez CSIRT sektorowy do CSIRT poziomu krajowego.	Uwaga uwzględniona
118.	Urząd Komisji Nadzoru Finansowego	Art. 44	Z perspektywy wyznaczenia CSIRT KNF jako podstawowego punktu kontaktowego dla EU-SCICF, tj. ram koordynacji ustanowionych w celu wykonania zalecenia Europejskiej Rady ds. Ryzyka Systemowego z dnia 2 grudnia 2021 r. w sprawie ogólnoeuropejskich ram koordynacji dla odpowiednich organów w odniesieniu do cyberincydentów o charakterze systemowym (ERRS/2021/17), korzystne byłoby wskazanie w ustawie na możliwość uczestnictwa CSIRT sektorowych w sieci CSIRT. W przypadku CSIRT KNF dałoby to m.in. możliwość nawiązywania bezpośrednich relacji z zespołami, z którymi CSIRT KNF może współpracować w ramach EU-SCICF. Przykładem CSIRT sektorowego z innego państwa UE, który jest członkiem sieci CSIRT, jest austriacki zespół CSIRT dla sektora energii (Austrian Energy CERT (AEC)). Obecnie do uczestnictwa w sieci CSIRT odnoszą się jedynie przepisy dotyczące zadań CSIRT poziomu krajowego.	Uwaga nieuwzględniona Zgodnie z dyrektywą NIS2 w sieci CSIRT uczestniczą National CSIRTs a nie CSIRT sektorowe.
119.	Urząd Komisji Nadzoru Finansowego	Art. 44	W projektowanym art. 44 ust. 1b UKSC występuje błędna numeracja (powtórzenie pkt 2).	Uwaga uwzględniona
120.	Urząd Komisji Nadzoru Finansowego	Art. 44	Podobnie jak w przypadku wpływu zasady z art. 4 dyrektywy 2022/2555 w kontekście środków zarządzania ryzykiem w cyberbezpieczeństwie na zadania organu właściwego do spraw cyberbezpieczeństwa dla sektora bankowego i infrastruktury rynków finansowych, tak i w przypadku CSIRT sektorowego dla tego sektora doprecyzowaniu powinien ulec zakres jego zadań w związku z zastosowaniem do podmiotów finansowych rozporządzenia 2022/2554 w odniesieniu do incydentów	Uwaga uwzględniona

Tabela uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

			związanych z ICT. W projektowanym art. 44 ust. 1a wskazuje się choćby na przekazywanie przez CSIRT sektorowy wczesnego ostrzeżenia do właściwego CSIRT MON, CSIRT NASK albo CSIRT GOV, podczas gdy odpowiednikiem tego rodzaju zgłoszenia w ramach rozporządzenia 2022/2554 jest wstępne powiadomienie. W związku z powyższym postuluje się wprowadzenie w art. 44 UKSC nowych ust. 5 i 6 o następującym brzmieniu: „5. Przepisy ust. 1-4 stosuje się odpowiednio do CSIRT sektorowego ustanowionego w sektorze bankowym i infrastruktury rynków finansowych, w szczególności w zakresie poważnych incydentów związanych z ICT zgłaszanych przez podmioty kluczowe lub podmioty ważne. 6. CSIRT sektorowy ustanowiony w sektorze bankowym i infrastruktury rynków finansowych może również realizować swoje zadania w odniesieniu do podmiotów finansowych niebędących podmiotami kluczowymi lub podmiotami ważnymi, w szczególności w zakresie wsparcia w obsłudze poważnych incydentów związanych z ICT, gdy nie stanowi to dla tego zespołu nieproporcjonalnego czy nadmiernego obciążenia, z uwzględnieniem priorytetowego traktowania poważnych incydentów związanych z ICT zgłaszanych przez podmioty finansowe będące podmiotami kluczowymi lub podmiotami ważnymi oraz z zastrzeżeniem odpowiedniego stosowania ust. 1-4 do realizacji zadań przez ten zespół.”. W kontekście wsparcia udzielonego przez CSIRT sektorowy ustanowiony w sektorze bankowym i infrastruktury rynków finansowych dodawany art. 44 ust. 6 UKSC ma na celu również zapewnienie możliwości realizowania zadań przez ten CSIRT sektorowy także wobec podmiotów finansowych nieobjętych dyrektywą 2022/2555. Jednocześnie w przepisie przewidziano przesłanki, które mają zapewnić priorytetowe traktowanie podmiotów kluczowych i ważnych, które wzorowane są na art. 30 ust. 3 UKSC. Zaproponowane podejście koresponduje z art. 22 ust. 1 rozporządzenia 2022/2554.	
121.	Prezes Urzędu Ochrony Danych Osobowych	Art. 44c	Proponowany art. 44c KSC (wprowadzany w art. 1 pkt 45 projektu) dotyczy możliwości powierzenia przez ministra właściwego do spraw cyberbezpieczeństwa CSIRT MON, CSIRT NASK albo CSIRT GOV realizacji zadania lub zadań CSIRT sektorowego. Należy wskazać, że poprzez powierzenie zadań innemu podmiotowi, to podmiot ten, zgodnie z funkcjonalną wykładnią art. 4 pkt 7 rozporządzenia 2016/679 i wytycznymi EROD w tej sprawie, staje się administratorem. Podmioty, którym	Uwaga wyjaśniona Mechanizm ten jest zgodny z zaproponowanym rozwiązaniem. Kwestia ta zostanie opisana w uzasadnieniu.

Tabela uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

			powierza się więc realizację wskazanych w przepisie zadań muszą pamiętać o ciążących na nich obowiązkach wynikających z faktu bycia administratorem.	
122.	Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy	Art. 45	W art. 45 projektowanemu pkt 10 rekomendujemy nadać następujące brzmienie: „10) koordynacja współpracy w obszarze cyberbezpieczeństwa z państwami trzecimi”. W naszej ocenie współpraca z zagranicznymi CSIRT powinna być zadaniem CSIRT poziomu krajowego.	Uwaga uwzględniona
123.	Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy	Art. 46 ust. 1 pkt 7	W proponowanym art. 46 ust. 1 pkt 7 proponujemy doprecyzować, że przekazywanie zgłoszeń naruszenia ochrony danych osobowych następuje <u>przez podmioty kluczowe i ważne</u> .	Uwaga uwzględniona
124.	Urząd Komisji Nadzoru Finansowego	Art. 46 ust. 4	W projektowanym art. 46 ust. 4 UKSC weryfikacji wymaga zasadność posłużenia się w tym przepisie zwrotem „inne niż w ust. 2” w odniesieniu do podmiotów kluczowych i ważnych. W zaproponowanym w projekcie brzmieniu art. 46 ust. 2 UKSC brak jest bowiem odniesienia się do podmiotów kluczowych lub ważnych.	Uwaga uwzględniona
125.	Prezes Urzędu Ochrony Danych Osobowych	art. 46 ust. 2	Projektowany art. 46 ust. 2 KSC (określony w art. 1 pkt 48 projektu), przewiduje uprawnienie organu nadzorczego – Prezesa Urzędu Ochrony Danych Osobowych – do korzystania z systemu teleinformatycznego wspierającego współpracę w ramach krajowego systemu cyberbezpieczeństwa, dotyczącą m.in. współpracy podmiotów wchodzących w skład krajowego systemu cyberbezpieczeństwa, generowania i przekazywania rekomendacji dotyczących działań podnoszących poziom cyberbezpieczeństwa, zgłaszanie i obsługę incydentów, szacowanie ryzyka na poziomie krajowym, ostrzeganie o zagrożeniach cyberbezpieczeństwa. Wprowadzenie takiego rozwiązania niewątpliwie usprawni realizację zakładanego celu, przy czym należy wyraźnie wskazać, że organ nadzorczy będąc użytkownikiem systemu, z uwagi na swoją niezależność i kompetencje ²³⁾ zachowuje także prawo do	Uwaga wyjaśniona Podłączenie do systemu nie oznacza braku możliwości zgłaszania uwag co do jego działania. Celem tego przepisu jest jedynie ułatwienie zgłaszania incydentów związanych z ochroną danych osobowych.

²³⁾ 1. Każdy organ nadzorczy podczas wypełniania swoich zadań i wykonywania swoich uprawnień zgodnie z niniejszym rozporządzeniem działa w sposób w pełni niezależny. 2. Członek lub członkowie każdego organu nadzorczego podczas wypełniania swoich zadań i wykonywania swoich uprawnień zgodnie z niniejszym rozporządzeniem pozostają wolni od bezpośrednich i pośrednich wpływów zewnętrznych, nie zwracają się do nikogo o instrukcje ani ich od nikogo nie przyjmują. 3. Członek lub członkowie każdego organu nadzorczego powstrzymują się od wszelkich czynności sprzecznych ze swoimi obowiązkami i podczas swojej kadencji nie podejmują żadnego zajęcia zarobkowego ani niezarobkowego sprzecznego z tymi obowiązkami. 4.

Tabela uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

			oceny ww. systemu w świetle rozporządzenia 2016/679. Uwzględniając obowiązek wynikający z przepisów dyrektywy NIS 2, co do obowiązku utworzenia jednego punktu konsultacyjnego, należy podkreślić, że stworzenie rozwiązania wspierającego współpracę w ramach krajowego systemu cyberbezpieczeństwa nie eliminuje uprawnień organu nadzorczego do oceny takiego systemu z punktu widzenia przepisów o ochronie danych oraz kontroli jego administratora i współadministratorów w zakresie przestrzegania przepisów rozporządzenia 2016/679.	
126.	Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy	Art. 46 ust. 5	Proponujemy nadanie następującego brzmienia art. 46 ust. 5: <i>„5. Uwierzytelnienie do systemu teleinformatycznego następuje za pomocą środków określonych w art. 20a ust. 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2024 r. poz. 307) lub w inny, wskazany przez ministra właściwego do spraw informatyzacji, sposób.”.</i>	Uwaga częściowo uwzględniona Przepis zostanie uzupełniony o wskazanie uwierzytelniania wieloskładnikowego.
127.	Prezes Urzędu Komunikacji Elektronicznej	Art. 46 ust. 6	Art. 1 pkt 48 lit. e w zakresie dotyczącym projektowanego art. 46 ust. 6 ustawy o ksc – określony w projektowanym przepisie termin 3 miesięcy na zapewnienie przez podmioty kluczowe i podmioty ważne zgodności swoich systemów informacyjnych z minimalnymi wymaganiami technicznymi i funkcjonalnymi korzystania z systemu teleinformatycznego, o którym mowa w art. 46 ust. 1 ustawy o ksc, wydaje się zbyt krótki. W związku z tym proponuje się jego wydłużenie do 6 miesięcy.	Uwaga uwzględniona
128.	Rzecznik Małych i Średnich Przedsiębiorców	Art. 46 ust. 6	W odniesieniu do art. 1 pkt 48 Projektu (nadający nowe brzmienie art. 46 ustawy zmienianej), w odniesieniu do dodawanego do art. 46 ust. 6, nakładającym na podmioty kluczowe i podmioty ważne obowiązek dostosowania ich systemów informacyjnych do minimalnych wymogów krajowego systemu bezpieczeństwa w terminie 3 miesięcy od udostępnienia tych wymagań - postuluje się wydłużenie okresu dostosowawczego do okresu co najmniej 6 miesięcy. Uzasadnieniem postulatu jest chęć urealnienia tego okresu, aby każdy podmiot był w stanie podołać nałożonym na niego obowiązkom.	Uwaga uwzględniona

Każde państwo członkowskie zapewnia, by każdy organ nadzorczy dysponował zasobami kadrowymi, technicznymi i finansowymi, pomieszczeniami i infrastrukturą niezbędnymi do skutecznego wypełniania swoich zadań i wykonywania swoich uprawnień, w tym w zakresie wzajemnej pomocy, współpracy i uczestnictwa w pracach Europejskiej Rady Ochrony Danych. 5. Każde państwo członkowskie zapewnia, by każdy organ nadzorczy wybierał i posiadał własny personel, działający pod wyłącznym kierownictwem członka lub członków danego organu nadzorczego. 6. Każde państwo członkowskie zapewnia, by każdy organ nadzorczy podlegał kontroli finansowej w sposób nienaruszający jego niezależności oraz dysponował odrębnym, publicznym budżetem rocznym, który może być częścią ogólnego budżetu państwowego lub krajowego.

Tabela uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

129.	Prezes Urzędu Ochrony Danych Osobowych	art. 46 ust. 1 pkt 7	W art. 1 pkt 48 proponowane jest wprowadzenie art. 46 ust. 1 pkt 7 KSC, dotyczącego dokonywania zgłoszenia naruszenia ochrony danych osobowych, o którym mowa w art. 33 rozporządzenia 2016/679. Przepis nie określa ról w procesie dokonywania zgłoszenia naruszeń. Z przepisu nie wynika kto w systemie teleinformatycznym ma dokonywać zgłoszenia. Niejasne jest również w jaki sposób poprzez system teleinformatyczny wspierane ma być dokonywanie zgłoszenia naruszenia ochrony danych osobowych i jakie obowiązki rodzi to dla organu nadzorczego lub innych podmiotów.	Uwaga wyjaśniona Zgłoszenia będzie mógł dokonać każdy podmiot w systemie i to on będzie odpowiadał za przekazane dane. Będzie on zgłaszał incydent, który wystąpił u danego podmiotu, a zgłoszenie będzie przekazane bezpośrednio do UODO.
130.	Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy	Art. 46 ust. 8	W art. 46 ust. 8 proponujemy wprowadzenie odpowiedniego przepisu, który umożliwiłby utworzenie niewyczerpującego wykazu usług świadczonych przez podmioty kluczowe i ważne. W ocenie NASK, ze względu na liczbę podmiotów objętych krajowym systemem cyberbezpieczeństwa, nie jest obecnie możliwe wskazanie wyczerpująco wszystkich usług.	Uwaga uwzględniona Wykaz będzie miał charakter niewyczerpujący.
131.	Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy	Art. 48 pkt 6	W aktualnym brzmieniu art. 48 pkt 6 rekomendujemy usunięcie sformułowania „oraz Sieci CSIRT”. CSIRT poziomu krajowego są członkami sieci CSIRT, więc zapewnienie wymiany informacji przez ministra nie jest konieczne. W tym punkcie jednak warto rozważyć dodanie regulacji dot. EU-CyCLONE. Zwracamy się również z prośbą o rozważenie wyznaczenia przez ministra właściwego do spraw informatyzacji reprezentanta Polski w Sieci CSIRT (w roli Standing Representative). Dotychczas funkcję tę pełniła wyznaczona osoba z CSIRT NASK.	Uwaga nieuwzględniona Przedmiotowy przepis nie jest zmieniany w ramach niniejszej nowelizacji ani też nie otrzymywano zgłoszeń co do problemów ze stosowaniem tego przepisu. W związku z tym nie wymaga on zmiany.
132.	Urząd Komisji Nadzoru Finansowego	Art. 48	W art. 48 brak jest w aktualnym brzmieniu tego przepisu podziału na ustępy (a do ust. 1 odnosi się zmiana z art. 1 pkt 50 ustawy, zgodnie z którą „w art. 48 ust. 1 pkt 1 i 2 otrzymują brzmienie: (...)).”.	Uwaga uwzględniona
133.	Urząd Komisji Nadzoru Finansowego	Art. 48	W art. 48 UKSC postuluje się oznaczenie jego dotychczasowej treści jako ust. 1 i dodanie ust. 2 w brzmieniu: „Pojedynczy Punkt Kontaktowy współpracuje i wymienia informacje z właściwym organem w rozumieniu rozporządzenia 2022/2554 gdy jest to niezbędne dla realizacji zadań Pojedynczego Punktu Kontaktowego bądź realizacji zadań tego właściwego organu.”. Dodawany ust. 2 stanowi odzwierciedlanie art. 47 ust. 2 rozporządzenia 2022/2554, zgodnie z którym „W stosownych przypadkach właściwe organy mogą konsultować się i wymieniać informacje z pojedynczymi punktami kontaktowymi i CSIRT wyznaczonymi lub ustanowionymi zgodnie z dyrektywą (UE) 2022/2555.”.	Uwaga nieuwzględniona Przekazywanie informacji otrzymywanych z innych krajów przez Pojedynczy Punkt Kontaktowy jest już możliwa i będzie dalej możliwa na podstawie art. 49 ust. 3. W związku z tym nie ma konieczności dokonania zmiany.

Tabela uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

134.	Prezes Urzędu Ochrony Danych Osobowych	Art. 49 ust. 4	W proponowanym art. 49 ust. 4 KSC (wskazanym w art. 1 pkt 51 projektu) określono, że pojedynczy punkt kontaktowy przekazuje Agencji Unii Europejskiej do spraw Bezpieczeństwa Sieci i Informacji (ENISA) dane z wykazu podmiotów kluczowych i podmiotów ważnych. Przepis wymaga jednak doprecyzowania o cele przekazywania, o ile będzie dochodziło także do przekazywania danych osobowych, wraz ze wskazaniem ich zakresu.	Uwaga wyjaśniona Zakres danych przekazywanych przez pojedynczy punkt kontaktowy został określony przepisami wdrażanej dyrektywy NIS2. PPK będzie przekazywał przede wszystkim liczbę podmiotów ujętą w wykazie.
135.	Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy	Art. 53 ust. 1	W propozycji art. 53 ust. 1 pkt 1 zawarto przepis mówiący o możliwości prowadzenia kontroli doraźnej, a jednocześnie w art. 54 ust. 1 pkt planowane jest odesłanie do ustawy – Prawo przedsiębiorców i ustawy o kontroli w administracji rządowej, które nie zawierają regulacji dotyczących kontroli doraźnej. Mając to na uwadze oraz fakt, że organy administracji publicznej zobowiązane są do działania na podstawie i w granicach prawa, rekomendujemy dookreślenie zasad, na jakich wykonywana ma być ta kontrola przez odesłanie do innych regulacji lub stworzenie odrębnych procedur.	Uwaga uwzględniona Dodany został przepis art. 59c określający zasady przeprowadzania kontroli doraźnej.
136.	Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy	Art. 53	W zakresie proponowanego art. 53 ust. 8 warto również rozważyć wprowadzenie odpowiadającej mu normy w ustawie – Prawo przedsiębiorców. Co prawda, w przepisach regulujących poszczególne rodzaje działalności gospodarczej często zawarte są przepisy umożliwiające cofnięcie koncesji czy zezwolenia ze względu na naruszenie innych przepisów regulujących daną działalność, jednak, w celu zapewnienia pewności prawa, warto rozważyć dodanie przepisów umożliwiających realizację kompetencji przez organy, o których mowa w ust. 8.	Uwaga wyjaśniona Został wprowadzony przepis regulujący procedurę określoną w art. 53 ust. 8 projektu.
137.	Rzecznik Małych i Średnich Przedsiębiorców	Art. 53	Sankcje określone w art. 1 pkt 56 Projektu (nadający nowe brzmienie art. 53 ustawy zmienianej), w szczególności zawarte w projektowanym art. 53 ust. 8 ustawy zmienianej uznać należy za nieproporcjonalnie dotkliwe. Wobec czego postuluje się, aby: – w projektowanym art. 53 ust. 8 pkt 1 ustawy zmienianej - organ właściwy do spraw cyberbezpieczeństwa był uprawniony, aby zwrócić się do organu, który udzielił koncesji podmiotowi kluczowemu lub podmiotowi ważnemu - wyłącznie o jej zawieszenie, w odniesieniu do podmiotu kluczowego (a nie także podmiotu ważnego oraz również nie o ograniczenie lub cofnięcie), ewentualnie przeprowadzenie kontroli, o której mowa w art. 40 ustawy z dnia 6 marca 2018 r. Prawo przedsiębiorców, – w projektowanym art. 53 ust. 8 pkt 1 ustawy zmienianej - organ właściwy do spraw cyberbezpieczeństwa był uprawniony, aby zwrócić się do organu, który dokonał	Uwaga częściowo uwzględniona Środki nadzorcze, o których mowa w art. 53 ust. 8 projektu, stosowane będą wyłącznie do podmiotów kluczowych. Zdecydowano również o wykreśleniu uprawnienia do wykreślenia z rejestru działalności regulowanej i cofnięcia koncesji. Został także wprowadzony przepis regulujący procedurę określoną w art. 53 ust. 8.

Tabela uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

			wpisu podmiotu kluczowego lub podmiotu ważnego do rejestru działalności regulowanej - wyłącznie o przeprowadzenie kontroli, o której mowa w art. 43 ust. 7 ustawy Prawo przedsiębiorców (a nie o wykreślenie z rejestru). Uzasadnienie: Sankcje proponowane w art. 53, w szczególności w ust. 8 pkt 1 i 2 tego artykułu mogą być nieproporcjonalnie duże oraz mogą powodować trudne lub niemożliwe do odwrócenia skutki dla podmiotów nimi objętymi. Uzasadnienie Projektu⁹ nie zawiera wyjaśnienia intencji projektodawców w zakresie dotkliwości proponowanych środków egzekucji. Również wdrażana do krajowego porządku prawnego Dyrektywa 2022/2555 (NIS 2), w jej art. 31 i 32, w szczególności art. 32 ust. 1 wskazuje, iż środki nadzoru lub egzekwowania przepisów nakładane na podmioty kluczowe w odniesieniu powinny być proporcjonalne i stosowne do okoliczności każdego indywidualnego przypadku - a nie nieograniczone, jak w treści omawianej regulacji. Ponadto w art. 32 ust. 5 lit. a) wskazuje się jedynie na możliwość tymczasowego zawieszenia lub o tymczasowe zawieszenie zezwolenia na niektóre lub wszystkie odpowiednie usługi lub działalności i sankcja taka jest nakładana tylko w odniesieniu do podmiotów kluczowych. Odesłanie do regulacji zawartych w Rozdziale 4 (Reglamentacja działalności gospodarczej) ustawy Prawo przedsiębiorców w zakresie kontroli działalności koncesjonowanej i regulowanej (art. 40 oraz art. 43 ust 7 tej ustawy) uznać należy za wystarczające narzędzia prawne pozwalające na osiągnięcie egzekucji przepisów zawartych w Projekcie. W takich okolicznościach powyższe postulaty uznać należy za w pełni zasadne.	
138.	Rzecznik Praw Obywatelskich	Art. 53 ust. 7	W art. 53 ust. 7 przewidziano standardową ścieżkę odwoławczą (skarga do WSA na zasadach ogólnych) do decyzji w sprawach cyberbezpieczeństwa, które są niestandardowe, bo mogą wywołać nieodwracalne skutki - tym samym przepis budzi wątpliwości z punktu widzenia prawa do skutecznego środka odwoławczego. Przykładowo organ może nakazać w drodze decyzji podanie do wiadomości publicznej informacji o naruszeniach przepisów ustawy (art. 53 ust. 5 pkt 7) - nawet jeśli podmiot kluczowy będzie miał inną ocenę prawną zdarzenia, nadal będzie musiał publicznie zszargać swoje dobre imię, przyznając się, że albo sam naruszył prawo, albo przyzwolił na naruszenie prawa. Zanim WSA i NSA zdążą rozpatrzyć jego skargę, opinia publiczna zdąży utrwalić sobie przekonanie, że podmiot złamał prawo. Innym przykładem nieodwracalnych zmian mogą być zmiany w systemie teleinformatycznym wymuszone decyzją, o której mowa w art. 53 ust. 5 pkt 4.	Uwaga uwzględniona Przepis art. 53 ust. 9 został doprecyzowany, że środków, o których mowa w ust. 8, nie stosuje się do czasu rozstrzygnięcia sprawy przez sąd administracyjny. W zakresie ust. 7 zostanie doprecyzowane uzasadnienie wskazujące na fakt, że przysługuje skarga do sądu a zatem stosuje się przepisy prawa o postępowaniu przed sądami administracyjnymi, w szczególności art. 61.

Tabela uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

139.	Rzecznik Praw Obywatelskich	Art. 53 ust. 7	Niektóre decyzje - jak decyzja nakazująca publiczne przyznanie się do naruszenia prawa - nie powinny być wykonywane do czasu wydania wyroku WSA. W art. 53 ust. 7 należałoby zatem zastrzec, że w przypadku decyzji wywołujących nieodwracalne skutki (prawne lub faktyczne) wniesienie skargi do WSA wstrzymuje ich wykonanie. Niezależnie od tego, warto byłoby rozważyć wyznaczenie WSA instrukcyjnego terminu na rozpatrywanie tego typu spraw.	Uwaga uwzględniona Przepis art. 53 ust. 9 został doprecyzowany, że środków o których mowa w ust. 8, nie stosuje się do czasu rozstrzygnięcia sprawy przez sąd administracyjny. W zakresie ust. 7 zostanie doprecyzowane uzasadnienie wskazujące na fakt, że przysługuje skarga do sądu a zatem stosuje się przepisy prawa o postępowaniu przed sądami administracyjnymi, w szczególności art. 61.
140.	Rzecznik Praw Obywatelskich	Art. 53 ust. 14 pkt 2	W art. 53 ust. 14 pkt 2 powinno być zobowiązanie organu do wskazania przyczyn odrzucenia stanowiska podmiotu kluczowego;	Uwaga uwzględniona Przepis został uzupełniony o obowiązek szczegółowego uzasadnienia przyczyn odrzucenia stanowiska podmiotu.
141.	Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy	Art. 53b ust. 2	W zakresie art. 53b ust. 2 warto wskazać, że zawarte w pkt 1 i 2 elementy analizy ryzyka wydają się wykraczać poza obszar tematyczny ustawy, a tym samym mogą być bardzo trudne do oceny dla organu właściwego.	Uwaga nieuwzględniona Wskazane elementy analizy ryzyka są zdaniem projektodawcy ściśle związane z obszarem tematycznym ustawy. Cyberbezpieczeństwa nie sposób jest odłączyć od kwestii związanych z bezpieczeństwem narodowym, porządkiem publicznym, gospodarką i społeczeństwem, a także pozostałymi zagadnieniami związanymi ze stratami finansowymi, szkodami wizerunkowymi czy zakłóceniami w funkcjonowaniu systemów i infrastruktury. Elementy te oddziałują bowiem silnie na funkcjonowanie państwa na poziomie ekonomicznym i

Tabela uwag zgłoszonych w ramach opiniowania do *projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)*

				społecznym. W związku z tym uwzględnienie tych elementów w analizie ryzyka przy tworzeniu hierarchii priorytetów w sprawowaniu nadzoru po stworzeniu metodyki w ocenie projektodawcy są konieczne. Jednocześnie projektodawca nie wyklucza, że analizie będą poddane inne elementy dlatego posłużył się sformułowaniem „w szczególności”. Metodyki nadzoru oraz hierarchizacja nie są ponadto obligatoryjne a mają jedynie na celu sprawniejsze zarządzanie zadaniami i ich prawidłową realizację.
142.	Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy	Art. 53c ust. 3	W odniesieniu do art. 53c ust. 3 proponujemy, aby żądanie, o jakim mowa w tym przepisie – w kontekście art. 46 ust. 1 pkt 6 ustawy - przekazywane było za pośrednictwem Systemu S46. Ułatwi to komunikację między podmiotem a organem właściwym. Analogicznie także w przypadku przekazywania rekomendacji Pełnomocnika, o których mowa w dodawanym art. 67a ust. 2, warto rozważyć wykorzystanie do ich przesłania podmiotom System S46.	Uwaga uwzględniona Przeredagowano brzmienie art. 53c ust. 3
143.	Prezes Urzędu Ochrony Danych Osobowych	Art. 53d ust. 1 pkt 3	W odniesieniu do projektowanego art. 53d ust. 1 pkt 3 KSC (wprowadzanym w art. 1 pkt 57 projektu) dotyczącego uprawnień urzędnika monitorującego, należy podkreślić, że w zakresie przetwarzania przez niego danych osobowych będzie on związany przepisami rozporządzenia 2016/679, jako osoba realizująca zadania w imieniu i na rzecz administratora.	Uwaga uwzględniona Kwestia ta zostanie opisana w uzasadnieniu.
144.	Rzecznik Praw Obywatelskich	Art. 54 ust. 2	W art. 54 ust. 2 trzeba doprecyzować maksymalny czas trwania kontroli u przedsiębiorców. Obecnie jest napisane, że taka kontrola "nie może przekroczyć 48 dni roboczych" - podobnie jak w art. 55 ust. 1 prawa przedsiębiorców. W praktyce jednak urzędnicy przeinaczają znaczenie tego limitu w sposób przekreślający jego praktyczne znaczenie: wychodzą oni z założenia, że przez „dni robocze” nie należy rozumieć kolejnych dni powszednich między poniedziałkiem a piątkiem, lecz	Uwaga uwzględniona Przepis zmieniono zgodnie z propozycją.

Tabela uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

			wyłącznie takie dni, w których kontrolerzy faktycznie przebywali w siedzibie przedsiębiorcy i wykonywali czynności kontrolne. W konsekwencji organy administracji przekraczały terminy ustawowe o kilka tygodni, miesiące, a nawet o rok bądź dwa lata. Dlatego w art. 54 ust. 2 ustawy o cyberbezpieczeństwie powinno się sprecyzować, że taka kontrola "nie może przekroczyć kolejnych 48 dni roboczych od wszczęcia kontroli".	
145.	Prezes Urzędu Komunikacji Elektronicznej	Art. 58 ust. 6	Art. 1 pkt 60 w zakresie dotyczącym projektowanego art. 58 ust. 6 i nast. ustawy o ksc – należy podkreślić, że określenie osoby analizującej zastrzeżenia do protokołu kontroli mianem „kierownika komórki do spraw kontroli” (na skutek zdjęcia tego obowiązku z osoby prowadzącej czynności kontrolne) może powodować problemy w toku stosowania tych przepisów. Warto bowiem zauważyć, że nie każdy organ właściwy do spraw cyberbezpieczeństwa musi dysponować tego rodzaju komórką organizacyjną, a ponadto nie zawsze osoba prowadząca czynności kontrolne będzie pracownikiem takiej komórki, którą w projekcie określono mianem komórki do spraw kontroli. W konsekwencji proponuje się korektę brzmienia przepisu, która polegać mogłaby np. na tym, że przedmiotowe zastrzeżenia analizowane byłyby przez kierownika komórki organizacyjnej, której pracownikiem jest osoba prowadząca czynności kontrolne.	Uwaga wyjaśniona Kierownik komórki ds. kontroli rozumiany jest przez projektodawcę szeroko – tj. jako kierownik komórki niekoniecznie wyodrębnionej do kontroli ale która w ramach swoich zadań zajmuje się kontrolą tj. właśnie będzie to np. kierownik komórki organizacyjnej, której pracownikiem jest osoba prowadząca czynności kontrolne. Doprecyzowano uzasadnienie w tym zakresie.
146.	Prezes Urzędu Ochrony Danych Osobowych	Art. 59a	Rola Prezesa Urzędu Ochrony Danych Osobowych Art. 1 ust. 62 projektu przewiduje dodanie art. 59a KSC w brzmieniu: „W przypadku stwierdzenia w toku kontroli podejrzenia naruszenia ochrony danych osobowych, organ właściwy do spraw cyberbezpieczeństwa informuje o tym Prezesa Urzędu Ochrony Danych Osobowych”. Przepis ten wymaga uzupełnienia poprzez wskazanie że informacja, o której mowa w projektowanym przepisie, powinna zostać przekazana Prezesowi Urzędu Ochrony Danych Osobowych bez zbędnej zwłoki. Przepis ten w obecnym kształcie nie przewiduje bowiem żadnego terminu, w jakim organy właściwe do spraw cyberbezpieczeństwa powinny wykonać dyspozycję normy. Przepis powinien zostać uzupełniony również o wskazanie w jaki sposób organ właściwy do spraw cyberbezpieczeństwa informuje organ nadzorczy o podejrzeniu naruszenia ochrony danych. Ponadto wątpliwości budzi czy sformułowanie „w toku	Uwaga częściowo uwzględniona Zostanie wprowadzony termin 7 dni na poinformowanie UODO. Zastąpiono sformułowanie „w toku kontroli” na „podczas sprawowania nadzoru”.

Tabela uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

			kontroli” nie zawęży nadmiernie obowiązku implementowanego do porządku krajowego na podstawie dyrektywy NIS 2 (art. 35 ust. 1 dyrektywy NIS 2 ²⁴).	
147.	Prezes Urzędu Ochrony Danych Osobowych	Art. 59a i art. 76c	Jednocześnie organ nadzorczy z aprobatą przyjmuje rozwiązania zaproponowane w art. 1 pkt 62 projektu dodającym propozycję art. 59a KSC (dotyczącego informowania organu nadzorczego w przypadku stwierdzenia w toku kontroli podejrzenia naruszenia ochrony danych osobowych) oraz w art. 1 pkt 79 projektu dodającym propozycję art. 76c KSC (dotyczącego nałożenia przez organ nadzorczy kary pieniężnej w związku z naruszeniem ochrony danych osobowych) i ocenia je jako właściwie chroniące dane podmiotów danych.	Uwaga wyjaśniona Poparcie dla zawartych w ustawie rozwiązań projektodawca przyjmuje jako potwierdzenie słuszności wprowadzonych regulacji.
148.	Narodowy Bank Polski	Art. 59b ust. 3 pkt 3	Ad art. 1 pkt 62 projektu ustawy w zakresie dodawanego art. 59b ust. 3 pkt 3: 3) organ innego państwa żąda o udostępnienie informacji lub dokumentów, których udostępnienie narusza podstawowy interes bezpieczeństwa państwa, bezpieczeństwa i porządku publiczności lub obronności. Proponujemy przeredagować wstęp do punktu 3, aby miał on następujące brzmienie np.: „ <i>organ innego państwa żąda udostępnienia informacji lub dokumentów</i> ”. Ponadto zamiast wyrażenia „ <i>bezpieczeństwa i porządku publiczności</i> ” należy użyć sformułowania „ <i>bezpieczeństwa i porządku publicznego</i> ”.	Uwaga uwzględniona
149.	Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy	Art. 62a ust. 6 pkt 5	W projektowanym art. 62a ust. 6 pkt 5 rekomendujemy doprecyzowanie – jeśli intencją projektodawcy jest wprowadzenie wymiany informacji dotyczących sytuacji kryzysowych w cyberbezpieczeństwie. Jeśli jednak intencją projektodawcy jest wprowadzenie nowej kategorii „sytuacji kryzysowych w cyberprzestrzeni” , rekomendujemy uściślenie tego terminu i dodanie do projektu odpowiedniej definicji.	Uwag uwzględniona Zostanie dodana proponowana definicja.
150.	Prezes Urzędu Komunikacji Elektronicznej	Art. 62a ust. 2	Art. 1 pkt 65 w zakresie dotyczącym projektowanego art. 62a ust. 2 ustawy o ksc – proponuje się rozważenie uzupełnienia składu nowotworzonego Połączonego Centrum Operacyjnego Cyberbezpieczeństwa o przedstawiciela Szefa Agencji Bezpieczeństwa Wewnętrznego.	Uwaga uwzględniona Zostanie dodany przedstawiciel ABW.

²⁴⁾ Jeżeli w czasie nadzoru lub egzekwowania przepisów właściwe organy powzięły wiedzę, że naruszenie przez podmiot kluczowy lub ważny obowiązków określonych w art. 21 i 23 niniejszej dyrektywy może pociągać za sobą naruszenie ochrony danych osobowych zdefiniowane w art. 4 pkt 12 rozporządzenia (UE) 2016/679, które podlega zgłoszeniu na podstawie art. 33 tego rozporządzenia, bez zbędnej zwłoki informują o tym organy nadzorcze, o których mowa w art. 55 i 56 tego rozporządzenia.

Tabela uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

151.	Urząd Komisji Nadzoru Finansowego	Art. 65	W ocenie UKNF zakres zadań Kolegium do Spraw Cyberbezpieczeństwa powinien być uzupełniony o możliwość wydawania przez nie opinii w sprawach dot. współdziałania zespołów CSIRT oraz krajowych właściwych organów w rozumieniu rozporządzenia 2022/2554. W związku z powyższym w art. 65 ust. 1 postuluje się dodanie nowego pkt 9 o następującym brzmieniu: „współdziałania zespołów CSIRT MON, CSIRT GOV, CSIRT NASK i CSIRT sektorowego w sektorze bankowym i infrastruktury rynków finansowych oraz właściwego organu w rozumieniu rozporządzenia 2022/2554, w zakresie działalności podmiotów finansowych będących podmiotami kluczowymi lub podmiotami ważnymi.”.	Uwaga uwzględniona
152.	Prezes Urzędu Komunikacji Elektronicznej	Art. 66 ust. 1 pkt 4 lit. h	Art. 1 pkt 68 lit. a w zakresie dotyczącym projektowanego art. 66 ust. 1 pkt 4 lit. h ustawy o ksc – w projektowanym przepisie rozszerzono skład Kolegium do spraw Cyberbezpieczeństwa o nowych członków, którymi będą organy właściwe do spraw cyberbezpieczeństwa (w tym m.in. Prezes Urzędu Komunikacji Elektronicznej). Stosownie do brzmienia art. 66 ust. 3 ustawy o ksc, jedynie niektórzy członkowie Kolegium mogą być zastępowani przez upoważnionych przedstawicieli. Proponuje się zatem umożliwienie wzięcia udziału w pracach Kolegium także upoważnionym przedstawicielom nowych członków Kolegium - organów właściwych do spraw cyberbezpieczeństwa.	Uwaga uwzględniona
153.	Urząd Komisji Nadzoru Finansowego	Nowa propozycja	W ocenie UKNF do podmiotów finansowych niebędących podmiotami kluczowymi lub podmiotami ważnymi (z wyłączeniem podmiotów finansowych niebędących podmiotami kluczowymi lub podmiotami ważnymi, do których stosuje się uproszczone ramy zarządzania ryzykiem związanym z ICT), powinny znaleźć zastosowanie przepisy ustawy dotyczące polecenia zabezpieczającego oraz obowiązku wycofania sprzętu lub oprogramowania pochodzącego od dostawcy wysokiego ryzyka. Jak wskazano powyżej w kontekście projektowanego art. 8i UKSC, przepisy takie można uznać w ocenie UKNF za mające na celu ochronę bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego, przez co zgodnie z art. 1 ust. 3 rozporządzenia 2022/2554 stosowanie tego rodzaju obowiązków w stosunku do podmiotów finansowych nie będzie naruszać przepisów tego rozporządzenia. Co zaś istotne, instrumenty te przyczynią się do podniesienia poziomu cyberbezpieczeństwa na rynku finansowym i zminimalizują zagrożenia związane choćby z dostawcą sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka.	Uwaga uwzględniona Przepis zostanie dodany.

			Dodatkowo, powyższe rozwiązanie będzie spójne z podejściem zaproponowanym w ramach uwagi do projektowanego art. 8i UKSC, zgodnie z którym obowiązki te miałyby zastosowanie do podmiotów finansowych będących podmiotami kluczowymi lub ważnymi. W ocenie UKNF, zachowanie tego rodzaju spójnego podejścia w przypadku podmiotów o podobnej skali działalności prowadzonej na rynku finansowym, jest kluczowe dla zapewnienia wysokiego poziomu cyberbezpieczeństwa tego rynku. W przypadku bowiem braku wprowadzenia omawianego rozwiązania mogłoby dochodzić do sytuacji, w których sprzęt lub oprogramowanie dostawcy wysokiego ryzyka zobowiązane byłyby wycofać np. banki, ale już nie zakłady ubezpieczeń czy firmy inwestycyjne. Jednocześnie jednak, aby uwzględnić proporcjonalność nakładanych obowiązków oraz niższy poziom ryzyka, jaki na rynku finansowym wiąże się z funkcjonowaniem podmiotów o mniejszej skali działalności, proponowany jest brak stosowania omawianych przepisów do podmiotów finansowych niebędących podmiotami kluczowymi lub podmiotami ważnymi, do których stosuje się uproszczone ramy zarządzania ryzykiem związanym z ICT (dotyczy to przykładowo małych instytucji płatniczych, czy biur usług płatniczych). Jeśli chodzi o sprawowanie nadzoru nad przestrzeganiem omawianych obowiązków, to odpowiedzialny byłby w tym zakresie organ właściwy do spraw cyberbezpieczeństwa dla sektora bankowego i infrastruktury rynków finansowych. Jeśli chodzi zaś o przepisy dotyczące nadzoru i kontroli oraz kar pieniężnych nakładanych za naruszenia w/w obowiązków, to postulowane jest odpowiednie stosowanie przepisów rozdziału 11 i 14 UKSC. W związku z powyższym postulowany nowy przepis UKSC mógłby przyjąć następujące brzmienie: „Art. ... 1. Do podmiotów finansowych niebędących podmiotami kluczowymi lub podmiotami ważnymi stosuje się art. 67c, art. 67d, art. 67g, oraz art. 67h ustawy. 2. Obowiązków, o których mowa w ust. 1, nie stosuje się wobec podmiotów finansowych niebędących podmiotami kluczowymi lub podmiotami ważnymi, do których zastosowanie ma art. 16 ust. 1 rozporządzenia 2022/2554. 3. Nadzór nad wykonywaniem obowiązków, o których mowa w ust. 1, sprawuje organ właściwy do spraw cyberbezpieczeństwa dla sektora bankowego i infrastruktury rynków finansowych.	

Tabela uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

			4. Do nadzoru i kontroli wykonywania obowiązków wymienionych w ust. 1, oraz do kar pieniężnych nakładanych za naruszenia tych obowiązków, odpowiednio stosuje się przepisy rozdziałów 11 i 14 ustawy.”	
154.	Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy	Art. 67g	W art. 67g ust. 10 pkt 2 proponujemy doprecyzować, że nakaz ten odnosi się do planów dotyczących systemów teleinformatycznych, aby pozostać w spójności z pozostałą częścią tego przepisu. Z kolei w art. 67g ust. 10 pkt 7 proponujemy do adresów IP oraz adresów URL, które mogą być przedmiotem nakazu wprowadzenia ograniczenia ruchu sieciowego, dodać również domeny.	Uwaga uwzględniona
155.	Narodowy Bank Polski	Art. 67a oraz art. 67g	Ad art. 1 pkt 70 projektu ustawy w zakresie dodawanych art. 67a oraz art. 67g. Sugerujemy rozszerzenie zakresu wyłączenia podmiotowego wobec Narodowego Banku Polskiego sformułowanego w art. 67j o zagadnienia wskazane zarówno w art. 67a (rekomendacje Pełnomocnika) jak i w art. 67g (polecenia zabezpieczające). Uwzględnienie niniejszego postulatu skutkować będzie holistycznym podejściem do niezależności Narodowego Banku Polskiego pozostawiając decyzyjność odnoszącą się do podejmowanych działań po stronie banku centralnego. Proponujemy rozszerzenie zakresu art. 67j ust. 2 o przekazywanie informacji z zakresu rekomendacji pełnomocnika oraz poleceń zabezpieczających, co do których realizacja miałaby charakter fakultatywny.	Uwaga częściowo uwzględniona Uzupełniono w odniesieniu do poleceń. Stosowanie rekomendacji jest dobrowolne.
156.	Rzecznik Małych i Średnich Przedsiębiorców	Art. 67b, art. 67c i art. 67e	Art. 1 pkt 70 Projektu (dodający po art. 67 ustawy zmienianej art. 67a - 67k) określa m.in. (w art. 67b i kolejne) zasady oraz procedury postępowania w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. W odniesieniu do powyższego - zmiany wymagać mogą następujące projektowane regulacje: – dodawany do ustawy zmienianej art. 67b ust. 1 pkt 2 powinien przy określeniu kręgu przedsiębiorców telekomunikacyjnych podlegających regulacji posługiwać się pojęciami stosowanymi już w Projekcie - w tym przypadku mikroprzedsiębiorcy, – dodawany do ustawy zmienianej art. 67b ust. 4 zawiera niedopuszczalną dyskryminację mniejszych podmiotów przez uniemożliwienie im uprawnienia do wnioskowego przystąpienia do postępowania na prawach strony - należy całkowicie zaniechać uzależnienia uprawnienia od wartości przychodu lub obrotu podmiotu chcącego wstąpić do postępowania o uznanie za dostawcę wysokiego ryzyka, – dodawany do ustawy zmienianej art. 67b ust. 18 i 19 - ze względu na możliwe skutki, w szczególności dla podmiotów kluczowych i podmiotów ważnych, decyzji ministra	Uwaga nieuwzględniona Wyłączenia podmiotowe w zakresie strony postępowania mają zapewnić sprawność postępowania. Wyłączenie wniosku o ponowne rozpatrzenie sprawy jest konieczne – przyspieszy to możliwość odwołania się do sądu administracyjnego. Zróżnicowanie okresów wycofania sprzętu/oprogramowania od wielkości podmiotu spowoduje to, że duży podmiot będzie miał inny termin na wycofanie sprzętu, niż jego podwykonawca, co spowoduje kolejne zagrożenia.

Tabela uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

		ds. informatyzacji o uznaniu dostawcy sprzętu lub usługi za dostawcę wysokiego ryzyka - obligatoryjnie powinien przysługiwać wniosek o ponowne rozpatrzenie sprawy, – obowiązki oraz okresy zawarte w dodawanym art. 67c ust. 1,2 i 5 ustawy zmienianej dla podmiotów, o których mowa w art. 67b ust. 1 (dodawanym do ustawy zmienianej) — wymagają ponownej analizy oraz ewentualnie możliwości wydłużenia okresów użytkowania sprzętu lub usług pochodzących od dostawców uznanych za dostawców wysokiego ryzyka, – dodawany do ustawy zmienianej art. 67e ust. 2 powinien przewidywać możliwość doręczenia wyroku skarżącemu w treści i w zakresie umożliwiającym mu skuteczną ochronę swoich praw, dlatego treść tego przepisu wymaga zmiany. Uzasadnienie: W dodawanym do ustawy zmienianej art. 67b ust. 1 pkt 2 projektodawcy wprowadzają nową siatkę pojęciową - kryterium 10 min złotych przychodu w poprzednim roku obrotowym, mimo iż kwota ta może być nieco wyższa niż próg ekonomiczny dla mikroprzedsiębiorcy - to jednak warto zastanowić się nad użyciem powszechnie stosowanego pojęcia (także w Projekcie) oraz nad rozszerzeniem wyjątku także na małych przedsiębiorców (oba pojęcia w rozumieniu Rozporządzenia 651/2014, stosowanym w Projekcie). Wskazać należy, iż możliwy zasięg niezamierzonego stosowania sprzętu lub usług pochodzących od dostawców wysokiego ryzyka - w przypadku podmiotów będących mikroprzedsiębiorcami i małymi przedsiębiorcami jest ograniczony, a prawdopodobny wpływ na poziom cyberbezpieczeństwa adekwatnie mniejszy. Dodawany art. 67b ust. 4 ogranicza możliwość wstąpienia do postępowania o uznanie za dostawcę wysokiego ryzyka tylko dla przedsiębiorców komunikacji elektronicznej, którzy w poprzednim roku obrotowym uzyskali przychód z tytułu prowadzenia działalności telekomunikacyjnej w wysokości co najmniej dwudziestotysięcznej krotności przeciętnego wynagrodzenia w gospodarce narodowej wskazanego w ostatnim komunikacie Prezesa Głównego Urzędu Statystycznego, o którym mowa w art. 20 pkt 1 lit. a ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych. W pierwszej kolejności uprawnienie niniejsze powinno przysługiwać każdemu podmiotowi objętemu zakresem regulacji, czyjego interesu prawnego lub obowiązku dotyczy postępowanie albo kto żąda czynności organu ze względu na swój interes prawny lub obowiązek, zgodnie z ogólnymi zasadami postępowania	Nie można wprowadzić obowiązku doręczenia uzasadnienia wyroku zawierającego informacje niejawne.

			administracyjnego określonymi w art. 28 ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego. Powyższe pozwoli na skuteczną ochronę praw każdemu podmiotowi, na sytuację którego mogą mieć wpływ skutki postępowania. Z tego względu postulat ten jest zasadny. W odniesieniu do art. 67c ust. 1, 2 i 5 dodawanych do ustawy zmienianej wskazać należy, iż proponowane Projektem regulacje wymagają przekonstruowania. Projektodawcy pomijają skalę kosztów oraz utrudnień organizacyjnych związanych z całkowitym wycofaniem produktów lub usług pochodzących od dostawcy wysokiego ryzyka. Dotkliwość skutków proponowanych przepisów jest niemożliwa do oszacowania ze względu na nieograniczoną skalę konsekwencji, które zwłaszcza dla najmniejszych podmiotów mogą być niemożliwe do podołania. Według art. 66 ust. 1 ustawy Prawo Przedsiębiorców oraz kolejnych zawartych w Rozdziale 6 „Zasady opracowywania projektów aktów normatywnych z zakresu prawa gospodarczego oraz oceny ich funkcjonowania” - przed rozpoczęciem prac nad opracowaniem projektu aktu normatywnego określającego zasady podejmowania, wykonywania lub zakończenia działalności gospodarczej dokonuje się analizy możliwości osiągnięcia celu tego aktu normatywnego za pomocą innych środków oraz oceny przewidywanych skutków społeczno-gospodarczych, w tym oceny wpływu na sytuację mikroprzedsiębiorców, małych i średnich przedsiębiorców oraz analizy zgodności projektowanych regulacji z przepisami (przywołanej) ustawy. Obowiązkiem Projektodawcy nie uczynili zadość, w szczególności biorąc pod uwagę istotne poszerzenie kręgu podmiotów, których regulacje zawarte w Projekcie będą mogły dotyczyć. Podkreślić należy, iż w przypadku stwierdzenia wpływu projektu aktu normatywnego na sytuację mikroprzedsiębiorców, małych i średnich przedsiębiorców, przy opracowaniu projektu aktu normatywnego należy dążyć do proporcjonalnego ograniczenia obowiązków wobec tych przedsiębiorców (art. 68 ustawy Prawo przedsiębiorców). Dodawany do ustawy zmienianej art. 67e ust. 2 wprowadza możliwość doręczenia skarżącemu wyroku z ograniczeniem treści jego uzasadnienia. Regulacja taka jest niedopuszczalna i wymaga zmiany, gdyż uniemożliwia skarżącemu skuteczną ochronę swoich praw i stanowi zaprzeczenie realizowanej przez Rzeczypospolitą Polską idei demokratycznego państwa prawa. Ochrona tej wartości nie może się odbywać przez jej zaprzeczenie, do czego dążą projektodawcy. Omawiany przepis powinien przewidywać możliwość doręczenia wyroku skarżącemu w treści i w zakresie umożliwiającym mu skuteczną ochronę	

Tabela uwag zgłoszonych w ramach opiniowania do *projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)*

			swoich praw, przy jednoczesnej ochronie ewentualnych informacji niejawnych ważnych dla bezpieczeństwa państwa, dlatego treść tego przepisu wymaga postulowanej zmiany.	
157.	Krajowa Rada Radiofonii i Telewizji	Art. 67b ust. 2	W projektowanym przepisie art. 67b ust. 2 ustawy, dotyczącym postępowania w sprawie uznania za dostawcę wysokiego ryzyka, wyłączono stosowanie przepisu art. 31 Kodeksu postępowania administracyjnego, natomiast w przepisie art. 67b ust. 4, także dotyczącym postępowania w sprawie uznania za dostawcę wysokiego ryzyka, nakazano odpowiednie stosowanie przepisów art. 31 § 2 i 3 Kpa. Ponadto, jeśli wyłączenie stosowania określonych przepisów Kpa, zawarte w art. 67b ust. 2 ustawy, argumentuje się kwestiami bezpieczeństwa narodowego, to zasadne jest rozważenie czy powyższe wyłączenie jest kompletne i czy ograniczeniu stosowania nie powinny podlegać także przepisy art. 9, 10 i 73 Kpa.	Uwaga uwzględniona Przepis zostanie poprawiony. Co do zasady wyłączone jest stosowanie art. 31 KPA, natomiast w drodze wyjątku w art. 67b ust. wprowadzono odpowiednie stosowanie przepisów art. 31 § 2 i 3 KPA.
158.	Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy	Art. 67b ust. 12 oraz art. 69 ust. 2	Dodatkowo rekomendujemy zachować spójność merytoryczną na poziomie całego projektu nowelizacji ustawy o KSC tj. w art. 67b ust. 12 pkt 1 mówiącym o sporządzeniu opinii w procedurze wszczynania postępowania w sprawie uznania dostawcy sprzętu lub oprogramowania, które są wykorzystywane przez podmioty kluczowe lub podmioty ważne lub przedsiębiorców telekomunikacyjnych, za dostawcę wysokiego ryzyka, wskazuje się, że opinia powinna uwzględniać „ <i>certyfikaty wydane dla produktów ICT, usług ICT lub procesów ICT, (...) wydane w ramach europejskich programów certyfikacji cyberbezpieczeństwa</i> ”. Z kolei w art. 69 ust. 2 pkt 1 i 2 mówiącym o Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej i elementach, które powinny być uwzględnione przy jej określaniu pomija się procesy ICT - „ <i>Przy opracowaniu strategii uwzględnia się: 1) rozwiązania dotyczące cyberbezpieczeństwa w łańcuchu dostaw <u>produktów ICT i usług ICT</u> wykorzystywanych przez podmioty do świadczenia usług; 2) rozwiązania dotyczące uwzględniania w zamówieniach publicznych wymogów związanych z cyberbezpieczeństwem w odniesieniu do <u>produktów ICT i usług ICT</u> oraz specyfikacji tych wymogów na potrzeby takich zamówień, w tym w odniesieniu do certyfikacji cyberbezpieczeństwa, szyfrowania oraz wykorzystywania produktów z zakresu cyberbezpieczeństwa opartych na otwartym oprogramowaniu;</i> ”. Należy podkreślić, że procesy ICT są równie istotne w zabezpieczeniu łańcucha dostaw, jak produkty czy usługi. Podobnie rzecz się ma w zamówieniach publicznych szczególnie na potrzeby państwa. W związku z tym rekomendujemy, w całym projekcie nowelizacji ustawy o KSC, wymieniać w kontekście certyfikacji	Uwaga uwzględniona Ujednolicono przepisy w tym zakresie. Należy równocześnie zauważyć, że sama dyrektywa NIS2 nie posługuje się jednolicie tymi pojęciami, np. zgodnie z definicją podatności dotyczą one jedynie produktów i usług ICT. W takich przypadkach priorytetem jest prawidłowa implementacja przepisów dyrektywy.

Tabela uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

			cyberbezpieczeństwa, jak i samego cyberbezpieczeństwa, jako nierozdzielne trio produkty, usługi i procesy ICT.	
159.	Krajowa Rada Radiofonii i Telewizji	Art. 67b ust. 17	Należy rozważyć czy w projektowanym przepisie art. 67b ust. 17 nie powinno zostać zawarte ograniczenie dotyczące publikacji decyzji wyłącznie w tej części, która nie zawiera informacji niejawnych – analogicznie do ograniczenia wyrażonego w przepisie art. 67e ust. 2 ustawy, dotyczącego odpisu wyroku sądu administracyjnego doręczanego skarżącemu. Ewentualnie, można rozważyć czy dla osiągnięcia celu art. 67b ust. 17 wystarczająca nie okaże się publikacja samej sentencji decyzji.	Uwaga wyjaśniona W tej kwestii znajdują zastosowanie ogólne przepisy o ochronie informacji niejawnych.
160.	Najwyższa Izba Kontroli	Art. 67b	W projekcie uregulowano mechanizm pozwalający na identyfikację i potencjalne wykluczenie dostawców uznanych za dostawców wysokiego ryzyka. Kontrowersje mogą budzić przy tym rozwiązania, których konsekwencją dla przedsiębiorców będzie konieczność wycofania sprzętu i oprogramowania uznanego za niebezpieczne. Decyzje uprawnionych podmiotów będą miały walor natychmiastowej wykonalności. Nowelizacja KSC przewiduje również nową kompetencję dla ministra właściwego ds. informatyzacji do wydania polecenia zabezpieczającego w drodze decyzji administracyjnej, która będzie miała charakter generalny. Powodować może to zagrożenie dla ochrony tajemnic ustawowo chronionych, jak tajemnica kontrolerska ² . W ocenie Izby przy prowadzeniu procedury uznania za dostawcę wysokiego ryzyka niezwykle istotne jest zatem wprowadzenie mechanizmów umożliwiających ochronę ww. dóbr, z uwzględnieniem bezpieczeństwa narodowego.	Uwaga wyjaśniona Zdaniem MC w przypadku dostawców wysokiego ryzyka, przeważa ochrona bezpieczeństwa państwa nad innymi wartościami konstytucyjnymi.
161.	Rzecznik Praw Obywatelskich	Art. 67b i art. 67c	Największe wątpliwości Rzecznika budzi procedura wynikająca z art. 67b-67c projektu nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa (art. 1 pkt 70, s. 69 i n.). W ramach tej procedury minister ds. informatyzacji będzie mógł w drodze decyzji administracyjnej uznać dostawcę określonego sprzętu lub oprogramowania za "dostawcę wysokiego ryzyka" (art. 67b ust. 15), która będzie miała <i>ex lege</i> rygor natychmiastowej wykonalności (art. 67b ust. 18). Skutkiem decyzji będzie nakaz pozbycia się przez przedsiębiorców i inne instytucje uznane za "podmioty kluczowe" lub "podmioty ważne" tych sprzętów i oprogramowani (art. 67c ust. 1) Do postępowania nie będzie mógł przystąpić każdy przedsiębiorca, który będzie zmuszony do wymiany sprzętu, ale tylko najbogatsi tylko przedsiębiorca komunikacji elektronicznej, który w poprzednim roku obrotowym uzyskał przychód z tytułu prowadzenia działalności telekomunikacyjnej w wysokości co najmniej dwudziestotysięcznej krotności przeciętnego wynagrodzenia (art. 67b ust. 4). Od decyzji przysługuje co prawda skarga do WSA, ale już ustawodawca wykluczył	Uwaga wyjaśniona Z uwagi na charakter postępowania należy wprowadzić pewne wyłączenia. Nie jest możliwe uczestnictwo wszystkich podmiotów wykorzystujących sprzęt dostawcy w postępowaniu. Wyłączenia pewnych praw procesowych w postępowaniu sądowoadministracyjnym są wzorowane na ustawie o ochronie informacji niejawnych i są związane z zapewnieniem ochrony informacji niejawnych.

Tabela uwag zgłoszonych w ramach opiniowania do *projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)*

			możliwość przeprowadzenia rozprawy (art. 67e ust. 1), a wyrok z pełnym uzasadnieniem ma dostać tylko minister (art. 67e ust. 2), natomiast skarżący jedynie uzasadnienie w okrojonej wersji. W tym zakresie, ograniczenia te mogą naruszać prawo do uczciwego procesu sądowego.	
162.	Rzecznik Praw Obywatelskich	Art. 67b i art. 67c	Powyższa procedura stanowi też nieproporcjonalne ograniczenie wolności gospodarczej dla podmiotów w Polsce. Możliwe są przypadki, gdy minister zakwalifikuje jakiś sprzęt jako niebezpieczny, przedsiębiorca wstrzyma jego dystrybucję i wymieni, ponosząc koszty, a po rozpoznaniu sprawy przez WSA i NSA okaże się, że decyzja ministra była bezprawna. Przedsiębiorca formalnie wygra, ale utraconych korzyści z wstrzymanej dystrybucji oraz wydatków na nowych sprzęt nikt mu nie zwróci.	Uwaga wyjaśniona Przepisy Kodeksu cywilnego przewidują odpowiedzialność Skarbu Państwa za decyzję wydaną niezgodnie z prawem.
163.	Rzecznik Praw Obywatelskich	Art. 67b	Rygor natychmiastowej wykonalności <i>ex lege</i> może zostać uznany za niezgodny z zasadą proporcjonalności (zakazem nadmiernej ingerencji - art. 2 Konstytucji RP), a procedura odwoławcza jest niezgodna z prawem do skutecznego środka odwoławczego (art. 13 EKPC, art. 45 Konstytucji RP).	Uwaga wyjaśniona Rygor natychmiastowej wykonalności jest związany z tym, że dostawca wysokiego ryzyka stwarza poważne zagrożenie dla bezpieczeństwa narodowego. Poza tym sąd administracyjny będzie mógł uchylić ten rygor zgodnie z PPSA.
164.	Rzecznik Praw Obywatelskich	Art. 67b i art. 67c	W projektowanej procedurze należałoby: – zagwarantować możliwość udziału wszystkim zainteresowanym przedsiębiorcom, którzy mogą zostać zmuszeni do wymiany sprzętu. Żeby nie tamować przebiegu postępowania w przypadku dużej liczby chętnych, można ograniczyć ich prawa proceduralne, ale powinni mieć przynajmniej możliwość jednorazowego przedstawienia stanowiska, – zapewnić możliwość organizacjom pozarządowym przedstawiania opinii, a może też i organom rzecznikowskim - RPO i Rzecznikowi Małych i Średnich Przedsiębiorców, – znieść natychmiastową wykonalność <i>ex lege</i> . Organ powinien każdorazowo o tym decydować na zasadach ogólnych, z uwzględnieniem okoliczności indywidualnych, – zapewnić równość stron w postępowaniu przed WSA, a także zapewnić możliwość przeprowadzenia rozprawy. Jeśli projektodawcom zależy na czasie, to można zawsze wprowadzić instrukcyjny termin na rozpoznanie sprawy, ale nie powinno się blankietowo wyłączać jawności postępowania.	Uwaga wyjaśniona Stanowisko w postępowaniu będą mogły przedstawić organizacje społeczne. Rygor natychmiastowej wykonalności jest związany z tym, że dostawca wysokiego ryzyka stwarza poważne zagrożenie dla bezpieczeństwa narodowego. Poza tym sąd administracyjny będzie mógł uchylić ten rygor zgodnie z PPSA.

Tabela uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

165.	Rzecznik Praw Obywatelskich	Art. 67g i art. 67h	Podobne problemy proceduralne występują w przypadku tzw. poleceń zabezpieczających ministra - art. 67g-67h na s. 75 i n.	Uwaga wyjaśniona Uwaga jest zbyt ogólnikowa, aby do niej się odnieść.
166.	Prezes Urzędu Komunikacji Elektronicznej	Art. 67c ust. 2	Art. 1 pkt 70 w zakresie dotyczącym projektowanego art. 67c ust. 2 ustawy o ksc – w odniesieniu do niniejszego przepisu (dotyczącego kwestii wycofywania w ciągu 4 lat, przez przedsiębiorców telekomunikacyjnych, o których mowa w projektowanym art. 67b ust. 1 pkt 2 ustawy o ksc, typów produktów ICT, rodzajów usług ICT, konkretnych procesów ICT wskazanych w decyzji i określonych w wykazie kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług w załączniku nr 3 do ustawy o ksc) proponuje się jego uszczegółowienie w sposób, z którego wynikałoby, iż wycofywanie, o którym mowa w tym przepisie, powinno być dokonywane: a) niezwłocznie, jednakże nie później niż w ciągu 12 miesięcy, w przypadkach: – obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej przedsiębiorcy telekomunikacyjnego (ujętych w jednolitym wykazie, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2023 r. poz. 122)), – typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT używanych w celu wykonywania zadań i obowiązków na potrzeby systemu kierowania bezpieczeństwem narodowym, w tym obroną państwa (na zasadach określonych w planach, decyzjach lub umowach zawartych między przedsiębiorcami telekomunikacyjnymi a uprawnionymi podmiotami), b) w pozostałych przypadkach – sukcesywnie, w okresie od 1 roku do 4 lat, z uwzględnieniem pierwszeństwa obszarów o największej gęstości zaludnienia. Niniejsza propozycja jest zgodna z wymaganiami określonymi na potrzeby aukcji 5G, które uzyskały w dniu 23 marca 2023 r. pozytywną opinię Kolegium do Spraw Cyberbezpieczeństwa.	Uwaga nieuwzględniona Projektodawca chce utrzymać kompromis, jakim są obecne postanowienia tego przepisu.
167.	Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy	Art. 67g	Proponujemy, aby polecenie zabezpieczające było doręczane za pomocą S46; w tym celu konieczne jest dokonanie zmiany w brzmieniu art. 67g ust. 16.	Uwaga częściowo uwzględniona Informacja o poleceniu zabezpieczającym może być udostępniana w S46, natomiast z racji tego, że jest to akt administracyjny o charakterze generalnym musi być on publikowany w dzienniku urzędowym.

Tabela uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

168.	Urząd Komisji Nadzoru Finansowego	Art. 70	W art. 70 ust. 1 UKSC po wyrazach „właściwymi kierownikami urzędów centralnych” postuluje się dodanie przecinka oraz wyrazów „a także właściwym organem w rozumieniu rozporządzenia 2022/2554”. Zgodnie z wytycznymi Komisji dotyczącymi stosowania art. 4 ust. 1 i 2 dyrektywy (UE) 2022/2555 (NIS 2) (2023/C 328/02) państwa członkowskie powinny uwzględniać sektor finansowy w swoich strategiach cyberbezpieczeństwa, a odpowiednie przepisy określone w art. 7 dyrektywy 2022/2555 powinny nadal obowiązywać w przypadku sektorów, podsektorów i rodzajów podmiotów, w odniesieniu do których obowiązują sektorowe akty prawne Unii w rozumieniu art. 4 dyrektywy 2022/2555. Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej będzie wpływała więc na cyberbezpieczeństwo rynku finansowego, co uzasadnia udział właściwego organu w rozumieniu rozporządzenia 2022/2554 w jej opracowywaniu, pomimo stosowania w stosunku do podmiotów finansowych przepisów rozporządzenia 2022/2554 w obszarze środków zarządzania ryzykiem w cyberbezpieczeństwie i zgłaszania poważnych incydentów, a także powiązanych z nimi przepisów rozporządzenia 2022/2554 dotyczących nadzoru i egzekwowania przepisów. Rozwiązanie takie zapewni również udział właściwego organu w rozumieniu rozporządzenia 2022/2554 w uzgadnianiu kwestii w ramach Strategii, które dotyczyć będą obszaru relacji dyrektywy 2022/2555 (w tym przepisów ją implementujących) do rozporządzenia 2022/2554.	Uwaga uwzględniona
169.	Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy	Art. 72b	W proponowanym art. 72b zwracamy się z prośbą o ponowną analizę pkt 3. Aktualna propozycja sugeruje integrację Krajowego Planu z Narodowym Planem Ochrony Infrastruktury Kryzysowej, co wydaje się daleko idącą zmianą. Zwracamy również uwagę, że w planowanej treści tego przepisu są pewne nieścisłości – brak informacji, co należy rozumieć pod pojęciem „rodzaje krytycznej infrastruktury informatycznej” (pkt 6), „zarządzanie incydentami i zarządzenie kryzysowe w cyberbezpieczeństwie na dużą skalę”. Część z tych wątpliwości wynika z bezpośredniego brzmienia dyrektywy 2022/2555, jednak wydaje się, że w ustawie wdrażającej dyrektywę do polskiego systemu prawnego powinno znaleźć się wyjaśnienie tych kwestii, by móc rozróżnić kwestie wprowadzane w tym przepisie od stanu uregulowanego w ustawie z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2023 r. poz. 122).	Uwaga uwzględniona Zmieniono brzmienie art. 72b, tak aby wyeliminować wskazane wątpliwości interpretacyjne.
170.	Rzecznik Małych i Średnich Przedsiębiorców	Art. 73	Art. 1 pkt 74 Projektu wprowadza nowy system kar, w tym kar pieniężnych za naruszenie regulacji wynikających z Projektu. Ze względu na złożoną istotę będącą przedmiotem projektowanych regulacji oraz znaczne poszerzenie kręgu podmiotów	Uwaga nieuwzględniona Kryteria, od których należy uzależniać wymiar kary zostały

Tabela uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

			nimi objętych, postuluje się uzupełnienie treści art. 1 pkt 74 Projektu o obligatoryjne uzależnienie wysokości ewentualnie nakładanych kar od wielkości podmiotu oraz proporcjonalne ograniczenie wysokości kar dla mikroprzedsiębiorców i małych przedsiębiorców. Ze względu na konieczność wdrożenia przez wiele podmiotów, w tym również mniejszych, które wcześniej nie podlegały tego typu regulacjom – nowych rozwiązań oraz związanego z tym wysiłku organizacyjnego i finansowego – zasadny jest postulat, aby w ciągu pierwszych 6 miesięcy od wejścia w życie regulacji wynikających z projektu, w pierwszej kolejności pouczać przedsiębiorców, a nie karać finansowo.	bezpośrednio wskazane w dyrektywie NIS2. Jednocześnie należy zwrócić uwagę na fakt, że ustawa przewiduje okres dostosowawczy 6 miesięczny, w którym nie obowiązują przepisy o karach.
171.	Urząd Komisji Nadzoru Finansowego	Art. 73a	W ocenie UKNF zakres możliwości nałożenia na kierownika podmiotu kluczowego lub podmiotu ważnego kary pieniężnej powinien być skorelowany z projektowanym art. 8c ust. 1 UKSC, zgodnie z którym kierownik ten ponosi odpowiedzialność za wykonywanie obowiązków w zakresie cyberbezpieczeństwa przez podmiot kluczowy lub podmiot ważny, o których mowa w art. 7, art. 8, art. 8d, art. 8e, art. 8f ust. 2, art. 8h, art. 9–11 i art. 15. W przeciwnym razie odpowiedzialność ta może przybierać charakter iluzoryczny, jako pozbawiona w niektórych przypadkach sankcji. Dotyczy to w szczególności odpowiedzialności za brak audytu bądź jego nieterminowe przeprowadzenie.	Uwaga uwzględniona Przepis został doprecyzowany o odpowiedzialność za niewykonanie obowiązków o których mowa w art. 15. Pozostałe obowiązki zostały już przewidziane w przepisie i pokrywają się z odpowiedzialnością kierownika podmiotu określoną na podstawie art. 8c ust. 1. Różnica w odwołaniu wynika z konieczności zapewnienia najwyższej precyzji przy określaniu przepisów o charakterze represyjnym (przepis o karze pieniężnej). Z tego względu zdecydowano się szczegółowo wskazać ustępy przy właściwych artykułach – wśród nich wskazane są obowiązki podmiotów, za które odpowiada również kierownik. Odwołanie przy sankcji karnej do całości przepisu byłoby nieprecyzyjne z uwagi na to, że przepisy te mają niekiedy charakter techniczny lub odnoszą się do uprawnień i obowiązków ministra właściwego do spraw informatyzacji czy innych organów

Tabela uwag zgłoszonych w ramach opiniowania do *projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)*

				właściwych do spraw cyberbezpieczeństwa.
172.	Narodowy Bank Polski	Art. 73 ust. 1	Ad. art. 1 pkt 74 lit. a projektu ustawy w zakresie zmiany brzmienia art. 73 ust. 1. Kara pieniężna, o której mowa w ust. 1–3, może być wymierzona w kwocie nie większej niż 600% otrzymywanego przez ukaranego wynagrodzenia obliczanego według zasad obowiązujących przy ustalaniu ekwiwalentu pieniężnego za urlop. Przedstawiony wskaźnik procentowy nie precyzuje przedziału czasowego za jaki otrzymywane było wynagrodzenie, a zatem pojawia się dowolność interpretacji w tym zakresie. Powyższe nie jest w naszej ocenie właściwe, w związku z czym sugerujemy doprecyzowanie zapisu.	Uwaga nieuwzględniona W przedmiocie wynagrodzenia kierownika podmiotu wskazać należy, że podobne instytucje funkcjonują już w obrocie prawnym. Jednakże nie doprecyzowują okresu otrzymywanego wynagrodzenia. W ocenie projektodawcy nie zachodzi potrzeba dookreślenia tego w przepisie – organ będzie brał pod uwagę wynagrodzenie otrzymywane obecnie, które zostanie ustalone na podstawie dokumentacji przekazanej przez kierownika podmiotu.
173.	Prezes Głównego Urzędu Statystycznego	Art. 74 ust. 3	W art. 74 ust. 3 otrzymuje brzmienie: „3. Wpływy z tytułu kar pieniężnych, o których mowa w art. 73 i art. 73a, stanowią przychód Funduszu Cyberbezpieczeństwa, o którym mowa w art. 2 ustawy z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa.” Projekt ustawy (poza środkami dla CSIRT MON, CSIRT NASK, CSIRT GOV, organach właściwych do spraw cyberbezpieczeństwa, CSIRT sektorowych) nie przewiduje żadnych środków dla podmiotów publicznych, które uznane zostaną za podmioty kluczowe lub ważne. W związku z niskim poziomem zarobków w administracji publicznej, w porównaniu do podmiotów komercyjnych, ogromnym problemem dla publicznych podmiotów jest pozyskanie pracowników wykwalifikowanych w zakresie cyberbezpieczeństwa, bezpieczeństwa informacji, ochrony danych osobowych. Mimo, że w roku 2022 podjęto prace nad projektem nowelizacji ustawy z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa, w którym między innymi rozszerzono katalog podmiotów które uzyskiwałyby środki z tego funduszu (w tym GUS i inne jednostki	Uwaga nieuwzględniona W ramach niniejszego projektu skupiono się na zmianach w ustawie o krajowym systemie cyberbezpieczeństwa, a zmiany w innych ustawach są wprowadzane tylko gdy wynika to z konieczności zapewnienia spójności rozwiązań. W związku z tym jedyne zmiany w ustawie o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa są konsekwencją zmian w ustawie o krajowym systemie cyberbezpieczeństwa. Zaproponowana regulacja jest już wystarczająco rozbudowana i

Tabela uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

			służ statystyki publicznej) projekt nie został sfinalizowany i nie trafił pod obrady sejmu. (Numer projektu: UD390) https://legislacja.rcl.gov.pl/projekt/12360152/katalog/12882662#12882662) Obecnie w obliczu wdrażania dyrektywy NIS 2 jeszcze bardziej niż w 2022 roku potrzebne jest wprowadzenie systemowych rozwiązań, zapewniających podmiotom publicznym środki finansowe na cyberbezpieczeństwo i bezpieczeństwo informacji. Środki powinny być przeznaczone nie tylko na wynagrodzenia pracowników, ale też na dofinansowanie zakupu infrastruktury i oprogramowania oraz na usługi zewnętrzne np. szkolenia, testy bezpieczeństwa i audyty bezpieczeństwa informacji.	niecelowe byłoby rozszerzanie jej o nowe obszary merytoryczne. Dokładna analiza zapotrzebowania poszczególnych podmiotów na świadczenie teleinformatyczne, zostanie przeprowadzona w toku ewentualnych prac legislacyjnych nad osobnym projektem ustawy. Jednocześnie uprzejmie informuję, że w ramach inwestycji C3.1.1 Cyberbezpieczeństwo – CyberPL, infrastruktura przetwarzania danych i dostarczania usług cyfrowych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo – Komponent Cyberbezpieczeństwo (subinwestycja C3.1.1.1), planowane jest uruchomienie czterech projektów dedykowanych dla wybranych grup podmiotów krajowego systemu cyberbezpieczeństwa, w tym dla jednostek sektora finansów publicznych. Aktualnie trwają prace do przygotowania naborów, z uwzględnieniem ich celu określonego w Krajowym Planie Odbudowy i zwiększania odporności. Docelowe grupy odbiorców wsparcia będą wynikały bezpośrednio z tych założeń. Uruchamianie naborów dla tych projektów planowane jest

Tabela uwag zgłoszonych w ramach opiniowania do *projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)*

				sukcesywnie w kolejnych kwartałach bieżącego roku.
UWAGI do przepisów przejściowych i przepisów końcowych				
174.	Prezes Urzędu Ochrony Danych Osobowych	Art. 3	W art. 3 projektu projektowana jest zmiana art. 299i § 1 ustawy z dnia 29 sierpnia 1997 r. – Ordynacja podatkowa (Dz. U. z 2023 r. poz. 2383 i 2760), dotycząca udostępniania danych przez szefa Krajowej Administracji Skarbowej organom właściwym do spraw cyberbezpieczeństwa oraz Zespołowi Reagowania na Incydenty Bezpieczeństwa Komputerowego. Jeśli wśród udostępnianych danych znajdują się dane osobowe, przepisy powinny wskazywać szczegółowo na cel, zakres i sposób przetwarzania. Prawodawca określił również, że udostępnianie danych odbywać się ma „w drodze teletransmisji” – jeśli zatem przedmiotem udostępnienia będą też dane osobowe wymaga to dookreślenia wymagań technicznych, dookreślenia ról w procesie przetwarzania danych, w tym podmiotu odpowiedzialnego za bezpieczeństwo i zgodność przetwarzanych danych z prawem. Projektodawca przeprowadzić powinien również test prywatności, w tym ocenę skutków dla ochrony danych w zakresie udostępniania danych.	Uwaga wyjaśniona Dane osobowe mogą się tutaj znaleźć w nazwie (firmie) podmiotu. Cel przepisu został już w nim wskazany. Organ właściwy do spraw cyberbezpieczeństwa stanie się administratorem danych osobowych uzyskanych w trakcie tej teletransmisji. Teletransmisja musi być zgodna z art. 8 ustawy o krajowym systemie cyberbezpieczeństwa, oraz z Rozporządzeniem Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych. Dublowanie przepisów jest niewskazane.
175.	Prezes Urzędu Komunikacji Elektronicznej	Art. 5	Art. 5 wprowadzający zmiany w ustawie z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne – należy zauważyć, że uchylenie ustawy – Prawo telekomunikacyjne przewidziano w projekcie ustawy – Przepisy wprowadzające ustawę – Prawo komunikacji elektronicznej (zob. art. 66 ust. 1 tego projektu), który wpłynął do Sejmu w dniu 21 maja 2024 r. W związku z powyższym konieczne będzie skorelowanie brzmienia przepisów opiniowanego projektu ustawy (art. 5 oraz innych, które odsyłają do przepisów uchylanej ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne) z przepisami projektu ustawy – Prawo komunikacji elektronicznej zastępującej ustawę z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne, a także z regulacjami projektu ustawy – Przepisy wprowadzające ustawę – Prawo	Uwaga uwzględniona

Tabela uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

			komunikacji elektronicznej odraczającymi utratę mocy m. in. przepisów działu VIIa ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne do czasu wejścia w życie przepisów wdrażających dyrektywę NIS 2 (zob. art. 66 ust. 3 projektu ustawy – Przepisy wprowadzające ustawę – Prawo komunikacji elektronicznej). Na marginesie należy zauważyć, że także samo uchylenie przepisów działu VIIa wiąże się z konsekwencjami w postaci konieczności dokonania zmian przepisów ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne, które odsyłają do uchylanych w tym dziale jednostek redakcyjnych.	
176.	Prezes Urzędu Komunikacji Elektronicznej	Art. 5	Art. 5 pkt 1 w zakresie dotyczącym projektowanego art. 10 ust. 5a ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne – w dodawanym ust. 5a w art. 10 ustawy – Prawo telekomunikacyjne zaproponowano, aby dane, o których mowa w art. 7 ust. 2 pkt 1–17 ustawy o ksc, były przekazywane „do wniosku o wpis do rejestru”. Należy zaznaczyć, że kwestie wpisu do rejestru przedsiębiorców telekomunikacyjnych regulują przepisy dyrektywy Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiającej Europejski kodeks łączności elektronicznej, zwanej dalej „EKŁE”, której wdrożenie przewidziano w projekcie ustawy – Prawo komunikacji elektronicznej oraz projekcie ustawy – Przepisy wprowadzające ustawę – Prawo komunikacji elektronicznej (wpłynęły do Sejmu w dniu 21 maja 2024 r.). Należy podkreślić, że projektowany obowiązek „przekazywania do wniosku o wpis do rejestru” danych innych niż zezwala na to art. 12 ust. 3 EKŁE jest niezgodny z tym przepisem. EKŁE określa bowiem wyczerpujący katalog danych, jakich można wymagać przy wpisie do rejestru podkreślając, że państwa członkowskie nie mogą nakładać żadnych dodatkowych ani odrębnych wymogów w zakresie zgłaszania (wpisu do rejestru). W konsekwencji tego, że część danych określonych w ust. 2 pkt 1–17 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa wykraczać będzie poza określone dyrektywą ramy (np. art. 7 ust. 2 pkt 7, 9, 13 -17), uznać należy, że projektowany art. 10 ust. 5a jest niezgodny z przepisami art. 12 EKŁE.	Uwaga uwzględniona Przepis zostanie usunięty.
177.	Rzecznik Małych i Średnich Przedsiębiorców	Art. 7	Należy całkowicie zaniechać zmiany objętej art. 7 Projektu. Postulat usunięcia art. 7 z treści projektu. Uzasadnienie: W pierwszej kolejności treść zaproponowanej zmiany nie koresponduje z art. 1 pkt 58 Projektu, w dalszej kolejności wskazać należy na bezpodstawne rozszerzenie wyłączenia stosowania przepisów o prowadzeniu więcej niż jednej kontroli.	Uwaga nieuwzględniona Należy zwrócić uwagę na fakt, że w ustawie – Prawo przedsiębiorców, w przepisie zmienianym niniejszą ustawą zawarte są także inne przypadki, kiedy ustawy – Prawo przedsiębiorców się nie stosuje.

Tabela uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

			Proponowana treść wskazanego wyżej przepisu ma charakter nadregulacji i będzie sprzeczna z fundamentalnymi zasadami ustawy Prawo przedsiębiorców (Konstytucja Biznesu). Art. 45 ust. 1 i 2 ustawy Prawo przedsiębiorców stanowi: „Kontrola działalności gospodarczej przedsiębiorców jest przeprowadzana na zasadach określonych w niniejszej ustawie, chyba że zasady i tryb kontroli wynikają z ratyfikowanych umów międzynarodowych albo bezpośrednio stosowanych przepisów prawa Unii Europejskiej”. Jedynie „w zakresie nieuregulowanym w niniejszym rozdziale stosuje się odrębne przepisy.”. Odrębne przepisy mają służyć przede wszystkim do wskazania zakresu przedmiotowego kontroli działalności gospodarczej przedsiębiorcy oraz organów upoważnionych do jej przeprowadzenia – jak stanowi art. 45 ust. 3 ustawy Prawo przedsiębiorców. Znaczenie Prawa przedsiębiorców wielokrotnie było podkreślane przez Radę Ministrów, która projektowi temu nie bez przyczyny nadała robocze miano Konstytucji Biznesu – co miało dodatkowo podkreślać rangę wydanych przepisów i które miały mieć walor porządkujący najistotniejsze zagadnienia z punktu widzenia prowadzenia działalności gospodarczej. Powyższe uregulowania jasno wskazują, że wszystkie przepisy szczególne dotyczące sposobu kontroli przedsiębiorców zawarto w ustawie Prawo przedsiębiorców (Konstytucja Biznesu). Wydawanie kolejnych przepisów, w kwestiach uregulowanych już w Rozdziale 5 (ograniczenia kontroli działalności gospodarczej) ustawy Prawo przedsiębiorców będzie mogło stanowić zachętę do naruszania przepisów tej ustawy. Rozpraszanie przepisów o ograniczaniu uprawnień podczas kontroli przedsiębiorców, niezależnie od tego, że jest zasadniczo niewłaściwe metodologiczne – to w sposób nieunikniony, jak wskazuje praktyka poszczególnych resortów kształtowania tych przepisów na własne potrzeby – prowadzi do trudnych, zawiłych, nieprzyswajalnych i chaotycznych regulacji. Proponowana w Projekcie, niewłaściwa metoda regulacji, może stanowić pretekst do obchodzenia przepisów ustawy Prawo Przedsiębiorców (Konstytucji Biznesu) przez organy kontroli i być nie tyle użytecznym i niezbędnym narzędziem do zwalczania działań niepożądanych, co elementem kształtującym szkodliwą praktykę legislacyjną i środkiem blokującym rozwój przedsiębiorczości. Z przytoczonych powodów – wnoszę o zaniechanie zmiany zawartej w art. 7 Projektu.	Tym samym projektowana ustawa nie wprowadza precedensowego wyłomu z dotychczasowej praktyki, a jedynie dokonuje zmiany koniecznej dla zapewnienia skuteczności prowadzonej kontroli. Jest to niezwykle istotne z uwagi na zakres przedmiotowy ustawy oraz jej istotne znaczenie dla bezpieczeństwa państwa.
178.	Rzecznik Praw Obywatelskich	Art. 9	Wnoszę o dołączenie Biura Rzecznika Praw Obywatelskich do listy podmiotów uprawnionych do stosowania ustawy z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa	Uwaga nieuwzględniona W ramach niniejszego projektu skupiono się na zmianach w ustawie

Tabela uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

	(Dz. U. z 2023 r. poz. 667). Zmiana ta mogłaby polegać na dopisaniu w art. 5 pkt 2) tej ustawy Biura Rzecznika Praw Obywatelskich, co upoważniałoby pracowników Biura do pobierania dodatku do wynagrodzenia z tytułu realizacji zadań związanych z cyberbezpieczeństwem. W sprawie dołączenia pracowników Biura Rzecznika Praw Obywatelskich korespondencja z Ministerstwem Cyfryzacji jest już prowadzona od marca 2022 r. (pisma z dnia 1 marca 2022 r., z dnia 15 grudnia 2022 r. i z dnia 15 grudnia 2023 r. – kopie w załączeniu), w której w sposób jednoznaczny wykazano, że uwagi na okoliczność, iż Rzecznik Praw Obywatelskich wchodzi w skład krajowego systemu bezpieczeństwa (art. 4 pkt 7 nowelizowanej ustawy) i w tym zakresie wykonuje zadania publiczne jako podmiot kluczowy, to niezrozumiałe jest pozbawienie Rzecznika możliwości finansowania dodatków do wynagrodzeń dla pracowników zapewniających wysoki poziom bezpieczeństwa systemów informatycznych służących do świadczenia usług kluczowych i cyfrowych oraz do obsługi incydentów. W przypadku uwzględnienia Biura Rzecznika Praw Obywatelskich w katalogu instytucji, o których mowa w przedmiotowej ustawie, których pracownicy mogą być uprawnieni do otrzymywania świadczenia teleinformatycznego, szacunkowy koszt roczny dodatków dla 16 pracowników Biura wyniesie ok. 960 000 zł.	o krajowym systemie cyberbezpieczeństwa, a zmiany w innych ustawach są wprowadzane tylko gdy wynika to z konieczności zapewnienia spójności rozwiązań. W związku z tym jedyne zmiany w ustawie o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa są konsekwencją zmian w ustawie o krajowym systemie cyberbezpieczeństwa. Zaproponowana regulacja jest już wystarczająco rozbudowa i niecelowe byłoby rozszerzanie jej o nowe obszary merytoryczne. Dokładna analiza zapotrzebowania poszczególnych podmiotów na świadczenie teleinformatyczne, zostanie przeprowadzona w toku ewentualnych prac legislacyjnych nad osobnym projektem ustawy.																
	<table><tr><th>Stanowisko</th><th>ilość etatów</th></tr><tr><td>Kierownik jednostki</td><td>1</td></tr><tr><td>Dyrektor i Zastępca Dyrektora</td><td>2</td></tr><tr><td>Naczelnik WI</td><td>1</td></tr><tr><td>Pracownicy działu Cyberbezpieczeństwa</td><td>2</td></tr><tr><td>IOD</td><td>2</td></tr><tr><td>Radca prawny</td><td>1</td></tr><tr><td>Administratorzy WI</td><td>4</td></tr></table>	Stanowisko	ilość etatów	Kierownik jednostki	1	Dyrektor i Zastępca Dyrektora	2	Naczelnik WI	1	Pracownicy działu Cyberbezpieczeństwa	2	IOD	2	Radca prawny	1	Administratorzy WI	4	
Stanowisko	ilość etatów																	
Kierownik jednostki	1																	
Dyrektor i Zastępca Dyrektora	2																	
Naczelnik WI	1																	
Pracownicy działu Cyberbezpieczeństwa	2																	
IOD	2																	
Radca prawny	1																	
Administratorzy WI	4																	

Tabela uwag zgłoszonych w ramach opiniowania do *projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)*

			Pracownicy WI - dział wsparcia technicznego	3	
			razem etatów:	16	
			kwota (ilość etatów * średnia kwota dodatku 5000 zł * 12 miesięcy)	960 000,00 zł	
179.	Prezes Urzędu Zamówień Publicznych	Art. 8	Ponadto proszę o uwzględnienie uwagi redakcyjnej w odniesieniu do przepisu art. 8 Projektu, który dokonuje zmian art. 226 ust. 1 ustawy Pzp regulującego sytuację, w których zamawiający odrzuca ofertę złożoną w ramach postępowania o udzielenie zamówienia publicznego. Pierwsza projektowana zmiana polega na nadaniu nowego brzmienia art. 226 ust. 1 pkt 17 ustawy Pzp. Przepis ten dotyczy odrzucenia oferty, która obejmuje produkt ICT, usługę ICT lub proces ICT wskazane w rekomendacji, o której mowa w art. 33 ust. 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, stwierdzającej ich negatywny wpływ na bezpieczeństwo publiczne lub bezpieczeństwo narodowe. Druga zmiana polega na dodaniu w art. 226 ust. 1 pkt 19 kolejnej przesłanki odrzucenia oferty w sytuacji, gdy oferta obejmuje produkt ICT, którego typ został określony w decyzji w sprawie uznania dostawcy za dostawcę wysokiego ryzyka, o której mowa w art. 66a ust. 13 ustawy o krajowym systemie cyberbezpieczeństwa oraz usługę ICT lub proces ICT, określone w tej decyzji. Obie przesłanki odrzucenia oferty złożonej w ramach postępowania o udzielenie zamówienia publicznego są rodzajowo podobne. W celu zapewnienia skrótości i przejrzystości tekstu proponuje się połączyć je w jednej jednostce redakcyjnej art. 226 ust. 1 pkt 17 ustawy Pzp. W przypadku zaś, gdyby takie połączenie obu przesłanek odrzucenia oferty było niemożliwe, proponuje się zamieścić przepisy regulujące obie przesłanki bezpośrednio po sobie.		Uwaga uwzględniona Proponujemy umieścić przepisy obok siebie.
180.	Rzecznik Praw Obywatelskich	Art. 9	Mając na względzie to, że projektowana nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa wprost zalicza Rzecznika Praw Obywatelskich do podmiotów kluczowych w rozumieniu art. 5 ust. 1 pkt 1) ustawy, to rozszerzenie możliwości przyznawania dodatku do wynagrodzenia o pracowników Biura RPO zapewni m.in. możliwość utworzenia nowych etatów do obsługi incydentów oraz zapobiegnie odpływowi kadry do sektora prywatnego. Obecne wynagrodzenie specjalistów w BRPO nie jest bowiem konkurencyjne względem rynku prywatnego.		Uwaga nieuwzględniona W ramach niniejszego projektu skupiono się na zmianach w ustawie o krajowym systemie cyberbezpieczeństwa, a zmiany w innych ustawach są wprowadzane tylko gdy wynika to z konieczności zapewnienia spójności rozwiązań.

Tabela uwag zgłoszonych w ramach opiniowania do *projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw* (UC32)

				W związku z tym jedyne zmiany w ustawie o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa są konsekwencją zmian w ustawie o krajowym systemie cyberbezpieczeństwa. Zaproponowana regulacja jest już wystarczająco rozbudowa i niecelowe byłoby rozszerzanie jej o nowe obszary merytoryczne. Dokładna analiza zapotrzebowania poszczególnych podmiotów na świadczenie teleinformatyczne, zostanie przeprowadzona w toku ewentualnych prac legislacyjnych nad osobnym projektem ustawy.
181.	Rzecznik Praw Obywatelskich	Art. 9	Dodatkowo wskazuję, że zgodnie z rządowym projektem ustawy o ochronie sygnalistów (druk sejmowy nr 317) Rzecznik Praw Obywatelskich został wskazany jako podmiot odpowiedzialny za realizację zupełnie nowych zadań publicznych związanych ze zgłaszaniem informacji o naruszeniach prawa, co wiąże się z przygotowaniem nowego elektronicznego kanału zgłaszania naruszeń. Tym samym wiąże się też z koniecznością zapewnienia obsługi informatycznej i bezpieczeństwa systemu, którego celem ma być ochrona praw osób zgłaszających naruszenia prawa, tzw. „sygnalistów”.	Uwaga nieuwzględniona W ramach niniejszego projektu skupiono się na zmianach w ustawie o krajowym systemie cyberbezpieczeństwa, a zmiany w innych ustawach są wprowadzane tylko gdy wynika to z konieczności zapewnienia spójności rozwiązań. W związku z tym jedyne zmiany w ustawie o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa są konsekwencją zmian w ustawie o krajowym systemie cyberbezpieczeństwa. Zaproponowana regulacja jest już wystarczająco rozbudowa i

Tabela uwag zgłoszonych w ramach opiniowania do *projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)*

				niecelowe byłoby rozszerzanie jej o nowe obszary merytoryczne. Dokładna analiza zapotrzebowania poszczególnych podmiotów na świadczenie teleinformatyczne, zostanie przeprowadzona w toku ewentualnych prac legislacyjnych nad osobnym projektem ustawy.
182.	Urząd Patentowy Rzeczypospolitej Polskiej	Art. 9	W art. 9 pkt 2 projektu ustawy, wprowadzana jest zmiana w ustawie z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa i zasadnym wydaje się uwzględnienie również art. 5 pkt 2 lit d poprzez nadanie następującego brzmienia: <i>„d) jednostkach organizacyjnych podległych Radzie Ministrów, Prezesowi Rady Ministrów lub ministrom,”.</i> W ocenie Urzędu Patentowego wprowadzenie postulowanej zmiany pozwoli na uwzględnienie wśród podmiotów uprawnionych do ubiegania się do przyznania świadczenia teleinformatycznego szerszego kręgu podmiotów tj. również jednostek podległych Radzie Ministrów. Zauważyć należy, że zgodnie z art. 260 ust. 1 ustawy z dnia 30 czerwca 2000 r. – Prawo własności przemysłowej (Dz. U. z 2023 r. poz. 1170), Urząd Patentowy podlega Radzie Ministrów, a nadzór na działalnością Urzędu, z ramienia Rady Ministrów, sprawuje minister właściwy do spraw gospodarki. Obecnie, z uwagi na to, że Urząd Patentowy jest organem podległym Radzie Ministrów, a nie Prezesowi Rady Ministrów, jest wyłączony z możliwości ubiegania się o przyznanie świadczenia teleinformatycznego. Powyższe nie wydaje się słuszne, gdyż decyzja prawodawcy, iż dany organ podlega Radzie Ministrów, a nie Prezesowi Rady Ministrów, czy określone ministrowi, nie powinna przesądzać o możliwości ubiegania się o świadczenie teleinformatyczne. Kwestia ta powinna być rozstrzygana w oparciu o zakres wykonywanych zadań. W tym kontekście warto podkreślić, iż niewątpliwie Urząd Patentowy realizuje zadania z zakresu cyberbezpieczeństwa w rozumieniu ww. ustawy. Co więcej, mając na uwadze charakter wykonywanych przez Urząd Patentowy zadań, w szczególności dostęp do rozwiązań objętych zgłoszeniami wynalazków, czy wzorów użytkowych, w tym takich, które mogą zostać uznane za	Uwaga nieuwzględniona W ramach niniejszego projektu skupiono się na zmianach w ustawie o krajowym systemie cyberbezpieczeństwa, a zmiany w innych ustawach są wprowadzane tylko gdy wynika to z konieczności zapewnienia spójności rozwiązań. W związku z tym jedyne zmiany w ustawie o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa są konsekwencją zmian w ustawie o krajowym systemie cyberbezpieczeństwa. Zaproponowana regulacja jest już wystarczająco rozbudowa i niecelowe byłoby rozszerzanie jej o nowe obszary merytoryczne. Dokładna analiza zapotrzebowania poszczególnych podmiotów na świadczenie teleinformatyczne, zostanie przeprowadzona w toku ewentualnych prac legislacyjnych nad osobnym projektem ustawy.

Tabela uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

			tajne, należy stwierdzić, iż prawidłowe wykonywanie zadań z zakresu cyberbezpieczeństwa jest szczególnie istotne.	
183.	Prezes Urzędu Ochrony Danych Osobowych	Art. 9	Jednocześnie zwrócić należy uwagę, że projektodawca nie przewidział w projekcie odpowiedniej zmiany w treści art. 5 ²⁵⁾ ustawy z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa (Dz. U. z 2023 r. poz. 667). Kwestia ta była przedmiotem odrębnego wystąpienia Prezesa UODO do Ministra Cyfryzacji dotyczącego potrzeby zmiany art. 5 ustawy o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa ²⁶⁾ . Nawiązując do odpowiedzi Ministra Cyfryzacji z dnia 24 maja br. na wskazane wystąpienie, w związku z pracami nad ustawą zmieniającą m.in. ustawę o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa, organ nadzorczy ponawia uprzejmie sugestię zmiany art. 5 tej ustawy, gdyż przedmiotowy projekt taką przestrzeń regulacyjną stwarza. Włączenie pracowników Urzędu Ochrony Danych Osobowych (osób prowadzących czynności kontrolne oraz analizujących zgłoszenia naruszeń, realizujących w organie nadzorczym zadania z zakresu cyberbezpieczeństwa) do grupy osób uprawnionych do świadczenia teleinformatycznego, o którym mowa w ww. ustawie, przyczyni się niewątpliwie do ograniczania ryzyk związanych z naruszeniem zasad cyberbezpieczeństwa, które opierają się w znacznej części także na zasadach ochrony danych osobowych (art. 5 rozporządzenia 2016/679). Ze względu na charakter wykonywanych działań pracownicy Urzędu Ochrony Danych Osobowych pośrednio lub bezpośrednio realizują niewątpliwie zadania zmierzające do zapewnienia bezpieczeństwa systemów teleinformatycznych przed cyberzagrożeniami, spełniając tym samym warunek, o którym mowa w art. 2 ust. 9 ww. ustawy. Czynności podejmowane przede wszystkim przez osoby prowadzące czynności kontrolne oraz analizujące zgłoszenia naruszeń są działaniami na rzecz oceny stanu bezpieczeństwa systemów teleinformatycznych. W konsekwencji wpływają oni na podniesienie poziomu bezpieczeństwa tych systemów, zgodnie z zasadami cyberbezpieczeństwa.	Uwaga uwzględniona W związku z innymi zmianami m.in. umożliwieniu zgłaszania naruszeń w zakresie danych osobowych poprzez system S46 zasadne jest dodanie Urzędu Ochrony Danych Osobowych do art. 5 ustawy o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa.

²⁵⁾ Dodatek do wynagrodzenia za pracę, a w przypadku funkcjonariuszy i żołnierzy zawodowych świadczenie pieniężne, zwane dalej „świadczeniem teleinformatycznym”, może być przyznane osobom realizującym zadania: 1) w organach i podmiotach, o których mowa w art. 26, art. 41, art. 44 lub art. 60 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, 2) w zakresie zapewnienia cyberbezpieczeństwa w: a) Agencji Bezpieczeństwa Wewnętrznego, b) Agencji Wywiadu, c) Centralnym Biurze Antykorupcyjnym, d) jednostkach organizacyjnych podległych Prezesowi Rady Ministrów lub ministrom, e) Kancelarii Prezesa Rady Ministrów oraz w urzędach obsługujących ministrów, f) Kancelarii Prezydenta Rzeczypospolitej Polskiej, g) Kancelarii Sejmu, h) Kancelarii Senatu, i) Policji, j) prokuraturze, k) Służbie Kontrwywiadu Wojskowego, l) Służbie Wywiadu Wojskowego, m) Straży Granicznej, n) Służbie Ochrony Państwa - zwane dalej „zadaniami z zakresu cyberbezpieczeństwa”.

²⁶⁾ DOL.413.4.2024.

Tabela uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

			Ponadto, co warto podkreślić, kwestię tę poruszono także w uzasadnieniu projektu, którego autor wskazał: „Obowiązki z zakresu cyberbezpieczeństwa oraz ochrona danych osobowych często wzajemnie się przenikają. W obydwu przypadkach należy wdrożyć proporcjonalne środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych. Bardzo często incydent w rozumieniu ustawy o KSC stanowi jednocześnie naruszenie ochrony danych osobowych”. Jednocześnie planowane w projekcie włączenie Urzędu Ochrony Danych Osobowych do systemu S46 oraz wynikająca z tej inicjatywy ścisła współpraca pomiędzy Prezesem Urzędu Ochrony Danych Osobowych a podmiotami krajowego systemu cyberbezpieczeństwa dodatkowo przyczyni się do wspólnego przeciwdziałania cyberzagrożeniom oraz wzmacniania ochrony sieci i systemów informatycznych, a także przetwarzanych za ich pośrednictwem danych osobowych. Co oczywiste, nowe obowiązki, którymi objęty miałby być organ nadzorczy, wymagają utworzenia dodatkowych etatów oraz uzyskania dodatkowych środków finansowych. Mając to na uwadze nieobjęcie pracowników Urzędu Ochrony Danych Osobowych możliwością ubiegania się o wsparcie ze środków Funduszu Cyberbezpieczeństwa, a także brak możliwości utworzenia dodatkowych etatów oraz uzyskania dodatkowych środków finansowych, w ocenie organu nadzorczego, nie znajduje dalszego uzasadnienia.	
184.	Główny Urząd Nadzoru Budowlanego	Art. 9 pkt 2	Artykuł 9 pkt 2 projektu ustawy, przewidujący nowelizację ustawy z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa, proponuję uzupełnić o zmianę w art. 5 w pkt 2 polegającą na dodaniu po lit. n lit. o w brzmieniu: <i>„o) urzędach centralnych”.</i> Alternatywnie poddaję pod rozwałę nadanie nowego brzmienia art. 5 pkt 2 lit. d ustawy o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa: <i>„d) jednostkach organizacyjnych podległych Prezesowi Rady Ministrów lub ministrom, lub jednostkach organizacyjnych przez nich nadzorowanych,”.</i> Pragnę wyjaśnić, że przy coraz większej grupie podmiotów dostarczających usługi cyfrowe zasadne wydaje się przyznanie świadczenia teleinformatycznego osobom realizującym zadania z zakresu cyberbezpieczeństwa zatrudnionym nie tylko w urzędach obsługujących ministrów, czy jednostkach organizacyjnych podległych ministrom, ale także osobom zatrudnionym w urzędach centralnych lub jednostkach organizacyjnych nadzorowanych przez poszczególnych ministrów. Pracownicy tych	Uwaga nieuwzględniona W ramach niniejszego projektu skupiono się na zmianach w ustawie o krajowym systemie cyberbezpieczeństwa, a zmiany w innych ustawach są wprowadzane tylko gdy wynika to z konieczności zapewnienia spójności rozwiązań. W związku z tym jedyne zmiany w ustawie o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa są konsekwencją zmian w ustawie o krajowym systemie cyberbezpieczeństwa. Zaproponowana regulacja jest już wystarczająco rozbudowa i

Tabela uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

			jednostek wykonują praktycznie takie same zadania jak pracownicy organów wymienionych w art. 5 pkt 2 ustawy szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa. Dlatego też, w mojej ocenie, za wykonywaną pracę powinno im zostać przyznane świadczenie teleinformatyczne, o którym mowa w art. 5 ww. ustawy.	niecelowe byłoby rozszerzanie jej o nowe obszary merytoryczne. Dokładna analiza zapotrzebowania poszczególnych podmiotów na świadczenie teleinformatyczne, zostanie przeprowadzona w toku ewentualnych prac legislacyjnych nad osobnym projektem ustawy.
185.	Prezes Urzędu Transportu Kolejowego	Art. 9 pkt 2	W świetle stanowiska Ministra Cyfryzacji pracownicy Urzędu Transportu Kolejowego wykonujący zadania z zakresu cyberbezpieczeństwa nie są uprawnieni do otrzymania świadczenia teleinformatycznego z uwagi na fakt, że Prezes UTK jest jednostką nadzorowaną przez Prezesa Rady Ministrów, ale nie podległą Prezesowi Rady Ministrów. W obowiązującej treści ustawodawca nie przewidział w swojej regulacji niezależnych i objętych zasadą kadencyjności co spowodowało wprowadzenie niedopuszczalnej luki systemowej w przepisach prawa. W związku z tym proponuje się, aby dodać słowo „nadzorowane” aby zlikwidować lukę systemową w przepisach dotyczących świadczeń teleinformatycznych. Nie ulega wątpliwości, że UTK jako administrator rejestrów rangi rejestru państwowego czy zaawansowanej infrastruktury IT powinien również posiadać w zasobie narzędzia odpowiedniego wynagradzania pracowników z zakresu cyberbezpieczeństwa. Proponuje się dotychczasową zmianę pkt 1 oznaczyć jako lit. a i dodać lit. b w brzmieniu: „b) w pkt 2 lit. d otrzymuje brzmienie: „d) jednostkach organizacyjnych podległych lub nadzorowanych przez Prezesa Rady Ministrów lub ministrów,””.	Uwaga nieuwzględniona W ramach niniejszego projektu skupiono się na zmianach w ustawie o krajowym systemie cyberbezpieczeństwa, a zmiany w innych ustawach są wprowadzane tylko gdy wynika to z konieczności zapewnienia spójności rozwiązań. W związku z tym jedyne zmiany w ustawie o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa są konsekwencją zmian w ustawie o krajowym systemie cyberbezpieczeństwa. Zaproponowana regulacja jest już wystarczająco rozbudowa i niecelowe byłoby rozszerzanie jej o nowe obszary merytoryczne. Dokładna analiza zapotrzebowania poszczególnych podmiotów na świadczenie teleinformatyczne, zostanie przeprowadzona w toku ewentualnych prac legislacyjnych nad osobnym projektem ustawy.

Tabela uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

186.	Prezes Urzędu Komunikacji Elektronicznej	Art. 9 pkt 2	Art. 9 pkt 2 w zakresie dotyczącym projektowanego art. 5 pkt 1 ustawy z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa (Dz. U. z 2023 r. poz. 667) – należy zauważyć, iż z uwagi na zmiany w ustawie o ksc (art. 41 oraz art. 41a i art. 41b) zaprojektowane brzmienie przepisu art. 5 pkt 1 ustawy z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa będzie niekompletne. Projektowany przepis art. 41 ustawy o ksc określa wyłącznie organy właściwe do spraw cyberbezpieczeństwa dla podmiotów kluczowych. Natomiast organy właściwe do spraw cyberbezpieczeństwa dla podmiotów ważnych oraz organy właściwe do spraw cyberbezpieczeństwa w sektorze administracji publicznej określają dodawane odpowiednio art. 41a oraz art. 41b ustawy o ksc. W konsekwencji przepisy te również należy uwzględnić (poprzez odesłanie do nich po odesłaniu do art. 41) w nowelizowanym art. 5 pkt 1 ustawy z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa.	Uwaga wyjaśniona Ten przepis ma dotyczyć wszystkich organów właściwych.
187.	Prezes Urzędu Zamówień Publicznych	Art. 9 pkt 2	Na podstawie art. 9 pkt 2 projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw, zwanego dalej „Projektem”, planowane jest dokonanie zmiany w art. 5 pkt 1 ustawy z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa (Dz. U. z 2023 r. poz. 667). Przepis art. 5 ustawy o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa określa katalog organów, podmiotów i jednostek, których pracownicy mogą mieć przyznany dodatek za wykonywanie zadań z zakresu cyberbezpieczeństwa, zwany „świadczeniem teleinformatycznym”. W katalogu tym nie został wymieniony Urząd Zamówień Publicznych (UZP), co w praktyce uniemożliwia objęcie UZP świadczeniem teleinformatycznym, pomimo faktycznego wykonywania zadań z zakresu cyberbezpieczeństwa przez niektórych pracowników UZP. Chciałbym podkreślić, że UZP obsługuje szereg narzędzi i systemów informatycznych wymagających szczególnej ochrony pod kątem ich bezpieczeństwa cybernetycznego. Kluczowym systemem pod tym względem jest Platforma e-Zamówienia, której obsługę zapewnia UZP. Platforma e-Zamówienia stanowiąca bezpłatne narzędzie zarówno dla zamawiających – podmiotów, zwłaszcza z sektora finansów publicznych, zobowiązanych do udzielania zamówień publicznych na podstawie ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych (Dz. U. z 2023 r. poz. 1605 i 1720), zwanej dalej „ustawą Pzp”, jak i wykonawców – osób fizycznych i osób prawnych zainteresowanych udziałem w postępowaniach o	Uwaga nieuwzględniona W ramach niniejszego projektu skupiono się na zmianach w ustawie o krajowym systemie cyberbezpieczeństwa, a zmiany w innych ustawach są wprowadzane tylko gdy wynika to z konieczności zapewnienia spójności rozwiązań. W związku z tym jedyne zmiany w ustawie o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa są konsekwencją zmian w ustawie o krajowym systemie cyberbezpieczeństwa. Zaproponowana regulacja jest już wystarczająco rozbudowana i niecelowe byłoby rozszerzanie jej o nowe obszary merytoryczne.

Tabela uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

		udzielenie zamówienia publicznego lub konkursach. Beneficjentami są również dostawcy platform zakupowych, którzy wnioskują o integrację z Platformą e-Zamówienia. Konieczność utrzymania i rozwoju Platformy e-Zamówienia jako systemu wspierającego elektroniczną zamówień publicznych powoduje, że niezbędne jest zabezpieczenie zasobów osobowych i finansowych w celu zapewnienia bezpieczeństwa cybernetycznego tego systemu jak również ciągłości jego działania zarówno po stronie usług infrastrukturalnych, jak i usług utrzymania wsparcia użytkowników w bieżącej obsłudze produkcyjnej w zakresie rozwiązywania problemów technicznych. Z punktu widzenia bezpieczeństwa Platformy e-Zamówienia kluczowym elementem jest Moduł Ofert i Wniosków jako najbardziej istotny dla całego procesu ofertowego. Jego zadaniem jest szyfrowanie składanych ofert i wniosków oraz prac konkursowych, zabezpieczenie ich przed dostępem osób trzecich przed upływem wyznaczonych terminów, w szczególności otwarcia ofert w postępowaniu. Dodatkowym zadaniem Modułu Ofert i Wniosków jest zabezpieczenie oferty w taki sposób, żeby nie dopuścić do zapoznania się z jej treścią w sposób nieuprawniony. Dane gromadzone w trakcie procesu ofertowego wymagają szczególnego bezpieczeństwa, gdyż naruszenie integralności Platformy e-Zamówienia mogłoby prowadzić do szeregu zdarzeń, których skutki negatywnie wpłynęłyby na samą poufność tych danych. W kontekście zapewnienia bezpieczeństwa cybernetycznego kluczowym modułem Platformy e-Zamówienia jest Biuletyn Zamówień Publicznych, m.in. ze względu na fakt, że nie ma alternatywnych rozwiązań systemowych umożliwiających realizowanie przez zamawiających obowiązków wynikających z ustawy Pzp w zakresie zamieszczania ogłoszeń związanych z postępowaniami o udzielenie zamówienia publicznego lub konkursami. W UZP prowadzone są również działania zmierzające do informatyzacji Krajowej Izby Odwoławczej (KIO), w szczególności poprzez system e-Protokół (oparty o system ReCourt wykorzystywany w sądach powszechnych). Wdrożenie systemu e-Protokół gwarantuje orzekającym członkom KIO usprawnienie pracy poprzez jej elektroniczną, co pozwala przede wszystkim na większą efektywność w rozpoznawaniu wnoszonych odwołań. W ww. systemie są również przetwarzane dane osobowe, przede wszystkim zamawiających i wykonawców, co wymaga objęcia go szczególną ochroną i nadzorem przed atakami hakerskimi. W planach jest także objęcie elektroniczną rozpraw przed KIO. Planowane jest ponadto wdrożenie elektronicznego systemu obsługi dokumentów EZD RP oraz jego integracja z Platformą e-Zamówienia.	Dokładna analiza zapotrzebowania poszczególnych podmiotów na świadczenie teleinformatyczne, zostanie przeprowadzona w toku ewentualnych prac legislacyjnych nad osobnym projektem ustawy.

Tabela uwag zgłoszonych w ramach opiniowania do *projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)*

			Wszystkie wymienione wyżej narzędzia wymagają należytego bieżącego zabezpieczenia cybernetycznego i opracowania planów ciągłości działania przed atakami hakerskimi. W związku z potrzebą zapewnienia stałego bezpieczeństwa funkcjonowania powyższych systemów informatycznych istotne jest objęcie świadczeniem teleinformatycznym, o którym mowa w art. 5 <i>ustawy o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa</i>, pracowników pionu IT oraz pionów wspomagających UZP zajmujących się obsługą tych systemów, co wzmocni wdrażanie nowych rozwiązań zabezpieczających w obszarze cyberbezpieczeństwa i zdolność UZP do szybkiego reagowania na wzrastającą liczbę incydentów cyberbezpieczeństwa oraz pojawiające się nowe zagrożenia. Utrzymanie stałego zespołu specjalistów z zakresu cyberbezpieczeństwa jest wręcz niezbędne dla prawidłowego wykonywania stojących przed Prezesem UZP zadań związanych z informatyzacją zamówień publicznych w tym również w związku z sukcesywnie poszerzanym katalogiem usług on-line udostępnianych przez UZP. Chciałbym także nadmienić, że podczas procesu legislacyjnego związanego z projektem <i>ustawy o zmianie ustawy o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa oraz niektórych innych ustaw</i> (nr UD390) projekt skierowany na komisję prawniczą (wersja z dnia 13 grudnia 2022 r.) zawierał zmiany w zakresie art. 5 pkt 2 <i>ustawy o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa</i> jednoznacznie wskazujące, że UZP mieści się w katalogu podmiotów objętych świadczeniem teleinformatycznym. Ponadto podczas prac komisji prawniczej zapewniono, że Prezes UZP jest objęty katalogiem podmiotów wskazanych w wówczas projektowanym art. 3 ust. 9 tej ustawy. Proces legislacyjny dotyczący ww. projektu ustawy jednak nie zakończył się i ostatecznie założenia powyższe nie znalazły do tej pory odzwierciedlenia w przepisach <i>ustawy o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa</i>. Mając na względzie powyższe wnoszę o uwzględnienie przedstawionej argumentacji tak, aby z przepisów <i>ustawy o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa</i>, w szczególności z art. 5 pkt 2 tej ustawy, wyraźnie wynikało i nie budziło wątpliwości, że pracownicy UZP realizujący zadania z zakresu cyberbezpieczeństwa objęci są świadczeniem teleinformatycznym.	

Tabela uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

188.	Najwyższa Izba Kontroli	Art. 9 ust. 2	Jak wynika z oceny skutków regulacji sporządzonej przez Ministerstwo Cyfryzacji w ramach Inwestycji C3.1.1. KPO Cyberbezpieczeństwo - CyberPL, infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo, przewiduje się m.in. realizację projektu pn. „Wsparcie 500 podmiotów krajowego systemu cyberbezpieczeństwa w modernizacji i rozbudowie infrastruktury cyberbezpieczeństwa w sieciach IT, w tym wsparcie podmiotów wykorzystujących technologie informacyjne (IT) oraz operacyjne (OT) stosowane w przemysłowych systemach sterowania (ICS)”. Projekt ten zakłada udzielenie wsparcia o wartości - ok. 700,5 mln zł m.in. dla ok. 70 urzędów administracji centralnej i rządowej. W ramach tego projektu urzędy administracji centralnej i rządowej będą mogły uzyskać wsparcie finansowe na dostosowanie się do niniejszej ustawy. NIK nie należy do administracji centralnej i rządowej i jako naczelny organ kontroli państwowej nie znalazła się w grupie podmiotów, którym przyznano dodatkowe wsparcie finansowe na realizację nowych zadań i obowiązków związanych z cyberbezpieczeństwem. Tymczasem, nowe obowiązki nałożone także na NIK przewidziane w projekcie, to m.in. zgłaszanie incydentów, wdrożenie systemu zarządzania bezpieczeństwem, przeprowadzanie co dwa lata audytów bezpieczeństwa systemów informacyjnych (jak to obecnie wynika z § 20 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych), czy wyznaczenia dwóch osób odpowiedzialnych za utrzymywanie kontaktów z innymi podmiotami kluczowymi i podmiotami ważnymi. Należy przy tym zauważyć, że wielokrotnie postulowałem w pismach kierowanych do Ministra Cyfryzacji¹ o włączenie Najwyższej Izby Kontroli do grupy podmiotów, które mogą się ubiegać o przyznanie dodatku do wynagrodzenia za pracę, o których mowa w art. 5 ustawy z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu Cyberbezpieczeństwa (Dz. U. z 2023 r. poz. 667.) tj. podmiotów uprawnionych do ubiegania się o środki na sfinansowanie świadczenia teleinformatycznego (dodatku do wynagrodzenia za pracę dla osób realizujących zadania z zakresu Cyberbezpieczeństwa.) Powyższy postulat związany jest z procedowanym projektem ustawy o zmianie ustawy o szczegółowych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa oraz niektórych innych ustaw.	Uwaga nieuwzględniona W ramach niniejszego projektu skupiono się na zmianach w ustawie o krajowym systemie cyberbezpieczeństwa, a zmiany w innych ustawach są wprowadzane tylko gdy wynika to z konieczności zapewnienia spójności rozwiązań. W związku z tym jedyne zmiany w ustawie o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa są konsekwencją zmian w ustawie o krajowym systemie cyberbezpieczeństwa. Zaproponowana regulacja jest już wystarczająco rozbudowa i niecelowe byłoby rozszerzanie jej o nowe obszary merytoryczne. Dokładna analiza zapotrzebowania poszczególnych podmiotów na świadczenie teleinformatyczne, zostanie przeprowadzona w toku ewentualnych prac legislacyjnych nad osobnym projektem ustawy.

Tabela uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

189.	Prezes Urzędu Komunikacji Elektronicznej	Art. 15 ust. 2	Art. 15 ust. 2 – proponuje się, aby organem właściwym do wpisania z urzędu do wykazu podmiotów kluczowych i podmiotów ważnych, tych operatorów usług kluczowych, którzy byli wpisani do wykazu operatorów usług kluczowych przed dniem wejścia w życie projektowanej ustawy, był minister właściwy do spraw informatyzacji (będący organem prowadzącym oba te wykazy), nie zaś organ właściwy do spraw cyberbezpieczeństwa.	Uwaga nieuwzględniona Minister będzie prowadził system teleinformatyczny, w którym będą znajdować się wykazy, ale możliwość dokonywania wpisu będzie miało wiele podmiotów w tym organy właściwe. To organy właściwe najlepiej znają swoje sektory i dlatego uzasadnione jest by to one dokonały wpisów.
190.	Urząd Komisji Nadzoru Finansowego	Art. 28	W art. 28 ust. 14 zdanie drugie projektu ustawy występuje odniesienie do ministra właściwego do spraw gospodarki morskiej, zamiast do Szefa Kancelarii Prezesa Rady Ministrów.	Uwaga uwzględniona
191.	Rzecznik Małych i Średnich Przedsiębiorców	Art. 29	Wejście w życie przedmiotowej (projektowanej) ustawy, określone w art. 29 Projektu, powinno nastąpić po upływie co najmniej 6 miesięcy od dnia jej ogłoszenia. Taki okres vacatio legis sprzyjał będzie procesowi sprawnego i bezpiecznego, a nie szybkiego i obciążonego ryzykiem błędów - dostosowaniu się podmiotów zobowiązanych do nowych regulacji, które będą wymagać poniesienia znacznych kosztów i wysiłku organizacyjnego. Poza powyższym - wejście w życie części regulacji objętych Projektem powinno nastąpić dopiero po publikacji niezbędnych aktów wykonawczych (o czym mowa również w pkt 3 niniejszego pisma).	Uwaga nieuwzględniona Okres dostosowawczy pozostanie 6 miesięcy
UWAGI do załączników do projektu ustawy				
192.	Prezes Urzędu Transportu Kolejowego	Załącznik nr 1 (część dotycząca podmiotów kluczowych w transporcie kolejowym)	Zaproponowany kształt przepisów nie obejmuje producentów taboru, infrastruktury sterowania ruchem kolejowym, którzy niejednokrotnie świadczą usługi utrzymania pojazdów i infrastruktury w ramach wieloletnich kontraktów z przewoźnikami lub zarządcami infrastruktury. Większość umów w tym zakresie jest zawierana w surowym reżimie PZP albo objęta okresem trwałości projektu. Ich zmiana może nie być możliwa, a tym samym przewoźnik czy zarządca mogą nie mieć możliwości wprowadzenia wymagań w stosunku do podmiotu utrzymującego wynikających z projektu ustawy. Dlatego proponuje się, aby w ramach projektu objąć obowiązkami również podmioty świadczące usługi utrzymania infrastruktury kolejowej i pojazdów kolejowych ze względu na ich krytyczność w bezpieczeństwie systemu kolejowego,	Uwaga wyjaśniona Producenci taboru oraz infrastruktury sterowania ruchem kolejowym, o których mowa w zgłoszonej uwadze, będą podlegali pod sektor Produkcji (usługi: produkcja pozostałego sprzętu transportowego, produkcja maszyn i urządzeń, gdzie indziej niesklasyfikowana). Zgodnie z projektem ustawy miałyby to być

Tabela uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

			oraz aby osiągnąć spójność systemową w zakresie cyberbezpieczeństwa podsektora kolejowego. Do wykazu podmiotów kluczowych w sektorze „Transport”, w podsektorze „Transport kolejowy”, w kolumnie „Rodzaj podmiotu”, proponuje się dodanie kolejnego wiersza w brzmieniu: „Podmioty świadczące na rzecz przewoźników kolejowych lub zarządców infrastruktury usługi utrzymania pojazdów kolejowych lub infrastruktury kolejowej.”.	„Przedsiębiorca prowadzący którykolwiek z rodzajów działalności gospodarczej, o których mowa w sekcji C dział 30 klasyfikacji NACE Rev. 2.”. W sekcji C dział 30, znajduje się „Produkcja lokomotyw kolejowych oraz taboru szynowego”.
193.	Prezes Głównego Urzędu Statystycznego	Załącznik nr 1	W załączniku nr 1 do projektu ustawy wskazano, że w zakresie administracji publicznej podmiotami kluczowymi są jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 1–6, 8 i 10–13 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2023 r. poz. 1270, z późn. zm.) Z art. 9. ustawy o finansach publicznych wynika, że Sektor finansów publicznych tworzą: 1) organy władzy publicznej, w tym organy administracji rządowej, organy kontroli państwowej i ochrony prawa oraz sądy i trybunały; (...) 3) jednostki budżetowe; Oznacza to, że podmiotem kluczowym będzie zarówno organ administracji publicznej np. Prezes GUS oraz urząd (jednostka budżetowa) obsługujący organ, np. GUS. Dodatkowo podmiotami kluczowymi będą również wszystkie inne jednostki budżetowe podległe i nadzorowane przez organ administracji publicznej, które realizują zadania ustawowe organu. W wielu sektorach i resortach administracji publicznej organ adm. publicznej powołał wyspecjalizowane podmioty pomocnicze świadczące usługi informatyczne, które obsługują część lub wszystkie jednostki budżetowe danego resortu, w tym realizują zadania związane z cyberbezpieczeństwem. W części przypadków wszystkie jednostki resortu funkcjonują i pracują w ramach jednej wspólnej sieci. W wielu tego rodzaju przypadkach systemy informatyczne, które są wykorzystywane przez jednostki, to systemy centralne, udostępnione zazwyczaj przez organ lub urząd go obsługujący (centrałę). Wszystkie jednostki budżetowe, które uznane będą za podmioty kluczowe, będą musiały spełnić odrębnie wszystkie wymienione w ustawie obowiązki np. wyznaczyć 2 osoby do kontaktu, przeprowadzić wymagane audyty, co może okazać się bezcelowe, bo zadania związane z cyberbezpieczeństwem, obsługą incydentów, nadzorem nad bezpieczeństwem sieci, realizuje dla całego resortu jeden podmiot.	Uwaga uwzględniona Zostaną wprowadzone odrębne regulacje dotyczące wykonywania obowiązków z zakresu cyberbezpieczeństwa w podmiotach publicznych.

Tabela uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

			Zgodnie z Dyrektywą NIS 2, podmiot jest podmiotem administracji publicznej: (i) na poziomie rządu centralnego, zdefiniowanym przez państwo członkowskie, zgodnie z prawem krajowym; lub (ii) na poziomie regionalnym, zdefiniowanym przez państwo członkowskie zgodnie z prawem krajowym, który zgodnie z oceną opartą na analizie ryzyka świadczy usługi, których zakłócenie mogłoby mieć znaczący wpływ na krytyczną działalność społeczną lub gospodarczą. Nowelizowana ustawa nie wskazuje natomiast żadnych regulacji szczególnych dla ww. sytuacji specyficznych dla administracji publicznej. Ustawodawca powinien przewidzieć w ustawie odrębne regulacje w odniesieniu do pojęcia podmiotu publicznego w kontekście specyfiki jednostek budżetowych, które są jednostkami podległymi, podporządkowanymi lub nadzorowanymi przez organ administracji publicznej.	
194.	Prezes Urzędu Komunikacji Elektronicznej	Załącznik nr 3	Załącznik nr 3 do projektowanej ustawy – wątpliwości budzi użycie w lp. 3 w kolumnie „opis funkcji” zapis „przydzielanie zasobów radiowych”, w szczególności w kontekście przepisów ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne dotyczących gospodarowania częstotliwościami. Niejasne jest m. in. komu zasoby radiowe, o których mowa w tym zapisie, miałyby być przydzielane.	Uwaga uwzględniona Chodzi o czynność techniczną wykonywaną przez radiową sieć dostępową. The gNB performs the following tasks: - Functions for Radio Resource Management: Radio Bearer Control, Radio Admission Control, Connection Mobility Control, Dynamic allocation of resources to UEs in both uplink and downlink (scheduling);²⁷⁾
UWAGI do OSR				
195.	Prezes Urzędu Komunikacji Elektronicznej	OSR	Ocena Skutków Regulacji (OSR) – proponuje się w części 6 OSR doprecyzować tabelę zatytułowaną „Podsumowanie nowych etatów” poprzez zamieszczenie wyjaśnienia, że etaty tam wskazane (łącznie 54 dla UKE) są przeznaczone na obsługę organów właściwych do spraw cyberbezpieczeństwa i nie obejmują etatów przeznaczonych do obsługi CSIRT sektorowych. Ponadto przyjęta w OSR kwota miesięcznego wynagrodzenia w CSIRT sektorowym na poziomie 16 413 zł (wzorem Centrum Cyberbezpieczeństwa w Zamościu) nie jest adekwatna do rynkowych	Uwaga wyjaśniona 54 etaty dot. etatów nadzorczych, a nie CSIRT. Per CSIRT sektorowy wskazano 20 etatów.

²⁷⁾ <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3389>

Tabela uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

			wynagrodzeń pracowników IT w Warszawie, a tym samym nie umożliwi organom prowadzącym CSIRT sektorowe pozyskanie specjalistów posiadających odpowiednie kompetencje i doświadczenie. Należy również zauważyć, że w załączniku nr 4 do OSR w zakresie części budżetowej 76 – Urząd Komunikacji Elektronicznej przyjęto zaniżony koszt utworzenia nowego stanowiska pracy w kwocie 11 tys. zł oraz nie uwzględniono kosztów utrzymania nowoutworzonych stanowisk pracy. Proponuje się zatem przyjęcie do obliczeń kosztu utworzenia 1 stanowiska pracy w wysokości 20 tys. zł oraz uwzględnienie kosztu jego utrzymania w kwocie 5 tys. zł/miesiąc/etat.	
196.	Polski Komitet Normalizacyjny	OSR	Warto wskazać, że Polskie Normy mogą być powoływane w przepisach prawa po opublikowaniu ich w języku polskim (art. 5 ust. 4 ustawy o normalizacji). Z tego względu, sugeruje się, aby Ustawodawca przewidział środki na tłumaczenia norm, w tym ich znowelizowanych wersji, których należy się spodziewać w przyszłości. Proponujemy zatem aby w preliminarzu budżetowym przewidzieć środki na tłumaczenia Polskich Norm: - z zakresu nadrzędnych wymagań dotyczących świadczenia prywatnych usług ochrony dla infrastruktury krytycznej, które to normy mogą wspierać zapisy ustawy (m.in w art. 1 pkt 14 projektowanej ustawy dot. art. 10 ust.1 i 3 pkt 2) lit. f) – str.21: - PN-EN 17483-1:2021-11 Prywatne usługi ochrony - Zabezpieczenie infrastruktury krytycznej - Część 1: Wymagania ogólne - PN-EN 17483-2:2024-03 Prywatne usługi ochrony - Zabezpieczenie infrastruktury krytycznej - Część 2: Usługi ochrony portów lotniczych i lotnictwa - PN-EN 17483-3:2024-03 Prywatne usługi ochrony - Zabezpieczenie infrastruktury krytycznej - Część 3: Usługi ochrony morskiej i portowej - które mogą być wykorzystywane jako wspierające wdrożenie środków organizacyjnych i technicznych przewidzianych w projekcie tj.: -PN-EN ISO/IEC 27002:2023-01Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności - Zabezpieczanie informacji -PN-EN ISO 27007:2022-06Bezpieczeństwoinformacji, cyberbezpieczeństwo i ochrona prywatności -Wytyczne dotyczące audytu systemów zarządzania bezpieczeństwem informacji -PN-EN ISO 22313:2020-08 Bezpieczeństwo i odporność -Systemy zarządzania ciągłością działania -Wytyczne dotyczące stosowania ISO 22301 oraz opracowywane w chwili obecnej projekty Polskich Norm: -prPN-prEN ISO/IEC 27005 Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności -Wytyczne do zarządzania ryzykami w bezpieczeństwie informacji	Uwaga nieuwzględniona Z uwagi na rezygnację z przywoływania Polskich Norm w projekcie nie przewiduje się ujmowania kosztów w OSR.

Tabela uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

			-prPN-EN ISO/IEC 27006-1, Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności -Wymagania dla jednostek prowadzących audyt i certyfikację systemów zarządzania bezpieczeństwem informacji -Część 1: Postanowienia ogólne.	
Dodatkowe propozycje – nowa propozycja				
197.	Urząd Komisji Nadzoru Finansowego	Nowa propozycja	Z uwagi na usunięcie z ustawy kategorii incydentów istotnych, art. 29 UKSC dotyczący informowania o takich incydentach innych państw członkowskich UE powinien zostać w ocenie UKNF uchylony.	Uwaga uwzględniona
198.	Zakład Ubezpieczeń Społecznych	Nowa propozycja	Projekt przewiduje udostępnianie przez ZUS informacji o rocznej liczbie pracowników lub ubezpieczonych u płatnika składek drogą elektroniczną. Naszym zdaniem „roczna liczba pracowników lub ubezpieczonych” jest pojęciem nieprecyzyjnym, ponieważ nie jest wskazane jak ustalić tą liczbę – czy chodzi o średnią, łączną czy może unikatową liczbę pracowników lub ubezpieczonych na dany dzień. Dodatkowo projekt zakłada, że powyższe dane mają być przekazywane drogą elektroniczną. Przypuszczalnie wiąże się to z utworzeniem dedykowanego interfejsu lub usługi, co oznacza, że Zakład powinien mieć zapewniony odpowiedni termin na jego przygotowanie – obecnie projekt przewiduje wejście w życie ustawy w terminie 1 miesiąca od dnia ogłoszenia, co może nie wystarczyć do wdrożenia operacyjnego. Korzystając z okazji, uprzejmie proszę Pana Ministra o rozważenie możliwości dokonania zmiany ustawy z dnia 2 grudnia 2021r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa (t.j. Dz. U. z 2023r. poz. 667), w taki sposób aby w art. 5 pkt 2 został wskazany Zakład Ubezpieczeń Społecznych. ZUS nie jest ani jednostką podległą Prezesowi Rady Ministrów, ani któremukolwiek z ministrów (nadzór nad ZUS sprawuje Minister Rodziny, Pracy i Polityki Społecznej). Jednocześnie ZUS jest jednostką sektora finansów publicznych wskazanych w art. 4 pkt 7 ustawy o z dnia 5 lipca 2018r. o krajowym systemie cyberbezpieczeństwa, co uwzględniając również zadania realizowane przez Zakład jak i użytkowaną infrastrukturę krytyczną wydaje się w pełni uzasadniać potrzebę sygnalizowanej zmiany. Jednocześnie należy wskazać, że obowiązujące przepisy prawa pracy nie pozostawiają swobody umożliwiającej takie kształtowanie wynagrodzeń grupy pracowników realizujących zadania z zakresu cyberbezpieczeństwa, aby były one konkurencyjne w relacji do wynagrodzenia oferowanych przez podmioty wskazane w ustawie. W przypadku jakichkolwiek pytań lub wątpliwości pozostajemy do dyspozycji pana Ministra.	Uwaga częściowo uwzględniona Chodzi o roczną liczbę ubezpieczonych. Jeśli chodzi o drogę elektroniczną, to wystarczający będzie EPUAP/edoreczenia.

Zestawienie nieuwzględnionych uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

Lp.	Zgłaszający uwagę	Jednostka redakcyjna	Treść uwagi	Stanowisko Ministra Cyfryzacji
1.	Rzecznik Małych i Średnich Przedsiębiorców	Uwaga ogólna	Poza wskazanymi powyżej zastrzeżeniami i postulatami zmian, Rzecznik Małych i Średnich Przedsiębiorców zwraca uwagę, iż: Projekt nie różnicuje obowiązków w zależności od wielkości, charakteru oraz realizowanych zadań - przez podmioty publiczne. Sytuacja taka może prowadzić do konieczności wdrażania niepotrzebnych lub nieadekwatnych rozwiązań organizacyjnych oraz ponoszenia kosztów nieznajdujących oparcia w zasadach gospodarowania środkami publicznymi i w konsekwencji pozostających w sprzeczności z regulacjami ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych.	Uwaga nieuwzględniona Od 2012 r. podmioty publiczne, bez względu na wielkość są obowiązane wdrożyć system zarządzania bezpieczeństwem informacji. Tym samym środki na ten system powinny być od tego czasu budżetowane.
2.	Narodowy Bank Polski	Art. 2 pkt 3c	Ad. art. 1 pkt 2 lit. a projektu ustawy w zakresie dodawanego pkt 3c: 3c) bezpieczeństwo systemów informacyjnych – odporność systemów informacyjnych na zdarzenia naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy. Proponujemy rozważyć, czy nie należałoby wskazać w tym punkcie „zdarzeń mających na celu naruszenie poufności, integralności” zamiast „naruszeń”. W naszej ocenie odporność, o której mowa w definicji bezpieczeństwa systemów informacyjnych, ma zapobiegać, aby do takiego naruszenia poufności, czy integralności nie doszło.	Uwaga nieuwzględniona Określenie celu może być w wielu przypadkach niemożliwe, poza tym część zdarzeń wpływających na system informacyjny nie jest celowa, np. awarie techniczne czy błędy ludzkie.
3.	Prezes Urzędu Komunikacji Elektronicznej	Art. 8	Art. 1 pkt 12 w zakresie dotyczącym projektowanego art. 8 ustawy o ksc – mając na uwadze brzmienie niniejszego przepisu proponuje się uzupełnić projektowaną ustawę o dodatkową regulację, na podstawie której kierownik podmiotu kluczowego lub podmiotu ważnego będzie mógł powierzyć podmiotowi zewnętrznemu (tj. działającemu poza strukturą organizacyjną podmiotu kluczowego lub podmiotu ważnego) realizację wymagań, o których mowa w projektowanym art. 8 ustawy o ksc, z zastrzeżeniem, iż: – podmiot zewnętrzny dysponuje zdolnościami technicznymi i organizacyjnymi niezbędnymi do realizacji ww. wymagań, – infrastruktura podmiotu zewnętrznego, wykorzystywana do realizacji ww. wymagań, znajduje się na terytorium Unii Europejskiej, – dane przetwarzane w związku z realizacją ww. wymagań powinny być dostępne na terytorium Rzeczypospolitej Polskiej, – umowa zawarta przez kierownika podmiotu kluczowego lub podmiotu ważnego z podmiotem zewnętrznym będzie zawierać wymóg, zgodnie z którym świadczenie usług na rzecz podmiotu kluczowego lub podmiotu ważnego będzie podlegać regulacjom prawa Rzeczypospolitej Polskiej.	Uwaga nieuwzględniona Z uwagi na transgraniczność usług społeczeństwa informacyjnego te wymogi mogą być niemożliwe do spełnienia. Bywa tak, że są manager security services providers, którzy mają swoje centra przetwarzania danych w kilku państwach, a nawet na kilku kontynentach. Wprowadzenie takich wymogów znacznie ograniczyłoby liczbę takich dostawców.

Zestawienie nieuwzględnionych uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

			Niniejsza propozycja jest zgodna z wymaganiami określonymi na potrzeby aukcji 5G, które uzyskały w dniu 23 marca 2023 r. pozytywną opinię Kolegium do Spraw Cyberbezpieczeństwa.	
4.	Prezes Urzędu Komunikacji Elektronicznej	Art. 11 ust. 1 pkt 4b	Art. 1 pkt 15 lit. a tiret czwarte w zakresie dotyczącym projektowanego art. 11 ust. 1 pkt 4b ustawy o ksc – niejasne jest jaki okres czasu ma obejmować „sprawozdanie okresowe”, o którym mowa w tym przepisie.	Uwaga nieuwzględniona Należy zauważyć, że „sprawozdanie okresowe” będzie przekazywane na wniosek CSiRT sektorowego, w którym zostaną określone szczegółowe informacje dotyczące obsługi incydentu. Ponadto część informacji dot. incydentu będzie wskazana we wstępnym ostrzeżeniu, więc można założyć, że sprawozdanie będzie zawierało uzupełnienie tych informacji, np. czas trwania incydentu.
5.	Narodowy Bank Polski	Art. 11 ust. 1 pkt 4	Art. 1 pkt 15 projektu ustawy w zakresie zmiany brzmienia art. 11 pkt 4: 4) zgłasza wczesne ostrzeżenie o incydencie poważnym niezwłocznie, nie później niż w ciągu 24 godzin od momentu jego wykrycia, do właściwego CSiRT sektorowego;”. Biorąc pod uwagę, że w dalszej części tego punktu uszczegóławia się treść przepisu o fragment „niezwłocznie, nie później niż w ciągu 24 godzin”, proponujemy wykreślenie z przedmiotowego punktu wyrazu „wczesne” albo doprecyzowanie, co rozumie się przez „wczesne ostrzeżenie o incydencie”.	Uwaga nieuwzględniona Pojęcie „wczesne ostrzeżenie” występuje w NIS 2, co więcej dyrektywa ta określa co jest elementem „wczesnego ostrzeżenia”.
6.	Prezes Urzędu Komunikacji Elektronicznej	Art. 12 ust. 2	Art. 1 pkt 16 w zakresie dotyczącym projektowanego art. 12 ust. 2 ustawy o ksc – zgodnie z niniejszym przepisem zgłaszane przez podmiot kluczowy i podmiot ważny wczesne ostrzeżenie o incydencie poważnym może zawierać skierowany do CSiRT sektorowego wniosek m. in. o wsparcie techniczne przy obsłudze incydentu. W związku z tym należy podkreślić, że zakres ww. „wsparcia technicznego” na gruncie projektowanego przepisu jest niejasny, a tym samym budzi on poważne wątpliwości interpretacyjne, tj. na czym owo wsparcie techniczne miałyby polegać? Jednocześnie nasuwa się wątpliwość – jeżeli wsparcie to miałyby być związane np. z zaangażowaniem środków rzeczowych lub	Uwaga nieuwzględniona Udzielanie wsparcia jest jednym z zadań CSiRT wskazanych w dyrektywie NIS 2 dlatego nie możemy wyłączyć tego obowiązku. Należy podkreślić, że już obecnie jednym z zadań sektorowych zespołów ds. cyberbezpieczeństwa jest wspieranie operatorów usług kluczowych w wykonywaniu ich

Zestawienie nieuwzględnionych uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

			osobowych po stronie CSIRT sektorowego (koszty), czy nie powinno to znaleźć odzwierciedlenia w OSR dla projektowanej ustawy?	obowiązków w tym w obsłudze incydentów. Proponuje się doprecyzowanie tego określenia przez dodanie wyrazu „dodatkowego”, w związku z tym we wczesnym ostrzeżeniu podmiot kluczowy i ważny będzie mógł wystąpić o „dodatkowe wsparcie techniczne” – to doprecyzowanie jest zgodne z art. 23 ust. 5 NIS 2, który mówi właśnie o „dodatkowym wsparciu”.
7.	Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy	Art. 26 ust. 2a	W projektowanym art. 26 ust. 2a zaproponowano przepisy, zgodnie z którymi Pełnomocnik może zlecić zapewnienie wsparcia w obsłudze incydentów wymienionym podmiotom – CSIRT MON, CSIRT NASK, CSIRT GOV. W przypadku CSIRT MON oraz CSIRT GOV, projektodawca przewidział konieczność udzielenia zgody przez Ministra Obrony Narodowej (w przypadku CSIRT MON) oraz Szefa Agencji Bezpieczeństwa Wewnętrznego (w przypadku CSIRT GOV). Analogicznie, taki sam sposób postępowania powinien dotyczyć CSIRT NASK. Biorąc to pod uwagę zwracamy się z prośbą o dodanie w art. 26 ust. 2a pkt 2 obowiązku wyrażenia zgody przez dyrektora NASK-PIB, czyli jednostki, w której prowadzony jest CSIRT NASK. Pozwoli to uspoźnić rozwiązanie z pkt 1 i 3 z pkt 2.	Uwaga nieuwzględniona Zasadą wynikającą z ustawy o Radzie Ministrów czy ustawy o działach administracji rządowej jest to, że minister nadzorujący może kierować do jednostek podległych i nadzorowanych wiążące wytyczne i polecenia. Pełnomocnik Rządu do spraw cyberbezpieczeństwa będzie ministrem lub wiceministrem cyfryzacji a minister cyfryzacji nadzoruje NASK-PIB.
8.	Najwyższa Izba Kontroli	Art. 36b	Stosownie do art. 36b ust. 7 komisja powołana do zniszczenia informacji uzyskanych podczas przeprowadzania oceny bezpieczeństwa systemu informacyjnego składa się z trzech osób powołanych przez osobę kierującą zespołem CSIRT spośród pracowników, funkcjonariuszy lub żołnierzy realizujących zadania odpowiednio w CSIRT MON, CSIRT NASK, CSIRT GOV albo CSIRT sektorowym. W przypadku badania bezpieczeństwa systemu informacyjnego NIK, Izba zgłasza rozszerzenie składu komisji o swojego przedstawiciela.	Uwaga nieuwzględniona Ze względu na konieczność zapewnienia ochrony działania zespołów CSIRT nie przewiduje się możliwości rozszerzania komisji o przedstawiciela podmiotu, którego system podlegał badaniu.
9.	Prezes Urzędu Komunikacji Elektronicznej	Art. 39 ust. 10	Art. 1 pkt 37 lit. h dotyczący projektowanego art. 39 ust. 10 ustawy o ksc – proponuje się rozważyć dodanie przepisu zawierającego upoważnienie ustawowe do wydania	Uwaga nieuwzględniona Zrezygnowano z narzucania grupie różnorodnych podmiotów sposobu, w jaki mają usuwać i anonimizować

Zestawienie nieuwzględnionych uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

			rozporządzenia określającego sposób usuwania i anonimizowania danych, o których mowa w art. 39 ust. 4 ustawy o ksc.	przetwarzane dane. W ocenie projektodawcy są to czynności techniczne, które powinny być rozstrzygnięte na poziomie danej jednostki.
10.	Prezes Urzędu Transportu Kolejowego	Art. 41	Prezes UTK jest centralnym organem administracji rządowej niezależnym od ministra właściwego do spraw transportu. Jako regulator i organ nadzorujący bezpieczeństwo transportu kolejowego, Prezes UTK dysponuje specjalistyczną wiedzą na temat funkcjonowania tego rynku. To pozwala na pełne zrozumienie specyficznych zagrożeń i potrzeb związanych z cyberbezpieczeństwem, które jest nieodłącznym elementem bezpieczeństwa infrastruktury kolejowej i przewozów kolejowych. Obecnie Prezes UTK nie posiada żadnych kompetencji w zakresie cyberbezpieczeństwa. Włączenie cyberbezpieczeństwa do istniejących ram regulacyjnych i nadzorczych Prezesa UTK pozwoli na bardziej holistyczne podejście do zarządzania ryzykiem w transporcie kolejowym. Prezes UTK ma bowiem doświadczenie w monitorowaniu przestrzegania przepisów prawnych i norm bezpieczeństwa oraz certyfikacji w sektorze kolejowym. Prezes UTK mógłby wdrożyć procedury oceny zgodności i audyty bezpieczeństwa w zakresie zgodności z krajowym systemem cyberbezpieczeństwa jako część standardowych procedur audytowych realizowanych wobec przewoźników, zarządców infrastruktury oraz inne podmioty kolejowe. Rozszerzenie zadań tego organu o cyberbezpieczeństwo w podsektorze transportu kolejowego może wpłynąć na efektywniejsze egzekwowanie przepisów dotyczących ochrony infrastruktury cyfrowej w kolejnictwie Proponuje się w zmienianym art. 41 nadać następujące brzmienie pkt 2: „2) dla sektora transportu z wyłączeniem podsektora transportu wodnego oraz podsektora transportu kolejowego – minister właściwy do spraw transportu;” oraz po pkt 2 dodać pkt 2a w brzmieniu: „2a) dla podsektora transportu kolejowego – Prezes Urzędu Transportu Kolejowego;”.	Uwaga nieuwzględniona Minister Infrastruktury (MI) jest organem właściwym ds. cyberbezpieczeństwa dla sektora transportu, w tym podsektora transportu kolejowego od 2018 r. - zadania organu właściwego są realizowane przez MI już od dłuższego czasu, w związku z czym MI nie tylko zbudowało i posiada wiedzę i kompetencje dziedziczne, ale także przeniesienie zadań dla tego podsektora do UTK jako organu właściwego doprowadziłoby do nieproporcjonalnego rozdziału obowiązków nadzorczych pomiędzy podsektor kolejowy i pozostałe podsektory w sektorze transportu. Postulat ustanowienia UTK jako organu właściwego ds. cyberbezpieczeństwa jest tym bardziej nieuzasadniony, gdy weźmie się pod uwagę, że UTK nie jest jednostką podległą i nadzorowaną przez MI. Wyłączenie podsektora kolejowego spod właściwości MI oddziałuje negatywnie nie tylko w kontekście wyżej przedstawionych

Zestawienie nieuwzględnionych uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

				argumentów, ponieważ taka sytuacja rodziłaby konieczność dokonania szeregu zmian: czy to w przestrzeni prawnej, czy w zakresie współpracy w obszarze sektora transportu, czy chociażby wymiany informacji.
11.	Prezes Urzędu Transportu Kolejowego	Art. 42 ust. 9	Niniejsza uwaga wiąże się z uwagą nr 2 powyżej, której konsekwencją jest konieczność zapewnienia możliwości finansowania zadań Prezesa UTK jako organu właściwego do spraw cyberbezpieczeństwa dla podmiotów kluczowych. W zmienianym art. 42 proponuje się następujące brzmienie dodawanego ust. 9: „9. Komisja Nadzoru Finansowego oraz Prezes Urzędu Transportu Kolejowego otrzymują dotację celową na realizację swoich zadań ustawowych z części budżetowej, której dysponentem jest Szef Kancelarii Prezesa Rady Ministrów”.	Uwaga nieuwzględniona W zw. z nieuwzględnieniem uwagi UTK do projektowanego art. 41.
12.	Urząd Komisji Nadzoru Finansowego	Art. 44	Z perspektywy wyznaczenia CSIRT KNF jako podstawowego punktu kontaktowego dla EU-SCICF, tj. ram koordynacji ustanowionych w celu wykonania zalecenia Europejskiej Rady ds. Ryzyka Systemowego z dnia 2 grudnia 2021 r. w sprawie ogólnoeuropejskich ram koordynacji dla odpowiednich organów w odniesieniu do cyberincydentów o charakterze systemowym (ERRS/2021/17), korzystne byłoby wskazanie w ustawie na możliwość uczestnictwa CSIRT sektorowych w sieci CSIRT. W przypadku CSIRT KNF dałoby to m.in. możliwość nawiązywania bezpośrednich relacji z zespołami, z którymi CSIRT KNF może współpracować w ramach EU-SCICF. Przykładem CSIRT sektorowego z innego państwa UE, który jest członkiem sieci CSIRT, jest austriacki zespół CSIRT dla sektora energii (Austrian Energy CERT (AEC)). Obecnie do uczestnictwa w sieci CSIRT odnoszą się jedynie przepisy dotyczące zadań CSIRT poziomu krajowego.	Uwaga nieuwzględniona Zgodnie z dyrektywą NIS2 w sieci CSIRT uczestniczą National CSIRTs a nie CSIRT sektorowe.
13.	Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy	Art. 48 pkt 6	W aktualnym brzmieniu art. 48 pkt 6 rekomendujemy usunięcie sformułowania „oraz Sieci CSIRT”. CSIRT poziomu krajowego są członkami sieci CSIRT, więc zapewnienie wymiany informacji przez ministra nie jest konieczne. W tym punkcie jednak warto rozważyć dodanie regulacji dot. EU-CyCLONE. Zwracamy się również z prośbą o rozważenie wyznaczenia przez ministra właściwego do spraw informatyzacji reprezentanta Polski w Sieci CSIRT (w roli Standing Representative). Dotychczas funkcję tę pełniła wyznaczona osoba z CSIRT NASK.	Uwaga nieuwzględniona Przedmiotowy przepis nie jest zmieniany w ramach niniejszej nowelizacji ani też nie otrzymywano zgłoszeń co do problemów ze stosowaniem tego przepisu. W związku z tym nie wymaga on zmiany.

Zestawienie nieuwzględnionych uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

14.	Urząd Komisji Nadzoru Finansowego	Art. 48	W art. 48 UKSC postuluje się oznaczenie jego dotychczasowej treści jako ust. 1 i dodanie ust. 2 w brzmieniu: „Pojedynczy Punkt Kontaktowy współpracuje i wymienia informacje z właściwym organem w rozumieniu rozporządzenia 2022/2554 gdy jest to niezbędne dla realizacji zadań Pojedynczego Punktu Kontaktowego bądź realizacji zadań tego właściwego organu.”. Dodawany ust. 2 stanowi odzwierciedlanie art. 47 ust. 2 rozporządzenia 2022/2554, zgodnie z którym „W stosownych przypadkach właściwe organy mogą konsultować się i wymieniać informacje z pojedynczymi punktami kontaktowymi i CSIRT wyznaczonymi lub ustanowionymi zgodnie z dyrektywą (UE) 2022/2555.”.	Uwaga nieuwzględniona Przekazywanie informacji otrzymywanych z innych krajów przez Pojedynczy Punkt Kontaktowy jest już możliwa i będzie dalej możliwa na podstawie art. 49 ust. 3. W związku z tym nie ma konieczności dokonania zmiany.
15.	Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy	Art. 53b ust. 2	W zakresie art. 53b ust. 2 warto wskazać, że zawarte w pkt 1 i 2 elementy analizy ryzyka wydają się wykraczać poza obszar tematyczny ustawy, a tym samym mogą być bardzo trudne do oceny dla organu właściwego.	Uwaga nieuwzględniona Wskazane elementy analizy ryzyka są zdaniem projektodawcy ściśle związane z obszarem tematycznym ustawy. Cyberbezpieczeństwa nie sposób jest odłączyć od kwestii związanych z bezpieczeństwem narodowym, porządkiem publicznym, gospodarką i społeczeństwem, a także pozostałymi zagadnieniami związanymi ze stratami finansowymi, szkodami wizerunkowymi czy zakłóceniami w funkcjonowaniu systemów i infrastruktury. Elementy te oddziałują bowiem silnie na funkcjonowanie państwa na poziomie ekonomicznym i społecznym. W związku z tym uwzględnienie tych elementów w analizie ryzyka przy tworzeniu hierarchii priorytetów w sprawowaniu nadzoru po stworzeniu metodyki w ocenie projektodawcy są konieczne. Jednocześnie projektodawca nie

Zestawienie nieuwzględnionych uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

				wyklucza, że analizie będą poddane inne elementy dlatego posłużył się sformułowaniem „w szczególności”. Metodyki nadzoru oraz hierarchizacja nie są ponadto obligatoryjne a mają jedynie na celu sprawniejsze zarządzanie zadaniami i ich prawidłową realizację.
16.	Rzecznik Małych i Średnich Przedsiębiorców	Art. 67b, art. 67c i art. 67e	Art. 1 pkt 70 Projektu (dodający po art. 67 ustawy zmienianej art. 67a - 67k) określa m.in. (w art. 67b i kolejne) zasady oraz procedury postępowania w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. W odniesieniu do powyższego - zmiany wymagać mogą następujące projektowane regulacje: – dodawany do ustawy zmienianej art. 67b ust. 1 pkt 2 powinien przy określeniu kręgu przedsiębiorców telekomunikacyjnych podlegających regulacji posługiwać się pojęciami stosowanymi już w Projekcie - w tym przypadku mikroprzedsiębiorcy, – dodawany do ustawy zmienianej art. 67b ust. 4 zawiera niedopuszczalną dyskryminację mniejszych podmiotów przez uniemożliwienie im uprawnienia do wnioskowego przystąpienia do postępowania na prawach strony - należy całkowicie zaniechać uzależnienia uprawnienia od wartości przychodu lub obrotu podmiotu chcącego wstąpić do postępowania o uznanie za dostawcę wysokiego ryzyka, – dodawany do ustawy zmienianej art. 67b ust. 18 i 19 - ze względu na możliwe skutki, w szczególności dla podmiotów kluczowych i podmiotów ważnych, decyzji ministra ds. informatyzacji o uznaniu dostawcy sprzętu lub usługi za dostawcę wysokiego ryzyka - obligatoryjnie powinien przysługiwać wniosek o ponowne rozpatrzenie sprawy, – obowiązki oraz okresy zawarte w dodawanym art. 67c ust. 1, 2 i 5 ustawy zmienianej dla podmiotów, o których mowa w art. 67b ust. 1 (dodawanym do ustawy zmienianej) — wymagają ponownej analizy oraz ewentualnie możliwości wydłużenia okresów użytkowania sprzętu lub usług pochodzących od dostawców uznanych za dostawców wysokiego ryzyka, – dodawany do ustawy zmienianej art. 67e ust. 2 powinien przewidywać możliwość doręczenia wyroku skarżącemu w treści i w zakresie umożliwiającym mu skuteczną ochronę swoich praw, dlatego treść tego przepisu wymaga zmiany.	Uwaga nieuwzględniona Wyłączenia podmiotowe w zakresie strony postępowania mają zapewnić sprawność postępowania. Wyłączenie wniosku o ponowne rozpatrzenie sprawy jest konieczne – przyspieszy to możliwość odwołania się do sądu administracyjnego. Zróźnicowanie okresów wycofania sprzętu/oprogramowania od wielkości podmiotu spowoduje to, że duży podmiot będzie miał inny termin na wycofanie sprzętu, niż jego podwykonawca, co spowoduje kolejne zagrożenia. Nie można wprowadzić obowiązku doręczenia uzasadnienia wyroku zawierającego informacje niejawne.

Zestawienie nieuwzględnionych uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

			Uzasadnienie: W dodawanym do ustawy zmienianej art. 67b ust. 1 pkt 2 projektodawcy wprowadzają nową siatkę pojęciową - kryterium 10 mln złotych przychodu w poprzednim roku obrotowym, mimo iż kwota ta może być nieco wyższa niż próg ekonomiczny dla mikroprzedsiębiorcy - to jednak warto zastanowić się nad użyciem powszechnie stosowanego pojęcia (także w Projekcie) oraz nad rozszerzeniem wyjątku także na małych przedsiębiorców (oba pojęcia w rozumieniu Rozporządzenia 651/2014, stosowanym w Projekcie). Wskazać należy, iż możliwy zasięg niezamierzonego stosowania sprzętu lub usług pochodzących od dostawców wysokiego ryzyka - w przypadku podmiotów będących mikroprzedsiębiorcami i małymi przedsiębiorcami jest ograniczony, a prawdopodobny wpływ na poziom cyberbezpieczeństwa adekwatnie mniejszy. Dodawany art. 67b ust. 4 ogranicza możliwość wstąpienia do postępowania o uznanie za dostawcę wysokiego ryzyka tylko dla przedsiębiorców komunikacji elektronicznej, którzy w poprzednim roku obrotowym uzyskali przychód z tytułu prowadzenia działalności telekomunikacyjnej w wysokości co najmniej dwudziestotysięcznej krotności przeciętnego wynagrodzenia w gospodarce narodowej wskazanego w ostatnim komunikacie Prezesa Głównego Urzędu Statystycznego, o którym mowa w art. 20 pkt 1 lit. a ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych. W pierwszej kolejności uprawnienie niniejsze powinno przysługiwać każdemu podmiotowi objętemu zakresem regulacji, czyjego interesu prawnego lub obowiązku dotyczy postępowanie albo kto żąda czynności organu ze względu na swój interes prawny lub obowiązek, zgodnie z ogólnymi zasadami postępowania administracyjnego określonymi w art. 28 ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego. Powyższe pozwoli na skuteczną ochronę praw każdemu podmiotowi, na sytuację którego mogą mieć wpływ skutki postępowania. Z tego względu postulat ten jest zasadny. W odniesieniu do art. 67c ust. 1, 2 i 5 dodawanych do ustawy zmienianej wskazać należy, iż proponowane Projektem regulacje wymagają przekonstruowania. Projektodawcy pomijają skalę kosztów oraz utrudnień organizacyjnych związanych z całkowitym wycofaniem produktów lub usług pochodzących od dostawcy wysokiego ryzyka. Dotkliwość skutków proponowanych przepisów jest niemożliwa do oszacowania ze względu na nieograniczoną skalę konsekwencji, które zwłaszcza dla najmniejszych podmiotów mogą być niemożliwe do podołania. Według art. 66 ust. 1 ustawy Prawo Przedsiębiorców oraz kolejnych zawartych w Rozdziale 6 „Zasady opracowywania projektów aktów normatywnych z zakresu prawa gospodarczego oraz oceny ich funkcjonowania” - przed rozpoczęciem prac nad opracowaniem projektu aktu normatywnego określającego zasady podejmowania,	

Zestawienie nieuwzględnionych uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

			wykonywania lub zakończenia działalności gospodarczej dokonuje się analizy możliwości osiągnięcia celu tego aktu normatywnego za pomocą innych środków oraz oceny przewidywanych skutków społeczno-gospodarczych, w tym oceny wpływu na sytuację mikroprzedsiębiorców, małych i średnich przedsiębiorców oraz analizy zgodności projektowanych regulacji z przepisami (przywołanej) ustawy. Obowiązkiem Projektodawcy nie uczynili zadość, w szczególności biorąc pod uwagę istotne poszerzenie kręgu podmiotów, których regulacje zawarte w Projekcie będą mogły dotyczyć. Podkreślić należy, iż w przypadku stwierdzenia wpływu projektu aktu normatywnego na sytuację mikroprzedsiębiorców, małych i średnich przedsiębiorców, przy opracowaniu projektu aktu normatywnego należy dążyć do proporcjonalnego ograniczenia obowiązków wobec tych przedsiębiorców (art. 68 ustawy Prawo przedsiębiorców). Dodawany do ustawy zmienianej art. 67e ust. 2 wprowadza możliwość doręczenia skarżącemu wyroku z ograniczeniem treści jego uzasadnienia. Regulacja taka jest niedopuszczalna i wymaga zmiany, gdyż uniemożliwia skarżącemu skuteczną ochronę swoich praw i stanowi zaprzeczenie realizowanej przez Rzeczypospolitą Polską idei demokratycznego państwa prawa. Ochrona tej wartości nie może się odbywać przez jej zaprzeczenie, do czego dążą projektodawcy. Omawiany przepis powinien przewidywać możliwość doręczenia wyroku skarżącemu w treści i w zakresie umożliwiającym mu skuteczną ochronę swoich praw, przy jednoczesnej ochronie ewentualnych informacji niejawnych ważnych dla bezpieczeństwa państwa, dlatego treść tego przepisu wymaga postulowanej zmiany.	
17.	Prezes Urzędu Komunikacji Elektronicznej	Art. 67c ust. 2	Art. 1 pkt 70 w zakresie dotyczącym projektowanego art. 67c ust. 2 ustawy o ksc – w odniesieniu do niniejszego przepisu (dotyczącego kwestii wycofywania w ciągu 4 lat, przez przedsiębiorców telekomunikacyjnych, o których mowa w projektowanym art. 67b ust. 1 pkt 2 ustawy o ksc, typów produktów ICT, rodzajów usług ICT, konkretnych procesów ICT wskazanych w decyzji i określonych w wykazie kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług w załączniku nr 3 do ustawy o ksc) proponuje się jego uszczegółowienie w sposób, z którego wynikałoby, iż wycofywanie, o którym mowa w tym przepisie, powinno być dokonywane: a) niezwłocznie, jednakże nie później niż w ciągu 12 miesięcy, w przypadkach: – obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej przedsiębiorcy telekomunikacyjnego (ujętych w jednolitym wykazie, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2023 r. poz. 122)),	Uwaga nieuwzględniona Projektodawca chce utrzymać kompromis, jakim są obecne postanowienia tego przepisu.

Zestawienie nieuwzględnionych uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

			– typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT używanych w celu wykonywania zadań i obowiązków na potrzeby systemu kierowania bezpieczeństwem narodowym, w tym obroną państwa (na zasadach określonych w planach, decyzjach lub umowach zawartych między przedsiębiorcami telekomunikacyjnymi a uprawnionymi podmiotami), b) w pozostałych przypadkach – sukcesywnie, w okresie od 1 roku do 4 lat, z uwzględnieniem pierwszeństwa obszarów o największej gęstości zaludnienia. Niniejsza propozycja jest zgodna z wymaganiami określonymi na potrzeby aukcji 5G, które uzyskały w dniu 23 marca 2023 r. pozytywną opinię Kolegium do Spraw Cyberbezpieczeństwa.	
18.	Rzecznik Małych i Średnich Przedsiębiorców	Art. 73	Art. 1 pkt 74 Projektu wprowadza nowy system kar, w tym kar pieniężnych za naruszenie regulacji wynikających z Projektu. Ze względu na złożoną istotę będącą przedmiotem projektowanych regulacji oraz znaczne poszerzenie kręgu podmiotów nimi objętych, postuluje się uzupełnienie treści art. 1 pkt 74 Projektu o obligatoryjne uzależnienie wysokości ewentualnie nakładanych kar od wielkości podmiotu oraz proporcjonalne ograniczenie wysokości kar dla mikroprzedsiębiorców i małych przedsiębiorców. Ze względu na konieczność wdrożenia przez wiele podmiotów, w tym również mniejszych, które wcześniej nie podlegały tego typu regulacjom – nowych rozwiązań oraz związanego z tym wysiłku organizacyjnego i finansowego – zasadny jest postulat, aby w ciągu pierwszych 6 miesięcy od wejścia w życie regulacji wynikających z projektu, w pierwszej kolejności pouczać przedsiębiorców, a nie karać finansowo.	Uwaga nieuwzględniona Kryteria, od których należy uzależniać wymiar kary zostały bezpośrednio wskazane w dyrektywie NIS2. Jednocześnie należy zwrócić uwagę na fakt, że ustawa przewiduje okres dostosowawczy 6 miesięczny, w którym nie obowiązują przepisy o karach.
19.	Narodowy Bank Polski	Art. 73 ust. 1	Ad. art. 1 pkt 74 lit. a projektu ustawy w zakresie zmiany brzmienia art. 73 ust. 1. Kara pieniężna, o której mowa w ust. 1–3, może być wymierzona w kwocie nie większej niż 600% otrzymywanego przez ukaranego wynagrodzenia obliczanego według zasad obowiązujących przy ustalaniu ekwiwalentu pieniężnego za urlop. Przedstawiony wskaźnik procentowy nie precyzuje przedziału czasowego za jaki otrzymywane było wynagrodzenie, a zatem pojawia się dowolność interpretacji w tym zakresie. Powyższe nie jest w naszej ocenie właściwe, w związku z czym sugerujemy doprecyzowanie zapisu.	Uwaga nieuwzględniona W przedmiocie wynagrodzenia kierownika podmiotu wskazać należy, że podobne instytucje funkcjonują już w obrocie prawnym. Jednakże nie doprecyzowują okresu otrzymywanego wynagrodzenia. W ocenie projektodawcy nie zachodzi potrzeba dookreślenia tego w przepisie – organ będzie brał pod

Zestawienie nieuwzględnionych uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

				uwagę wynagrodzenie otrzymywane obecnie, które zostanie ustalone na podstawie dokumentacji przekazanej przez kierownika podmiotu.
20.	Prezes Głównego Urzędu Statystycznego	Art. 74 ust. 3	W art. 74 ust. 3 otrzymuje brzmienie: „3. Wpływy z tytułu kar pieniężnych, o których mowa w art. 73 i art. 73a, stanowią przychód Funduszu Cyberbezpieczeństwa, o którym mowa w art. 2 ustawy z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa.” Projekt ustawy (poza środkami dla CSIRT MON, CSIRT NASK, CSIRT GOV, organach właściwych do spraw cyberbezpieczeństwa, CSIRT sektorowych) nie przewiduje żadnych środków dla podmiotów publicznych, które uznane zostaną za podmioty kluczowe lub ważne. W związku z niskim poziomem zarobków w administracji publicznej, w porównaniu do podmiotów komercyjnych, ogromnym problemem dla publicznych podmiotów jest pozyskanie pracowników wykwalifikowanych w zakresie cyberbezpieczeństwa, bezpieczeństwa informacji, ochrony danych osobowych. Mimo, że w roku 2022 podjęto prace nad projektem nowelizacji ustawy z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa, w którym między innymi rozszerzono katalog podmiotów które uzyskiwałyby środki z tego funduszu (w tym GUS i inne jednostki służ statystyki publicznej) projekt nie został sfinalizowany i nie trafił pod obrady sejmu. (Numer projektu: UD390) https://legislacja.rcl.gov.pl/projekt/12360152/katalog/12882662#12882662) Obecnie w obliczu wdrażania dyrektywy NIS 2 jeszcze bardziej niż w 2022 roku potrzebne jest wprowadzenie systemowych rozwiązań, zapewniających podmiotom publicznym środki finansowe na cyberbezpieczeństwo i bezpieczeństwo informacji. Środki powinny być przeznaczone nie tylko na wynagrodzenia pracowników, ale też na dofinansowanie zakupu infrastruktury i oprogramowania oraz na usługi zewnętrzne np. szkolenia, testy bezpieczeństwa i audyty bezpieczeństwa informacji.	Uwaga nieuwzględniona W ramach niniejszego projektu skupiono się na zmianach w ustawie o krajowym systemie cyberbezpieczeństwa, a zmiany w innych ustawach są wprowadzane tylko gdy wynika to z konieczności zapewnienia spójności rozwiązań. W związku z tym jedyne zmiany w ustawie o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa są konsekwencją zmian w ustawie o krajowym systemie cyberbezpieczeństwa. Zaproponowana regulacja jest już wystarczająco rozbudowana i niecelowe byłoby rozszerzanie jej o nowe obszary merytoryczne. Dokładna analiza zapotrzebowania poszczególnych podmiotów na świadczenie teleinformatyczne, zostanie przeprowadzona w toku ewentualnych prac legislacyjnych nad osobnym projektem ustawy.

Zestawienie nieuwzględnionych uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

				Jednocześnie uprzejmie informuję, że w ramach inwestycji C3.1.1 Cyberbezpieczeństwo - CyberPL, infrastruktura przetwarzania danych i dostarczania usług cyfrowych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo – Komponent Cyberbezpieczeństwo (subinwestycja C3.1.1.1), planowane jest uruchomienie czterech projektów dedykowanych dla wybranych grup podmiotów krajowego systemu cyberbezpieczeństwa, w tym dla jednostek sektora finansów publicznych. Aktualnie trwają prace do przygotowania naborów, z uwzględnieniem ich celu określonego w Krajowym Planie Odbudowy i Zwiększania Odporności. Docelowe grupy odbiorców wsparcia będą wynikały bezpośrednio z tych założeń. Uruchamianie naborów dla tych projektów planowane jest sukcesywnie w kolejnych kwartałach bieżącego roku.
UWAGI do przepisów przejściowych i przepisów końcowych				
21.	Rzecznik Małych i Średnich Przedsiębiorców	Art. 7	Należy całkowicie zaniechać zmiany objętej art. 7 Projektu. Postulat usunięcia art. 7 z treści projektu. Uzasadnienie:	Uwaga nieuwzględniona Należy zwrócić uwagę na fakt, że w ustawie – Prawo przedsiębiorców, w przepisie zmienianym niniejszą

Zestawienie nieuwzględnionych uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

		W pierwszej kolejności treść zaproponowanej zmiany nie koresponduje z art. 1 pkt 58 Projektu, w dalszej kolejności wskazać należy na bezpodstawne rozszerzenie wyłączenia stosowania przepisów o prowadzeniu więcej niż jednej kontroli. Proponowana treść wskazanego wyżej przepisu ma charakter nadregulacji i będzie sprzeczna z fundamentalnymi zasadami ustawy Prawo przedsiębiorców (Konstytucja Biznesu). Art. 45 ust. 1 i 2 ustawy Prawo przedsiębiorców stanowi: „Kontrola działalności gospodarczej przedsiębiorców jest przeprowadzana na zasadach określonych w niniejszej ustawie, chyba że zasady i tryb kontroli wynikają z ratyfikowanych umów międzynarodowych albo bezpośrednio stosowanych przepisów prawa Unii Europejskiej”. Jedynie „w zakresie nieuregulowanym w niniejszym rozdziale stosuje się odrębne przepisy.” Odrębne przepisy mają służyć przede wszystkim do wskazania zakresu przedmiotowego kontroli działalności gospodarczej przedsiębiorcy oraz organów upoważnionych do jej przeprowadzenia – jak stanowi art. 45 ust. 3 ustawy Prawo przedsiębiorców. Znaczenie Prawa przedsiębiorców wielokrotnie było podkreślane przez Radę Ministrów, która projektowi temu nie bez przyczyny nadała robocze miano Konstytucji Biznesu – co miało dodatkowo podkreślać rangę wydanych przepisów i które miały mieć walor porządkujący najistotniejsze zagadnienia z punktu widzenia prowadzenia działalności gospodarczej. Powyższe uregulowania jasno wskazują, że wszystkie przepisy szczególne dotyczące sposobu kontroli przedsiębiorców zawarto w ustawie Prawo przedsiębiorców (Konstytucja Biznesu). Wydawanie kolejnych przepisów, w kwestiach uregulowanych już w Rozdziale 5 (ograniczenia kontroli działalności gospodarczej) ustawy Prawo przedsiębiorców będzie mogło stanowić zachętę do naruszania przepisów tej ustawy. Rozpraszenie przepisów o ograniczaniu uprawnień podczas kontroli przedsiębiorców, niezależnie od tego, że jest zasadniczo niewłaściwe metodologiczne – to w sposób nieunikniony, jak wskazuje praktyka poszczególnych resortów kształtowania tych przepisów na własne potrzeby – prowadzi do trudnych, zawiłych, nieprzyswajalnych i chaotycznych regulacji. Proponowana w Projekcie, niewłaściwa metoda regulacji, może stanowić pretekst do obchodzenia przepisów ustawy Prawo Przedsiębiorców (Konstytucji Biznesu) przez organy kontroli i być nie tyle użytecznym i niezbędnym narzędziem do zwalczania działań niepożądanych, co elementem kształtującym szkodliwą praktykę legislacyjną i środkiem blokującym rozwój przedsiębiorczości. Z przytoczonych powodów – wnoszę o zaniechanie zmiany zawartej w art. 7 Projektu.	ustawą zawarte są także inne przypadki, kiedy ustawy – Prawo przedsiębiorców się nie stosuje. Tym samym projektowana ustawa nie wprowadza precedensowego wyłomu z dotychczasowej praktyki, a jedynie dokonuje zmiany koniecznej dla zapewnienia skuteczności prowadzonej kontroli. Jest to niezwykle istotne z uwagi na zakres przedmiotowy ustawy oraz jej istotne znaczenie dla bezpieczeństwa państwa.

Zestawienie nieuwzględnionych uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

22.	Rzecznik Praw Obywatelskich	Art. 9	Wnoszę o dołączenie Biura Rzecznika Praw Obywatelskich do listy podmiotów uprawnionych do stosowania ustawy z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa (Dz. U. z 2023 r. poz. 667). Zmiana ta mogłaby polegać na dopisaniu w art. 5 pkt 2) tej ustawy Biura Rzecznika Praw Obywatelskich, co upoważniałoby pracowników Biura do pobierania dodatku do wynagrodzenia z tytułu realizacji zadań związanych z cyberbezpieczeństwem. W sprawie dołączenia pracowników Biura Rzecznika Praw Obywatelskich korespondencja z Ministerstwem Cyfryzacji jest już prowadzona od marca 2022 r. (pisma z dnia 1 marca 2022 r., z dnia 15 grudnia 2022 r. i z dnia 15 grudnia 2023 r. – kopie w załączeniu), w której w sposób jednoznaczny wykazano, że uwagi na okoliczność, iż Rzecznik Praw Obywatelskich wchodzi w skład krajowego systemu bezpieczeństwa (art. 4 pkt 7 nowelizowanej ustawy) i w tym zakresie wykonuje zadania publiczne jako podmiot kluczowy, to niezrozumiałe jest pozbawienie Rzecznika możliwości finansowania dodatków do wynagrodzeń dla pracowników zapewniających wysoki poziom bezpieczeństwa systemów informatycznych służących do świadczenia usług kluczowych i cyfrowych oraz do obsługi incydentów. W przypadku uwzględnienia Biura Rzecznika Praw Obywatelskich w katalogu instytucji, o których mowa w przedmiotowej ustawie, których pracownicy mogą być uprawnieni do otrzymywania świadczenia teleinformatycznego, szacunkowy koszt roczny dodatków dla 16 pracowników Biura wyniesie ok. 960 000 zł.	<table><tr><td>Stanowisko</td><td>ilość etatów</td></tr><tr><td>Kierownik jednostki</td><td>1</td></tr><tr><td>Dyrektor i Zastępca Dyrektora</td><td>2</td></tr><tr><td>Naczelnik WI</td><td>1</td></tr><tr><td>Pracownicy działu Cyberbezpieczeństwa</td><td>2</td></tr><tr><td>IOD</td><td>2</td></tr><tr><td>Radca prawny</td><td>1</td></tr></table>	Stanowisko	ilość etatów	Kierownik jednostki	1	Dyrektor i Zastępca Dyrektora	2	Naczelnik WI	1	Pracownicy działu Cyberbezpieczeństwa	2	IOD	2	Radca prawny	1	Uwaga nieuwzględniona W ramach niniejszego projektu skupiono się na zmianach w ustawie o krajowym systemie cyberbezpieczeństwa, a zmiany w innych ustawach są wprowadzane tylko gdy wynika to z konieczności zapewnienia spójności rozwiązań. W związku z tym jedyne zmiany w ustawie o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa są konsekwencją zmian w ustawie o krajowym systemie cyberbezpieczeństwa. Zaproponowana regulacja jest już wystarczająco rozbudowa i niecelowe byłoby rozszerzanie jej o nowe obszary merytoryczne. Dokładna analiza zapotrzebowania poszczególnych podmiotów na świadczenie teleinformatyczne, zostanie przeprowadzona w toku ewentualnych prac legislacyjnych nad osobnym projektem ustawy.
Stanowisko	ilość etatów																		
Kierownik jednostki	1																		
Dyrektor i Zastępca Dyrektora	2																		
Naczelnik WI	1																		
Pracownicy działu Cyberbezpieczeństwa	2																		
IOD	2																		
Radca prawny	1																		

Zestawienie nieuwzględnionych uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

			Administratorzy WI	4		
			Pracownicy WI - dział wsparcia technicznego	3		
			razem etatów:	16		
			kwota (ilość etatów * średnia kwota dodatku 5000 zł * 12 miesięcy)	960 000,00 zł		
23.	Rzecznik Praw Obywatelskich	Art. 9	Mając na względzie to, że projektowana nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa wprost zalicza Rzecznika Praw Obywatelskich do podmiotów kluczowych w rozumieniu art. 5 ust. 1 pkt 1) ustawy, to rozszerzenie możliwości przyznawania dodatku do wynagrodzenia o pracowników Biura RPO zapewni m.in. możliwość utworzenia nowych etatów do obsługi incydentów oraz zapobiegnie odpływowi kadry do sektora prywatnego. Obecne wynagrodzenie specjalistów w BRPO nie jest bowiem konkurencyjne względem rynku prywatnego.			Uwaga nieuwzględniona W ramach niniejszego projektu skupiono się na zmianach w ustawie o krajowym systemie cyberbezpieczeństwa, a zmiany w innych ustawach są wprowadzane tylko gdy wynika to z konieczności zapewnienia spójności rozwiązań. W związku z tym jedyne zmiany w ustawie o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa są konsekwencją zmian w ustawie o krajowym systemie cyberbezpieczeństwa. Zaproponowana regulacja jest już wystarczająco rozbudowa i niecelowe byłoby rozszerzanie jej o nowe obszary merytoryczne. Dokładna analiza zapotrzebowania poszczególnych podmiotów na świadczenie teleinformatyczne, zostanie przeprowadzona w toku ewentualnych prac legislacyjnych nad osobnym projektem ustawy.

Zestawienie nieuwzględnionych uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

24.	Rzecznik Praw Obywatelskich	Art. 9	Dodatkowo wskazuję, że zgodnie z rządowym projektem ustawy o ochronie sygnalistów (druk sejmowy nr 317) Rzecznik Praw Obywatelskich został wskazany jako podmiot odpowiedzialny za realizację zupełnie nowych zadań publicznych związanych ze zgłaszaniem informacji o naruszeniach prawa, co wiąże się z przygotowaniem nowego elektronicznego kanału zgłaszania naruszeń. Tym samym wiąże się też z koniecznością zapewnienia obsługi informatycznej i bezpieczeństwa systemu, którego celem ma być ochrona praw osób zgłaszających naruszenia prawa, tzw. „sygnalistów”.	Uwaga nieuwzględniona W ramach niniejszego projektu skupiono się na zmianach w ustawie o krajowym systemie cyberbezpieczeństwa, a zmiany w innych ustawach są wprowadzane tylko gdy wynika to z konieczności zapewnienia spójności rozwiązań. W związku z tym jedyne zmiany w ustawie o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa są konsekwencją zmian w ustawie o krajowym systemie cyberbezpieczeństwa. Zaproponowana regulacja jest już wystarczająco rozbudowa i niecelowe byłoby rozszerzanie jej o nowe obszary merytoryczne. Dokładna analiza zapotrzebowania poszczególnych podmiotów na świadczenie teleinformatyczne, zostanie przeprowadzona w toku ewentualnych prac legislacyjnych nad osobnym projektem ustawy.
25.	Urząd Patentowy Rzeczypospolitej Polskiej	Art. 9	W art. 9 pkt 2 projektu ustawy, wprowadzana jest zmiana w ustawie z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa i zasadnym wydaje się uwzględnienie również art. 5 pkt 2 lit d poprzez nadanie następującego brzmienia: <i>„d) jednostkach organizacyjnych podległych Radzie Ministrów, Prezesowi Rady Ministrów lub ministrom,”.</i> W ocenie Urzędu Patentowego wprowadzenie postulowanej zmiany pozwoli na uwzględnienie wśród podmiotów uprawnionych do ubiegania się do przyznanie	Uwaga nieuwzględniona W ramach niniejszego projektu skupiono się na zmianach w ustawie o krajowym systemie cyberbezpieczeństwa, a zmiany w innych ustawach są wprowadzane tylko gdy wynika to z konieczności zapewnienia spójności rozwiązań. W związku z tym jedyne zmiany w

Zestawienie nieuwzględnionych uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

			świadczenia teleinformatycznego szerszego kręgu podmiotów tj. również jednostek podległych Radzie Ministrów. Zauważyć należy, że zgodnie z art. 260 ust. 1 ustawy z dnia 30 czerwca 2000 r. – Prawo własności przemysłowej (Dz. U. z 2023 r. poz. 1170), Urząd Patentowy podlega Radzie Ministrów, a nadzór na działalnością Urzędu, z ramienia Rady Ministrów, sprawuje minister właściwy do spraw gospodarki. Obecne, z uwagi na to, że Urząd Patentowy jest organem podległym Radzie Ministrów, a nie Prezesowi Rady Ministrów, jest wyłączony z możliwości ubiegania się o przyznanie świadczenia teleinformatycznego. Powyższe nie wydaje się słuszne, gdyż decyzja prawodawcy, iż dany organ podlega Radzie Ministrów, a nie Prezesowi Rady Ministrów, czy określone ministrowi, nie powinna przesądzać o możliwości ubiegania się świadczenie teleinformatyczne. Kwestia ta powinna być rozstrzygana w oparciu o zakres wykonywanych zadań. W tym kontekście warto podkreślić, iż niewątpliwie Urząd Patentowy realizuje zadania z zakresu cyberbezpieczeństwa w rozumieniu ww. ustawy. Co więcej, mając na uwadze charakter wykonywanych przez Urząd Patentowy zadań, w szczególności dostęp do rozwiązań objętych zgłoszeniami wynalazków, czy wzorów użytkowych, w tym takich, które mogą zostać uznane za tajne, należy stwierdzić, iż prawidłowe wykonywanie zadań z zakresu cyberbezpieczeństwa jest szczególnie istotne.	ustawie o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa są konsekwencją zmian w ustawie o krajowym systemie cyberbezpieczeństwa. Zaproponowana regulacja jest już wystarczająco rozbudowa i niecelowe byłoby rozszerzanie jej o nowe obszary merytoryczne. Dokładna analiza zapotrzebowania poszczególnych podmiotów na świadczenie teleinformatyczne, zostanie przeprowadzona w toku ewentualnych prac legislacyjnych nad osobnym projektem ustawy.
26.	Główny Urząd Nadzoru Budowlanego	Art. 9 pkt 2	Artykuł 9 pkt 2 projektu ustawy, przewidujący nowelizację ustawy z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa, proponuję uzupełnić o zmianę w art. 5 w pkt 2 polegającą na dodaniu po lit. n lit. o w brzmieniu: <i>„o) urzędach centralnych”.</i> Alternatywnie poddaję pod rozważenie nadanie nowego brzmienia art. 5 pkt 2 lit. d ustawy o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa: <i>„d) jednostkach organizacyjnych podległych Prezesowi Rady Ministrów lub ministrom, lub jednostkach organizacyjnych przez nich nadzorowanych,”.</i> Pragnę wyjaśnić, że przy coraz większej grupie podmiotów dostarczających usługi cyfrowe zasadne wydaje się przyznanie świadczenia teleinformatycznego osobom realizującym zadania z zakresu cyberbezpieczeństwa zatrudnionym nie tylko w urzędach obsługujących ministrów, czy jednostkach organizacyjnych podległych ministrom, ale także osobom zatrudnionym w urzędach centralnych lub jednostkach organizacyjnych nadzorowanych	Uwaga nieuwzględniona W ramach niniejszego projektu skupiono się na zmianach w ustawie o krajowym systemie cyberbezpieczeństwa, a zmiany w innych ustawach są wprowadzane tylko gdy wynika to z konieczności zapewnienia spójności rozwiązań. W związku z tym jedyne zmiany w ustawie o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa są konsekwencją zmian w ustawie o krajowym systemie cyberbezpieczeństwa. Zaproponowana regulacja jest już

Zestawienie nieuwzględnionych uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

			przez poszczególnych ministrów. Pracownicy tych jednostek wykonują praktycznie takie same zadania jak pracownicy organów wymienionych w art. 5 pkt 2 ustawy szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa. Dlatego też, w mojej ocenie, za wykonywaną pracę powinno im zostać przyznane świadczenie teleinformatyczne, o którym mowa w art. 5 ww. ustawy.	wystarczająco rozbudowa i niecelowe byłoby rozszerzanie jej o nowe obszary merytoryczne. Dokładna analiza zapotrzebowania poszczególnych podmiotów na świadczenie teleinformatyczne, zostanie przeprowadzona w toku ewentualnych prac legislacyjnych nad osobnym projektem ustawy.
27.	Prezes Urzędu Transportu Kolejowego	Art. 9 pkt 2	W świetle stanowiska Ministra Cyfryzacji pracownicy Urzędu Transportu Kolejowego wykonujący zadania z zakresu cyberbezpieczeństwa nie są uprawnieni do otrzymania świadczenia teleinformatycznego z uwagi na fakt, że Prezes UTK jest jednostką nadzorowaną przez Prezesa Rady Ministrów, ale nie podległą Prezesowi Rady Ministrów. W obowiązującej treści ustawodawca nie przewidział w swojej regulacji niezależnych i objętych zasadą kadencyjności co spowodowało wprowadzenie niedopuszczalnej luki systemowej w przepisach prawa. W związku z tym proponuje się, aby dodać słowo „nadzorowane” aby zlikwidować lukę systemową w przepisach dotyczących świadczeń teleinformatycznych. Nie ulega wątpliwości, że UTK jako administrator rejestrów rangi rejestru państwowego czy zaawansowanej infrastruktury IT powinien również posiadać w zasobie narzędzia odpowiedniego wynagradzania pracowników z zakresu cyberbezpieczeństwa. Proponuje się dotychczasową zmianę pkt 1 oznaczyć jako lit. a i dodać lit. b w brzmieniu: „b) w pkt 2 lit. d otrzymuje brzmienie: „d) jednostkach organizacyjnych podległych lub nadzorowanych przez Prezesa Rady Ministrów lub ministrów,””.	Uwaga nieuwzględniona W ramach niniejszego projektu skupiono się na zmianach w ustawie o krajowym systemie cyberbezpieczeństwa, a zmiany w innych ustawach są wprowadzane tylko gdy wynika to z konieczności zapewnienia spójności rozwiązań. W związku z tym jedyne zmiany w ustawie o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa są konsekwencją zmian w ustawie o krajowym systemie cyberbezpieczeństwa. Zaproponowana regulacja jest już wystarczająco rozbudowa i niecelowe byłoby rozszerzanie jej o nowe obszary merytoryczne. Dokładna analiza zapotrzebowania poszczególnych podmiotów na świadczenie teleinformatyczne, zostanie przeprowadzona w toku

Zestawienie nieuwzględnionych uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

				ewentualnych prac legislacyjnych nad osobnym projektem ustawy.
28.	Prezes Urzędu Zamówień Publicznych	Art. 9 pkt 2	Na podstawie art. 9 pkt 2 projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw, zwanego dalej „Projektem”, planowane jest dokonanie zmiany w art. 5 pkt 1 ustawy z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa (Dz. U. z 2023 r. poz. 667). Przepis art. 5 ustawy o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa określa katalog organów, podmiotów i jednostek, których pracownicy mogą mieć przyznany dodatek za wykonywanie zadań z zakresu cyberbezpieczeństwa, zwany „świadczeniem teleinformatycznym”. W katalogu tym nie został wymieniony Urząd Zamówień Publicznych (UZP), co w praktyce uniemożliwia objęcie UZP świadczeniem teleinformatycznym, pomimo faktycznego wykonywania zadań z zakresu cyberbezpieczeństwa przez niektórych pracowników UZP. Chciałbym podkreślić, że UZP obsługuje szereg narzędzi i systemów informatycznych wymagających szczególnej ochrony pod kątem ich bezpieczeństwa cybernetycznego. Kluczowym systemem pod tym względem jest Platforma e-Zamówienia, której obsługę zapewnia UZP. Platforma e-Zamówienia stanowiąca bezpłatne narzędzie zarówno dla zamawiających – podmiotów, zwłaszcza z sektora finansów publicznych, zobowiązanych do udzielania zamówień publicznych na podstawie ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych (Dz. U. z 2023 r. poz. 1605 i 1720), zwanej dalej „ustawą Pzp”, jak i wykonawców – osób fizycznych i osób prawnych zainteresowanych udziałem w postępowaniach o udzielenie zamówienia publicznego lub konkursach. Beneficjentami są również dostawcy platform zakupowych, którzy wnioskuje o integrację z Platformą e-Zamówienia. Konieczność utrzymania i rozwoju Platformy e-Zamówienia jako systemu wspierającego elektroniczną realizację zamówień publicznych powoduje, że niezbędne jest zabezpieczenie zasobów osobowych i finansowych w celu zapewnienia bezpieczeństwa cybernetycznego tego systemu jak również ciągłości jego działania zarówno po stronie usług infrastrukturalnych, jak i usług utrzymania wsparcia użytkowników w bieżącej obsłudze produkcyjnej w zakresie rozwiązywania problemów technicznych. Z punktu widzenia bezpieczeństwa Platformy e-Zamówienia kluczowym elementem jest Moduł Ofert i Wniosków jako najbardziej istotny dla całego procesu ofertowego. Jego zadaniem jest szyfrowanie składanych ofert i wniosków oraz prac konkursowych, zabezpieczenie ich przed dostępem osób trzecich przed upływem wyznaczonych terminów, w szczególności otwarcia ofert w postępowaniu. Dodatkowym zadaniem Modułu Ofert i Wniosków jest zabezpieczenie oferty w taki sposób, żeby nie dopuścić do zapoznania się z	Uwaga nieuwzględniona W ramach niniejszego projektu skupiono się na zmianach w ustawie o krajowym systemie cyberbezpieczeństwa, a zmiany w innych ustawach są wprowadzane tylko gdy wynika to z konieczności zapewnienia spójności rozwiązań. W związku z tym jedyne zmiany w ustawie o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa są konsekwencją zmian w ustawie o krajowym systemie cyberbezpieczeństwa. Zaproponowana regulacja jest już wystarczająco rozbudowana i niecelowe byłoby rozszerzanie jej o nowe obszary merytoryczne. Dokładna analiza zapotrzebowania poszczególnych podmiotów na świadczenie teleinformatyczne, zostanie przeprowadzona w toku ewentualnych prac legislacyjnych nad osobnym projektem ustawy.

Zestawienie nieuwzględnionych uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

		jej treścią w sposób nieuprawniony. Dane gromadzone w trakcie procesu ofertowego wymagają szczególnego bezpieczeństwa, gdyż naruszenie integralności Platformy e-Zamówienia mogłoby prowadzić do szeregu zdarzeń, których skutki negatywnie wpłynęłyby na samą poufność tych danych. W kontekście zapewnienia bezpieczeństwa cybernetycznego kluczowym modulem Platformy e-Zamówienia jest Biuletyn Zamówień Publicznych, m.in. ze względu na fakt, że nie ma alternatywnych rozwiązań systemowych umożliwiających realizowanie przez zamawiających obowiązków wynikających z ustawy Pzp w zakresie zamieszczania ogłoszeń związanych z postępowaniami o udzielenie zamówienia publicznego lub konkursami. W UZP prowadzone są również działania zmierzające do informatyzacji Krajowej Izby Odwoławczej (KIO), w szczególności poprzez system e-Protokół (oparty o system ReCourt wykorzystywany w sądach powszechnych). Wdrożenie systemu e-Protokół gwarantuje orzekającym członkom KIO usprawnienie pracy poprzez jej elektronizację, co pozwala przede wszystkim na większą efektywność w rozpoznawaniu wnoszonych odwołań. W ww. systemie są również przetwarzane dane osobowe, przede wszystkim zamawiających i wykonawców, co wymaga objęcia go szczególną ochroną i nadzorem przed atakami hakerskimi. W planach jest także objęcie elektronizacją rozpraw przed KIO. Planowane jest ponadto wdrożenie elektronicznego systemu obsługi dokumentów EZD RP oraz jego integracja z Platformą e-Zamówienia. Wszystkie wymienione wyżej narzędzia wymagają należytego bieżącego zabezpieczenia cybernetycznego i opracowania planów ciągłości działania przed atakami hakerskimi. W związku z potrzebą zapewnienia stałego bezpieczeństwa funkcjonowania powyższych systemów informatycznych istotne jest objęcie świadczeniem teleinformatycznym, o którym mowa w art. 5 ustawy o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa, pracowników pionu IT oraz pionów wspomagających UZP zajmujących się obsługą tych systemów, co wzmocni wdrażanie nowych rozwiązań zabezpieczających w obszarze cyberbezpieczeństwa i zdolność UZP do szybkiego reagowania na wzrastającą liczbę incydentów cyberbezpieczeństwa oraz pojawiające się nowe zagrożenia. Utrzymanie stałego zespołu specjalistów z zakresu cyberbezpieczeństwa jest wręcz niezbędne dla prawidłowego wykonywania stojących przed Prezesem UZP zadań związanych z informatyzacją zamówień publicznych w tym również w związku z sukcesywnie poszerzanym katalogiem usług on-line udostępnianych przez UZP. Chciałbym także nadmienić, że podczas procesu legislacyjnego związanego z projektem ustawy o zmianie ustawy o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa oraz niektórych innych ustaw (nr UD390) projekt skierowany na komisję prawniczą (wersja z dnia 13 grudnia 2022 r.) zawierał zmiany w	

Zestawienie nieuwzględnionych uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

			zakresie art. 5 pkt 2 ustawy o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa jednoznacznie wskazujące, że UZP mieści się w katalogu podmiotów objętych świadczeniem teleinformatycznym. Ponadto podczas prac komisji prawniczej zapewniono, że Prezes UZP jest objęty katalogiem podmiotów wskazanych w wówczas projektowanym art. 3 ust. 9 tej ustawy. Proces legislacyjny dotyczący ww. projektu ustawy jednak nie zakończył się i ostatecznie założenia powyższe nie znalazły do tej pory odzwierciedlenia w przepisach ustawy o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa. Mając na względzie powyższe wnoszę o uwzględnienie przedstawionej argumentacji tak, aby z przepisów ustawy o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa, w szczególności z art. 5 pkt 2 tej ustawy, wyraźnie wynikało i nie budziło wątpliwości, że pracownicy UZP realizujący zadania z zakresu cyberbezpieczeństwa objęci są świadczeniem teleinformatycznym.	
29.	Najwyższa Izba Kontroli	Art. 9 ust. 2	Jak wynika z oceny skutków regulacji sporządzonej przez Ministerstwo Cyfryzacji w ramach Inwestycji C3.1.1. KPO Cyberbezpieczeństwo - CyberPL, infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo, przewiduje się m.in. realizację projektu pn. „Wsparcie 500 podmiotów krajowego systemu cyberbezpieczeństwa w modernizacji i rozbudowie infrastruktury cyberbezpieczeństwa w sieciach IT, w tym wsparcie podmiotów wykorzystujących technologie informacyjne (IT) oraz operacyjne (OT) stosowane w przemysłowych systemach sterowania (ICS)”. Projekt ten zakłada udzielenie wsparcia o wartości - ok. 700,5 mln zł m.in. dla ok. 70 urzędów administracji centralnej i rządowej. W ramach tego projektu urzędy administracji centralnej i rządowej będą mogły uzyskać wsparcie finansowe na dostosowanie się do niniejszej ustawy. NIK nie należy do administracji centralnej i rządowej i jako naczelny organ kontroli państwowej nie znalazła się w grupie podmiotów, którym przyznano dodatkowe wsparcie finansowe na realizację nowych zadań i obowiązków związanych z cyberbezpieczeństwem. Tymczasem, nowe obowiązki nałożone także na NIK przewidziane w projekcie, to m.in. zgłaszanie incydentów, wdrożenie systemu zarządzania bezpieczeństwem, przeprowadzanie co dwa lata audytów bezpieczeństwa systemów informacyjnych (jak to obecnie wynika z § 20 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych), czy wyznaczenia dwóch osób odpowiedzialnych za utrzymywanie kontaktów z innymi podmiotami kluczowymi i podmiotami ważnymi.	Uwaga nieuwzględniona W ramach niniejszego projektu skupiono się na zmianach w ustawie o krajowym systemie cyberbezpieczeństwa, a zmiany w innych ustawach są wprowadzane tylko gdy wynika to z konieczności zapewnienia spójności rozwiązań. W związku z tym jedyne zmiany w ustawie o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa są konsekwencją zmian w ustawie o krajowym systemie cyberbezpieczeństwa. Zaproponowana regulacja jest już wystarczająco rozbudowa i niecelowe byłoby rozszerzanie jej o nowe obszary merytoryczne. Dokładna analiza zapotrzebowania poszczególnych podmiotów na

Zestawienie nieuwzględnionych uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

			Należy przy tym zauważyć, że wielokrotnie postulowałem w pismach kierowanych do Ministra Cyfryzacji¹ o włączenie Najwyższej Izby Kontroli do grupy podmiotów, które mogą się ubiegać o przyznanie dodatku do wynagrodzenia za pracę, o których mowa w art. 5 ustawy z dnia 2 grudnia 2021 r o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu Cyberbezpieczeństwa (Dz. U. z 2023 r. poz. 667.) tj. podmiotów uprawnionych do ubiegania się o środki na sfinansowanie świadczenia teleinformatycznego (dodatku do wynagrodzenia za pracę dla osób realizujących zadania z zakresu Cyberbezpieczeństwa.) Powyższy postulat związany jest z procedowanym projektem ustawy o zmianie ustawy o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa oraz niektórych innych ustaw.	świadczenie teleinformatyczne, zostanie przeprowadzona w toku ewentualnych prac legislacyjnych nad osobnym projektem ustawy.
30.	Prezes Urzędu Komunikacji Elektronicznej	Art. 15 ust. 2	Art. 15 ust. 2 – proponuje się, aby organem właściwym do wpisania z urzędu do wykazu podmiotów kluczowych i podmiotów ważnych, tych operatorów usług kluczowych, którzy byli wpisani do wykazu operatorów usług kluczowych przed dniem wejścia w życie projektowanej ustawy, był minister właściwy do spraw informatyzacji (będący organem prowadzącym oba te wykazy), nie zaś organ właściwy do spraw cyberbezpieczeństwa.	Uwaga nieuwzględniona Minister będzie prowadził system teleinformatyczny, w którym będą znajdować się wykazy, ale możliwość dokonywania wpisu będzie miało wiele podmiotów w tym organy właściwe. To organy właściwe najlepiej znają swoje sektory i dlatego uzasadnione jest by to one dokonały wpisów.
31.	Rzecznik Małych i Średnich Przedsiębiorców	Art. 29	Wejście w życie przedmiotowej (projektowanej) ustawy, określone w art. 29 Projektu, powinno nastąpić po upływie co najmniej 6 miesięcy od dnia jej ogłoszenia. Taki okres vacatio legis sprzyjał będzie procesowi sprawnego i bezpiecznego, a nie szybkiego i obciążonego ryzykiem błędów - dostosowaniu się podmiotów zobowiązanych do nowych regulacji, które będą wymagać poniesienia znacznych kosztów i wysiłku organizacyjnego. Poza powyższym - wejście w życie części regulacji objętych Projektem powinno nastąpić dopiero po publikacji niezbędnych aktów wykonawczych (o czym mowa również w pkt 3 niniejszego pisma).	Uwaga nieuwzględniona Okres dostosowawczy pozostanie 6 miesięcy
32.	Polski Komitet Normalizacyjny	OSR	Warto wskazać, że Polskie Normy mogą być powoływane w przepisach prawa po opublikowaniu ich w języku polskim (art. 5 ust. 4 ustawy o normalizacji). Z tego względu, sugeruje się, aby Ustawodawca przewidział środki na tłumaczenia norm, w tym ich znowelizowanych wersji, których należy się spodziewać w przyszłości.	Uwaga nieuwzględniona Z uwagi na rezygnację z przywoływania Polskich Norm w projekcie nie przewiduje się ujmowania kosztów w OSR.

Zestawienie nieuwzględnionych uwag zgłoszonych w ramach opiniowania do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

			Proponujemy zatem aby w preliminarzu budżetowym przewidzieć środki na tłumaczenia Polskich Norm: 1. z zakresu nadrzędnych wymagań dotyczących świadczenia prywatnych usług ochrony dla infrastruktury krytycznej, które to normy mogą wspierać zapisy ustawy (m.in w art. 1 pkt 14 projektowanej ustawy dot. art. 10 ust.1 i 3 pkt 2) lit. f) – str.21: - PN-EN 17483-1:2021-11 Prywatne usługi ochrony - Zabezpieczenie infrastruktury krytycznej - Część 1: Wymagania ogólne - PN-EN 17483-2:2024-03 Prywatne usługi ochrony - Zabezpieczenie infrastruktury krytycznej - Część 2: Usługi ochrony portów lotniczych i lotnictwa - PN-EN 17483-3:2024-03 Prywatne usługi ochrony - Zabezpieczenie infrastruktury krytycznej - Część 3: Usługi ochrony morskiej i portowej 2. które mogą być wykorzystywane jako wspierające wdrożenie środków organizacyjnych i technicznych przewidzianych w projekcie tj.: -PN-EN ISO/IEC 27002:2023-01Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności - Zabezpieczanie informacji -PN-EN ISO 27007:2022-06Bezpieczeństwoinformacji, cyberbezpieczeństwo i ochrona prywatności -Wytyczne dotyczące audytu systemów zarządzania bezpieczeństwem informacji -PN-EN ISO 22313:2020-08 Bezpieczeństwo i odporność -Systemy zarządzania ciągłością działania -Wytyczne dotyczące stosowania ISO 22301 oraz opracowywane w chwili obecnej projekty Polskich Norm: -prPN-prEN ISO/IEC 27005 Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności -Wytyczne do zarządzania ryzykami w bezpieczeństwie informacji -prPN-EN ISO/IEC 27006-1, Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności -Wymagania dla jednostek prowadzących audyt i certyfikację systemów zarządzania bezpieczeństwem informacji -Część 1: Postanowienia ogólne.	

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

TYTUŁ PROJEKTU	Projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)
TYTUŁ WDRAŻANEGO AKTU PRAWNEGO	Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz. Urz. UE L 333 z 27.12.2022, str. 80).
WYJAŚNIENIE TERMINU WEJŚCIA W ŻYCIE PROJEKTU	Projektowana ustawa wejdzie w życie po upływie miesiąca od dnia jej ogłoszenia. Termin ten uwzględnia zakres regulacji projektu, do którego muszą dostosować się podmioty, których on dotyczy oraz konieczność pilnego wdrożenia dyrektywy NIS 2, z uwagi na przekroczenie terminu implementacji, tj. dnia 17 października 2024 r. Projekt ustawy przewiduje 6 miesięczny okres dostosowawczy dla podmiotów kluczowych i podmiotów ważnych.

JEDN. RED.	TREŚĆ PRZEPISU UE	KONIECZNOŚĆ WDROŻENIA TAK/NIE*	JEDN. RED.	TREŚĆ PRZEPISU/PRZEPISÓW PROJEKTU
Art. 1	ROZDZIAŁ I PRZEPISY OGÓLNE Artykuł 1 Przedmiot 1. Niniejszą dyrektywą ustanawia się środki mające na celu osiągnięcie wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii, aby poprawić funkcjonowanie rynku wewnętrznego. 2. W tym celu niniejsza dyrektywa określa: a) obowiązki państw członkowskich dotyczące przyjęcia krajowych strategii cyberbezpieczeństwa oraz wyznaczenia lub powołania właściwych organów, organów ds. zarządzania kryzysowego w cyberbezpieczeństwie, pojedynczych punktów kontaktowych ds. cyberbezpieczeństwa (pojedyncze punkty kontaktowe) oraz zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT); b) środki zarządzania ryzykiem w cyberbezpieczeństwie oraz obowiązki w zakresie zgłaszania incydentów spoczywające na podmiotach w rodzaju tych, o których mowa w załączniku I lub II, jak również na podmiotach zidentyfikowanych jako podmioty o charakterze krytycznym podmiotów dyrektywy (UE) 2022/2557;	NIE		

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

	c) zasady i obowiązki w zakresie wymiany informacji o cyberbezpieczeństwie; d) obowiązki w zakresie nadzoru i egzekwowania przepisów spoczywające na państwach członkowskich.			
Art. 2	Artykuł 2 Zakres 1. Niniejsza dyrektywa ma zastosowanie do podmiotów publicznych lub prywatnych w rodzaju tych, o których mowa w załączniku I lub II, które kwalifikują się jako średnie przedsiębiorstwa na podstawie art. 2 załącznika do zalecenia 2003/361/WE lub które przekraczają pułapy dla średnich przedsiębiorstw określone w ust. 1 tego artykułu oraz które świadczą usługi lub prowadzą działalność w Unii. Art. 3 ust. 4 załącznika do tego zalecenia nie ma zastosowania do celów niniejszej dyrektywy.	TAK	Art. 1 pkt 10 (art. 5 ust. 1–11)	Art. 5. 1. Podmiotem kluczowym jest: 1) osoba fizyczna, osoba prawna albo jednostka organizacyjna nieposiadająca osobowości prawnej wskazana w załączniku nr 1 do ustawy, która przewyższa wymogi dla średniego przedsiębiorstwa określone w art. 2 ust. 1 załącznika I do rozporządzenia Komisji (UE) nr 651/2014 z dnia 17 czerwca 2014 r. uznającego niektóre rodzaje pomocy za zgodne z rynkiem wewnętrznym w zastosowaniu art. 107 i 108 Traktatu (Dz. Urz. UE L 187 z 26.06.2014, str. 1, z późn. zm.¹⁾), zwanego dalej „rozporządzeniem 651/2014/UE”; 2) przedsiębiorca komunikacji elektronicznej, który co najmniej spełnia wymogi dla średniego przedsiębiorcy określone w art. 2 ust. 1 załącznika I do rozporządzenia 651/2014/UE albo je przewyższa; 3) dostawca usług zarządzanych w zakresie cyberbezpieczeństwa, który co najmniej spełnia wymogi dla małego albo średniego przedsiębiorcy określone w art. 2 ust. 1 załącznika I do rozporządzenia 651/2014/UE albo je przewyższa; 4) niezależnie od wielkości podmiotu: a) dostawca usług DNS,

¹⁾ Zmiany wymienionego rozporządzenia zostały ogłoszone w Dz. Urz. UE L 329 z 15.12.2025, str. 28, Dz. Urz. UE L 149 z 07.06.2016, str. 10, Dz. Urz. UE L 156 z 20.06.2017, str. 1, Dz. Urz. UE L 26 z 31.01.2018, str. 53, Dz. Urz. UE L 215 z 07.07.2020, str. 3, Dz. Urz. UE L 89 z 16.03.2021, str. 1, Dz. Urz. UE L 270 z 29.07.2021, str. 39, Dz. Urz. UE L 119 z 05.05.2023, str. 159 oraz Dz. Urz. UE L 167 z 30.06.2023, str. 1.

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				b) kwalifikowany dostawca usług zaufania w rozumieniu art. 3 pkt 20 rozporządzenia 910/2014, c) podmiot krytyczny, d) podmiot publiczny wskazany w załączniku nr 1 do ustawy w sektorze podmioty publiczne, e) podmiot zidentyfikowany jako podmiot kluczowy na podstawie art. 71 ust. 2 pkt 1, f) państwowa osoba prawna zidentyfikowana jako podmiot kluczowy na podstawie art. 7m, g) podmiot, który nie jest przedsiębiorcą, a jest wskazany w załączniku nr 1 do ustawy z nazwy albo przez określenie jego rodzaju, h) podmiot będący operatorem obiektu energetyki jądrowej, o którym mowa w art. 2 pkt 2 ustawy z dnia 29 czerwca 2011 r. o przygotowaniu i realizacji inwestycji w zakresie obiektów energetyki jądrowej oraz inwestycji towarzyszących (Dz. U. z 2025 r. poz.1156), i) rejestr nazw domen najwyższego poziomu (TLD), j) podmiot świadczący usługi rejestracji nazw domen. 2. Podmiotem ważnym jest: 1) osoba fizyczna, osoba prawna albo jednostka organizacyjna nieposiadająca osobowości prawnej wskazana w załączniku nr 1 do ustawy, która spełnia wymogi dla średniego przedsiębiorcy określone w art. 2 ust. 1 załącznika I do

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				rozporządzenia 651/2014/UE oraz która nie jest podmiotem kluczowym; 2) osoba fizyczna, osoba prawna albo jednostka organizacyjna nieposiadająca osobowości prawnej wskazana w załączniku nr 2 do ustawy, która spełnia wymogi dla średniego przedsiębiorcy określone w art. 2 ust. 1 załącznika I do rozporządzenia 651/2014/UE lub przewyższa te wymogi oraz która nie jest podmiotem kluczowym; 3) niekwalifikowany dostawca usług zaufania będący mikro-, małym lub średnim przedsiębiorcą, o którym mowa w art. 2 ust. 1 załącznika I do rozporządzenia 651/2014/UE; 4) przedsiębiorca komunikacji elektronicznej będący mikro- lub małym przedsiębiorcą, o którym mowa w art. 2 ust. 2 i 3 załącznika I do rozporządzenia 651/2014/UE; 5) podmiot będący inwestorem obiektu energetyki jądrowej, o którym mowa w art. 2 pkt 2 ustawy z dnia 29 czerwca 2011 r. o przygotowaniu i realizacji inwestycji w zakresie obiektów energetyki jądrowej oraz inwestycji towarzyszących, który uzyskał decyzję zasadniczą, o której mowa w art. 3a ust. 1 tej ustawy – niezależnie od jego wielkości; 6) podmiot zidentyfikowany jako podmiot ważny na podstawie art. 71 ust. 2 pkt 2; 7) podmiot, który nie jest przedsiębiorcą, a jest wskazany w załączniku nr 2 do ustawy z nazwy albo przez określenie jego rodzaju; 8) podmiot publiczny, który nie jest podmiotem kluczowym oraz jest

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				samorządową jednostką budżetową, samorządowym zakładem budżetowym, samorządową instytucją kultury albo spółką wykonującą zadania o charakterze użyteczności publicznej w rozumieniu art. 1 ust. 2 ustawy z dnia 20 grudnia 1996 r. o gospodarce komunalnej (Dz. U. z 2021 r. poz. 679), jeżeli realizuje zadanie publiczne z wykorzystaniem systemów informacyjnych. 3. Przy określaniu wymogów dla podmiotów, o których mowa w ust. 1 pkt 1–3, ust. 2 pkt 1–4, nie stosuje się art. 3 ust. 4 załącznika I do rozporządzenia 651/2014/UE. 4. Jeżeli podmiot, o którym mowa w ust. 1, spełnia wymogi zarówno dla podmiotu kluczowego, jak i dla podmiotu ważnego, to jest podmiotem kluczowym. 5. Jeżeli status podmiotu kluczowego lub podmiotu ważnego zależy od wielkości podmiotu, to przesłanki uznania za podmiot kluczowy lub podmiot ważny bada się według stanu na dzień sporządzenia sprawozdania finansowego. 6. Jeżeli podmiot spełnia wymogi do uznania za podmiot kluczowy, ponieważ przewyższa kryteria dla średniego przedsiębiorstwa zgodnie z art. 6 ust. 2–4 załącznika I do rozporządzenia 651/2014/UE, ale jego system informacyjny jest niezależny od systemów informacyjnych jego przedsiębiorstw powiązanych lub przedsiębiorstw partnerskich lub nie świadczy on usług wspólnie z jego przedsiębiorstwami powiązanymi lub przedsiębiorstwami partnerskimi, to nie jest podmiotem kluczowym.

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				7. Jeżeli podmiot spełnia wymogi do uznania za podmiot ważny, ponieważ spełnia kryteria dla średniego przedsiębiorstwa zgodnie z art. 6 ust. 2–4 załącznika I do rozporządzenia 651/2014/UE, ale jego system informacyjny jest niezależny od systemów informacyjnych jego przedsiębiorstw powiązanych lub przedsiębiorstw partnerskich lub nie świadczy on usług wspólnie z jego przedsiębiorstwami powiązanymi lub przedsiębiorstwami partnerskimi, to nie jest podmiotem ważnym. 8. Podmiot leczniczy, który nie jest przedsiębiorcą: 1) jest podmiotem ważnym, jeżeli zatrudnia od 50 do 249 osób; 2) jest podmiotem kluczowym, jeżeli zatrudnia co najmniej 250 osób. 9. Podmiot, o którym mowa w ust. 1 pkt 4 lit. h, staje się podmiotem kluczowym z dniem: 1) uzyskania zezwolenia na eksploatację, o której mowa w art. 4 ust. 1 pkt 3 ustawy z dnia 29 listopada 2000 r. – Prawo atomowe (Dz. U. z 2024 r. poz. 1277, 1897 i 1907) – w przypadku operatora składowiska odpadów promieniotwórczych; 2) uzyskania zezwolenia na eksploatację, o której mowa w art. 4 ust. 1 pkt 2 ustawy z dnia 29 listopada 2000 r. – Prawo atomowe, lub uzyskania koncesji na wytwarzanie energii elektrycznej lub ciepła, o których mowa w art. 32 ust. 1 pkt 1 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne (Dz. U. z 2024 r. poz. 266, z późn. zm.), w zależności od tego, które zostanie uzyskane pierwsze – w przypadku operatora elektrowni jądrowej;

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				3) uzyskania zezwolenia na eksploatację, o której mowa w art. 4 ust. 1 pkt 2 ustawy z dnia 29 listopada 2000 r. – Prawo atomowe, lub uzyskania koncesji na wydobywanie kopalin, o której mowa w art. 22 ust. 1 pkt 2 ustawy z dnia 9 czerwca 2011 r. – Prawo geologiczne i górnicze (Dz. U. z 2024 r. poz. 1290 oraz z 2025 r. poz. 769 i 1023), w zależności od tego, które zostanie uzyskane pierwsze – w przypadku operatora zakładu do wydobywania rud uranu i toru ze złóż i do ich wstępnego przetwarzania; 4) uzyskania zezwolenia na eksploatację, o której mowa w art. 4 ust. 1 pkt 2 ustawy z dnia 29 listopada 2000 r. – Prawo atomowe – w przypadku operatorów pozostałych obiektów energetyki jądrowej. 10. Do podmiotów kluczowych lub podmiotów ważnych nie zalicza się służb specjalnych w rozumieniu art. 11 ustawy z dnia 24 maja 2022 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2025 r. poz. 902), a także podmiotów podległych lub nadzorowanych przez Ministra Obrony Narodowej. 11. Minister Obrony Narodowej wskaże, w drodze decyzji niepodlegającej ogłoszeniu, jednostki jemu podległe lub przez niego nadzorowane, które uznaje się za podmioty kluczowe lub podmioty ważne oraz określi sektor lub sektory, a także w razie potrzeby podsektor, do jakiego przypisuje dany podmiot.
Art. 2	2. Niniejsza dyrektywa ma również zastosowanie do podmiotów w rodzaju tych, o których mowa w załączniku I lub II, w przypadku gdy:	TAK	Art. 1 pkt 4 (zmiany w art. 2	Art. 2: 11j) przedsiębiorca komunikacji elektronicznej – przedsiębiorcę komunikacji elektronicznej w

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

	a) usługi świadczone są przez: (i) dostawców publicznych sieci łączności elektronicznej lub dostawców publicznych usług łączności elektronicznej; (ii) dostawców usług telekomunikacyjnych; (iii) rejestry nazw domen najwyższego poziomu, oraz dostawców usług telekomunikacyjnych; b) podmiot jest jedynym w danym państwie członkowskim dostawcą usługi, która ma kluczowe znaczenie dla utrzymania krytycznej działalności państwa lub gospodarki; c) zakłócenie usługi świadczonej przez podmiot mogłoby mieć znaczący wpływ na porządek publiczny, bezpieczeństwo publiczne lub zdrowie publiczne; d) zakłócenie usługi świadczonej przez podmiot mogłoby prowadzić do powstania poważnego ryzyka systemowego, w szczególności w sektorach, w których takie zakłócenie mogłoby mieć wpływ transgraniczny; e) podmiot ma charakter krytyczny ze względu na jego szczególne znaczenie na poziomie krajowym lub regionalnym dla konkretnego sektora lub rodzaju usługi lub dla innych współzależnych sektorów w państwie członkowskim; f) podmiot jest podmiotem administracji publicznej: (i) na poziomie rządu centralnego, zdefiniowanym przez państwo członkowskie, zgodnie z prawem krajowym; lub (ii) na poziomie regionalnym, zdefiniowanym przez państwo członkowskie zgodnie z prawem krajowym, który zgodnie z oceną opartą na analizie ryzyka świadczy usługi, których zakłócenie mogłoby mieć znaczący wpływ na krytyczną działalność społeczną lub gospodarczą.		w zakresie art. 2 pkt 11j–11k) Art. 1 pkt 10 (art. 5 ust. 1 pkt 2, 4 lit. a, b oraz e)	rozumieniu art. 2 pkt 39 ustawy z dnia 12 lipca 2024 r. – Prawo komunikacji elektronicznej (Dz. U. poz. 1221 oraz z 2025 r. poz. 637 i 820); 11k) przedsiębiorca telekomunikacyjny – przedsiębiorcę telekomunikacyjnego w rozumieniu art. 2 pkt 40 ustawy z dnia 12 lipca 2024 r. – Prawo komunikacji elektronicznej; Art. 5. 1. Podmiotem kluczowym jest: 2) przedsiębiorca komunikacji elektronicznej, który co najmniej spełnia wymogi dla średniego przedsiębiorcy określone w art. 2 ust. 1 załącznika I do rozporządzenia 651/2014/UE albo je przekracza; 4) niezależnie od wielkości podmiotu: a) dostawca usług DNS, b) kwalifikowany dostawca usług zaufania w rozumieniu art. 3 pkt 20 rozporządzenia 910/2014, e) podmiot zidentyfikowany jako podmiot kluczowy na podstawie art. 71 ust. 2 pkt 1.
Art. 2	3. Niniejsza dyrektywa ma zastosowanie do podmiotów zidentyfikowanych jako podmioty mające charakter krytyczny na mocy dyrektywy (UE) 2022/2557, niezależnie od ich wielkości.	TAK	Art. 1 pkt 4 (art. 2 pkt 11d), art. 1 pkt 10 (art. 5 ust. 1 pkt 4 lit. c)	Art. 2: 11d) podmiot krytyczny – podmiot krytyczny w rozumieniu art. 2 pkt 1 dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylającej dyrektywę Rady

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				2008/114/WE (Dz. Urz. UE L 333 z 27.12.2022, str. 164), zwanej dalej „dyrektywą 2022/2557”; Art. 5. 1. Podmiotem kluczowym jest: 4) niezależnie od wielkości podmiotu: c) podmiot krytyczny,
Art. 2	4. Niniejsza dyrektywa ma zastosowanie do podmiotów świadczących usługi rejestracji nazw domen, niezależnie od ich wielkości.	TAK	Art. 1 pkt 10 (art. 5 ust. 1 pkt 4 lit. j)	Art. 5. 1. Podmiotem kluczowym jest: 4) niezależnie od wielkości podmiotu: j) podmiot świadczący usługi rejestracji nazw domen.
Art. 2	5. Państwa członkowskie mogą postanowić, że niniejsza dyrektywa ma zastosowanie do: a) podmiotów publicznych; b) instytucji edukacyjnych, zwłaszcza gdy prowadzą one działalność badawczą o krytycznym znaczeniu.	TAK	Art. 1 pkt 10 (art. 5 ust. 1 pkt 4 lit. d), art. 1 pkt 16 (art. 8 ust. 3) i art. 1 pkt 21 (art. 12c)	Art. 5. 1. Podmiotem kluczowym jest: 4) niezależnie od wielkości podmiotu: d) podmiot publiczny wskazany w załączniku nr 1 do ustawy w sektorze podmioty publiczne, Art. 8. 3. Podmiot ważny będący podmiotem publicznym nie stosuje przepisu ust. 1. Podmiot ważny będący podmiotem publicznym opracowuje, wdraża, realizuje, monitoruje i utrzymuje w systemach informacyjnych kontrolowanych przez ten podmiot system zarządzania bezpieczeństwem informacji spełniający wymogi określone w załączniku nr 4 do ustawy. Art. 12c. Do podmiotu ważnego będącego podmiotem publicznym stosuje się przepisy art. 11–12, z wyjątkiem przepisów o przekazywaniu wczesnego ostrzeżenia, sprawozdania okresowego, sprawozdania z postępu obsługi incydentu i sprawozdania końcowego.
Art. 2	6. Niniejsza dyrektywa pozostaje bez uszczerbku dla spoczywającego na państwach członkowskich obowiązku ochrony	NIE		

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

	bezpieczeństwa narodowego oraz dla ich uprawnień do zabezpieczania innych podstawowych funkcji państwa, w tym zapewniania integralności terytorialnej państwa i utrzymywania porządku publicznego.			
Art. 2	7. Niniejsza dyrektywa nie ma zastosowania do podmiotów administracji publicznej, które prowadzą działalność w dziedzinach bezpieczeństwa narodowego, bezpieczeństwa publicznego, obronności lub egzekwowania prawa, w tym zapobiegania im, prowadzenia postępowań w sprawie przestępstw, ich wykrywania oraz ścigania.	TAK	Art. 1 pkt 10 (art. 5 ust. 10 i 11)	10. Do podmiotów kluczowych i podmiotów ważnych nie zalicza się służb specjalnych w rozumieniu art. 11 ustawy z dnia 24 maja 2022 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2025 r. poz. 902), a także podmiotów podległych lub nadzorowanych przez Ministra Obrony Narodowej. 11. Minister Obrony Narodowej wskaże, w drodze decyzji niepodlegającej ogłoszeniu, jednostki jemu podległe lub przez niego nadzorowane, które uznaje się za podmioty kluczowe lub podmioty ważne oraz określi sektor lub sektory, a także w razie potrzeby podsektor, do jakiego przypisuje dany podmiot.”
Art. 2	8. Państwa członkowskie mogą zwolnić określone podmioty, które prowadzą działania w obszarach bezpieczeństwa narodowego, bezpieczeństwa publicznego, obronności lub egzekwowania prawa, w tym zapobieganie przestępstwom, prowadzenie postępowań w ich sprawie, wykrywanie ich i ściganie, lub które świadczą usługi wyłącznie na rzecz podmiotów administracji publicznej, o których mowa w ust. 7 niniejszego artykułu, z obowiązków ustanowionych w art. 21 lub 23 w odniesieniu do tych działań lub tych usług. W takich przypadkach środki nadzoru i egzekwowania przepisów, o których mowa w rozdziale VII, nie mają zastosowania do tej konkretnej działalności lub tych usług. W przypadku gdy podmioty prowadzą działalność lub świadczą usługi wyłącznie w rodzaju tych, o których mowa w niniejszym ustępie, państwa członkowskie mogą również podjąć decyzję o zwolnieniu tych podmiotów z obowiązków określonych w art. 3 i 27.	TAK	Art. 1 pkt 10 (art. 5 ust. 10 i 11)	10. Do podmiotów kluczowych i podmiotów ważnych nie zalicza się służb specjalnych w rozumieniu art. 11 ustawy z dnia 24 maja 2022 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2025 r. poz. 902), a także podmiotów podległych lub nadzorowanych przez Ministra Obrony Narodowej. 11. Minister Obrony Narodowej wskaże, w drodze decyzji niepodlegającej ogłoszeniu, jednostki jemu podległe lub przez niego nadzorowane, które uznaje się za podmioty kluczowe lub podmioty ważne oraz określi sektor lub sektory, a także w razie potrzeby podsektor, do jakiego przypisuje dany podmiot.”
Art. 2	9. Ust. 7 i 8 nie mają zastosowania w przypadku, gdy podmiot działa jako dostawca usług zaufania.	NIE		

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

Art. 2	10. Niniejsza dyrektywa nie ma zastosowania do podmiotów, które państwa członkowskie zwolniły z zakresu stosowania rozporządzenia (UE) 2022/2554 zgodnie z art. 2 ust. 4 tego rozporządzenia.	NIE		
Art. 2	11. Obowiązki ustanowione w niniejszej dyrektywie nie wiążą się z dostarczaniem informacji, których ujawnienie byłoby sprzeczne z podstawowymi interesami państw członkowskich w zakresie bezpieczeństwa narodowego, bezpieczeństwa publicznego lub obronności.	NIE		
Art. 2	12. Niniejszą dyrektywę stosuje się bez uszczerbku dla rozporządzenia (UE) 2016/679, dyrektywy 2002/58/WE, dyrektyw Parlamentu Europejskiego i Rady 2011/93/UE (27) i 2013/40/UE (28) oraz dyrektywy (UE) 2022/2557.	NIE		
Art. 2	13. Bez uszczerbku dla art. 346 TFUE informacje, które są poufne zgodnie z przepisami unijnymi lub krajowymi, takimi jak przepisy dotyczące tajemnicy przedsiębiorstwa, podlegają wymianie z Komisją i innymi odpowiednimi organami zgodnie z niniejszą dyrektywą tylko wtedy, gdy wymiana taka jest niezbędna do stosowania niniejszej dyrektywy. Informacje podlegające wymianie ogranicza się do tego, co jest istotne dla celów takiej wymiany i proporcjonalne do jej celów. Podczas wymiany informacji zachowuje się poufność tych informacji oraz chroni się bezpieczeństwo i interesy handlowe danych podmiotów.	NIE		
Art. 2	14. Podmioty, właściwe organy, pojedyncze punkty kontaktowe i CSIRT przetwarzają dane osobowe w zakresie niezbędnym do celów niniejszej dyrektywy i zgodnie z rozporządzeniem (UE) 2016/679, w szczególności takie przetwarzanie odbywa się na podstawie jego art. 6. Przetwarzanie danych osobowych na mocy niniejszej dyrektywy przez dostawców publicznych sieci łączności elektronicznej lub dostawców publicznie dostępnych usług łączności elektronicznej odbywa się zgodnie z unijnymi przepisami o ochronie danych i unijnym prawem dotyczącym prywatności, w szczególności dyrektywą 2002/58/WE.	TAK	Art. 1 pkt 41 (art. 39)	Art. 39. 1. W celu realizacji zadań, o których mowa w art. 26 ust. 3 pkt 1–11, 14 i 16–21 i ust. 5–8, art. 26a–26c oraz art. 44 ust. 1–1c i ust. 3, CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT sektorowe przetwarzają dane pozyskane w związku z incydentami i cyberzagrożeniami, w tym dane osobowe, obejmujące także dane określone w art. 9 ust. 1 i art. 10 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), zwanego dalej „rozporządzeniem 2016/679”, w zakresie i w celu niezbędnym do realizacji tych zadań.”, b) w ust. 2: – wyrazy „sektorowe zespoły cyberbezpieczeństwa” zastępuje się wyrazami „CSIRT sektorowe”, – po wyrazach „art. 9 ust. 1” dodaje się wyrazy „i art. 10”, c) w ust. 3: – wprowadzenie do wyliczenia otrzymuje brzmienie: „CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT sektorowe przetwarzają dane osobowe pozyskane w związku z incydentami i cyberzagrożeniami”, – pkt 3 i 4 otrzymują brzmienie: „3) gromadzone przez podmioty kluczowe lub podmioty ważne w związku ze świadczeniem usług; 4) dotyczące podmiotów zgłaszających incydent zgodnie z art. 30 ust. 1.”, d) w ust. 4: – wprowadzenie do wyliczenia otrzymuje brzmienie: „W celu realizacji zadań określonych w ustawie minister właściwy do spraw informatyzacji, dyrektor Rządowego Centrum Bezpieczeństwa, Pełnomocnik, minister właściwy do spraw zagranicznych oraz organy właściwe do spraw cyberbezpieczeństwa przetwarzają dane osobowe pozyskane w związku z incydentami i cyberzagrożeniami.”, – pkt 1 otrzymuje brzmienie:

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				„1) gromadzone przez podmioty kluczowe lub podmioty ważne w związku ze świadczeniem usług;”, – uchyla się pkt 2, e) po ust. 4 dodaje się ust. 4a w brzmieniu: „4a. Minister właściwy do spraw informatyzacji przetwarza dane osobowe zawierające imię i nazwisko oraz numer PESEL osób fizycznych lub niepowtarzalny identyfikator środka identyfikacji elektronicznej, o którym mowa w aktach wykonawczych Komisji Europejskiej, wydanych na podstawie art. 12 ust. 8 rozporządzenia 910/2014, które w imieniu podmiotu kluczowego lub podmiotu ważnego korzystają z systemu teleinformatycznego, o którym mowa w art. 46 ust. 1, w celu ich uwierzytelnienia w tym systemie.”, f) ust. 5 i 6 otrzymują brzmienie: „5. Dane, o których mowa w ust. 3 i 4, są anonimizowane przez CSIRT MON, CSIRT NASK i CSIRT sektorowy niezwłocznie po stwierdzeniu, że nie są niezbędne do realizacji zadań, o których mowa w art. 26 ust. 3 pkt 1–11, 14 i 16–21 i ust. 5–8, art. 26a–26c oraz art. 44 ust. 1–1c i ust. 3. 6. Dane, o których mowa w ust. 3 i 4, niezbędne do realizacji zadań, o których mowa w art. 26 ust. 3 pkt 1–11, 14 i 16–21 i ust. 5–8, art. 26a–26c oraz art. 44 ust. 1–1c i ust. 3, są anonimizowane przez CSIRT MON, CSIRT NASK i CSIRT sektorowy po upływie 5 lat od zakończenia obsługi incydentu, którego dotyczą, z uwzględnieniem ust. 6”; g) po ust. 6 dodaje się ust. 6a i 6b w brzmieniu: „6a. Dane, o których mowa w ust. 3 i 4, niezbędne do realizacji zadania, o którym mowa w art. 26a,

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				są anonimizowane przez CSIRT NASK po upływie 5 lat od dnia ich pozyskania. 6b. Dane, o których mowa w art. 26c ust. 2, są anonimizowane przez CSIRT NASK po upływie 5 lat od dnia ich pozyskania.”, h) w ust. 7 wyrazy „sektorowe zespoły cyberbezpieczeństwa” zastępuje się wyrazami „CSIRT sektorowe”, 8. Realizacja obowiązków wynikających z art. 15, art. 16, art. 18 ust. 1 lit. a i d oraz art. 19 zdanie drugie rozporządzenia 2016/679 przez CSIRT MON, CSIRT NASK i CSIRT sektorowe, w zakresie danych, o których mowa w ust. 3, jest możliwa dopiero po zakończeniu obsługi incydentu, w związku z którym dane zostały pozyskane, lub po zakończeniu obsługi incydentu, do którego obsługi te dane są niezbędne.”, j) w ust. 9 we wprowadzeniu do wyliczenia wyrazy „sektorowe zespoły cyberbezpieczeństwa” zastępuje się wyrazami „CSIRT sektorowe”, k) dodaje się ust. 10 i 11 w brzmieniu: „10. Dane, o których mowa w ust. 4, są anonimizowane przez ministra właściwego do spraw informatyzacji, dyrektora Rządowego Centrum Bezpieczeństwa, Pełnomocnika, ministra właściwego do spraw zagranicznych oraz organy właściwe do spraw cyberbezpieczeństwa niezwłocznie po stwierdzeniu, że nie są niezbędne do realizacji zadań wynikających z ustawy, nie później niż po 5 latach po ich uzyskaniu. 11. Minister właściwy do spraw informatyzacji przetwarza dane osobowe, w tym dane, o których mowa w art. 9 ust. 1 rozporządzenia 2016/679, które zostały zawarte w stanowiskach zgłoszonych w ramach konsultacji publicznych

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				projektu dokumentu, o którym mowa w art. 45 ust. 3.
Art. 3	Artykuł 3 Podmioty kluczowe i ważne 1. Do celów niniejszej dyrektywy następujące podmioty uznaje się za podmioty kluczowe: a) podmioty w rodzaju tych, o których mowa w załączniku I, przekraczające pułapy dla średnich przedsiębiorstw, określone w art. 2 ust. 1 załącznika do 2003/361/WE; b) kwalifikowanych dostawców usług zaufania i rejestry nazw domen najwyższego poziomu, a także dostawców usług DNS, i ich wiarygodności; c) dostawców publicznych sieci łączności elektronicznej lub dostawców publicznie dostępnych usług łączności elektronicznej, które kwalifikują się jako średnie przedsiębiorstwa na podstawie art. 2 załącznika do 2003/361/WE; d) podmioty administracji publicznej, o których mowa w art. 2 ust. 2 lit. f) ppkt (i); e) inne podmioty w rodzaju tych, o których mowa w załączniku I lub II, które zostały wskazane przez państwo członkowskie jako podmioty kluczowe zgodnie z art. 2 ust. 2 lit. b)–d); f) podmioty wskazane jako podmioty krytyczne na podstawie dyrektywy (UE) 2022/2557, o których mowa w art. 2 ust. 3 załącznika do dyrektywy; g) jeżeli państwo członkowskie tak postanowi, podmioty, które to państwo członkowskie wskazało przed 16 stycznia 2023 r. jako operatorów usług kluczowych zgodnie z dyrektywą (UE) 2016/1148 lub prawem krajowym.	TAK	Art. 1 pkt 10 (art. 5 ust. 1), art. 1 pkt 14 (art. 71 i art. 7m) i art. 15 pkt 1	Art. 5. 1. Podmiotem kluczowym jest: 1) osoba fizyczna, osoba prawna albo jednostka organizacyjna nieposiadająca osobowości prawnej wskazana w załączniku nr 1 do ustawy, która przewyższa wymogi dla średniego przedsiębiorstwa określone w art. 2 ust. 1 załącznika I do rozporządzenia Komisji (UE) nr 651/2014 z dnia 17 czerwca 2014 r. uznającego niektóre rodzaje pomocy za zgodne z rynkiem wewnętrznym w zastosowaniu art. 107 i 108 Traktatu (Dz. Urz. UE L 187 z 26.06.2014, str. 1, z późn. zm.²⁾), zwanego dalej „rozporządzeniem 651/2014/UE”; 2) przedsiębiorca komunikacji elektronicznej, który co najmniej spełnia wymogi dla średniego przedsiębiorcy określone w art. 2 ust. 1 załącznika I do rozporządzenia 651/2014/UE albo je przewyższa; 3) dostawca usług zarządzanych w zakresie cyberbezpieczeństwa, który co najmniej spełnia wymogi dla małego albo średniego przedsiębiorcy określone w art. 2 ust. 1 załącznika I do rozporządzenia 651/2014/UE albo je przewyższa; 4) niezależnie od wielkości podmiotu: a) dostawca usług DNS, b) kwalifikowany dostawca usług zaufania w rozumieniu art. 3 pkt 20 rozporządzenia 910/2014, c) podmiot krytyczny, d) podmiot publiczny wskazany w załączniku nr 1 do ustawy w sektorze podmioty publiczne,

²⁾ Zmiany wymienionego rozporządzenia zostały ogłoszone w Dz. Urz. UE L 329 z 15.12.2025, str. 28, Dz. Urz. UE L 149 z 07.06.2016, str. 10, Dz. Urz. UE L 156 z 20.06.2017, str. 1, Dz. Urz. UE L 26 z 31.01.2018, str. 53, Dz. Urz. UE L 215 z 07.07.2020, str. 3, Dz. Urz. UE L 89 z 16.03.2021, str. 1, Dz. Urz. UE L 270 z 29.07.2021, str. 39, Dz. Urz. UE L 119 z 05.05.2023, str. 159 oraz Dz. Urz. UE L 167 z 30.06.2023, str. 1.

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				e) podmiot zidentyfikowany jako podmiot kluczowy na podstawie art. 71 ust. 2 pkt 1, f) państwowa osoba prawna zidentyfikowana jako podmiot kluczowy na podstawie art. 7m, g) podmiot, który nie jest przedsiębiorcą, a jest wskazany w załączniku nr 1 do ustawy z nazwy albo przez określenie jego rodzaju, h) podmiot będący operatorem obiektu energetyki jądrowej, o którym mowa w art. 2 pkt 2 ustawy z dnia 29 czerwca 2011 r. o przygotowaniu i realizacji inwestycji w zakresie obiektów energetyki jądrowej oraz inwestycji towarzyszących (Dz. U. z 2025 r. poz. 1156), i) rejestr nazw domen najwyższego poziomu (TLD), j) podmiot świadczący usługi rejestracji nazw domen. Art. 71. 1. Organ właściwy do spraw cyberbezpieczeństwa, w drodze decyzji, może uznać osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej za podmiot kluczowy lub podmiot ważny, która nie spełnia przesłanek określonych w art. 5 ust. 1 pkt 1-3, pkt 4 lit. a-d oraz g-j, ust. 2 pkt 1-5 oraz 7 i 8, ust. 3-11, jeżeli: 1) jest podmiotem określonym w załączniku nr 1 lub 2 do ustawy; 2) spełnia co najmniej jedną z poniższych przesłanek: a) jako jedyna świadczy usługę, za pomocą systemu informacyjnego, która ma kluczowe znaczenie dla krytycznej działalności społecznej lub gospodarczej, b) zakłócenie usługi świadczonej przez nią za pomocą systemu informacyjnego spowoduje poważne zagrożenie dla bezpieczeństwa państwa,

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				bezpieczeństwa i porządku publicznego, obronności lub zdrowia publicznego, c) zakłócenie usługi świadczonej przez nią za pomocą systemu informacyjnego spowoduje ryzyko systemowe zaprzestania świadczenia usług przez podmioty kluczowe lub podmioty ważne lub d) świadczenie przez nią, za pomocą systemu informacyjnego, usługi ma istotne znaczenie na poziomie wojewódzkim lub krajowym lub ma znaczenie dla dwóch lub więcej sektorów określonych w załączniku nr 1 lub 2 do ustawy. 2. Podmiot uznaje się za: 1) podmiot kluczowy, jeżeli prowadzi działalność określoną w załączniku nr 1 do ustawy; 2) podmiot ważny, jeżeli prowadzi działalność określoną w załączniku nr 2 do ustawy. 3. W decyzji, o której mowa w ust. 1, organ właściwy do spraw cyberbezpieczeństwa: 1) określa sektor i podsektor, do którego należy przypisać podmiot; 2) wzywa podmiot do uzupełnienia brakujących danych w wykazie, w terminie 2 miesięcy od dnia doręczenia decyzji, pod rygorem nałożenia kary pieniężnej. 4. Do wezwania do uzupełnienia brakujących danych w wykazie stosuje się przepis art. 7b ust. 3. 5. Decyzja, o której mowa w ust. 1, podlega natychmiastowemu wykonaniu. 6. Organ właściwy do spraw cyberbezpieczeństwa niezwłocznie wpisuje do wykazu podmiot, wobec którego wydano decyzję, o której mowa w ust. 1.

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				7. Podmiot, wobec którego wydano decyzję, o której mowa w ust. 1: 1) realizuje obowiązki, o których mowa w rozdziale 3, w terminie 12 miesięcy, 2) zapewnia przeprowadzenie po raz pierwszy audytu, o którym mowa w art. 15 ust. 1, w terminie 24 miesięcy – od dnia doręczenia tej decyzji. Art. 7m. 1. Minister właściwy do spraw informatyzacji może uznać, w drodze decyzji, państwową osobę prawną, o której mowa w art. 3 ust. 1 ustawy z dnia 16 grudnia 2016 r. o zasadach zarządzania mieniem państwowym (Dz. U. z 2024 r. poz. 125, 834, 1823, 1897 i 1940), za podmiot kluczowy w sektorze podmiotów publicznych, jeżeli realizuje, za pomocą systemu informacyjnego, zadanie publiczne: 1) którego zakłócenie spowoduje poważne zagrożenie dla bezpieczeństwa państwa, bezpieczeństwa i porządku publicznego, obronności lub zdrowia publicznego lub 2) które ma istotne znaczenie na poziomie krajowym. 2. Decyzja, o której mowa w ust. 1, podlega natychmiastowemu wykonaniu. 3. Minister właściwy do spraw informatyzacji wzywa państwową osobę prawną, wobec której wydano decyzję, o której mowa w ust. 1, do uzupełnienia brakujących danych w wykazie, w terminie 2 miesięcy od dnia doręczenia decyzji, o której mowa w ust. 1, pod rygorem nałożenia kary pieniężnej. 4. Do wezwania do uzupełnienia brakujących danych w wykazie, o którym mowa w ust. 3, stosuje się przepis art. 7b ust. 3.

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				5. Minister właściwy do spraw informatyzacji niezwłocznie wpisuje do wykazu państwową osobę prawną, wobec której wydano decyzję, o której mowa w ust. 1. 6. Państwowa osoba prawna, wobec której wydano decyzję, o której mowa w ust. 1: 1) realizuje obowiązki, o których mowa w rozdziale 3, w terminie 6 miesięcy, 2) zapewnia przeprowadzenie po raz pierwszy audytu, o którym mowa w art. 15 ust. 1, w terminie 24 miesięcy – od dnia doręczenia tej decyzji. Art. 15. W ustawie z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. z 2024 r. poz. 1725) wprowadza się następujące zmiany: 1) w art. 4 po ust. 5 dodaje się ust. 5a i 5b w brzmieniu: „5a. Do wniosku o wpis, o którym mowa w ust. 1, dołącza się dane i informacje, o których mowa w art. 7 ust. 3 pkt 1–17 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077 i 1222 oraz z 2025 r. poz. 1017, 1069 i...). 5b. Po wpisie do rejestru, minister właściwy do spraw informatyzacji dane i informacje, o których mowa w art. 7 ust. 3 pkt 1–17 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, wpisuje do wykazu podmiotów kluczowych i podmiotów ważnych, o którym mowa w art. 7 ust. 1 tej ustawy. Danych tych i informacji w rejestrze”;
Art. 3	2. Do celów niniejszej dyrektywy podmioty w rodzaju tych, o których mowa w załączniku I lub II, które nie kwalifikują się jako podmioty kluczowe zgodnie z ust. 1 niniejszego artykułu, uznaje się	TAK	Art. 1 pkt 10 (art. 5 ust. 2 i 3)	Art. 5. 2. Podmiotem ważnym jest: 1) osoba fizyczna, osoba prawna albo jednostka organizacyjna

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

	za podmioty ważne. Odnosi się to również do podmiotów, które zostały wskazane przez państwa członkowskie jako podmioty ważne zgodnie z art. 2 ust. 2 lit. b)–e).			nieposiadająca osobowości prawnej wskazana w załączniku nr 1 do ustawy, która spełnia wymogi dla średniego przedsiębiorcy określone w art. 2 ust. 1 załącznika I do rozporządzenia 651/2014/UE oraz która nie jest podmiotem kluczowym; 2) osoba fizyczna, osoba prawna albo jednostka organizacyjna nieposiadająca osobowości prawnej wskazana w załączniku nr 2 do ustawy, która spełnia wymogi dla średniego przedsiębiorcy określone w art. 2 ust. 1 załącznika I do rozporządzenia 651/2014/UE lub przewyższa te wymogi oraz która nie jest podmiotem kluczowym; 3) niekwalifikowany dostawca usług zaufania będący mikro-, małym lub średnim przedsiębiorcą, o którym mowa w art. 2 ust. 1 załącznika I do rozporządzenia 651/2014/UE; 4) przedsiębiorca komunikacji elektronicznej będący mikro- lub małym przedsiębiorcą, o którym mowa w art. 2 ust. 2 i 3 załącznika I do rozporządzenia 651/2014/UE; 5) podmiot będący inwestorem obiektu energetyki jądrowej, o którym mowa w art. 2 pkt 2 ustawy z dnia 29 czerwca 2011 r. o przygotowaniu i realizacji inwestycji w zakresie obiektów energetyki jądrowej oraz inwestycji towarzyszących, który uzyskał decyzję zasadniczą, o której mowa w art. 3a ust. 1 tej ustawy – niezależnie od jego wielkości;

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				6) podmiot zidentyfikowany jako podmiot ważny na podstawie art. 71 ust. 2 pkt 2; 7) podmiot, który nie jest przedsiębiorcą, a jest wskazany w załączniku nr 2 do ustawy z nazwy albo przez określenie jego rodzaju; 8) podmiot publiczny, który nie jest podmiotem kluczowym oraz jest samorządową jednostką budżetową, samorządowym zakładem budżetowym, samorządową instytucją kultury albo spółką wykonującą zadania o charakterze użyteczności publicznej w rozumieniu art. 1 ust. 2 ustawy z dnia 20 grudnia 1996 r. o gospodarce komunalnej (Dz. U. z 2021 r. poz. 679), jeżeli realizuje zadanie publiczne z wykorzystaniem systemów informacyjnych. 3. Przy określaniu wymogów dla podmiotów, o których mowa w ust. 1 pkt 1–3, ust. 2 pkt 1–4, nie stosuje się art. 3 ust. 4 załącznika I do rozporządzenia 651/2014/UE.
Art. 3	3. Do dnia 17 kwietnia 2025 r. państwa członkowskie ustanawiają wykaz podmiotów kluczowych i ważnych, a także podmiotów świadczących usługi rejestracji nazw domen. Państwa członkowskie regularnie, i nie rzadziej niż co dwa lata po wyżej wymienionej dacie, dokonują przeglądu i – w stosownych przypadkach – aktualizacji tego wykazu.	TAK	Art. 22 i art. 34	Art. 22. 1 Operatorzy usług kluczowych, o których mowa w ustawie zmienianej w art. 1, stają się podmiotami kluczowymi, z dniem wejścia w życie niniejszej ustawy. 2. Do operatorów usług kluczowych, o których mowa w ust. 1, będących podmiotami podległymi lub nadzorowanymi przez Ministra Obrony Narodowej, nie stosuje się art. 5 ust. 10 i 11 ustawy zmienianej w art. 1 w brzmieniu nadanym niniejszą ustawą.

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				Art. 34. 1. Minister właściwy do spraw informatyzacji utworzy wykaz podmiotów kluczowych i podmiotów ważnych, w terminie miesiąca od dnia wejścia w życie niniejszej ustawy. 2. Minister właściwy do spraw informatyzacji wpisuje, z urzędu, do wykazu podmiotów kluczowych i podmiotów ważnych operatorów usług kluczowych wpisanych przed dniem wejścia w życie niniejszej ustawy do wykazu operatorów usług kluczowych. Przepis art. 7b ustawy zmienianej w art. 1 dodany niniejszą ustawą stosuje się odpowiednio. 3. Minister właściwy do spraw informatyzacji ogłasza w swoim dzienniku urzędowym, komunikat określający harmonogram: 1) złożenia wniosków o wpis do wykazu podmiotów kluczowych i podmiotów ważnych przez podmioty kluczowe i podmioty ważne, które w dniu wejścia w życie niniejszej ustawy spełniają przesłanki uznania ich za podmiot kluczowy albo podmiot ważny; 2) rozpoczęcia korzystania przez podmioty, o których mowa w pkt 1, z systemu teleinformatycznego, o którym mowa w art. 46 ust. 1 ustawy zmienianej w art. 1, w brzmieniu nadanym niniejszą ustawą. 4. W harmonogramie, o którym mowa w ust. 3, wskazuje się terminy dokonywania czynności przez poszczególne rodzaje podmiotów kluczowych lub podmiotów ważnych. 5. Komunikat, o którym mowa w ust. 3, może być zmieniany, jeżeli z powodów technicznych lub organizacyjnych niemożliwe jest dokonanie wpisów i rozpoczęcie korzystania z systemu teleinformatycznego, o którym mowa w art. 46

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				ust. 1, ustawy zmienianej w art. 1 przez podmioty kluczowe i podmioty ważne w wyznaczonym harmonogramie.
Art. 3	4. W celu ustanowienia wykazu, o którym mowa w ust. 3, państwa członkowskie wymagają od podmiotów, o których mowa w tym ustępie, przedłożenia właściwym organom co najmniej następujących informacji: a) nazwy podmiotu; b) adresu i aktualnych danych kontaktowych, w tym adresów poczty elektronicznej, adresów dróg IP i numerów telefonów; c) w stosownych przypadkach, odpowiedniego sektora i podsektora, o którym mowa w załączniku I lub II; oraz d) w stosownych przypadkach, wykazu państw członkowskich, w których świadczą one usługi objęte zakresem stosowania niniejszej dyrektywy. Podmioty, o których mowa w ust. 3, niezwłocznie powiadamiają o zmianach danych przedłożonych zgodnie z akapitem pierwszym niniejszego ustępu, a w każdym razie w terminie dwóch tygodni od dnia, w którym nastąpiła zmiana. Komisja, z pomocą Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA), bez zbędnej zwłoki podaje wytyczne i wzory dokumentów związane z obowiązkami ustanowionymi w niniejszym ustępie. Państwa członkowskie mogą ustanowić krajowe mechanizmy umożliwiające podmiotom samodzielną rejestrację.	TAK	Art. 1 pkt 4 (art. 2 pkt 3c), art. 1 pkt 13 (art. 7), art. 1 pkt 14 (art. 7a–7k), art. 1 pkt 53 (art. 46 ust. 1a–9), art. 1 pkt 54 (art. 46a i art. 46b)	Art. 2: 3c) adres do doręczeń elektronicznych – adres, o którym mowa w art. 2 pkt 1 ustawy z dnia 18 listopada 2020 r. o doręczeniach elektronicznych (Dz. U. z 2024 r. poz. 1045 i 1841), wpisany do bazy adresów elektronicznych, o której mowa w art. 25 tej ustawy; Art. 7. 1. Wykaz podmiotów kluczowych i podmiotów ważnych, zwany dalej „wykazem”, jest prowadzony w celu: 1) identyfikacji podmiotów kluczowych i podmiotów ważnych; 2) zapewnienia wymiany informacji w zakresie cyberbezpieczeństwa, w tym o incydentach, podatnościach i cyberzagrożeniach między podmiotami kluczowymi i podmiotami ważnymi a CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT sektorowymi i organami właściwymi do spraw cyberbezpieczeństwa; 3) umożliwienia prowadzenia czynności nadzorczych nad podmiotami kluczowymi i podmiotami ważnymi. 2. Wykaz zawiera: 1) nazwę (firmę) podmiotu kluczowego lub podmiotu ważnego; 2) sektor, podsektor i rodzaj lub rodzaje podmiotu, zgodnie z załącznikiem nr 1 lub 2 do tej ustawy; 3) adresy e-mail i adresy do korrespondencji; 4) adres do doręczeń elektronicznych, jeżeli został wpisany do bazy adresów elektronicznych; 5) adresy podmioty elektronicznej;

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				6) numer identyfikacji podatkowej (NIP), jeżeli dotyczy; 7) numer identyfikacyjny podmiotu publicznego w krajowym rejestrze urzędowym podmiotów gospodarki narodowej (REGON), jeżeli dotyczy; 8) numer we właściwym rejestrze działalności regulowanej, jeżeli dotyczy; 9) zakres publicznych adresów IP wykorzystywanych przez podmiot kluczowy lub podmiot w związku w sposób ciągły; 10) domeny internetowe wykorzystywane przez podmiot kluczowy lub podmiot ważny w sposób ciągły; 11) dane osób do kontaktu z podmiotami z krajowego systemu cyberbezpieczeństwa zawierające: imię i nazwisko, numer telefonu służbowego oraz adres służbowej poczty elektronicznej, a w przypadku osoby, która będzie pełnić rolę administratora konta podmiotu w systemie teleinformatycznym, o którym mowa w art. 46 ust. 1, dodatkowo numer PESEL lub niepowtarzalny identyfikator środka identyfikacji elektronicznej, o którym mowa w aktach wykonawczych Komisji Europejskiej, wydanych na podstawie art. 12 ust. 8 rozporządzenia 910/2014; 12) numer telefonu przyporządkowany do wykonywania działalności; 13) deklarację podmiotu kluczowego lub podmiotu ważnego, czy spełnia kryteria mikroprzedsiębiorcy, małego przedsiębiorcy, średniego przedsiębiorcy, o którym mowa w art. 2 ust. 1 załącznika I do rozporządzenia 651/2014/UE, albo przekracza te kryteria, a w przypadku podmiotu leczniczego, który nie jest

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				przedsiębiorcą, oraz urzędu gminy – deklarację wskazującą liczbę osób zatrudnionych według stanu na dzień sporządzenia sprawozdania finansowego; 14) informację określającą, w których państwach członkowskich Unii Europejskiej podmiot kluczowy lub podmiot ważny wykonuje działalność, wraz z określeniem rodzaju wykonywanej działalności; 15) w przypadku dostawcy usług DNS, rejestru nazw domen najwyższego poziomu (TLD), podmiotu świadczącego usługi rejestracji nazw domen, dostawcy chmury obliczeniowej, dostawcy usługi centrum przetwarzania danych, dostawcy sieci dostarczania treści, dostawcy usług zarządzanych, dostawcy usług zarządzanych w zakresie cyberbezpieczeństwa, dostawcy internetowej platformy handlowej, dostawcy wyszukiwarki internetowej oraz dostawcy platformy usług sieci społecznościowych - główne miejsce prowadzenia działalności ustalone zgodnie z art. 5a ust. 3-6; 16) informację o zawarciu umowy z dostawcą usług zarządzanych w zakresie cyberbezpieczeństwa na realizację zadań, o których mowa w art. 8 i art. 11, wraz z danymi tego dostawcy zawierającymi nazwę (firmę) dostawcy, adres siedziby, adres do korespondencji, numer telefonu, adres poczty elektronicznej; 17) informację o ustanowieniu przedstawiciela podmiotu kluczowego lub podmiotu ważnego, o którym mowa w art. 5a ust. 7, wraz z danymi kontaktowymi do tego przedstawiciela obejmujące:

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				a) w przypadku osób fizycznych: imię i nazwisko, adres do korespondencji, numer telefonu służbowego oraz adres służbowej poczty elektronicznej, b) w przypadku osób prawnych i jednostek organizacyjnych nieposiadających osobowości prawnej: nazwę (firmę) przedstawiciela, adres siedziby, adres siedziby do korespondencji, numer telefonu oraz adres poczty elektronicznej; 18) informację o zawarciu przez podmiot kluczowy lub podmiot ważny porozumienia, o którym mowa w art. 8h ust. 6; 19) informację o uznaniu podmiotu kluczowego lub podmiotu ważnego za podmiot krytyczny; 20) wskazanie organu właściwego do spraw cyberbezpieczeństwa dla podmiotu kluczowego lub podmiotu węższego; 21) wskazanie CSIRT sektorowego właściwego dla podmiotu kluczowego lub podmiotu węższego; 22) wskazanie CSIRT MON, CSIRT NASK lub CSIRT GOV właściwego dla podmiotu kluczowego lub podmiotu węższego; 23) umieszczenie w wykazie; 24) datę wpisania do wykazu; 25) podjęcie próby wpisania do wykazu; 26) datę wykreślenia z wykazu. 3. Do danych, o których mowa w ust. 2, nie stosuje się przepisów ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2022 r. poz. 902) oraz ustawy z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego (Dz. U. z 2023 r. poz. 1524).

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				4. Organ właściwy do spraw cyberbezpieczeństwa prowadzi wykaz podmiotów kluczowych i podmiotów ważnych w zakresie nadzorowanego sektora i w tym zakresie jest administratorem danych zawartych w wykazie. 5. Organ właściwy do spraw cyberbezpieczeństwa: 1) wpisuje podmiot do wykazu zgodnie z art. 7j i § 7l u.u. 6; 2) wykreśla podmiot z wykazu zgodnie z art. 7f u.u. 2; 3) może dokonać czynności sprawdzające, o których mowa w art. 7k. 6. Minister właściwy do spraw informatyzacji zapewnia utrzymanie i rozwój systemu teleinformatycznego, o którym mowa w art. 46 ust. 1, za pomocą którego wykaz jest prowadzony. 7. Minister właściwy do spraw informatyzacji jest współadministratorem danych, w tym danych osobowych, gromadzonych w wykazie. 8. Minister właściwy do spraw informatyzacji podejmuje czynności, o których mowa w art. 7a, art. 7b ust. 1 i 2, art. 7d ust. 6, art. 7e, art. 7f ust. 1, art. 7g ust. 1 i 2, art. 7i oraz art. 7m.”; Art. 7a. 1. Dane, o których mowa w art. 7 ust. 2 pkt 19–26, uzupełnia minister właściwy do spraw informatyzacji. 2. W przypadku: 1) przedsiębiorców telekomunikacyjnych, 2) dostawców usług zaufania, 3) podmiotów publicznych, 4) podmiotów krytycznych – minister właściwy do spraw informatyzacji wpisuje do wykazu dane, o których mowa w art. 7 ust. 3 pkt 1–8 oraz pkt 19–26, dotyczące tych podmiotów – na podstawie danych zawartych w

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				rejestrach publicznych, bazie adresów elektronicznych lub przekazanych przez właściwe organy nadzorcze. Art. 7b. 1. Zawiadomienie o wpisie do wykazu z urzędu, minister właściwy do spraw informatyzacji doręcza podmiotom kluczowym lub podmiotom ważnym. 2. Minister właściwy do spraw informatyzacji wzywa podmioty kluczowe lub podmioty ważne, o których mowa w art. 7a ust. 2, do uzupełnienia brakujących danych w wykazie, w terminie 2 miesięcy od dnia doręczenia wezwania, pod rygorem nałożenia kary pieniężnej. 3. Wezwanie, o którym mowa w ust. 2, zawiera: 1) podmiotową część wpisu do wykazu; 2) numer podmiotu w wykazie; 3) dane podmiotu wpisane do wykazu oraz wskazanie źródeł ich pochodzenia; 4) wskazanie brakujących danych, które podmiot musi uzupełnić. 4. Podmioty kluczowe lub podmioty ważne, o których mowa w art. 7a ust. 2, uzupełniają dane w wykazie, składając wniosek o zmianę wpisu w tym wykazie, w tym również uzupełniają dane w wykazie w zakresie ich działalności, która nie została objęta wpisem z urzędu. 5. Zawiadomienie o wpisie do wykazu z urzędu oraz wezwanie, o którym mowa w ust. 2, doręcza się w sposób określony w dziale I rozdziale 8 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (Dz. U. z 2024 r. poz. 572 oraz z 2025 r. poz. 769). 6. W przypadku przedsiębiorców telekomunikacyjnych zawiadomienie o wpisie do wykazu z urzędu oraz wezwanie, o którym mowa w ust. 2, może być doręczone za pomocą

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				Platformy Usług Elektronicznych Urzędu Komunikacji Elektronicznej w ramach współpracy ministra właściwego do spraw informatyzacji z Prezesem Urzędu Komunikacji Elektronicznej. 7. Sprawy, o których mowa w ust. 1 i 2, mogą być załatwiane w sposób, o którym mowa w art. 14 § 1b ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego. Art. 7c. 1. Podmiot kluczowy lub podmiot ważny składają wniosek o wpis do wykazu, w terminie 3 miesięcy od dnia spełnienia przesłanek uznania za podmiot kluczowy lub podmiot ważny. 2. Wniosek o wpis do wykazu zawiera dane, o których mowa w art. 7 ust. 2 pkt 1–18. 3. Podmiot kluczowy lub podmiot ważny składają wniosek o zmianę wpisu w wykazie w zakresie danych, o których mowa w art. 7 ust. 2 pkt 1–18, w terminie 14 dni od dnia ich zmiany. 4. Wniosek o zmianę wpisu w wykazie zawiera wskazanie zmienianych danych oraz numer podmiotu w tym wykazie. 5. Wniosek o wpis, zmianę wpisu albo o wykreślenie z wykazu zawiera oświadczenie kierownika podmiotu kluczowego lub podmiotu ważnego o następującej treści: „Świadomy odpowiedzialności karnej za złożenie fałszywego oświadczenia wynikającej z art. 233 § 6 Kodeksu karnego oświadczam, że dane zawarte we wniosku są zgodne z prawdą.”. Klauzula ta zastępuje pouczenie o odpowiedzialności karnej za złożenie fałszywego oświadczenia. Odpowiedzialność za złożenie fałszywego oświadczenia nie obejmuje podania zakresów adresów IP oraz zakresów nazw domenowych.

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				6. Wniosek o wpis, zmianę wpisu albo o wykreślenie z wykazu sporządza się w postaci elektronicznej i opatruje kwalifikowanym podpisem elektronicznym, podpisem zaufanym, podpisem osobistym kierownika podmiotu kluczowego lub podmiotu ważnego lub osoby przez niego upoważnionej albo kwalifikowaną pieczęcią elektroniczną ze wskazaniem w treści pisma osoby opatrującej pismo pieczęcią. Wniosek składa się w systemie teleinformatycznym, o którym mowa w art. 46 ust. 1. 7. W przypadku działania przez pełnomocnika do wniosku dołącza się pełnomocnictwo w postaci elektronicznej podpisane kwalifikowanym podpisem elektronicznym, podpisem zaufanym, podpisem osobistym albo kwalifikowaną pieczęcią elektroniczną. W przypadku pełnomocnika podmiotu ujawnionego w Centralnej Ewidencji i Informacji o Działalności Gospodarczej lub prokurenta ujawnionego w Krajowym Rejestrze Sądowym nie dołącza się pełnomocnictwa. Art. 7d. 1. Wpis podmiotu do wykazu dokonuje się z chwilą złożenia wniosku w systemie teleinformatycznym, o którym mowa w art. 46 ust. 1. 2. Podmiot kluczowy lub podmiot ważny prowadzący kilka rodzajów działalności wykazują odrębnie te działalności we wniosku. 3. Wpisu do wykazu nie dokonuje się, jeżeli wniosek: 1) nie zawiera danych podlegających wpisowi zgodnie z art. 7 ust. 2 pkt 1–18; 2) dotyczy podmiotu kluczowego lub podmiotu w § 10go już wpisanego do wykazu;

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				3) nie zawiera oświadczenia, o którym mowa w art. 7 ust. 5; 4) nie został podpisany. 4. Zmiany wpisu do wykazu nie dokonuje się, jeżeli wniosek o zmianę wpisu: 1) nie zawiera nazwy podmiotu oraz numeru podmiotu w wykazie; 2) nie zawiera wskazania danych osobowych; 3) nie zawiera oświadczenia, o którym mowa w art. 7 ust. 5; 4) nie został podpisany. 5. Wpis, zmiana wpisu oraz wykreślenie wpisu z wykazu jest czynnością materialno-techniczną i ma charakter deklaratoryjny. 6. Minister właściwy do spraw informatyzacji wydaje, na żądanie podmiotu wpisanego do wykazu, zaświadczenie o wpisie podmiotu do wykazu albo o zmianie tego wpisu wraz ze wskazaniem aktualnych danych zawartych w wykazie dotyczących podmiotu. 7. Zaświadczenie, o którym mowa w ust. 6, jest wydawane w postaci dokumentu elektronicznego, opatrzonego kwalifikowaną pieczęcią elektroniczną, za pomocą systemu teleinformatycznego, o którym mowa w art. 46 ust. 1. Art. 7e. Minister właściwy do spraw informatyzacji co najmniej raz w roku aktualizuje dane zawarte we wpisach w wykazie w zakresie nazwy podmiotu na podstawie danych pozyskanych z publicznie dostępnych rejestrów publicznych. Art. 7f. 1. Minister właściwy do spraw informatyzacji wykreśla podmiot z wykazu, po uzyskaniu informacji o wykreśleniu podmiotu z

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				krajowego rejestru urzędowego podmiotów gospodarki narodowej (REGON), Krajowego Rejestru Sądowego lub Centralnej Ewidencji i Informacji o Działalności Gospodarczej. 2. Organ właściwy do spraw cyberbezpieczeństwa wykreśla podmiot z wykazu, w zakresie nadzorowanego sektora, podsektora lub rodzaju działalności, jeżeli: 1) podmiot wpisany do wykazu nie jest podmiotem kluczowym albo podmiotem ważnym, 2) podmiot wpisany do wykazu utracił status podmiotu kluczowego albo podmiotu ważnego po wpisie do wykazu. 3. Podmiot kluczowy lub podmiot ważny składają za pomocą systemu teleinformatycznego, o którym mowa w art. 46 ust. 1, wniosek o wykreślenie z wykazu w zakresie sektora, podsektora lub rodzaju działalności, jeżeli przestały spełniać przesłanki uznania za podmiot kluczowy lub podmiot ważny w tym sektorze, podsektorze lub dla określonego rodzaju działalności. Wniosek o wykreślenie z wykazu zawiera uzasadnienie. 4. Organ właściwy do spraw cyberbezpieczeństwa rozpatruje wniosek w terminie miesiąca od dnia złożenia wniosku i informuje o wykreśleniu albo odmowie wykreślenia z wykazu. 5. Organ właściwy do spraw cyberbezpieczeństwa odmawia wykreślenia podmiotu z wykazu, jeżeli podmiot nadal spełnia przesłanki uznania za podmiot kluczowy lub podmiot ważny. 6. Odmowa wykreślenia jest inną czynnością z zakresu administracji publicznej, na którą przysługuje skarga do sądu administracyjnego i wymaga uzasadnienia.

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				7. Brak odmowy wykreślenia podmiotu z wykazu w terminie, o którym mowa w ust. 4, skutkuje wykreśleniem podmiotu z wykazu. 8. Wykreślenie podmiotu z wykazu jest inną czynnością z zakresu administracji publicznej, na którą przysługuje skarga do sądu administracyjnego. Art. 7g. 1. Minister właściwy do spraw informatyzacji udostępnia dane, o których mowa w art. 7 ust. 2, CSIRT MON, CSIRT NASK i CSIRT GOV oraz CSIRT sektorowemu w zakresie sektora lub podsektora, dla którego został ustanowiony, organowi właściwemu do spraw cyberbezpieczeństwa w zakresie nadzorowanego sektora lub podsektora, a także podmiotowi kluczowemu lub podmiotowi ważnemu w zakresie go dotyczącym. 2. Minister właściwy do spraw informatyzacji udostępnia dane, o których mowa w art. 7 ust. 2, na wniosek, następującym podmiotom: 1) Agencji Bezpieczeństwa Wewnętrznego, 2) Agencji Wywiadu, 3) dyrektorowi Rządowego Centrum Bezpieczeństwa, 4) organom Krajowej Administracji Skarbowej, 5) Najwyższej Izbie Kontroli, 6) Policji, 7) Prezesowi Urzędu Lotnictwa Cywilnego, 8) Prezesowi Urzędu Ochrony Danych Osobowych, 9) Prezesowi Urzędu Transportu Kolejowego, 10) Prokuraturii Generalnej Rzeczypospolitej Polskiej, 11) prokuratorowi,

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				12) sądom, 13) Służbie Kontrwywiadu Wojskowego, 14) Służbie Ochrony Państwa, 15) Służbie Wywiadu Wojskowego, 16) Straży Granicznej, 17) Żandarmerii Wojskowej – w zakresie niezbędnym do realizacji ich ustawowych zadań. 3. Udostępnianie danych, o których mowa w art. 7 ust. 2, odbywa się za pomocą systemu teleinformatycznego, o którym mowa w art. 46 ust. 1. 4. Informacja o zmianie wpisu w wykazie lub o wykreśleniu podmiotu z wykazu jest przechowywana, systemie teleinformatycznym o którym mowa w art. 46 ust. 1, przez 5 lat od dokonania tej zmiany lub wykreślenia. W informacji wskazuje się datę i czas dokonania zmiany lub wykreślenia. 5. Dane administratora konta podmiotu w systemie teleinformatycznym, o którym mowa w art. 46 ust. 1, w tym numer PESEL lub niepowtarzalny identyfikator środka identyfikacji elektronicznej, o którym mowa w aktach wykonawczych Komisji Europejskiej, wydanych na podstawie art. 12 ust. 8 rozporządzenia 910/2014, są dostępne wyłącznie dla ministra właściwego do spraw informatyzacji lub jednostki podległej temu ministrowi albo przez niego nadzorowanej, której powierzył realizację zadania rozwoju lub utrzymania systemu. Przepis ten nie narusza uprawnień sądu i prokuratora w postępowaniu karnym. Art. 7h. Informację o uznaniu podmiotu kluczowego lub podmiotu ważnego za podmiot krytyczny przekazuje ministrowi właściwemu do

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				spraw informatyzacji dyrektor Rządowego Centrum Bezpieczeństwa. Art. 7i. Minister właściwy do spraw informatyzacji udostępnia w portalu danych, o którym mowa w ustawie z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego, liczbę podmiotów kluczowych lub podmiotów ważnych w podziale na sektory, podsektory i rodzaj działalności. Dane te są aktualizowane nie rzadziej niż raz na kwartał. Art. 7j. 1. Organ właściwy do spraw cyberbezpieczeństwa może wpisać podmiot do wykazu, jeżeli podmiot ten spełnia przesłanki uznania go za podmiot kluczowy albo podmiot ważny oraz podmiot ten nie złożył wniosku, o którym mowa w art. 7c ust. 1. 2. Dokonując wpisu podmiotu do wykazu, organ właściwy do spraw cyberbezpieczeństwa korzysta z danych zawartych w publicznie dostępnych rejestrach publicznych, danych dostępnych organowi na podstawie przepisów odrębnych oraz informacji uzyskanych od podmiotu na podstawie art. 43 ust. 1. 3. Organ właściwy do spraw cyberbezpieczeństwa zawiadamia podmiot o wpisie do wykazu na podstawie ust. 1 oraz wzywa ten podmiot do uzupełnienia brakujących danych w wykazie, w terminie 2 miesięcy od dnia otrzymania zawiadomienia, pod rygorem nałożenia kary pieniężnej. 4. Zawiadomienie o wpisie do wykazu na podstawie ust. 1 oraz wezwanie, o którym mowa w ust. 3, doręcza się w sposób określony w dziale I rozdziale 8 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego.

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				5. Wpis do wykazu na podstawie ust. 1 jest inną czynnością z zakresu administracji publicznej, na którą przysługuje skarga do sądu administracyjnego i wymaga uzasadnienia. Art. 7k. 1. Organ właściwy do spraw cyberbezpieczeństwa może dokonywać czynności sprawdzających mających na celu weryfikację zgodności ze stanem faktycznym danych zawartych w wykazie. 2. W przypadku stwierdzenia, że dane w wykazie są niezgodne ze stanem faktycznym, organ właściwy do spraw cyberbezpieczeństwa wzywa podmiot do zmiany wpisu, w terminie 7 dni od dnia doręczenia wezwania, pod rygorem nałożenia kary pieniężnej. Do doręczenia wezwania stosuje się przepisy działu I rozdziału 8 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego. 3. Organ właściwy do spraw cyberbezpieczeństwa poprawia, z urzędu, oczywiste omyłki i błędy zawarte w wykazie. Art. 46. 1a. W systemie teleinformatycznym prowadzi się wykaz podmiotów kluczowych i podmiotów ważnych.”, 2. CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT sektorowe, organy właściwe do spraw cyberbezpieczeństwa oraz Prezes Urzędu Ochrony Danych Osobowych korzystają z systemu teleinformatycznego w celu realizacji swoich zadań ustawowych.”, d) uchyla się ust. 3, 4. Podmioty kluczowe lub podmioty ważne, korzystają z systemu teleinformatycznego w zakresie, o którym mowa w ust. 1, w terminie 6

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				miesiące od spełnienia przesłanek uznania za podmiot kluczowy lub podmiot ważny. 5. Uwierzytelnienie w systemie teleinformatycznym następuje za pomocą środków określonych w art. 20a ust. 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne. 6. W celu zapewnienia bezpiecznego korzystania z systemu teleinformatycznego podmioty kluczowe lub podmioty ważne są obowiązane zapewnić bezpieczeństwo, ciągłość działania, aktualność i skuteczność zabezpieczeń oraz rozliczalność stosowanych systemów teleinformatycznych. 7. W celu wykonania obowiązku, o którym mowa w ust. 6, podmioty kluczowe lub podmioty ważne dostosowują swoje systemy informacyjne do minimalnych wymagań technicznych i funkcjonalnych korzystania z systemu teleinformatycznego, opublikowanych przez ministra właściwego do spraw informatyzacji na jego stronie podmiotowej Biuletynu Informacji Publicznej w terminie 6 miesięcy od dnia opublikowania tych wymagań. 8. Minister właściwy do spraw informatyzacji publikuje na swojej stronie podmiotowej Biuletynu Informacji Publicznej wykaz usług stosowany w systemie teleinformatycznym, w szczególności świadczonych przez podmioty kluczowe lub podmioty ważne. 9. CSIRT MON, CSIRT NASK, CSIRT GOV, po uzyskaniu zgody właściwego CSIRT poziomu krajowego, mogą uzyskać dostęp do wszelkich informacji przetwarzanych w systemie teleinformatycznym, w zakresie dotyczącym

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				podmiotu będącego we właściwości innego CSIRT, w szczególności w celu szacowania ryzyka bezpieczeństwa łańcucha dostaw produktów ICT, usług ICT i procesów ICT, od których zależy świadczenie usługi przez podmiot pozostający we właściwości danego CSIRT.Art. 46a. W celu realizacji zadań, o których mowa w art. 11 ust. 2 oraz w art. 46 ust. 1 pkt 3, 4 i 6, Minister Obrony Narodowej, urząd go obsługujący oraz podmioty podległe Ministrowi Obrony Narodowej i przez niego nadzorowane mogą korzystać z środków komunikacji elektronicznej, innych niż system, o którym mowa w art. 46 ust. 1, zapewniających poufność, integralność, dostępność i autentyczność przetwarzanych danych. Art. 46b. 1. W przypadku doręczenia pisma w postaci elektronicznej za pośrednictwem systemu, o którym mowa w art. 46 ust. 1, przez organ administracji publicznej doręczenie jest skuteczne, jeżeli adresat potwierdzi odbiór pisma w systemie. 2. W przypadku nieodebrania pisma w postaci elektronicznej za pośrednictwem systemu, o którym mowa w art. 46 ust. 1, organ administracji publicznej po upływie 7 dni, licząc od dnia jego wysłania, przesyła zawiadomienie o możliwości odebrania tego pisma. 3. Zawiadomienie o możliwości odebrania pisma może być automatycznie tworzone i przesyłane za pośrednictwem systemu, o którym mowa w art. 46 ust. 1, a odbioru tego zawiadomienia nie potwierdza się. 4. W przypadku nieodebrania pisma w postaci elektronicznej za pośrednictwem systemu, o którym mowa w art. 46 ust. 1, doręczenie uważa

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				się za dokonane po upływie 14 dni, licząc od dnia wysłania pisma.
Art. 3	5. Do dnia 17 kwietnia 2025 r., a następnie co dwa lata właściwe organy powiadamiają: a) Komisję i Grupę Współpracy o liczbie podmiotów kluczowych i ważnych wymienionych w wykazie zgodnie z ust. 3 dla każdego sektora i podsektora, o których mowa w załączniku I lub II; oraz b) Komisję o istotnych informacjach na temat liczby podmiotów kluczowych i ważnych wskazanych na podstawie art. 2 ust. 2 lit. b)–e), sektora i podsektora, o których mowa w załączniku I lub II i do których podmioty te należą, rodzaju świadczonej przez nie usługi oraz przepisu spośród tych ustanowionych na podstawie art. 2 ust. 2 lit. b)–e), na podstawie którego zostały one wskazane.	TAK	Art. 1 pkt 58 (art. 50) i art. 37	Art. 1: 55) w art. 50 dotychczasową treść oznacza się jako ust. 1 i: a) w tym ust. pkt 2 otrzymuje brzmienie: „2) co 2 lata informacje dotyczące krajowego systemu cyberbezpieczeństwa w szczególności: a) liczbę podmiotów kluczowych w podziale na poszczególne sektory, b) liczbę podmiotów ważnych w podziale na poszczególne sektory, c) rodzaje usług świadczonych przez podmioty kluczowe lub podmioty ważne, d) przepisy, na podstawie których podmioty kluczowe lub podmioty ważne zostały wskazane.”, b) dodaje się ust. 2 w brzmieniu: „2. Pojedynczy Punkt Kontaktowy przekazuje Grupie Współpracy: 1) liczbę podmiotów kluczowych w podziale na poszczególne sektory; 2) liczbę podmiotów ważnych w podziale na poszczególne sektory.”; Art. 37. Minister właściwy do spraw informatyzacji, w terminie 3 miesięcy od dnia wejścia w życie ustawy, przekaze: 1) Komisji Europejskiej informacje o: a) liczbie podmiotów kluczowych w podziale na poszczególne sektory, b) liczbie podmiotów ważnych w podziale na poszczególne sektory, c) rodzajach usług świadczonych przez podmioty kluczowe i podmioty ważne,

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				d) przepisach na podstawie których podmioty kluczowe w żłob i w k; 2) Grupie Współpracy informacje o: a) liczbie podmiotów kluczowych w podziale na poszczególne sektory, b) liczbie podmiotów ważnych w podziale na poszczególne sektory.
Art. 3	6. Do dnia 17 kwietnia 2025 r. i na wniosek Komisji państwa członkowskie mogą zgłaszać Komisji nazwy podmiotów kluczowych i ważnych, o których mowa w ust. 5 lit. b).	NIE		Jest to fakultatywna kompetencja państwa członkowskiego UE i nie wymaga wdrożenia.
Art. 4	Artykuł 4 Sektorowe akty prawne Unii 1. W przypadku gdy na podstawie sektorowych aktów prawnych Unii wymaga się od podmiotów kluczowych lub ważnych przyjęcia środków zarządzania ryzykiem w cyberbezpieczeństwie lub zgłaszania poważnych incydentów i w przypadku gdy wymogi te są co najmniej równoważne pod względem skutku obowiązkom określonym w niniejszej dyrektywie, nie stosuje się do takich podmiotów odpowiednich przepisów niniejszej dyrektywy, w tym przepisów dotyczących nadzoru i egzekwowania przepisów określonych w rozdziale VII. Jeżeli sektorowe akty prawne Unii nie obejmują wszystkich podmiotów w konkretnym sektorze, objętych zakresem stosowania niniejszej dyrektywy, odpowiednie przepisy niniejszej dyrektywy nadal mają zastosowanie do podmiotów nieobjętych tymi sektorowymi aktami prawnymi Unii.	TAK	Art. 1 pkt 17 (art. 8b ust. 2 i 3 oraz art. 8i)	Art. 8b. 2. W ramach systemu, o którym mowa w art. 8 ust. 1, podmioty kluczowe lub podmioty ważne, inne niż określone w ust. 1, stosują środki zarządzania ryzykiem dla danego rodzaju podmiotu określone w aktach wykonawczych Komisji Europejskiej, wydanych na podstawie art. 21 ust. 5 dyrektywy 2022/2555. 3. Podmioty kluczowe lub podmioty ważne z podsektora energii elektrycznej, uznane za podmiot o dużym wpływie lub podmiot o krytycznym wpływie, o którym mowa w art. 52a ust. 2, dodatkowo stosują środki określone w rozporządzeniu delegowanym Komisji (UE) 2024/1366 z dnia 11 marca 2024 r. uzupełniającym rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/943 poprzez ustanowienie kodeksu sieci dotyczącego zasad sektorowych w zakresie aspektów cyberbezpieczeństwa w transgranicznych przepływach energii elektrycznej (Dz. Urz. UE L 2024/1366 z 24.05.2024), zwanym dalej „rozporządzeniem 2024/1366”. Art. 8i. 1. Do podmiotów kluczowych lub podmiotów ważnych z sektora bankowości i infrastruktury rynków finansowych nie stosuje się

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				przepisów ustawy dotyczących systemu zarządzania bezpieczeństwem informacji lub zgłaszania poważnych incydentów, z wyjątkiem art. 3a, art. 5 ust. 1–3, art. 7–7m, art. 8 ust. 1 pkt 1 i pkt 2 lit. j, art. 8h, art. 9, art. 11 ust. 1 pkt 5 i 6, art. 13, art. 16, art. 26a ust. 2–4, art. 32, art. 33 ust. 5, 7 i 8, art. 36a, art. 36b, art. 37, art. 43, art. 45 ust. 3, art. 46 ust. 1 pkt 1, 2, 4–7 i ust. 4–6, art. 67a, art. 67c, art. 67d oraz art. 67g–67i. 2. Do podmiotów kluczowych lub podmiotów ważnych z sektora bankowości i infrastruktury rynków finansowych stosuje się odpowiednio przepisy art. 8c–8f, art. 12 ust. 7 oraz art. 31 ust. 1. 3. Do podmiotów kluczowych lub podmiotów ważnych z sektora bankowości i infrastruktury rynków finansowych stosuje się przepisy rozdziałów 11 i 14 ustawy w zakresie art. 3a, art. 5 ust. 1–3, art. 7–7m, art. 8 ust. 1 pkt 1 i pkt 2 lit. j, art. 8h, art. 9, art. 11 ust. 1 pkt 5 i 6, art. 13, art. 15, art. 16, art. 26a ust. 2–4, art. 32, art. 33 ust. 5, 7 i 8, art. 36a, art. 36b, art. 37, art. 43, art. 45 ust. 3, art. 46 ust. 1 pkt 1, 2, 4–7 i ust. 4–6, art. 67a, art. 67c, art. 67d, art. 67g–67i oraz stosowanych odpowiednio przepisów art. 8c–8f, art. 12 ust. 7 oraz art. 31 ust. 1.
Art. 4	2. Wymogi, o których mowa w ust. 1 niniejszego artykułu, uznaje się za równoważne pod względem skutku obowiązkom określonym w niniejszej dyrektywie, jeżeli: a) środki zarządzania ryzykiem w cyberbezpieczeństwie są co najmniej równoważne pod względem skutku środkom określonym w art. 21 ust. 1 i 2; lub b) sektorowy akt prawny Unii przewiduje natychmiastowy dostęp CSIRT, właściwych organów lub pojedynczych punktów kontaktowych na mocy niniejszej dyrektywy do zgłoszeń incydentów – w stosownych przypadkach automatycznie i	NIE		

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

	bezpośrednio, oraz w przypadkach, gdy wymogi dotyczące zgłaszania poważnych incydentów są co najmniej równoważne pod względem skutku wymogom określonym w art. 23 ust. 1–6 niniejszej dyrektywy.			
Art. 4	3. Komisja do dnia 17 lipca 2023 r. podaje wytyczne wyjaśniające stosowanie ust. 1 i 2. Komisja regularnie dokonuje przeglądu tych wytycznych. Przygotowując te wytyczne, Komisja bierze pod uwagę uwagi Grupy Współpracy i ENISA.	NIE		
Art. 5	Artykuł 5 Harmonizacja minimalna Niniejsza dyrektywa nie uniemożliwia państwom członkowskim przyjęcia lub utrzymania przepisów zapewniających wyższy poziom cyberbezpieczeństwa, pod warunkiem że takie przepisy są spójne z obowiązkami państw członkowskich, ustanowionymi w prawie Unii.	NIE		
Art. 6	Artykuł 6 Definicje Do celów niniejszej dyrektywy stosuje się następujące definicje: 1) „sieci i systemy informatyczne” oznaczają: a) sieć łączności elektronicznej zdefiniowaną w art. 2 pkt 1 dyrektywy (UE) 2018/1972; b) urządzenie lub grupę wzajemnie połączonych lub powiązanych urządzeń, z których co najmniej jedno, na podstawie programu, oprogramowania lub oprogramowania lub c) dane cyfrowe przechowywane, przetwarzane, pobierane lub przekazywane przez elementy określone w lit. a) i b) w celu ich eksploatacji, użytkowania, przechowywania i utrzymania; ;	TAK	Art. 1 pkt 4 (art. 2 pkt 14)	w art. 2: 14) system informacyjny – oznacza to: a) system teleinformatyczny, o którym mowa w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2024 r. poz. 1557 i 1717 oraz z 2025 r. poz. 1006, 1019, 1158 i 1301) lub b) urządzenie lub grupę połączonych urządzeń i oprogramowania zaprogramowanych w celu przetwarzania danych – wraz z danymi przetwarzanymi w postaci elektronicznej;
Art. 6	2) „bezpieczeństwo sieci i systemów informatycznych” oznacza odporność sieci i systemów informatycznych, przy danym poziomie zaufania, na wszelkie zdarzenia, które mogą naruszyć dostępność, autentyczność, integralność lub poufność przechowywanych, przekazywanych lub przetwarzanych danych lub usług oferowanych przez te sieci i systemy informatyczne lub dostępnych za ich pośrednictwem;	TAK	Art. 1 pkt 4 (art. 2 pkt 3d)	Art. 2: 3d) bezpieczeństwo systemów informacyjnych – odporność systemów informacyjnych, przy danym poziomie pewności, na zdarzenia naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				związanych z nimi usług oferowanych przez te y i my;
Art. 6	3) „cyberbezpieczeństwo” oznacza cyberbezpieczeństwo d f i o w r t. 2 pkt 1 ro p o r a d i (UE) 2019/881;	TAK	Art. 1 pkt 4 (art. 2 pkt 4)	Art. 2: 4) cyberbezpieczeństwo – cyberbezpieczeństwo w rozumieniu art. 2 pkt 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylecia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz. Urz. UE L 151 z 07.06.2019, str. 15 oraz Dz. Urz. L. 37 z 15.1.2025), zwanego dalej „rozporządzeniem 2019/881”;
Art. 6	4) „krajowa strategia cyberbezpieczeństwa” oznacza spójne ramy państwa członkowskiego określające strategiczne cele i priorytety w obszarze cyberbezpieczeństwa oraz środki służące ich realizacji w tym p n t w i o k o w k i m;	NIE		Definicja nie jest konieczna, przepis dotyczący Strategii Cyberbezpieczeństwa RP wystarczająco dobrze ją opisuje.
Art. 6	5) „potencjalne zdarzenie dla cyberbezpieczeństwa” oznacza zdarzenie, które mogło naruszyć dostępność, autentyczność, integralność lub poufność przechowywanych, przekazywanych lub przetwarzanych danych lub usług oferowanych przez sieci i systemy informatyczne lub dostępnych za ich pośrednictwem, któremu udało i e j d k p o b i lub k t o r j d k i w y a p i o;	TAK	Art. 1 pkt 4 (art. 2 pkt 11f)	Art. 2: 11f) potencjalne zdarzenie dla cyberbezpieczeństwa – zdarzenie, które mogło mieć niekorzystny wpływ na bezpieczeństwo systemów informacyjnych, które jednak nie w y a p i o lub k t o r m u u d o i e p o b i;
Art. 6	6) „incydent” oznacza zdarzenie naruszające dostępność, autentyczność, integralność lub poufność przechowywanych, przekazywanych lub przetwarzanych danych lub usług oferowanych przez sieci i systemy informatyczne lub dostępnych za ich po s r d i t w m;	TAK	Art. 1 pkt 4 (art. 2 pkt 5)	Art. 2: „5) incydent – zdarzenie, które ma lub może mieć niekorzystny wpływ na bezpieczeństwo y t m o w i f o r m a c y j n e h;”,
Art. 6	7) „incydent w cyberbezpieczeństwie na dużą skalę” oznacza incydent, który powoduje zakłócenia na poziomie przekraczającym zdolność państwa członkowskiego do reagowania na ten incydent lub który wywiera znaczące skutki w co najmniej dwóch państwach członkow k i h;	TAK	Art. 1 pkt 4 (art. 2 pkt 8)	Art. 2: 8) incydent w cyberbezpieczeństwie na dużą skalę – incydent, którego skutki przekraczają możliwości reagowania państwa lub który ma

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				poważny wpływ na inne państwo członkowskie Unii Europejskiej;
Art. 6	8) „obsługa incydentu” oznacza działania i procedury mające na celu zapobieżenie incyidentowi, wykrywanie i analizowanie go, ograniczanie jego zasięgu lub reagowanie na niego i przywrócenie normalnego działania;	NIE		Definicja jest wdrożona w obecnie obowiązującej ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. 2024 r. poz. 1077 i 1222 oraz z 2025 r. poz. 1017 i 1069). W art. 2 w pkt 10: obsługa incydentu - czynności umożliwiające wykrywanie, rejestrowanie, analizowanie, klasyfikowanie, priorytetyzację, podejmowanie działań naprawczych i ograniczanie skutków incydentu;
Art. 6	9) „ryzyko” oznacza możliwość wystąpienia strat lub zakłóceń spowodowanych incydentem, wyrażoną jako wypadkową wielkości takiej straty lub takich zakłóceń oraz prawdopodobieństwo wystąpienia takiego i incydentu;	NIE		Definicja jest wdrożona w obecnie obowiązującej ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. W art. 2 12) ryzyko - kombinację prawdopodobieństwa wystąpienia zdarzenia niepożądanego i jego konsekwencji;
Art. 6	10) „cyberzagrożenie” oznacza cyberzagrożenie zdefiniowane w art. 2 pkt 8 rozporządzenia (UE) 2019/881;	TAK	Art. 1 pkt 4 (art. 2 pkt 4a)	Art. 2: 4a) cyberzagrożenie – cyberzagrożenie w rozumieniu art. 2 pkt 8 rozporządzenia 2019/881;
Art. 6	11) „poważne cyberzagrożenie” oznacza cyberzagrożenie, co do którego można założyć w oparciu o jego charakterystykę techniczną, że może wywrzeć znaczący wpływ na sieć i systemy informatyczne danego podmiotu lub użytkowników, korzystających z usług tego podmiotu, powodując i znaczne szkody majątkowe lub informacyjne;	TAK	Art. 1 pkt 4 (art. 2 pkt 11g)	Art. 2: 11g) poważne cyberzagrożenie – cyberzagrożenie, które przez swoje właściwości techniczne może mieć poważny wpływ na bezpieczeństwo systemów informacyjnych lub użytkowników tych systemów poprzez wywołanie poważnej szkody materialnej lub informacyjnej;
Art. 6	12) „produkt ICT” oznacza produkt ICT zdefiniowany w art. 2 pkt 12 rozporządzenia (UE) 2019/881;	TAK	Art. 1 pkt 4 (art. 2 pkt 11m)	Art. 2: 11m) produkt ICT – produkt ICT w rozumieniu art. 2 pkt 12 rozporządzenia 2019/881;
Art. 6	13) „usługa ICT” oznacza usługę ICT zdefiniowaną w art. 2 pkt 13 rozporządzenia (UE) 2019/881;	TAK	Art. 1 pkt 4 (art. 2 pkt 11n)	Art. 2: 11n) usługa ICT – usługa ICT w rozumieniu art. 2 pkt 13 rozporządzenia 2019/881;

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

Art. 6	14) „proces ICT” oznacza proces ICT zdefiniowany w art. 2 pkt 14 rozporządzenia (UE) 2019/881;	TAK	Art. 1 pkt 4 (art. 2 pkt 11)	Art. 2: 11) proces ICT – proces ICT w rozumieniu art. 2 pkt 14 rozporządzenia (UE) 2019/881;
Art. 6	15) „podatność” oznacza słabość, wrażliwość lub wadę produktów ICT lub usług ICT, które to cechy mogą zostać wykorzystane w wyniku cyberzagrożenia;	TAK	Art. 1 pkt 4 (art. 2 pkt 11)	Art. 2: „11) podatność – właściwość produktu ICT lub usługi ICT, które mogą być wykorzystane przez cyberzagrożenia”;
Art. 6	16) „norma” oznacza normę zdefiniowaną w art. 2 pkt 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1025/2012 (29);	NIE		
Art. 6	17) „specyfikacja techniczna” oznacza specyfikację techniczną określonych w art. 2 pkt 4 rozporządzenia (UE) nr 1025/2012;	NIE		
Art. 6	18) „punkt wymiany ruchu internetowego” oznacza obiekt sieciowy, który umożliwia połączenie międzysystemowe pomiędzy więcej niż dwoma niezależnymi sieciami (systemami autonomicznymi), głównymi w celu umożliwienia wymiany ruchu internetowego; punkt wymiany ruchu internetowego zapewnia połączenie międzysystemowe wyłącznie systemów autonomicznych i nie wymaga, aby ruch internetowy między jakąkolwiek parą uczestniczących systemów autonomicznych przechodził przez jakikolwiek trzeci system autonomiczny, ani nie powoduje zmian w tym ruchu, ani w innych połączeniach tego rodzaju;	NIE		Pojęcie to pojawia się tylko jeden raz w projekcie ustawy, w załączniku stąd nie ma potrzeby jego definiowania.
Art. 6	19) „system nazw domen” lub „DNS” oznacza hierarchiczny rozproszony system nazw, który umożliwia identyfikację usług i zasobów internetowych, pozwalając urządzeniom użytkowników końcowych na korzystanie z usług routingu internetowego i usług łączności w celu dostarczenia usług i zasobów;	NIE		Definicja nie pojawia się w dyrektywie NIS 2 poza słowniczkiem, stąd wdrażanie jej jest bezcelowe.
Art. 6	20) „dostawca usług DNS” oznacza podmiot świadczący: a) dostępne publicznie rekurencyjne usługi rozpoznawania nazw domen użytkowników końcowych internetu; lub b) autorytatywne usługi rozpoznawania nazw domen do użytku osób trzecich, z wyjątkiem głównych serwerów nazw	TAK	Art. 1 pkt 4 (art. 2 pkt 4f)	Art. 2: 4f) dostawca usług DNS – podmiot, który świadczy dostępne publicznie rekurencyjne usługi rozpoznawania nazw domen na rzecz ogółu użytkowników końcowych internetu lub autorytatywne usługi rozpoznawania nazw domen do użytku ogółu użytkowników końcowych internetu, z wyjątkiem głównych serwerów nazw;

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

Art. 6	21) „rejestr nazw domen najwyższego poziomu” lub „rejestr nazw TLD” oznacza podmiot, któremu powierzono konkretną domenę najwyższego poziomu (TLD) i który odpowiada za zarządzanie nią, w tym za rejestrację nazw domen w ramach TLD oraz za jej techniczne funkcjonowanie, w tym za obsługę jej serwerów nazw, utrzymanie jej baz danych oraz dystrybucję plików strefowych TLD we wszystkich serwerach nazw, bez względu na to, czy którekolwiek z tych działań jest wykonywane przez sam podmiot czy zlecane na zewnątrz, ale z wyłączeniem sytuacji, w których rejestr wykorzystuje nazwy TLD wyłącznie do własnego użytku;	TAK	Art. 1 pkt 4 (art. 2 pkt 11o)	Art. 2: 11o) rejestr nazw domen najwyższego poziomu (TLD) – podmiot, któremu powierzono konkretną domenę najwyższego poziomu (TLD) i który odpowiada za zarządzanie nią, w tym za rejestrację nazw domen w ramach TLD oraz za jej techniczne funkcjonowanie, w tym za obsługę jej serwerów nazw, utrzymanie jej baz danych oraz dystrybucję plików strefowych TLD we wszystkich serwerach nazw, bez względu na to, czy którekolwiek z tych działań jest wykonywane przez sam podmiot czy zlecane na zewnątrz, ale z wyłączeniem sytuacji, w których rejestr wykorzystuje nazwy TLD wyłącznie do własnego użytku;
Art. 6	22) „podmiot świadczący usługi rejestracji nazw domen” oznacza rejestratora lub agenta działającego w imieniu rejestratorów, np. dostawcę lub odsprzedańcę usług w zakresie rejestracji prywatności lub „rów proxy;	TAK	Art. 1 pkt 4 (art. 2 pkt 11e)	Art. 2: 11e) podmiot świadczący usługi rejestracji nazw domen – rejestratora lub agenta działającego w imieniu rejestratorów, w tym dostawcę lub odsprzedańcę usług w zakresie prywatnej rejestracji lub pośrednictwa w rejestracji;
Art. 6	23) „usługa cyfrowa” oznacza usługę zdefiniowaną w art. 1 ust. 1 lit. b) dyrektywy (UE) 2015/1535 Parlamentu Europejskiego i Rady (30);	NIE		
Art. 6	24) „usługa zaufania” oznacza usługę zaufania zdefiniowaną w art. 3 pkt 16 rozporządzenia (UE) nr 910/2014;	NIE		Przepisy projektu ustawy odnoszą się do dostawcy usług zaufania, który jest zdefiniowany. Nie ma potrzeby wprowadzania tej definicji.
Art. 6	25) „dostawca usług zaufania” oznacza dostawcę usług zaufania zdefiniowanego w art. 3 pkt 19 rozporządzenia (UE) nr 910/2014;	TAK	Art. 1 pkt 4 (art. 2 pkt 4j)	Art. 2: 4j) dostawca usług zaufania – dostawcę usług zaufania w rozumieniu art. 3 pkt 19 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE (Dz. Urz.

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				UE L 257 z 28.08.2014, str. 73), zwanego dalej „rozporządzeniem 910/2014”;
Art. 6	26) „kwalifikowana usługa zaufania” oznacza kwalifikowaną usługę zaufania zdefiniowaną w art. 3 pkt 17 rozporządzenia (UE) nr 910/2014;	NIE		Przepisy projektu ustawy odnoszą się do kwalifikowanego dostawcy usług zaufania. Nie ma potrzeby wprowadzania tej definicji.
Art. 6	27) „kwalifikowany dostawca usług zaufania” oznacza kwalifikowanego dostawcę usług zaufania zdefiniowanego w art. 3 pkt 20 rozporządzenia (UE) nr 910/2014;	NIE		Przepisy projektu w art. 5 odnoszą się do pojęcia kwalifikowanego dostawcy usług zaufania poprzez odwołanie do rozporządzenia 910/2014. Nie ma potrzeby wprowadzania definicji.
Art. 6	28) „internetowa platforma handlowa” oznacza internetową platformę handlową zdefiniowaną w art. 2 lit. n) dyrektywy 2005/29/WE Parlamentu Europejskiego i Rady (31);	TAK	Art. 1 pkt 4 (art. 2 pkt 4d)	Art. 2: 4d) dostawca internetowej platformy handlowej – osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, która dostarcza internetową platformę handlową, o której mowa w art. 2 pkt 8 ustawy z dnia 30 maja 2014 r. o prawach konsumenta (Dz. U. z 2024 r. poz. 1796 oraz z 2025 poz. 1172);
Art. 6	29) „wyszukiwarka internetowa” oznacza wyszukiwarkę internetową zdefiniowaną w art. 2 pkt 5 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/1150 (32);	TAK	Art. 1 pkt 4 (art. 2 pkt 4k)	Art. 2: 4k) dostawca wyszukiwarki internetowej – osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, która świadczy usługę wyszukiwarki internetowej, o której mowa w art. 2 pkt 5 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/1150 z dnia 20 czerwca 2019 r. w sprawie propagowania sprawiedliwości i przejrzystości dla użytkowników biznesowych korzystających z usług pośrednictwa internetowego (Dz. Urz. UE L 186 z 11.07.2019, str. 57);
Art. 6	30) „usługa chmurowa” oznacza usługę cyfrową umożliwiającą administrowanie na żądanie skalowalnym i elastycznym zbiorem zasobów obliczeniowych do wspólnego wykorzystywania oraz szeroki dostęp zdalny do tego zbioru, w tym również gdy takie zasoby są rozproszone w kilku lokalizacjach;	TAK	Art. 1 pkt 4 (art. 2 pkt 4e)	Art. 2: 4e) dostawca chmury obliczeniowej – osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, która świadczy usługę umożliwiającą dostęp do skalowalnego i elastycznego zbioru

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				zasobów obliczeniowych do wspólnego wykorzystywania i praca w celu użytkownikom;
Art. 6	31) „usługa ośrodka przetwarzania danych” oznacza usługę obejmującą struktury lub grupy struktur przeznaczone do scentralizowanego hostingu, zapewniania wzajemnego połączenia i eksploatacji sprzętu IT i sieciowego służącego do świadczenia usług przechowywania, przetwarzania i transportu danych wraz ze wszystkimi obiektami i całą infrastrukturą, zapewniającymi dystrybucję energii elektrycznej i kontrolę środowiskową;	TAK	Art. 1 pkt 4 (art. 2 pkt 4g)	Art. 2: 4g) dostawca usługi centrum przetwarzania danych – osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, która świadczy usługę obejmującą struktury lub grupy struktur przeznaczone do scentralizowanego hostingu, zapewniania wzajemnego połączenia i eksploatacji produktów ICT, usług ICT lub procesów ICT służącego do świadczenia usług przechowywania, przetwarzania i transportu danych wraz ze wszystkimi obiektami i całą infrastrukturą, zapewniającymi dystrybucję energii elektrycznej i kontrolę środowiskową;
Art. 6	32) „sieć dostarczania treści” oznacza sieć rozproszonych geograficznie serwerów służących zapewnieniu wysokiej i łatwej dostępności treści i usług cyfrowych lub ich szybkiego dostarczania na rzecz użytkowników internetu w imieniu dostawców treści i usług;	TAK	Art. 1 pkt 4 (art. 2 pkt 4b)	Art. 2: 4b) dostawca sieci dostarczania treści – osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, która dostarcza treści i usługi cyfrowe do sieci rozproszonych geograficznie serwerów służących zapewnieniu wysokiej i łatwej dostępności tych treści i usług cyfrowych lub ich szybkiego dostarczania na rzecz użytkowników internetu w imieniu dostawców treści i usług, z wyłączeniem przedsiębiorców komunikacji internetowej;
Art. 6	33) „platforma usług sieci społecznościowych” oznacza platformę umożliwiającą użytkownikom końcowym łączenie się i komunikowanie ze sobą, a także udostępnianie i odkrywanie treści przy użyciu wielu urządzeń, w szczególności za pośrednictwem czatów, postów, filmów wideo i rozmów;	TAK	Art. 1 pkt 4 (art. 2 pkt 11a)	Art. 2: „11a) platforma sieci usług społecznościowych – usługę świadczoną drogą elektroniczną w rozumieniu przepisów ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2024 r. poz. 1513), która umożliwia użytkownikom końcowym łączenie się z innymi osobami oraz komunikowanie się i wymianę,

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				udostępnianie i odkrywanie treści za pomocą wi
Art. 6	34) „przedstawiciel” oznacza osobę fizyczną lub prawną mającą miejsce zamieszkania lub miejsce prowadzenia działalności w Unii, wyraźnie wyznaczoną do występowania w imieniu dostawcy usług DNS, rejestru nazw TLD, podmiotu świadczącego usługi rejestracji nazw domen, dostawcy usług chmurowych, dostawcy usług ośrodka przetwarzania danych, dostawcy sieci dostarczania treści, dostawcy usług zarządzanych, dostawcy usług zarządzanych w zakresie bezpieczeństwa lub dostawcy internetowej platformy handlowej, wyszukiwarki internetowej lub platformy usług sieci społecznościowych, niemających miejsca prowadzenia działalności w Unii, do której właściwy organ krajowy lub CSIRT może się zwrócić zamiast do samego podmiotu w związku z obowiązkami tego podmiotu przewidzianymi w i	TAK	Art. 1 pkt 11 (art. 5a ust. 7 i 8)	Art. 5a. 7. Podmiot, o którym mowa w ust. 3, który nie posiada jednostki organizacyjnej w jednym z państw członkowskich Unii Europejskiej, ale oferuje swoje usługi na terytorium Rzeczypospolitej Polskiej, wyznacza przedstawiciela posiadającego jednostkę organizacyjną na terytorium Rzeczypospolitej Polskiej, o ile nie wyznaczył przedstawiciela posiadającego jednostkę organizacyjną w innym państwie członkowskim Unii Europejskiej. 8. Przedstawicielem, o którym mowa w ust. 7, może być osoba fizyczna, osoba prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej, ustanowiona na terytorium Rzeczypospolitej Polskiej lub w innym państwie członkowskim Unii Europejskiej, wyznaczona do występowania w imieniu podmiotu wskazanego w ust. 1, który nie posiada jednostki organizacyjnej w jednym z państw członkowskich w Unii Europejskiej, do którego organ właściwy do spraw cyberbezpieczeństwa, CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT sektorowy może się zwrócić w związku z obowiązkami podmiotu wynikającymi z ustawy.
Art. 6	35) „podmiot administracji publicznej” oznacza podmiot uznany za taki w danym państwie członkowskim zgodnie z prawem krajowym, z wyłączeniem sądownictwa, parlamentów lub banków centralnych, spełniający następujące kryteria: a) został utworzony w celu zaspokajania potrzeb leżących w interesie ogólnym i nie ma charakteru przemysłowego ani h b) ma osobowość prawną lub zgodnie z przepisami jest uprawniony do działania w imieniu innego podmiotu mającego osobowość pr	TAK	Art. 1 pkt 4 (art. 2 pkt 11c)	Art. 2: 11c) podmiot publiczny – podmiot wskazany w załączniku nr 1 lub 2 do ustawy w sektorze podmioty publiczne;

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

	c) jest finansowany w przeważającej części przez państwo, władze regionalne lub inne podmioty prawa publicznego, jego zarząd podlega nadzorowi ze strony tych organów lub podmiotów albo ponad połowa członków jego organu administrującego, zarządzającego lub nadzorczego została wyznaczona przez państwo, władze regionalne lub państwowe podmioty prawa publicznego; d) jest uprawniony do kierowania do osób fizycznych lub prawnych decyzji administracyjnych lub regulacyjnych mających wpływ na ich prawa w transgranicznym przepływie osób, towarów, usług lub informacji;			
Art. 6	36) „publiczna sieć łączności elektronicznej” oznacza publiczną sieć łączności elektronicznej zdefiniowaną w art. 2 pkt 8 dyrektywy (UE) 2018/1972;	NIE		
Art. 6	37) „usługa łączności elektronicznej” oznacza usługę łączności elektronicznej zdefiniowaną w art. 2 pkt 4 dyrektywy (UE) 2018/1972;	NIE		
Art. 6	38) „podmiot” oznacza osobę fizyczną lub prawną utworzoną i uznawaną za taką na podstawie prawa krajowego obowiązującego w miejscu, w którym osoba ta ma miejsce prowadzenia działalności, która może – działając we własnym imieniu – wykonywać prawa i podlegać obowiązkom;	NIE		W definicjach poszczególnych rodzajów podmiotów wskazano, że są to osoby fizyczne, osoby prawne albo jednostki organizacyjne nieposiadające osobowości prawnej.
Art. 6	39) „dostawca usług zarządzanych” oznacza podmiot, który świadczy usługi związane z instalacją, eksploatacją lub konserwacją produktów, sieci, infrastruktury, aplikacji ICT lub innych sieci i systemów informatycznych lub z zarządzaniem nimi, poprzez pomoc lub aktywną administrację prowadzoną u klientów lub użytkowników;	TAK	Art. 1 pkt 4 (art. 2 pkt 4h)	Art. 2: 4h) dostawca usług zarządzanych – osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, która świadczy usługi związane z instalacją, eksploatacją lub konserwacją produktów ICT, usług ICT, procesów ICT lub systemów informacyjnych przez wsparcie lub aktywną administrację przeprowadzane u użytkowników lub użytkowników lub użytkowników;
Art. 6	40) „dostawca usług zarządzanych w zakresie bezpieczeństwa” oznacza dostawcę usług zarządzanych, który prowadzi działania związane z zarządzaniem ryzykiem w zakresie cyberbezpieczeństwa lub pomocy dla podmiotów;	TAK	Art. 1 pkt 4 (art. 2 pkt 4i)	Art. 2: 4i) dostawca usług zarządzanych w zakresie cyberbezpieczeństwa – osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, która

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				świadczy usługi polegające na realizacji lub wsparciu dla realizacji działań związanych z zarządzaniem ryzykiem w cyberbezpieczeństwie, w tym obsługę incydentów, testów bezpieczeństwa, audytów systemów informacyjnych, doradztwo;
Art. 6	41) „organizacja badawcza” oznacza podmiot, którego głównym celem jest prowadzenie badań stosowanych lub eksperymentalnych prac rozwojowych z myślą o wykorzystaniu wyników tych badań do celów komercyjnych, z wyłączeniem instytucji edukacyjnych.	TAK	Art. 1 pkt 4 (art. 2 pkt 10a)	Art. 2: 10a) organizacja badawcza – osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, która prowadzi działalność, o której mowa w art. 4 ust. 2 pkt 2 lub ust. 3 ustawy z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce (Dz. U. z 2024 r. poz. 1571, z późn. zm.), z wyłączeniem podmiotów, o których mowa w art. 7 ust. 1 pkt 1–7 tej ustawy;
Art. 7	Artykuł 7 Krajowa strategia cyberbezpieczeństwa 1. Każde państwo członkowskie przyjmuje krajową strategię cyberbezpieczeństwa, która przewiduje cele strategiczne, zasoby kluczowe do osiągnięcia tych celów i odpowiednie środki z zakresu polityk publicznych i regulacji, z myślą o osiągnięciu i utrzymaniu wysokiego poziomu cyberbezpieczeństwa. Krajowa strategia cyberbezpieczeństwa zawiera: a) cele i priorytety strategii cyberbezpieczeństwa państwa członkowskiego obejmujące w szczególności sektory, o których mowa w załączniku I II; b) ramy zarządzania służące realizacji celów i priorytetów, o których mowa w lit. a) niniejszego ustępu, w tym polityki, o których mowa w u. 2; c) ramy zarządzania wyjaśniające role i obowiązki zainteresowanych stron na szczeblu krajowym, stanowiące podstawę współpracy i koordynacji na szczeblu krajowym między właściwymi organami, pojedynczymi punktami kontaktowymi i CSIRT na mocy niniejszej dyrektywy, a także koordynacji i	TAK	Art. 1 pkt 77–79 (art. 69 ust. 1 i ust. 3–5, art. 70 ust. 1 oraz ust. 3 i art. 70a)	Art. 69. 1. Strategia określa: 1) cele strategiczne i cele szczegółowe oraz środki organizacyjne i regulacyjne, służące ich realizacji; 2) mechanizm służący określeniu istotnych zasobów i szacowanie ryzyka związanego z cyberbezpieczeństwem; 3) zasady współpracy między sektorem publicznym i prywatnym; 4) podmioty zaangażowane we wdrażanie i realizację strategii; 5) środki służące koordynacji i wymianie informacji pomiędzy organami właściwymi w sprawach cyberbezpieczeństwa a właściwymi organami na podstawie dyrektywy 2022/2557 na temat ryzyka, cyberzagrożeń i incydentów, a także ryzyka, zagrożeń i incydentów poza cyberprzestrzenią oraz wykonywania zadań doradczych;

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

	współpracy między tymi podmiotami a właściwymi organami na podstawie art. 107 ust. 1 pkt 2 Ustawy; d) mechanizm służący określeniu istotnych zasobów i szacowanie ryzyka w tym podmiocie; e) wskazanie środków zapewniających gotowość na wypadek incydentów, zdolność reagowania na nie i przywracanie normalnego działania, z uwzględnieniem współpracy pomiędzy sektorami publicznym i prywatnym; f) wykaz poszczególnych organów i zainteresowanych stron zaangażowanych we wdrażanie krajowej strategii cyberbezpieczeństwa; g) ramy polityki na rzecz ściślejszej koordynacji między właściwymi organami na mocy niniejszej dyrektywy a właściwymi organami na mocy dyrektywy (UE) 2022/2557 do celu wymiany informacji na temat ryzyka, cyberzagrożeń i incydentów, a także ryzyka, zagrożeń i incydentów poza cyberprzestrzenią oraz wykonywania zadań dotyczących, które mogą być do przypisane; h) plan, zawierający kluczowe środki do podniesienia ogólnego poziomu wiedzy obywateli o cyberbezpieczeństwie.			6) działania w zakresie zwiększenia ogólnego poziomu wiedzy obywateli o cyberbezpieczeństwie; 7) cele i sposób realizacji interesów cyberbezpieczeństwa krajowego w wymiarze międzynarodowym. 3. Strategia obejmuje sektory, o których mowa w załączniku nr 1 i 2 do ustawy. 4. Strategia jest realizowana w oparciu o plan działań uwzględniający w szczególności koszty realizacji i źródła finansowania działań określonych w Strategii, a także podmioty odpowiedzialne i planowany termin realizacji poszczególnych działań. Plan działań stanowi załącznik do Strategii. 5. Strategia jest przyjmowana na okres pięcioletni z możliwością wprowadzania w niej zmian na podstawie wyników przeglądu i oceny, o których mowa w art. 71. Art. 70. 1. Projekt Strategii opracowuje minister właściwy do spraw informatyzacji we współpracy z Pełnomocnikiem, innymi ministrami, właściwymi kierownikami urzędów centralnych, a także właściwym organem w rozumieniu rozporządzenia 2022/2554. b) dodaje się ust. 3 w brzmieniu: „3. Strategia jest ogłaszana w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski”.”; Art. 70a. 1. Podmioty, o których mowa w art. 69 ust. 1 pkt 4, przekazują na żądanie ministra właściwego do spraw informatyzacji informację o

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				bieżącym stanie realizacji celów szczegółowych Strategii i działań określonych w planie działań. 2. CSIRT MON, CSIRT NASK i CSIRT GOV, CSIRT sektorowy, organ właściwy do spraw cyberbezpieczeństwa przekazuje ministrowi właściwemu do spraw informatyzacji, w terminie do dnia 30 marca, informacje o realizacji celów Strategii w poprzednim roku i działań określonych w planie działań.
Art. 7	2. W ramach krajowej strategii cyberbezpieczeństwa państwa członkowskie w szczególności przyjmują polityki: a) dotyczące cyberbezpieczeństwa w łańcuchu dostaw produktów ICT i usług ICT wykorzystywanych przez podmioty do świadczenia usług; b) dotyczące uwzględniania w zamówieniach publicznych wymogów związanych z cyberbezpieczeństwem w odniesieniu do produktów ICT i usług ICT oraz specyfikacji tych wymogów na potrzeby takich zamówień, w tym w odniesieniu do certyfikacji cyberbezpieczeństwa, szyfrowania oraz wykorzystywania produktów z zakresu cyberbezpieczeństwa opartych na otwartym oprogramowaniu; c) dotyczące zarządzania podatnościami, obejmującą promowanie i ułatwianie skoordynowanego ujawniania podatności na podstawie art. 12 ust. 1; d) związane z utrzymywaniem ogólnej dostępności, integralności i poufności publicznego rdzenia otwartego internetu, w tym, w stosownych przypadkach, cyberbezpieczeństwa podmorskich kabli komunikacyjnych; e) promującą rozwój i integrację odpowiednich zaawansowanych technologii służących wdrożeniu najnowocześniejszych środków obrony w cyberbezpieczeństwie; f) promujące i rozwijające kształcenie i szkolenie w dziedzinie cyberbezpieczeństwa, umiejętności z zakresu cyberbezpieczeństwa, podnoszenia świadomości oraz inicjatyw badawczo-rozwojowych, a także wytyczne dotyczące dobrych praktyk i kontroli w zakresie	TAK	Art. 1 pkt 77 (art. 69 ust. 2)	Art. 69. 2. Przy opracowaniu strategii uwzględnia się: 1) rozwiązania dotyczące cyberbezpieczeństwa w łańcuchu dostaw produktów ICT, usług ICT i procesów ICT wykorzystywanych przez podmioty do świadczenia usług; 2) rozwiązania dotyczące uwzględniania w zamówieniach publicznych wymogów związanych z cyberbezpieczeństwem w odniesieniu do produktów ICT, usług ICT i procesów ICT oraz specyfikacji tych wymogów na potrzeby takich zamówień, w tym w odniesieniu do certyfikacji cyberbezpieczeństwa, szyfrowania oraz wykorzystywania produktów z zakresu cyberbezpieczeństwa opartych na otwartym oprogramowaniu; 3) rozwiązania dotyczące zarządzania podatnościami, obejmujące promowanie i ułatwianie skoordynowanego ujawniania podatności na podstawie art. 12 ust. 1 dyrektywy 2022/2555; 4) utrzymanie ogólnej dostępności, integralności i poufności publicznego rdzenia otwartego internetu, w tym, w stosownych przypadkach, cyberbezpieczeństwa podmorskich kabli komunikacyjnych;

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

	cyberhigieny, skierowane do obywateli, zainteresowanych stron i podmiotów; g) wspierające instytucje akademickie i naukowe, w opracowywaniu, usprawnianiu i propagowaniu wprowadzania narzędzi z zakresu cyberbezpieczeństwa oraz bezpiecznej infrastruktury informacji; h) obejmującą właściwe procedury oraz odpowiednie narzędzia służące wymianie informacji mające na celu wspieranie dobrowolnej wymiany informacji o cyberbezpieczeństwie między podmiotami gospodarczymi; i) wzmacniające podstawowy poziom cyberodporności i cyberhigieny małych i średnich przedsiębiorstw, w szczególności tych wyłączonych z zakresu stosowania niniejszej dyrektywy, poprzez zapewnienie łatwo dostępnych wytycznych i pomocy w zakresie ich szczególnych potrzeb; j) propagujące aktywną cyberochronę.			5) promowanie rozwoju i integracji odpowiednich zaawansowanych technologii służących wdrożeniu najnowocześniejszych środków zarządzania ryzykiem w cyberbezpieczeństwie; 6) kształcenie i szkolenia w dziedzinie cyberbezpieczeństwa, umiejętności z zakresu cyberbezpieczeństwa, rozwój i promocję kwalifikacji rynkowych w zakresie cyberbezpieczeństwa w przemyśle, podnoszenie świadomości oraz inicjatywy badawczo-rozwojowe, a także wytyczne dotyczące dobrych praktyk i kontroli w cyberhigienie cyfrowej; 7) wspieranie instytucji akademickich i naukowych, w opracowywaniu, usprawnianiu i propagowaniu wprowadzania narzędzi z zakresu cyberbezpieczeństwa oraz bezpiecznej infrastruktury informacji; 8) zapewnienia odpowiednich procedur oraz narzędzi służących wymianom informacji; 9) rozwiązania wzmacniające podstawowy poziom cyberodporności i higieny cyfrowej małych i średnich przedsiębiorstw; 10) rozwiązania wspierające aktywne działania w cyberprzestrzeni.
Art. 7	3. Państwa członkowskie przekazują Komisji krajowe strategie cyberbezpieczeństwa w terminie trzech miesięcy od ich przyjęcia. Państwa członkowskie mogą wyłączyć z takich zgłoszeń informacje, które odnoszą się do ich bezpieczeństwa narodowego.	NIE		Wdrożone w art. 72 obecnej ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa
Art. 7	4. Państwa członkowskie regularnie, co najmniej co pięć lat, przeprowadzają na podstawie kluczowych wskaźników skuteczności ocenę krajowych strategii cyberbezpieczeństwa i w razie potrzeby je aktualizują. ENISA pomaga państwom członkowskim, na ich wniosek, w opracowaniu lub aktualizacji krajowej strategii cyberbezpieczeństwa i kluczowych wskaźników skuteczności działania stosowanych do oceny tej strategii w celu	TAK	Art. 1 pkt 80 (art. 71)	Art. 71. Minister właściwy do spraw informatyzacji we współpracy z Pełnomocnikiem, innymi ministrami i właściwymi kierownikami urzędów centralnych dokonuje przeglądu Strategii i oceny jej skuteczności, nie rzadziej niż co 2,5 roku.

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

	dostosowania jej do wymogów i obowiązków ustanowionych w niniejszej dyrektywie.			
Art. 8	Artykuł 8 Właściwe organy i pojedyncze punkty kontaktowe 1. Każde państwo członkowskie wyznacza lub ustanawia co najmniej jeden właściwy organ odpowiedzialny za cyberbezpieczeństwo oraz za zadania nadzorcze, o których mowa w rozdziale VII (właściwe organy).	TAK	Art. 1 pkt 44–46 (art. 41 pkt 1a, 8–9k, art. 41a i art. 42) i art. 1 pkt 56 (art. 48)	w art. 41: a) po pkt 1 dodaje się pkt 1a w brzmieniu: „1a) dla sektora inwestycji energii jądowej – minister właściwy do spraw energii;”, b) pkt 8 otrzymuje brzmienie: „8) dla sektora infrastruktury cyfrowej z wyłączeniem podmiotów, o których mowa w art. 26 ust. 5 pkt 1, oraz z wyłączeniem podsektora komunikacji elektronicznej – minister właściwy do spraw i formacji;”, c) po pkt 8 dodaje się pkt 8a w brzmieniu: „8a) dla podsektora komunikacji elektronicznej z wyłączeniem podmiotów, o których mowa w art. 26 ust. 5 pkt 1 – Prezes Urzędu Komunikacji Elektronicznej;”, d) w pkt 5, 6 i 9 wyrazy „o których mowa w art. 26 ust. 5” zastępuje się wyrazami „o których mowa w art. 26 ust. 5 pkt 1, e) po pkt 9 dodaje się pkt 9a–9k w brzmieniu: „9a) dla sektora zbiorowego odprowadzania ścieków – minister właściwy do spraw gospodarki wodnej; 9b) dla sektora zarządzania usług ICT – minister właściwy do spraw i formacji; 9c) dla sektora przestrzeni kosmicznej – minister właściwy do spraw gospodarki; 9d) dla sektora produkcji, wytwarzania i dystrybucji chemikaliów – minister właściwy do spraw gospodarki; 9e) dla sektora produkcji, przetwarzania i dystrybucji żywności – minister właściwy do spraw rolnictwa;

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				9f) dla sektora produkcji, z wyłączeniem podsektora produkcja wyrobów medycznych i wyrobów medycznych do diagnostyki in vitro – minister właściwy do spraw gospodarki; 9g) dla podsektora produkcji wyrobów medycznych i wyrobów medycznych do diagnostyki in vitro – minister właściwy do spraw zdrowia; 9h) dla sektora usług pocztowych – Prezes Urzędu Komunikacji Elektronicznej; 9i) dla sektora gospodarowania odpadami – minister właściwy do spraw klimatu; 9j) dla sektora dostawców usług cyfrowych – minister właściwy do spraw informatyki; 9k) dla sektora badań naukowych – minister właściwy do spraw szkolnictwa wyższego i nauki.”, f) uchyla się pkt 10 i 11. Art. 41a. 1. Organem właściwym do spraw cyberbezpieczeństwa w sektorze podmiotów publicznych, z wyłączeniem podmiotów podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych, jest minister właściwy do spraw informatyzacji. 2. Organem właściwym do spraw cyberbezpieczeństwa w sektorze podmiotów publicznych dla podmiotów podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych oraz dla urzędu obsługującego tego ministra jest Minister Obrony Narodowej. 3. Organem właściwym do spraw cyberbezpieczeństwa w sektorze podmiotów publicznych dla jednostek organizacyjnych podległych ministrowi właściwemu do spraw finansów publicznych lub przez niego

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				nadzorowanych, urzędu obsługującego tego ministra oraz spółki, o której mowa w art. 2 ust. 1 ustawy z dnia 29 kwietnia 2016 r. o szczególnych zasadach wykonywania niektórych zadań dotyczących informatyzacji w zakresie działań administracji rządowej budżet i finanse publiczne (Dz. U. z 2021 r. poz. 186 oraz z 2025 r. poz. 1158), jest minister właściwy do spraw finansów publicznych. 4. Dla podmiotu publicznego, który jest wymieniony w innym sektorze niż sektor podmiotów publicznych, organem właściwym do spraw cyberbezpieczeństwa jest organ właściwy dla danego sektora. Przepis nie dotyczy samorządowych podmiotów publicznych. 5. Minister właściwy do spraw informatyzacji może powierzyć realizację zadań nadzorczych nad podmiotami kluczowymi w sektorze podmiotów publicznych CSIRT NASK, z wyjątkiem wydawania decyzji administracyjnych. Zadania te są finansowane w ramach dotacji, o której mowa w art. 26 ust. 9. Przepisów art. 42 ust. 3–6, nie stosuje się w tym zakresie. w art. 42: a) w ust. 1: – pkt 1–3 otrzymuje brzmienie: „1) prowadzi bieżącą analizę podmiotów w danym sektorze lub podsektorze pod kątem uznania ich za podmiot kluczowy lub podmiot w[]y; 2) wpisuje z urzędu podmiot kluczowy lub podmiot ważny do wykazu podmiotów kluczowych lub podmiotów ważnych, jeżeli podmiot t[]i[]r[]trow[]ię w tym wyk[]i;

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				3) wydaje decyzję o uznaniu podmiotu za podmiot kluczowy lub podmiot ważny, o której mowa w art. 71 ust. 1; – uchyla się pkt 4, 6) monitoruje stosowanie przepisów ustawy przez podmioty kluczowe lub podmioty w UE; 7) wzywa na wniosek CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT sektorowego podmioty kluczowe lub podmioty ważne do usunięcia w wyznaczonym terminie podatności, które doprowadziły lub mogły doprowadzić do incydentu powstającego lub krytycznego; 8) prowadzi kontrole podmiotów kluczowych lub podmiotów w UE; „10) przetwarza informacje, w tym dane osobowe, dotyczące podmiotów kluczowych lub podmiotów ważnych oraz świadczonych przez nich usług, w zakresie niezbędnym do: a) identyfikacji podmiotów kluczowych lub podmiotów ważnych, b) zapewnienia wymiany informacji w zakresie cyberbezpieczeństwa, w tym o incydentach, podatnościach i cyberzagrożeniach między podmiotami kluczowymi lub podmiotami ważnymi a CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT sektorowymi i organami właściwymi do spraw cyberbezpieczeństwa, c) prowadzenia czynności nadzorczych nad podmiotami kluczowymi lub podmiotami w UE; 12) współpracuje oraz wymienia informacje i dokumenty z właściwym organem w rozumieniu rozporządzenia 2022/2554, w zakresie niezbędnym do wykonywania przez ten organ obowiązków wynikających z rozporządzenia 2022/2554;

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				13) współpracuje oraz wymienia informacje i dokumenty z organem właściwym do spraw podmiotów krytycznych w zakresie nadzoru nad podmiotem kluczowym będącym podmiotem krytycznym. b) uchylenie u.f. 2; c) dodaje się ust. 9–11 w brzmieniu: 9. Organ właściwy do spraw cyberbezpieczeństwa dla sektora bankowości i infrastruktury rynków finansowych realizuje swoje zadania, z uwzględnieniem zakresu zastosowania ustawy do podmiotów finansowych. 10. W ramach współpracy, o której mowa w ust. 1 pkt 12, mającej związek z podmiotem kluczowym lub podmiotem ważnym, który zgodnie z rozporządzeniem 2022/2554 został wyznaczony jako kluczowy zewnętrzny dostawca usług ICT, organ właściwy do spraw cyberbezpieczeństwa, w szczególności udziela informacji oraz istotnych zaleceń technicznych i pomocy technicznej, a także umożliwia skuteczną i szybką koordynację działań nadzorczych, w tym na potrzeby prowadzenia kontroli. 11. Organ właściwy do spraw cyberbezpieczeństwa prowadzi wykaz osób, wobec których wydana została decyzja o zastosowaniu środka nadzorczego, o którym mowa w art. 53 ust. 9 pkt 6, obejmujący: 1) imię (imiona); 2) nazwisko; 3) numer PESEL, a w przypadku jego nieposiadania – datę urodzenia; 4) nazwę podmiotu kluczowego; 5) datę wydania decyzji; 6) znak sprawy; 7) okres obowiązywania zakazu;

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				8) podstawę prawną wydania decyzji. art. 48: 1) odbieranie zgłoszeń incydentu dotyczącego więcej niż jednego sektora lub dotyczącego innych państw członkowskich Unii Europejskiej z pojedynczych punktów kontaktowych w innych państwach członkowskich Unii Europejskiej, a także przekazywanie tych zgłoszeń do CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT []torow[]go; 2) przekazywanie, na wniosek właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV, zgłoszenia incydentu dotyczącego więcej niż jednego sektora lub innych państw członkowskich Unii Europejskiej do pojedynczych punktów kontaktowych w innych państwach członkowskich Unii Europejskiej;
art. 8	2. Właściwe organy, o których mowa w ust. 1, monitorują wdrażanie niniejszej dyrektywy na poziomie krajowym.	TAK	Art. 1 pkt 46 (art. 42 ust. 1 pkt 6)	Art. 42.1: 6) monitoruje stosowanie przepisów ustawy przez podmioty kluczowe lub podmioty w [] [];
art. 8	3. Każde państwo członkowskie wyznacza lub ustanawia pojedynczy punkt kontaktowy. W przypadku gdy państwo członkowskie wyznacza lub ustanawia tylko jeden właściwy organ zgodnie z ust. 1, ten właściwy organ jest również pojedynczym punktem kontaktowym dla tego państwa członkowskiego.	NIE		Pojedynczy Punkt Kontaktowy został już wyznaczony na podstawie art. 48 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.
art. 8	4. Każdy pojedynczy punkt kontaktowy pełni funkcję łącznikową w celu zapewnienia transgranicznej współpracy organów ze swojego państwa członkowskiego z odpowiednimi organami w innych państwach członkowskich, a w stosownym przypadku z Komisją i ENISA, a także w celu zapewnienia międzysektorowej współpracy z innymi właściwymi organami krajowymi w swoim państwie członkowskim.	NIE		Pojedynczy Punkt Kontaktowy został już wyznaczony na podstawie art. 48 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.
art. 8	5. Państwa członkowskie zapewniają swoim właściwym organom i pojedynczym punktom kontaktowym odpowiednie zasoby, aby	TAK	Art. 46	Art. 46. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 20 – gospodarka,

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

	mogły one efektywnie i skutecznie wykonywać powierzone im zadania i tym samym realizować cele niniejszej dyrektywy.			będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi: 1) w 2025 r. - 0 tyś zł; 2) w 2026 r. - 5 662 tyś zł; 3) w 2027 r. - 5 353 tyś zł; 4) w 2028 r. - 5 587 tyś zł; 5) w 2029 r. - 5 836 tyś zł; 6) w 2030 r. - 6 101 tyś zł; 7) w 2031 r. - 6 384 tyś zł; 8) w 2032 r. - 6 682 tyś zł; 9) w 2033 r. - 7 000 tyś zł; 10) w 2034 r. - 7 338 tys. zł. 2. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 21 – gospodarka morska, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi: 1) w 2025 r. - 0 tyś zł; 2) w 2026 r. - 111 tyś zł; 3) w 2027 r. - 114 tyś zł; 4) w 2028 r. - 122 tyś zł; 5) w 2029 r. - 130 tyś zł; 6) w 2030 r. - 138 tyś zł; 7) w 2031 r. - 147 tyś zł; 8) w 2032 r. - 157 tyś zł; 9) w 2033 r. - 168 tyś zł; 10) w 2034 r. - 179 tys. zł. 3. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 22 – gospodarka wodna, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi: 1) w 2025 r. - 0 tyś zł; 2) w 2026 r. - 6 268 tyś zł; 3) w 2027 r. - 6 819 tyś zł; 4) w 2028 r. - 7 160 tyś zł; 5) w 2029 r. - 7 523 tyś zł; 6) w 2030 r. - 7 908 tyś zł;

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				7) w 2031 r. - 8 317 tyś zł; 8) w 2032 r. - 8 750 tyś zł; 9) w 2033 r. - 9 211 tyś zł; 10) w 2034 r. - 9 699 tys. zł. 4. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 27 – informatyzacja, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi: 1) w 2025 r. - 0 tyś zł; 2) w 2026 r. - 136 778 tyś zł; 3) w 2027 r. - 137 213 tyś zł; 4) w 2028 r. - 146 969 tyś zł; 5) w 2029 r. - 167 112 tyś zł; 6) w 2030 r. - 189 948 tyś zł; 7) w 2031 r. - 217 414 tyś zł; 8) w 2032 r. - 223 028 tyś zł; 9) w 2033 r. - 251 875 tyś zł; 10) w 2034 r. - 287 067 tys. zł. 5. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 28 – szkolnictwo wyższe i nauka, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi: 1) w 2025 r. - 0 tyś zł; 2) w 2026 r. - 5 754 tyś zł; 3) w 2027 r. - 6 289 tyś zł; 4) w 2028 r. - 6 594 tyś zł; 5) w 2029 r. - 6 917 tyś zł; 6) w 2030 r. - 7 259 tyś zł; 7) w 2031 r. - 7 622 tyś zł; 8) w 2032 r. - 8 007 tyś zł; 9) w 2033 r. - 8 415 tyś zł; 10) w 2034 r. - 8 848 tys. zł. 6. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 32 – rolnictwo, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				1) w 2025 r. - 0 tyś zł; 2) w 2026 r. - 7 295 tyś zł; 3) w 2027 r. - 7 878 tyś zł; 4) w 2028 r. - 8 294 tyś zł; 5) w 2029 r. - 8 736 tyś zł; 6) w 2030 r. - 9 207 tyś zł; 7) w 2031 r. - 9 706 tyś zł; 8) w 2032 r. - 10 237 tyś zł; 9) w 2033 r. - 10 801 tyś zł; 10) w 2034 r. - 11 401 tys. zł. 7. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 39 – transport, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi: 1) w 2025 r. - 0 tyś zł; 2) w 2026 r. - 6 473 tyś zł; 3) w 2027 r. - 7 030 tyś zł; 4) w 2028 r. - 7 387 tyś zł; 5) w 2029 r. - 7 766 tyś zł; 6) w 2030 r. - 8 168 tyś zł; 7) w 2031 r. - 8 595 tyś zł; 8) w 2032 r. - 9 048 tyś zł; 9) w 2033 r. - 9 529 tyś zł; 10) w 2034 r. - 10 040 tys. zł. 8. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 47 – energia, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi: 1) w 2025 r. - 0 tyś zł; 2) w 2026 r. - 6 268 tyś zł; 3) w 2027 r. - 6 819 tyś zł; 4) w 2028 r. - 7 160 tyś zł; 5) w 2029 r. - 7 523 tyś zł; 6) w 2030 r. - 7 908 tyś zł; 7) w 2031 r. - 8 317 tyś zł; 8) w 2032 r. - 8 750 tyś zł;

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				9) w 2033 r. - 9 211 tyś zł; 10) w 2034 r. - 9 699 tys. zł. 9. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 51 – klimat, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi: 1) w 2025 r. - 0 tyś zł; 2) w 2026 r. - 5 960 tyś zł; 3) w 2027 r. - 6 501 tyś zł; 4) w 2028 r. - 6 820 tyś zł; 5) w 2029 r. - 7 160 tyś zł; 6) w 2030 r. - 7 519 tyś zł; 7) w 2031 r. - 7 900 tyś zł; 8) w 2032 r. - 8 304 tyś zł; 9) w 2033 r. - 8 733 tyś zł; 10) w 2034 r. - 9 188 tys. zł. 10. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 57 – Agencja Bezpieczeństwa Wewnętrznego, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi: 1) w 2025 r. - 0 tys. zł; 2) w 2026 r. - 3 000 tyś zł; 3) w 2027 r. - 3 000 tyś zł; 4) w 2028 r. - 3 000 tyś zł; 5) w 2029 r. - 3 000 tyś zł; 6) w 2030 r. - 3 000 tyś zł; 7) w 2031 r. - 3 000 tyś zł; 8) w 2032 r. - 3 000 tyś zł; 9) w 2033 r. - 3 000 tyś zł; 10) w 2034 r. - 3 000 tys. zł. 11. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 76 – Urząd Komunikacji Elektronicznej, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				1) w 2025 r. - 0 tyś zł; 2) w 2026 r. - 8 014 tyś zł; 3) w 2027 r. - 8 619 tyś zł; 4) w 2028 r. - 9 087 tyś zł; 5) w 2029 r. - 9 586 tyś zł; 6) w 2030 r. - 10 115 tyś zł; 7) w 2031 r. - 10 678 tyś zł; 8) w 2032 r. - 11 277 tyś zł; 9) w 2033 r. - 11 915 tyś zł; 10) w 2034 r. - 12 593 tys. zł. 12. Minister właściwy do spraw gospodarki monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 1, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków minister właściwy do spraw gospodarki wdraża mechanizm korygujący polegający na ograniczeniu finansowania działalności: 1) organu właściwego do spraw cyberbezpieczeństwa dla sektorów produkcji i przetwarzania informacji; 2) CSIRT sektorowego dla sektorów produkcji i przestrzeni kosmicznej. 13. Minister właściwy do spraw gospodarki morskiej monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 2, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				dany rok budżetowy limitu wydatków minister właściwy do spraw gospodarki morskiej wdraża mechanizm korygujący polegający na ograniczeniu finansowania działalności: 1) organu właściwego do spraw cyberbezpieczeństwa dla podsektora transportu wodnego; 2) CSIRT sektorowego dla podsektora transportu wodnego. 14. Minister właściwy do spraw gospodarki wodnej monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 3, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków minister właściwy do spraw gospodarki wodnej wdraża mechanizm korygujący polegający na ograniczeniu finansowania działalności: 1) organu właściwego do spraw cyberbezpieczeństwa dla sektorów zaopatrzenia w wodę pitną i jej dystrybucji oraz ścieków; 2) CSIRT sektorowego dla sektorów zaopatrzenia w wodę pitną i jej dystrybucji oraz ścieków. 15. Minister właściwy do spraw informatyzacji monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 4, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków minister

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				właściwy do spraw informatyzacji wdraża mechanizm korygujący polegający na ograniczeniu finansowania: 1) organu właściwego do spraw cyberbezpieczeństwa dla sektorów dostawców usług cyfrowych, infrastruktury cyfrowej oraz <u>Urząd ds. usług IT</u>; 2) CSIRT sektorowego dla sektorów dostawców usług cyfrowych, infrastruktury <u>cyfrowej</u> oraz <u>Urząd ds. usług IT</u>; 3) realizacji zadań ministra w obszarze <u>Urząd ds. krytycznego w cyberprzestrzeni</u>; 4) dotacji podmiotów <u>dl CSIRT NASK</u>; 5) dotacji celowych udzielanych jednostkom podległym ministrowi właściwemu do spraw informatyzacji albo przez niego nadzorowanym w związku z powierzeniem realizacji zadań <u>mi IT</u>; 6) działalności edukacyjnej w zakresie <u>cyberbezpieczeństwa</u>; 7) realizacji zadań Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa. 16. Minister właściwy do spraw szkolnictwa wyższego i nauki monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 5, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków minister właściwy do spraw szkolnictwa wyższego i nauki wdraża mechanizm korygujący polegający na ograniczeniu finansowania działalności:

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				1) organu właściwego do spraw cyberbezpieczeństwa dla sektora badań naukowych; 2) CSIRT sektorowego dla sektora badań naukowych. 17. Minister właściwy do spraw rolnictwa monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 6, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków minister właściwy do spraw rolnictwa wdraża mechanizm korygujący polegający na ograniczeniu finansowania działalności: 1) organu właściwego do spraw cyberbezpieczeństwa dla sektora produkcji, przetwarzania i dystrybucji żywności; 2) CSIRT sektorowego dla sektora produkcji, przetwarzania i dystrybucji żywności. 18. Minister właściwy do spraw transportu monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 7, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków minister właściwy do spraw transportu wdraża mechanizm korygujący polegający na ograniczeniu finansowania działalności: 1) organu właściwego do spraw cyberbezpieczeństwa dla sektora produkcji, przetwarzania i dystrybucji żywności; 2) CSIRT sektorowego dla sektora produkcji, przetwarzania i dystrybucji żywności.

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				2) CSIRT sektorowego dla sektora transportu. 19. Minister właściwy do spraw energii monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 8, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków minister właściwy do spraw energii wdraża mechanizm korygujący polegający na ograniczeniu finansowania działalności CSIRT sektorowego: 1) organu właściwego do spraw cyberbezpieczeństwa dla sektora energii; 2) CSIRT sektorowego dla sektora energii. 20. Minister właściwy do spraw klimatu monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 9, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków minister właściwy do spraw klimatu wdraża mechanizm korygujący polegający na ograniczeniu finansowania 1) organu właściwego do spraw cyberbezpieczeństwa dla sektora gospodarowania odpadami; 2) CSIRT sektorowego dla sektora gospodarowania odpadami. 21. Szef Agencji Bezpieczeństwa Wewnętrznego monitoruje wykorzystanie limitu wydatków, o

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				którym mowa w ust. 10, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków Szef Agencji Bezpieczeństwa Wewnętrznego wdraża mechanizm korygujący polegający na ograniczeniu finansowania czynności nadzorczych wobec podmiotów publicznych w zakresie cyberbezpieczeństwa. Wdrożenie tego mechanizmu korygującego następuje w uzgodnieniu z ministrem – członkiem Rady Ministrów właściwym do spraw koordynowania działalności służb specjalnych albo z Prezesem Rady Ministrów, jeżeli minister – członek Rady Ministrów właściwy do spraw koordynowania działalności służb specjalnych nie został powołany. 22. Prezes Urzędu Komunikacji Elektronicznej monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 11, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków Prezes Urzędu Komunikacji Elektronicznej wdraża mechanizm korygujący polegający na ograniczeniu finansowania działalności 1) organu właściwego do spraw cyberbezpieczeństwa dla sektora poczty i podłkktorłkomułkłłji łłłtrołłłłj;

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				2) CSIRT sektorowego dla sektora poczty i podsektora komunikacji elektronicznej.
art. 8	6. Każde państwo członkowskie bez zbędnej zwłoki przekazuje Komisji dane identyfikacyjne właściwego organu, o którym mowa w ust. 1, i pojedynczego punktu kontaktowego, o którym mowa w ust. 3, oraz powiadamia ją o zadaniach tych organów i o późniejszych zmianach w tym zakresie. Każde państwo członkowskie podaje dane identyfikacyjne właściwego organu do wiadomości publicznej. Komisja udostępnia publicznie wykaz pojedynczych punktów kontaktowych.	TAK	Art. 1 pkt 50 lit. a (art. 45 ust. 1 pkt 13)	Art. 45.1: 13) przekazywanie Komisji Europejskiej aktualnych informacji o organach właściwych do spraw cyberbezpieczeństwa, ich danych identyfikacyjnych oraz zadaniach.
Art. 9	Artykuł 9 Krajowe ramy zarządzania kryzysowego w cyberbezpieczeństwie 1. Każde państwo członkowskie wyznacza lub ustanawia co najmniej jeden właściwy organ odpowiedzialny za zarządzanie incydentami i zarządzanie kryzysowe w cyberbezpieczeństwie na dużą skalę (organy ds. zarządzania kryzysowego w cyberbezpieczeństwie). Państwa członkowskie zapewniają tym organom odpowiednie zasoby, aby mogły one efektywnie i skutecznie wykonywać powierzone im zadania. Państwa członkowskie zapewniają spójność z istniejącymi ogólnymi krajowymi ramami zarządzania kryzysowego.	TAK	Art. 1 pkt 61 (Rozdział 10c) i art. 38	Rozdział 10c Organy odpowiedzialne za zarządzanie incydentami i zarządzanie kryzysowe w cyberbezpieczeństwie na dużą skalę Art. 52e. Minister właściwy do spraw informatyzacji pełni rolę organu odpowiedzialnego za zarządzanie incydentami i zarządzanie kryzysowe w cyberbezpieczeństwie na dużą skalę w wymiarze cywilnym, z wyłączeniem spraw dotyczących zagrożeń terrorystycznych oraz zagrożeń związanych ze szpiegostwem. Art. 52f. Minister Obrony Narodowej pełni rolę organu odpowiedzialnego za zarządzanie incydentami i zarządzanie kryzysowe w cyberbezpieczeństwie na dużą skalę w wymiarze militarnym. Art. 52g. Szef Agencji Bezpieczeństwa Wewnętrznego pełni rolę organu odpowiedzialnego za zarządzanie incydentami i zarządzanie kryzysowe w cyberbezpieczeństwie na dużą skalę w wymiarze cywilnym w sprawach dotyczących zagrożeń terrorystycznych oraz zagrożeń związanych ze szpiegostwem.

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				Art. 52h. Organ odpowiedzialny za zarządzanie incydentami i zarządzanie kryzysowe w cyberbezpieczeństwie na dużą skalę koordynuje działania organów państwa zgodnie z Krajowym Planem reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę. Art. 38. Minister właściwy do spraw informatyzacji, w terminie 3 miesięcy od dnia wejścia w życie ustawy, przekaze Komisji Europejskiej informację o wyznaczeniu organu do spraw zarządzania kryzysowego w cyberbezpieczeństwie wraz z jego danymi identyfikacyjnymi.
Art. 9	2. Jeżeli państwo członkowskie wyznaczy lub ustanowi więcej niż jeden organ ds. zarządzania kryzysowego w cyberbezpieczeństwie zgodnie z ust. 1, jasno wskazuje, który z tych organów ma pełnić rolę koordynatora zarządzania incydentami i zarządzania kryzysowego w cyberbezpieczeństwie na dużą skalę.	TAK	Art. 1 pkt 61 (Rozdział 10c)	Rozdział 10c Organy odpowiedzialne za zarządzanie incydentami i zarządzanie kryzysowe w cyberbezpieczeństwie na dużą skalę. Art. 52e. Minister właściwy do spraw informatyzacji pełni rolę organu odpowiedzialnego za zarządzanie incydentami i zarządzanie kryzysowe w cyberbezpieczeństwie na dużą skalę w wymiarze cywilnym, z wyłączeniem spraw dotyczących zagrożeń terrorystycznych oraz zagrożeń związanych ze szpiegostwem. Art. 52f. Minister Obrony Narodowej pełni rolę organu odpowiedzialnego za zarządzanie incydentami i zarządzanie kryzysowe w cyberbezpieczeństwie na dużą skalę w wymiarze militarnym. Art. 52g. Szef Agencji Bezpieczeństwa Wewnętrznego pełni rolę organu

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				odpowiedzialnego za zarządzanie incydentami i zarządzanie kryzysowe w cyberbezpieczeństwie na dużą skalę w wymiarze cywilnym w sprawach dotyczących zagrożeń terrorystycznych oraz zagrożeń związanych ze szpiegostwem. Art. 52h. Organ odpowiedzialny za zarządzanie incydentami i zarządzanie kryzysowe w cyberbezpieczeństwie na dużą skalę koordynuje działania organów państwa zgodnie z Krajowym Planem reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę.
Art. 9	3. Każde państwo członkowskie określa zdolności, zasoby i procedury, które można wykorzystać w razie sytuacji kryzysowej do celów niniejszej dyrektywy.	NIE		Elementy te zostały już określone w Krajowym Planie Zarządzania Kryzysowego wydanym na podstawie ustawy o zarządzaniu kryzysowym.
Art. 9	4. Każde państwo członkowskie przyjmuje krajowy plan reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę, w którym określa cele i tryb zarządzania incydentami i zarządzania kryzysowego w cyberbezpieczeństwie na dużą skalę. W planie tym określa się w szczególności: a) cele krajowych środków i działań służących w zakresie gotowości; b) zadania i obowiązki organów ds. zarządzania kryzysowego w państwie; c) procedury zarządzania kryzysowego w cyberprzestrzeni, w tym ich włączenie do ogólnych krajowych ram zarządzania kryzysowego, oraz ich wymiary i formy; d) krajowe środki w zakresie gotowości, w tym ćwiczenia i szkolenia; e) odpowiednie zainteresowane strony publiczne i prywatne oraz ich strukturę; f) krajowe procedury i ustalenia między odpowiednimi organami i instytucjami krajowymi mające na celu zapewnienie efektywnego uczestnictwa danego państwa członkowskiego w skoordynowanym	TAK	Art. 1 pkt 81 (Rozdział 13a)	Rozdział 13a Krajowy plan reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę. Art. 72a. Rada Ministrów przyjmuje, w drodze uchwały, Krajowy plan reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę, zwany dalej „Krajowym Planem”. Art. 72b. 1. Krajowy Plan określa cele i tryb zarządzania incydentami i zarządzania kryzysowego w cyberbezpieczeństwie na dużą skalę. 2. Krajowy Plan zawiera w szczególności: 1) cele działań w zakresie zarządzania kryzysowego w cyberbezpieczeństwie na dużą skalę;

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

zarządzaniu incydentami i zarządzaniu kryzysowym w cyberbezpieczeństwie na dużą skalę na poziomie Unii oraz efektywnego wsparcia ze strony danego państwa członkowskiego dla tego rodzaju skoordynowanego zarządzania.			2) zadania organów zaangażowanych w zarządzanie kryzysowym w cyberbezpieczeństwie; 3) procedury zarządzania kryzysowego w cyberprzestrzeni oraz kanały wymiany informacji; 4) krajowe środki służące zapewnieniu gotowości na wypadek wystąpienia incydentów w cyberbezpieczeństwie na dużą skalę w tym celu; 5) zasady współpracy między sektorem publicznym i prywatnym w obszarze zarządzania kryzysowego; 6) kryteria oceny infrastruktury informatycznej pod kątem jej znaczenia dla zarządzania kryzysowego; 7) krajowe procedury i ustalenia między odpowiednimi organami i instytucjami krajowymi mające na celu zapewnienie efektywnego uczestnictwa danego państwa członkowskiego Unii Europejskiej w skoordynowanym zarządzaniu incydentami i zarządzaniu kryzysowym w cyberbezpieczeństwie na dużą skalę na poziomie Unii Europejskiej oraz efektywnego wsparcia ze strony danego państwa członkowskiego Unii Europejskiej dla tego rodzaju skoordynowanego zarządzania; 8) postanowienia dotyczące zarządzania kryzysami i reagowania na nie w odniesieniu do transgranicznych przepływów energii elektrycznej, w rozumieniu art. 41 ust. 2 i 3 rozporządzenia (UE) 2024/1366; 9) uporządkowaną listę działań na rzecz ograniczenia ryzyka wystąpienia incydentu krytycznego w zakresie organizacyjnym i technicznym, z uwzględnieniem: a) hierarchii działań,

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				b) ram czasowych ich realizacji, c) podmiotów wiodących oraz współpracujących przy ich wykonywaniu, d) sposobów finansowania oraz wysokości nakładów finansowych, e) oceny osiągniętych efektów oraz wniosków z wdrożonych działań. Art. 72c. Podmioty realizujące zadania z zakresu zarządzania kryzysowego na żądanie ministra właściwego do spraw informatyzacji, przekazują informację o bieżącym stanie realizacji zadań wynikających z Krajowego Planu. Art. 72d. 1. Projekt Krajowego Planu opracowuje minister właściwy do spraw informatyzacji we współpracy z Pełnomocnikiem, Rządowym Centrum Bezpieczeństwa, oraz z innymi ministrami, właściwymi kierownikami urzędów centralnych oraz z właściwym organem określonym w art. 52a ust. 1. 2. W pracach nad projektem może uczestniczyć przedstawiciel Prezydenta Rzeczypospolitej Polskiej. 3. Krajowy Plan jest ogłaszany w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski”. Art. 72e. Krajowy Plan podlega aktualizacji nie rzadziej niż raz na dwa lata. Art. 72f. Minister właściwy do spraw informatyzacji przekazuje Komisji Europejskiej i europejskiej sieci organizacji łącznikowych do spraw kryzysów cyberbezpieczeństwa ważne informacje związane z Krajowym Planem, w

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				szczegółności procedury, o których mowa w art. 72b ust. 2 pkt 3, w terminie 3 miesięcy od dnia jego przyjęcia przez Radę Ministrów.
Art. 9	5. W terminie trzech miesięcy od wyznaczenia lub ustanowienia organu ds. zarządzania kryzysowego w cyberbezpieczeństwie, o którym mowa w ust. 1, każde państwo członkowskie przekazuje Komisji dane identyfikacyjne swojego organu oraz powiadamia ją o późniejszych zmianach w tym zakresie. Państwa członkowskie przedkładają Komisji i europejskiej sieci organizacji łącznikowych do spraw kryzysów cyberbezpieczeństwa (EU-CyCLONe) ważne informacje związane z wymogami określonymi w ust. 4, dotyczące krajowych planów reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę w terminie trzech miesięcy od daty przyjęcia tych planów. Państwa członkowskie mogą wyłączyć niektóre informacje, jeżeli i w zakresie w jakim jest to kluczowe z punktu widzenia ich bezpieczeństwa narodowego.	TAK	Art. 38.	Art. 38. Minister właściwy do spraw informatyzacji, w terminie 3 miesięcy od dnia wejścia w życie ustawy, przekaze Komisji Europejskiej informacje o wyznaczeniu organu do spraw zarządzania kryzysowego w cyberbezpieczeństwie wraz z jego danymi identyfikacyjnymi.
Art. 10	Artykuł 10 Zespoły reagowania na incydenty bezpieczeństwa komputerowego (CSIRT) 1. Każde państwo członkowskie wyznacza lub ustanawia co najmniej jeden CSIRT. CSIRT można wyznaczyć lub ustanowić w ramach właściwego organu. CSIRT spełniają wymogi określone w art. 11 ust. 1, obejmują co najmniej sektory, podsektory i rodzaje podmiotów, o których mowa w załącznikach I i II, i są odpowiedzialne za obsługę incydentów zgodnie z wyraźnie określoną procedurą.	TAK	Art. 1 pkt 28 (art. 26 ust. 1, 1a, 2, ust. 2a–2c, ust. 3, ust. 3a, ust. 5, ust. 6, ust. 7, ust. 13–15)	Art. 26: a) w ust. 1: – po wyrazie „informatyzacji” dodaje się wyrazy „, CSIRT sektorowymi”, – wyrazy „zagrożeniom cyberbezpieczeństwa” zastępuje się wyrazem „cyberzagrożeniom”, b) po ust. 1 dodaje się ust. 1a w brzmieniu: „1a. W czasie stanu wojennego lub w czasie wojny CSIRT MON, w imieniu Ministra Obrony Narodowej, koordynuje działania CSIRT NASK i CSIRT GOV.”, c) ust. 2 otrzymuje brzmienie: „2. CSIRT MON, CSIRT NASK i CSIRT GOV na wniosek podmiotów krajowego systemu cyberbezpieczeństwa mogą zapewnić wsparcie tym podmiotom w obsłudze incydentów, w przypadku gdy: 1) incydent może wpłynąć na inne podmioty krajowego systemu cyberbezpieczeństwa”

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				2) podmiot obsługujący incydent nie dysponuje środkami pozwalającymi mu na jego skuteczną obsługę, a incydent powoduje przerwanie ciągłości świadczenia usługi.”,,” d) po ust. 2 dodaje się ust. 2a–2c w brzmieniu: „2a. Pełnomocnik może zlecić zapewnienie wsparcia w obsłudze incydentów, o którym mowa w ust. 2: 1) CSIRT MON, za zgodą Ministra Obrony Narodowej lub 2) CSIRT NASK, lub 3) CSIRT GOV, za zgodą Szefa Agencji Bezpieczeństwa Wewnętrznego. 2b. Zgoda może być wyrażona w formie ustnej lub dokumentowej, w szczególności z wykorzystaniem środków komunikacji elektronicznej. Zgoda wyrażona w formie ustnej wymaga udokumentowania w ciągu 14 dni od dnia jej wydania 2c. O zapewnieniu wsparcia w obsłudze incydentów, o którym mowa w ust. 2 lub 2a, jest informowany właściwy CSIRT sektorowy.”, e) w ust. 3: – w pkt 1 wyrazy „zagrożeń cyberbezpieczeństwa” zastępuje się wyrazem „cyberzagrożeń”, – pkt 2–4 otrzymują brzmienie: „2) szacowanie ryzyka związanego z ujawnionym cyberzagrożeniem oraz zaistniałymi incydentami, w tym p[ro]wad[zi]enie dy[agn]ostyki i ry[zy]ka; 3) przekazywanie informacji dotyczących cyberzagrożeń, podatności, incydentów i ryzyk, wczesne ostrzeganie i alarmowanie podmiotów krajowego systemu cyberbezpieczeństwa; 4) wydawanie komunikatów o zidentyfikowanych cyberzagrożeniach”;

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				– pkt 6 i 7 otrzymują brzmienie: „6) klasyfikowanie incydentów, w tym incydentów poważnych, jako incydenty krytyczne oraz koordynowanie obsługi incydentów krytycznych; 7) „międzynarodowy klasyfikacji i incydentów;”, –w pkt 10: – – wyrazy „sektorowymi zespołami cyberbezpieczeństwa” zastępuje się wyrazami „CSIRT sektorowymi”, – – wyrazy „zagrożeniom cyberbezpieczeństwa” zastępuje się wyrazem „cyberzagrożeniom”, – pkt 11 i 12 otrzymują brzmienie: „11) przekazywanie do innych państw, w tym państw członkowskich Unii Europejskiej, i przyjmowanie z tych państw informacji o incydentach poważnych dotyczących dwóch lub większej liczby państw członkowskich, a także przekazywanie do Pojedynczego Punktu Kontaktowego zgłoszenia incydentu poważnego dotyczącego dwóch lub większej liczby państw Unii Europejskiej; 12) przekazywanie, w terminie 14 dni od zakończenia danego kwartału, do Pojedynczego Punktu Kontaktowego zestawienia zgłoszonych w poprzednich 3 miesiącach: a) poważnych incydentów, b) incydentów, c) cyberzagrożeń, d) potencjalnych zdarzeń dla cyberbezpieczeństwa”, – w pkt 14 w lit. b i c wyrazy „zagrożeń cyberbezpieczeństwa” zastępuje się wyrazem „cyberzagrożeń”, – uchyla się pkt 15, – pkt 16 otrzymuje brzmienie:

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				„16) udział w Sieci CSIRT składającej się z przedstawicieli CSIRT państw członkowskich Unii Europejskiej, CSIRT właściwego dla instytucji Unii Europejskiej oraz Komisji Europ[...];”, – dodaje się pkt 17–23 w brzmieniu: „17) w odpowiednich przypadkach gromadzenie i zabezpieczanie danych na potrzeby postępowań k[...]; 18) współpraca z sektorowymi i międzysektorowymi społecznościami podmiotów kluczowych lub podmiotów ważnych oraz wymiana informacji dotyczących cyberbezpieczeństwa jeżeli wymiana informacji zapewnia zwiększenie poziomu cyberbezpieczeństwa lub służy przeciwdziałaniu incydentom 19) współpraca z krajowymi zespołami reagowania na incydenty bezpieczeństwa komputerowego z p[...]; 20) udział we wdrażaniu bezpiecznych narzędzi wymiany informacji z podmiotami kluczowymi i podmiot[...]; 21) prowadzenie działań na rzecz podnoszenia poziomu bezpieczeństwa systemów informacyjnych podmiotów krajowego systemu cyberbezpieczeństwa przez: a) wykonywanie oceny bezpieczeństwa, b) identyfikowanie podatności systemów dostępnych w otwartych sieciach teleinformatycznych, a także powiadamianie właścicieli tych systemów o wykrytych podatnościach oraz zagrożeniach; 22) promowanie, przyjmowanie i stosowanie wspólnych lub znormalizowanych praktyk,

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				systemów klasyfikacji i systematyki związanych z: a) procedurami obsługi incydentu, b) zarządzaniem kryzysowym w obszarze cyberbezpieczeństwa, c) ujawnianiem podtłoczeń; 23) przekazywanie Pełnomocnikowi Rządu do Spraw Cyberbezpieczeństwa sprawozdania z wykonywania swoich zadań ustawowych zawierającego w szczególności informacje o zgłoszonych do zespołu CSIRT incydentach krytycznych, incydentach poważnych, incydentach, cyberzagrożeniach oraz potencjalnych zdarzeniach dla cyberbezpieczeństwa”, f) po ust. 3 dodaje się ust. 3a w brzmieniu: „3a. Przy realizacji zadania, o którym mowa w ust. 3 pkt 19, CSIRT MON, CSIRT NASK i CSIRT GOV mogą wymieniać informacje, w tym dane osobowe w celu informowania o potencjalnych cyberzagrożeniach oraz zastosowanych sposobach ich zwalczania, w celu przeciwdziałania cyberzagrożeniom o charakterze transgranicznym. Dane, o których mowa w zdaniu pierwszym, przekazuje się w postaci elektronicznej.”, g) w ust. 5 w pkt 2 kropkę zastępuje się średnikiem i dodaje się pkt 3 w brzmieniu: „3) Ministra Obrony Narodowej.”. h) w ust. 6: – w pkt 1: – – lit. a i b otrzymują brzmienie: „a) jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 2a–6 i 10–13 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych, z wyjątkiem podmiotów wymienionych w ust. 5,

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				b) jednostki podległe organom administracji rządowej lub przez nie nadzorowane, z wyjątkiem podmiotów, o których mowa w ust. 5, oraz jednostek, o których mowa w ust. 7 pkt 2”, – – po lit. a dodaje się lit. aa w brzmieniu: „aa) urzędy obsługujące jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 2 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych,”, – – po lit. c dodaje się lit. ca–cc w brzmieniu: „ca) międzynarodowe instytuty badawcze, cb) Centrum Łukasiewicz, cc) instytuty działające w ramach Sieci Badawczej Łukasiewicz,”, – – uchyla się lit. e, – – uchyla się lit. i, – – lit. j otrzymuje brzmienie: „j) podmioty kluczowe lub podmioty ważne, z wyjątkiem wymienionych w ust. 5 i 7,”, – w pkt 2 wyrazy „zagrożeniach cyberbezpieczeństwa” zastępuje się wyrazem „cyberzagrożeniach”, i) w ust. 7 – pkt 1 otrzymuje brzmienie: „1) jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 1, 8 i 9 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych, i urzędy je obsługujące, z wyjątkiem wymienionych w ust. 5 i 6,”, – po pkt 4 dodaje się pkt 4a–4e w brzmieniu: „4a) Poliką Agencję Żegluga Powiatowa; 4b) Poliką Agencję Prądową; 4c) Państwowe Gospodarstwo Wodne Wody Polskie; 4d) Polski Fundusz Rozwoju i inne instytucje rozwoju, o których mowa w art. 2 ust. 1 pkt 3–6

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				ustawy z dnia 4 lipca 2019 r. o systemie instytucji rozwoju (Dz. U. z 2024 r. poz. 923 oraz z 2025 r. poz. 352); 4) Urząd Komitetu Nadzoru Finansowego;”, 13. Przepisy ust. 2 i 3 stosuje się odpowiednio do zadań realizowanych przez CSIRT NASK lub CSIRT GOV w sektorze bankowym i infrastruktury rynków finansowych, w szczególności w zakresie poważnych incydentów związanych z ICT zgłaszanych przez podmioty kluczowe lub podmioty ważne z tego sektora. 14. CSIRT NASK lub CSIRT GOV może również realizować swoje zadania w odniesieniu do podmiotów finansowych niebędących podmiotami kluczowymi lub podmiotami ważnymi, gdy nie stanowi to dla tego zespołu nieproporcjonalnego czy nadmiernego obciążenia, z uwzględnieniem priorytetowego traktowania poważnych incydentów związanych z ICT zgłaszanych przez podmioty finansowe będące podmiotami kluczowymi lub podmiotami ważnymi, oraz z zastrzeżeniem odpowiedniego stosowania ust. 2 i 3 do realizacji zadań przez CSIRT NASK lub CSIRT GOV. 15. CSIRT NASK lub CSIRT GOV współpracują i wymieniają informacje z właściwym organem w rozumieniu rozporządzenia 2022/2554, gdy jest to niezbędne dla realizacji zadań CSIRT NASK lub CSIRT GOV bądź realizacji zadań tego właściwego organu.
Art. 10	2. Państwa członkowskie zapewniają, aby każdy CSIRT dysponował odpowiednimi zasobami, tak aby mógł skutecznie realizować swoje zadania określone w art. 11 ust. 3.	TAK	Art. 1 pkt 28 (art. 26 ust. 8a) i art. 46	Częściowo wdrożone w obecnej ustawie – są zapewnione środki budżetowe na funkcjonowanie CSIRT GOV, CSIRT MON, CSIRT NASK, w tym możliwość udzielenia dotacji celowej dla CSIRT NASK. Art. 26

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				8a. Minister właściwy do spraw informatyzacji może udzielić CSIRT NASK dotacji celowej na zakup, utrzymanie i rozbudowę infrastruktury teleinformatycznej niezbędnej do wykonywania zadań CSIRT NASK. Art. 46. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 20 – gospodarka, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi: 1) w 2025 r. - 0 tyś zł; 2) w 2026 r. - 5 662 tyś zł; 3) w 2027 r. - 5 353 tyś zł; 4) w 2028 r. - 5 587 tyś zł; 5) w 2029 r. - 5 836 tyś zł; 6) w 2030 r. - 6 101 tyś zł; 7) w 2031 r. - 6 384 tyś zł; 8) w 2032 r. - 6 682 tyś zł; 9) w 2033 r. - 7 000 tyś zł; 10) w 2034 r. - 7 338 tys. zł. 2. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 21 – gospodarka morska, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi: 1) w 2025 r. - 0 tyś zł; 2) w 2026 r. - 111 tyś zł; 3) w 2027 r. - 114 tyś zł; 4) w 2028 r. - 122 tyś zł; 5) w 2029 r. - 130 tyś zł; 6) w 2030 r. - 138 tyś zł; 7) w 2031 r. - 147 tyś zł; 8) w 2032 r. - 157 tyś zł; 9) w 2033 r. - 168 tyś zł; 10) w 2034 r. - 179 tys. zł. 3. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 22 – gospodarka

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				wodna, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi: 1) w 2025 r. - 0 tyś zł; 2) w 2026 r. - 6 268 tyś zł; 3) w 2027 r. - 6 819 tyś zł; 4) w 2028 r. - 7 160 tyś zł; 5) w 2029 r. - 7 523 tyś zł; 6) w 2030 r. - 7 908 tyś zł; 7) w 2031 r. - 8 317 tyś zł; 8) w 2032 r. - 8 750 tyś zł; 9) w 2033 r. - 9 211 tyś zł; 10) w 2034 r. - 9 699 tys. zł. 4. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 27 – informatyzacja, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi: 1) w 2025 r. - 0 tyś zł; 2) w 2026 r. - 136 778 tyś zł; 3) w 2027 r. - 137 213 tyś zł; 4) w 2028 r. - 146 969 tyś zł; 5) w 2029 r. - 167 112 tyś zł; 6) w 2030 r. - 189 948 tyś zł; 7) w 2031 r. - 217 414 tyś zł; 8) w 2032 r. - 223 028 tyś zł; 9) w 2033 r. - 251 875 tyś zł; 10) w 2034 r. - 287 067 tys. zł. 5. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 28 – szkolnictwo wyższe i nauka, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi: 1) w 2025 r. - 0 tyś zł; 2) w 2026 r. - 5 754 tyś zł; 3) w 2027 r. - 6 289 tyś zł; 4) w 2028 r. - 6 594 tyś zł; 5) w 2029 r. - 6 917 tyś zł; 6) w 2030 r. - 7 259 tyś zł;

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				7) w 2031 r. - 7 622 tyś zł; 8) w 2032 r. - 8 007 tyś zł; 9) w 2033 r. - 8 415 tyś zł; 10) w 2034 r. - 8 848 tys. zł. 6. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 32 – rolnictwo, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi: 1) w 2025 r. - 0 tyś zł; 2) w 2026 r. - 7 295 tyś zł; 3) w 2027 r. - 7 878 tyś zł; 4) w 2028 r. - 8 294 tyś zł; 5) w 2029 r. - 8 736 tyś zł; 6) w 2030 r. - 9 207 tyś zł; 7) w 2031 r. - 9 706 tyś zł; 8) w 2032 r. - 10 237 tyś zł; 9) w 2033 r. - 10 801 tyś zł; 10) w 2034 r. - 11 401 tys. zł. 7. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 39 – transport, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi: 1) w 2025 r. - 0 tyś zł; 2) w 2026 r. - 6 473 tyś zł; 3) w 2027 r. - 7 030 tyś zł; 4) w 2028 r. - 7 387 tyś zł; 5) w 2029 r. - 7 766 tyś zł; 6) w 2030 r. - 8 168 tyś zł; 7) w 2031 r. - 8 595 tyś zł; 8) w 2032 r. - 9 048 tyś zł; 9) w 2033 r. - 9 529 tyś zł; 10) w 2034 r. - 10 040 tys. zł. 8. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 47 – energia, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				1) w 2025 r. - 0 tyś zł; 2) w 2026 r. - 6 268 tyś zł; 3) w 2027 r. - 6 819 tyś zł; 4) w 2028 r. - 7 160 tyś zł; 5) w 2029 r. - 7 523 tyś zł; 6) w 2030 r. - 7 908 tyś zł; 7) w 2031 r. - 8 317 tyś zł; 8) w 2032 r. - 8 750 tyś zł; 9) w 2033 r. - 9 211 tyś zł; 10) w 2034 r. - 9 699 tys. zł. 9. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 51 – klimat, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi: 1) w 2025 r. - 0 tyś zł; 2) w 2026 r. - 5 960 tyś zł; 3) w 2027 r. - 6 501 tyś zł; 4) w 2028 r. - 6 820 tyś zł; 5) w 2029 r. - 7 160 tyś zł; 6) w 2030 r. - 7 519 tyś zł; 7) w 2031 r. - 7 900 tyś zł; 8) w 2032 r. - 8 304 tyś zł; 9) w 2033 r. - 8 733 tyś zł; 10) w 2034 r. - 9 188 tys. zł. 10. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 57 – Agencja Bezpieczeństwa Wewnętrznego, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi: 1) w 2025 r. - 0 tys. zł; 2) w 2026 r. - 3 000 tys. zł; 3) w 2027 r. - 3 000 tys. zł; 4) w 2028 r. - 3 000 tys. zł; 5) w 2029 r. - 3 000 tys. zł; 6) w 2030 r. - 3 000 tys. zł; 7) w 2031 r. - 3 000 tys. zł;

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				8) w 2032 r. - 3 000 tys. zł; 9) w 2033 r. - 3 000 tys. zł; 10) w 2034 r. - 3 000 tys. zł. 11. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 76 – Urząd Komunikacji Elektronicznej, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi: 1) w 2025 r. - 0 tys. zł; 2) w 2026 r. - 8 014 tys. zł; 3) w 2027 r. - 8 619 tys. zł; 4) w 2028 r. - 9 087 tys. zł; 5) w 2029 r. - 9 586 tys. zł; 6) w 2030 r. - 10 115 tys. zł; 7) w 2031 r. - 10 678 tys. zł; 8) w 2032 r. - 11 277 tys. zł; 9) w 2033 r. - 11 915 tys. zł; 10) w 2034 r. - 12 593 tys. zł. 12. Minister właściwy do spraw gospodarki monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 1, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków minister właściwy do spraw gospodarki wdraża mechanizm korygujący polegający na ograniczeniu finansowania działalności: 1) organu właściwego do spraw cyberbezpieczeństwa dla sektorów produkcji i przetwarzania informacji; 2) CSIRT sektorowego dla sektorów produkcji i przestrzeni kosmicznej.

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				13. Minister właściwy do spraw gospodarki morskiej monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 2, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków minister właściwy do spraw gospodarki morskiej wdraża mechanizm korygujący polegający na ograniczeniu finansowania działalności: 1) organu właściwego do spraw cyberbezpieczeństwa dla podsektora transportu wodnego; 2) CSIRT sektorowego dla podsektora transportu wodnego. 14. Minister właściwy do spraw gospodarki wodnej monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 3, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków minister właściwy do spraw gospodarki wodnej wdraża mechanizm korygujący polegający na ograniczeniu finansowania działalności: 1) organu właściwego do spraw cyberbezpieczeństwa dla sektorów zaopatrzenia w wodę pitną i jej dystrybucji oraz ścieków; 2) CSIRT sektorowego dla sektorów zaopatrzenia w wodę pitną i jej dystrybucji oraz ścieków.

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				15. Minister właściwy do spraw informatyzacji monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 4, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków minister właściwy do spraw informatyzacji wdraża mechanizm korygujący polegający na ograniczeniu finansowania: 1) organu właściwego do spraw cyberbezpieczeństwa dla sektorów dostawców usług cyfrowych, infrastruktury cyfrowej oraz <u>innych usług</u>; 2) CSIRT sektorowego dla sektorów dostawców usług cyfrowych, infrastruktury <u>cyfrowej</u> oraz <u>innych usług</u>; 3) realizacji zadań ministra w obszarze <u>innych</u> kryteriów w <u>innych</u>; 4) dotacji podmiotów dla <u>CSIRT</u> NASK; 5) dotacji celowych udzielanych jednostkom podległym ministrowi właściwemu do spraw informatyzacji albo przez niego nadzorowanym w związku z powierzeniem realizacji zadań <u>innych</u>; 6) działalności edukacyjnej w zakresie <u>innych</u>; 7) realizacji zadań Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa. 16. Minister właściwy do spraw szkolnictwa wyższego i nauki monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 5, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków minister właściwy do spraw szkolnictwa wyższego i nauki wdraża mechanizm korygujący polegający na ograniczeniu finansowania działalności: 1) organu właściwego do spraw cyberbezpieczeństwa dla sektora badań naukowych; 2) CSIRT sektorowego dla sektora badań naukowych. 17. Minister właściwy do spraw rolnictwa monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 6, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków minister właściwy do spraw rolnictwa wdraża mechanizm korygujący polegający na ograniczeniu finansowania działalności: 1) organu właściwego do spraw cyberbezpieczeństwa dla sektora produkcji, przetwarzania i dystrybucji żywności; 2) CSIRT sektorowego dla sektora produkcji, przetwarzania i dystrybucji żywności. 18. Minister właściwy do spraw transportu monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 7, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków minister właściwy do spraw transportu wdraża mechanizm korygujący polegający na ograniczeniu finansowania działalności: 1) organu właściwego do spraw ☐yb☐rb☐pi☐ń☐tw☐dl☐ktor☐tr☐portu; 2) CSIRT sektorowego dla sektora transportu. 19. Minister właściwy do spraw energii monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 8, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków minister właściwy do spraw energii wdraża mechanizm korygujący polegający na ograniczeniu finansowania działalności CSIRT sektorowego: 1) organu właściwego do spraw ☐yb☐rb☐pi☐ń☐tw☐dl☐ktor☐rgii; 2) CSIRT sektorowego dla sektora energii. 20. Minister właściwy do spraw klimatu monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 9, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków minister właściwy do spraw klimatu wdraża mechanizm

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				korygujący polegający na ograniczeniu finansowania 1) organu właściwego do spraw cyberbezpieczeństwa dla sektora gospodarowania odpadami; 2) CSIRT sektorowego dla sektora gospodarowania odpadami. 21. Szef Agencji Bezpieczeństwa Wewnętrznego monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 10, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków Szef Agencji Bezpieczeństwa Wewnętrznego wdraża mechanizm korygujący polegający na ograniczeniu finansowania czynności nadzorczych wobec podmiotów publicznych w zakresie cyberbezpieczeństwa. Wdrożenie tego mechanizmu korygującego następuje w uzgodnieniu z ministrem – członkiem Rady Ministrów właściwym do spraw koordynowania działalności służb specjalnych albo z Prezesem Rady Ministrów, jeżeli minister – członek Rady Ministrów właściwy do spraw koordynowania działalności służb specjalnych nie został powołany. 22. Prezes Urzędu Komunikacji Elektronicznej monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 11, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków Prezes Urzędu Komunikacji Elektronicznej wdraża mechanizm korygujący polegający na ograniczeniu finansowania działalności 1) organu właściwego do spraw cyberbezpieczeństwa dla sektora poczty i podsektora komunikacji elektronicznej; 2) CSIRT sektorowego dla sektora poczty i podsektora komunikacji elektronicznej.
Art. 10	3. Państwa członkowskie zapewniają, aby każdy CSIRT miał do dyspozycji odpowiednią, bezpieczną i odporną infrastrukturę komunikacyjno-informacyjną do wymiany informacji z podmiotami kluczowymi i ważnymi oraz innymi odpowiednimi zainteresowanymi stronami. W tym celu państwa członkowskie zapewniają, aby każdy CSIRT uczestniczył we wdrażaniu bezpiecznych narzędzi wymiany informacji.	TAK	Art. 1 pkt 28 (art. 26 ust. 3 pkt 20)	Art. 26.3. 20) udział we wdrażaniu bezpiecznych narzędzi wymiany informacji z podmiotami kluczowymi i podmiotami ważnymi oraz innymi podmiotami;
Art. 10	4. CSIRT współpracują z sektorowymi i międzysektorowymi społecznościami podmiotów kluczowych i ważnych oraz, w odpowiednich przypadkach, wymieniają z nimi stosowne informacje zgodnie z art. 29.	TAK	Art. 1 pkt 28 (art. 26 ust. 3 pkt 18)	Art. 26.3. 18) współpraca z sektorowymi i międzysektorowymi społecznościami podmiotów kluczowych lub podmiotów ważnych oraz wymiana informacji dotyczących cyberbezpieczeństwa jeśli wymiana informacji zapewnia zwiększenie poziomu cyberbezpieczeństwa lub służy przeciwdziałaniu incydentom;
Art. 10	5. CSIRT biorą udział w ocenie wzajemnej organizowanej zgodnie z art. 19.	TAK	Art. 1 pkt 28 (art. 26 ust. 12)	Art. 26.12. CSIRT MON, CSIRT NASK i CSIRT GOV mogą uczestniczyć w procesie wzajemnej oceny, o którym mowa w art. 19 dyrektywy 2022/2555.
Art. 10	6. Państwa członkowskie zapewniają skuteczną, efektywną i bezpieczną współpracę swoich CSIRT w sieci CSIRT.	TAK	Art. 1 pkt 28 (art. 26 ust. 3 pkt 16)	Art. 26.3. 16) udział w Sieci CSIRT składającej się z przedstawicieli CSIRT państw członkowskich Unii Europejskiej, CSIRT właściwego dla instytucji Unii Europejskiej oraz Komisji Europejskiej;

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

Art. 10	7. CSIRT mogą nawiązać stosunki współpracy z krajowymi zespołami reagowania na incydenty bezpieczeństwa komputerowego z państw trzecich. W ramach takich stosunków współpracy państwa członkowskie wspierają skuteczną, efektywną i bezpieczną wymianę informacji z tymi krajowymi zespołami reagowania na incydenty bezpieczeństwa komputerowego z państw trzecich, z wykorzystaniem odpowiednich protokołów wymiany informacji, w tym kodu poufności TLP. CSIRT mogą wymieniać ważne informacje z krajowymi zespołami reagowania na incydenty bezpieczeństwa komputerowego z państw trzecich, w tym dane osobowe zgodnie z unijnymi przepisami o ochronie danych.	TAK	Art. 1 pkt 28 (art. 26 ust. 3, ust. 3a)	Art. 26.3. 19) współpraca z krajowymi zespołami reagowania na incydenty bezpieczeństwa komputerowego państw trzecich; 3a. Przy realizacji zadania, o którym mowa w ust. 3 pkt 19, CSIRT MON, CSIRT NASK i CSIRT GOV mogą wymieniać informacje, w tym dane osobowe w celu informowania o potencjalnych cyberzagrożeniach oraz zastosowanych sposobach ich zwalczania w celu przeciwdziałania cyberzagrożeniom o charakterze transgranicznym. Informacje, w tym dane osobowe, o których mowa w zdaniu pierwszym, przekazuje się w postaci elektronicznej.
Art. 10	8. CSIRT mogą współpracować z krajowymi zespołami reagowania na incydenty bezpieczeństwa komputerowego z państw trzecich lub równoważnymi organami z państw trzecich, w szczególności w celu zapewnienia im pomocy w zakresie cyberbezpieczeństwa.	TAK	Art. 1 pkt 28 (art. 26 ust. 3 pkt 19)	Art. 26.3. 19) współpraca z krajowymi zespołami reagowania na incydenty bezpieczeństwa komputerowego państw trzecich;
Art. 10	9. Każde państwo członkowskie bez zbędnej zwłoki powiadamia Komisję o danych identyfikacyjnych CSIRT, o którym mowa w ust. 1 niniejszego artykułu, i CSIRT wyznaczonego na koordynatora zgodnie z art. 12 ust. 1, o ich odpowiednich zadaniach w odniesieniu do podmiotów kluczowych i ważnych oraz o późniejszych zmianach w tym zakresie.	TAK	Art. 1 pkt 50 (art. 45 ust. 1 pkt 14)	Art. 45.1. 14) przekazywanie Komisji Europejskiej aktualnych informacji o CSIRT MON, CSIRT NASK i CSIRT GOV oraz CSIRT sektorowych, w których dająymi kontaktowymi organami;
Art. 10	10. Państwa członkowskie mogą zwrócić się do ENISA o pomoc przy rozwijaniu CSIRT.	TAK	Art. 1 pkt 57 (art. 49 ust. 8)	Art. 49. 8. Organy właściwe do spraw cyberbezpieczeństwa, Szef Agencji Bezpieczeństwa Wewnętrznego, Minister Obrony Narodowej, minister właściwy do spraw informatyzacji mogą, za pomocą Pojedynczego Punktu Kontaktowego, zwrócić się do ENISA o udzielenie wsparcia przy rozwijaniu CSIRT sektorowych oraz CSIRT MON, CSIRT NASK lub CSIRT GOV.
Art. 11	Artykuł 11 Wymogi dotyczące CSIRT, ich zdolności techniczne i zadania	NIE		

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

	1. CSIRT spełniają następujące wymogi: a) CSIRT zapewniają wysoką dostępność swoich kanałów komunikacji poprzez takie ich ukształtowanie, aby wyłączenie jednego elementu systemu nie uniemożliwiało przesłania informacji do adresata, oraz dysponują różnymi kanałami, za pomocą których zawsze można się z nimi skontaktować i za pomocą których one mogą być koordynowane z innymi podmiotami; jedno z kanałów komunikacji i informują o nich podmioty będące w ich właściwości oraz współpracujące z nimi; b) pomieszczenia CSIRT oraz wspierające systemy informatyczne muszą być odpowiednio zabezpieczone i chronione; c) CSIRT dysponują odpowiednim systemem zarządzania w zakresie kierowanych do nich zgłoszeń oraz ich przekierowywania, w szczególności w celu ułatwienia skutecznego i efektywnego działania przy ich realizacji; d) CSIRT zapewniają poufność i wiarygodność swoich działań; e) CSIRT dysponują odpowiednio licznym personelem, aby zapewnić nieprzerwaną dostępność ich usług, oraz zapewniają odpowiedni poziom jakości usług; f) CSIRT dysponują systemami redundantnymi i rezerwowym miejscem pracy w celu zapewnienia ciągłości ich usług. CSIRT mogą uczestniczyć w międzynarodowych sieciach współpracy.			
Art. 11	2. Państwa członkowskie zapewniają, aby ich CSIRT wspólnie miały zdolności techniczne niezbędne do realizacji zadań, o których mowa w ust. 3. Państwa członkowskie zapewniają ich CSIRT zasoby gwarantujące odpowiedni poziom zatrudnienia, aby umożliwić CSIRT rozwój ich zdolności technicznych.	NIE		
Art. 11	3. CSIRT mają następujące zadania: a) monitorowanie i analizowanie cyberzagrożeń, podatności i incydentów na poziomie krajowym oraz, na wniosek, udzielanie pomocy danym podmiotom kluczowym i ważnym w zakresie monitorowania ich sieci i systemów informatycznych w czasie rzeczywistym lub zbliżonym do rzeczywistego; b) wczesne ostrzeganie i alarmowanie danych podmiotów kluczowych i ważnych oraz właściwych organów i innych	TAK	Art. 1 pkt 28 (art. 26) art. 1 pkt 33 (art. 32)	Częściowo wdrożone już w obecnym art. 26 (25) w art. 26: a) w ust. 1: – po wyrazie „informatyzacji” dodaje się wyrazy „, CSIRT sektorowymi”, – wyrazy „zagrożeniom cyberbezpieczeństwa” zastępuje się wyrazem „cyberzagrożeniom”, b) po ust. 1 dodaje się ust. 1a w brzmieniu:

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

	zainteresowanych stron o cyberzagrożeniach, podatnościach i incydentach, a także kierowanie do nich ogłoszeń oraz przekazywanie im informacji dotyczących cyberzagrożeń, podatności i incydentów, w miarę możliwości w czasie zbliżonym do rzeczywistego; c) reagowanie na incydenty i w stosownych przypadkach udzielanie pomocy innym podmiotom krajowym i w zagranicą; d) gromadzenie i analizowanie danych kryminalistycznych i zapewnianie dynamicznej analizy ryzyka i incydentów oraz świadomości ryzyka w krajowym i międzynarodowym; e) przeprowadzanie, na wniosek podmiotu kluczowego lub ważnego, aktywnego skanowania sieci i systemów informatycznych danego podmiotu w celu wykrycia podatności o potencjalnym negatywnym wpływie; f) uczestnictwo w sieci CSIRT oraz udzielanie wzajemnej pomocy innym członkom sieci CSIRT na ich wniosek, w miarę własnych możliwości i kompetencji; g) w stosownych przypadkach działanie w charakterze koordynatora w celu skoordynowanego ujawniania podatności na podstawie art. 12 ust. 1; h) udział we wdrażaniu bezpiecznych narzędzi wymiany informacji zgodnie z art. 10 ust. 3. CSIRT mogą prowadzić aktywne, nieinwazyjne skanowanie publicznie dostępnych sieci i systemów informatycznych podmiotów kluczowych i ważnych. Takie skanowanie przeprowadza się w celu wykrycia sieci i systemów informatycznych podatnych na zagrożenia lub skonfigurowanych bez właściwego zabezpieczenia i poinformowania o tym podmiotów, których to dotyczy. Takie skanowanie nie może mieć negatywnego wpływu na funkcjonowanie usług świadczonych przez te podmioty. Wykonując zadania, o których mowa w akapicie pierwszym, CSIRT mogą priorytetowo traktować niektóre zadania na podstawie podejścia opartego na analizie ryzyka.			„1a. W czasie stanu wojennego lub w czasie wojny CSIRT MON, w imieniu Ministra Obrony Narodowej, koordynuje działania CSIRT NASK i CSIRT GOV.”, c) ust. 2 otrzymuje brzmienie: „2. CSIRT MON, CSIRT NASK i CSIRT GOV na wniosek podmiotów krajowego systemu cyberbezpieczeństwa mogą zapewnić wsparcie tym podmiotom w obsłudze incydentów, w przypadku gdy: 1) incydent może wpłynąć na inne podmioty krajowego systemu cyberbezpieczeństwa; 2) podmiot obsługujący incydent nie dysponuje środkami pozwalającymi mu na jego skuteczną obsługę, a incydent powoduje przerwanie ciągłości działania podmiotu.”, d) po ust. 2 dodaje się ust. 2a–2c w brzmieniu: „2a. Pełnomocnik może zlecić zapewnienie wsparcia w obsłudze incydentów, o którym mowa w ust. 2: 1) CSIRT MON, za zgodą Ministra Obrony Narodowej lub 2) CSIRT NASK, lub 3) CSIRT GOV, za zgodą Szefa Agencji Bezpieczeństwa Wewnętrznego. 2b. Zgoda może być wyrażona w formie ustnej lub dokumentowej, w szczególności z wykorzystaniem środków porozumiewania się na odległość. Zgoda wyrażona w formie ustnej wymaga udokumentowania w ciągu 14 dni od dnia jej wydania 2c. O zapewnieniu wsparcia w obsłudze incydentów, o którym mowa w ust. 2 lub 2a, jest informowany właściwy CSIRT sektorowy.”, e) w ust. 3:

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				– w pkt 1 wyrazy „zagrożeń cyberbezpieczeństwa” zastępuje się wyrazem „cyberzagrożeń”, – pkt 2–4 otrzymują brzmienie: „2) szacowanie ryzyka związanego z ujawnionym cyberzagrożeniem oraz zaistniałymi incydentami, w tym – p[ro]wad[zi]e[n]i[e] dy[agn]o[zy]ki i li[st]y ryzyk; 3) przekazywanie informacji dotyczących cyberzagrożeń, podatności, incydentów i ryzyk, wczesne ostrzeganie i alarmowanie podmiotów krajow[ego] i mi[ędzypa]ni[ego]; 4) wydawanie komunikatów o zidentyfikowanych zagrożeniach;”, – pkt 6 i 7 otrzymują brzmienie: „6) klasyfikowanie incydentów, w tym incydentów poważnych, jako incydenty krytyczne oraz koordynowanie obsługi incydentów krytycznych; 7) mi[ędzypa]ni[ego] klasyfikacja i wyd[awanie] komunikatów;”, – w pkt 10: – – wyrazy „sektorowymi zespołami cyberbezpieczeństwa” zastępuje się wyrazami „CSIRT sektorowymi”, – – wyrazy „zagrożeniom cyberbezpieczeństwa” zastępuje się wyrazem „cyberzagrożeniom”, – pkt 11 i 12 otrzymują brzmienie: „11) przekazywanie do innych państw, w tym państw członkowskich Unii Europejskiej, i przyjmowanie z tych państw informacji o incydentach poważnych dotyczących dwóch lub większej liczby państw, a także przekazywanie do Pojedynczego Punktu Kontaktowego zgłoszenia incydentu poważnego dotyczącego dwóch lub większej liczby państw członkowskich Unii Europejskiej;

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				12) przekazywanie, w terminie 14 dni od zakończenia danego kwartału, do Pojedynczego Punktu Kontaktowego zestawienia zgłoszonych w poprzednich 3 miesiącach: a) poważnych incydentów, b) incydentów, c) cyberzagrożeń, d) potencjalnych zdarzeń dla „cyberbezpieczeństwa”, – w pkt 14 w lit. b i c wyrazy „zagrożeń cyberbezpieczeństwa” zastępuje się wyrazem „cyberzagrożeń”, – uchyla się pkt 15, – pkt 16 otrzymuje brzmienie: „16) udział w Sieci CSIRT składającej się z przedstawicieli CSIRT państw członkowskich Unii Europejskiej, CSIRT właściwego dla instytucji Unii Europejskiej oraz Komisji Europejskiej”, k) dodaje się ust. 12–16 w brzmieniu: „12. CSIRT MON, CSIRT NASK i CSIRT GOV mogą uczestniczyć w procesie wzajemnej oceny, o którym mowa w art. 19 dyrektywy 2022/2555. 13. Przepisy ust. 2 i 3 stosuje się odpowiednio do zadań realizowanych przez CSIRT NASK lub CSIRT GOV w sektorze bankowym i infrastruktury rynków finansowych, w szczególności w zakresie poważnych incydentów związanych z ICT zgłaszanych przez podmioty kluczowe lub podmioty ważne z tego sektora. 14. CSIRT NASK lub CSIRT GOV może również realizować swoje zadania w odniesieniu do podmiotów finansowych niebędących podmiotami kluczowymi lub podmiotami ważnymi, gdy nie stanowi to dla tego zespołu nieproporcjonalnego czy nadmiernego

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				obciążenia, z uwzględnieniem priorytetowego traktowania poważnych incydentów związanych z ICT zgłaszanych przez podmioty finansowe będące podmiotami kluczowymi lub podmiotami ważnymi, oraz z zastrzeżeniem odpowiedniego stosowania ust. 2 i 3 do realizacji zadań przez CSIRT NASK lub CSIRT GOV. 15. CSIRT NASK lub CSIRT GOV współpracują i wymieniają informacje z właściwym organem w rozumieniu rozporządzenia 2022/2554, gdy jest to niezbędne dla realizacji zadań CSIRT NASK lub CSIRT GOV bądź realizacji zadań tego właściwego organu. 16. CSIRT MON, CSIRT NASK i CSIRT GOV informują organ właściwy do spraw podmiotów krytycznych o poważnych incydentach, cyberzagrożeniach i potencjalnych zdarzeniach dla cyberbezpieczeństwa zgłoszonych przez podmiot krytyczny.”; Art. 32. 1. CSIRT MON, CSIRT NASK i CSIRT GOV mogą wykonywać niezbędne działania techniczne związane z analizą zagrożeń, koordynacją obsługi incydentu poważnego i incydentu krytycznego. 2. CSIRT MON, CSIRT NASK lub CSIRT GOV może wystąpić do organu właściwego do spraw cyberbezpieczeństwa z wnioskiem o wezwanie podmiotu kluczowego lub podmiotu ważnego, aby w wyznaczonym terminie usunął podatności, które doprowadziły lub mogłyby doprowadzić do incydentu poważnego lub krytycznego. 3. Podmiot kluczowy lub podmiot ważny na wniosek CSIRT MON, CSIRT NASK lub CSIRT GOV udostępnia informacje techniczne związane z incydentem, które będą niezbędne do

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				przeprowadzenia analizy lub koordynacji obsługi incydentu. 4. CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT sektorowe na podstawie informacji, o których mowa w art. 13 ust. 1 pkt 3 i 5, uzyskanych od podmiotu kluczowego lub podmiotu ważnego, mogą przekazywać im informacje o podatnościach i sposobie usunięcia podatności w wykorzystywanych technologiach.”.
Art. 11	4. CSIRT nawiązują współpracę z odpowiednimi zainteresowanymi stronami w sektorze prywatnym w celu realizacji celów niniejszej dyrektywy.	NIE		Art. 26 ust. 3 pkt 14 obecnie obowiązującej ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa spełni tą rolę.
Art. 11	5. Aby ułatwić współpracę, o której mowa w ust. 4, CSIRT promują przyjmowanie i stosowanie wspólnych lub znormalizowanych praktyk, systemów klasyfikacji i systematyki związanych z: a) procedurami obsługi incydentu; b) transferem informacji krytycznym; oraz c) skoordynowanym ujawnianiem podatności na mocy art. 12 ust. 1.	NIE		Art. 26 ust. 3 pkt 14 obecnie obowiązującej ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa spełni tą rolę.
Art. 12	Artykuł 12 Skoordynowane ujawnianie podatności i europejska baza danych dotyczących podatności 1. Każde państwo członkowskie wyznacza jeden spośród swoich CSIRT na koordynatora na potrzeby skoordynowanego ujawniania podatności. CSIRT wyznaczony na koordynatora działa w charakterze zaufanego pośrednika, w razie konieczności ułatwiając interakcję między osobą fizyczną lub prawną zgłaszającą podatność a producentem lub dostawcą potencjalnie podatnych produktów ITC lub usług ICT, na wniosek którejkolwiek ze stron. Zadania CSIRT wyznaczonego na koordynatora obejmują: a) identyfikację danych podmiotów i kontaktów ich pracowników; b) udzielanie pomocy osobom fizycznym lub prawnym zgłaszającym podatność; oraz c) negocjowanie harmonogramu ujawniania oraz zarządzanie podatnościami, których skutki mają wpływ na wiele podmiotów.	TAK	Art. 1 pkt 29 (art. 26a)	„Art. 26a. 1. CSIRT NASK pełni funkcję koordynatora na potrzeby skoordynowanego ujawniania podatności. 2. Osoba fizyczna, osoba prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej może zgłosić wykrytą podatność do CSIRT NASK. 3. Zgłoszenie podatności jest przekazywane w postaci elektronicznej, a w przypadku braku możliwości przekazania jej w postaci elektronicznej – przy użyciu innych dostępnych środków komunikacji. 4. CSIRT NASK zapewnia formularz do dokonywania zgłoszeń podatności, zapewniający możliwość zachowania anonimowości przez osobę fizyczną lub prawną zgłaszającą podatność. CSIRT NASK może przetwarzać przekazane dane

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

	Państwa członkowskie zapewniają, aby osoby fizyczne lub prawne mogły zgłaszać anonimowo, jeśli o to wystąpią, podatność wyznaczonemu na koordynatora CSIRT. CSIRT wyznaczony na koordynatora zapewnia przeprowadzenie z należytą starannością działań podjętych w związku ze zgłoszoną podatnością oraz zapewnia anonimowość osoby fizycznej lub prawnej zgłaszającej podatność. Jeżeli zgłoszona podatność może mieć znaczący wpływ na podmioty w więcej niż jednym państwie członkowskim, CSIRT wyznaczony na koordynatora każdego państwa członkowskiego, którego podatność dotyczy, współpracuje, w stosownych przypadkach z innymi CSIRT wyznaczonymi na koordynatorów w ramach sieci CSIRT.			osobowe w celu realizacji zadań, o których mowa w ust. 5. 5. W ramach zadania, o którym mowa w ust. 1, CSIRT NASK: 1) przyjmuje informacje o wykrytych podatnościach; 2) identyfikuje dostawców produktów ICT lub usług ICT, na które podatność może mieć wpływ i informuje o wykrytych podatnościach; 3) w razie konieczności, koordynuje komunikację między osobą fizyczną lub prawną zgłaszającą podatność a producentem lub dostawcą potencjalnie podatnych produktów ICT lub usług ICT, w zakresie weryfikacji zgłoszenia i terminu ujawnienia podatności; 4) udziela pomocy podmiotom zgłaszającym podatność; 5) identyfikuje i klasyfikuje podatności; 6) prowadzi działania służące likwidacji podatności oraz likwidacji ich skutków; 7) koordynuje i promuje ujawnienie podatności; 8) może publikować informacje o podatnościach; 9) zarządza ujawnionymi informacjami o podatnościach. 6. CSIRT NASK współpracuje z zespołami CSIRT innych państw członkowskich Unii Europejskiej przy podatnościach, które mają wpływ na podmioty, w pozostałych państwach członkowskich Unii Europejskiej.
Art. 12	2. ENISA opracowuje i prowadzi, po konsultacji z Grupą Współpracy, europejską bazę danych dotyczącą podatności. W tym celu ENISA ustanawia i utrzymuje odpowiednie systemy informatyczne, polityki i procedury oraz przyjmuje środki techniczne i organizacyjne niezbędne do zapewnienia bezpieczeństwa i integralności europejskiej bazy danych dotyczącej podatności, w szczególności aby umożliwić podmiotom, niezależnie	NIE		

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

	od tego czy są objęte zakresem stosowania niniejszej dyrektywy oraz ich dostawcom sieci i systemów informatycznych ujawnianie i rejestrowanie – na zasadzie dobrowolności – znanych publicznie podatności występujących w produktach ICT lub usługach ICT. Wszystkie zainteresowane strony otrzymują dostęp do informacji na temat podatności zawartych w europejskiej bazie danych dotyczącej podatności. Baza danych zawiera: a) informacje o podatności; b) produkty ICT lub usługi ICT, których dotyczy podatność, oraz dotkliwość podatności z punktu widzenia okoliczności, w jakich można było wykorzystać; c) dostępność powiązanych aktualizacji, a w razie braku dostępnych aktualizacji – wytyczne podane przez właściwe organy lub CSIRT, skierowane do użytkowników produktów ICT i usług ICT, których dotyczy podatność, na temat sposobów ograniczania ryzyka wynikającego z ujawnionych podatności.			
Art. 13	Artykuł 13 Współpraca na poziomie krajowym 1. Jeżeli właściwe organy, pojedynczy punkt kontaktowy i CSIRT z tego samego państwa członkowskiego są odrębne względem siebie, współpracują one ze sobą przy wypełnianiu obowiązków określonych w niniejszej dyrektywie.	TAK	Art. 1 pkt 28 (art. 26 ust. 3) i art. 1 pkt 35 (art. 34)	Art. 26.3. „11) przekazywanie do innych państw, w tym państw członkowskich Unii Europejskiej, i przyjmowanie z tych państw informacji o incydentach poważnych dotyczących dwóch lub większej liczby państw, a także przekazywanie do Pojedynczego Punktu Kontaktowego zgłoszenia incydentu poważnego dotyczącego dwóch lub większej liczby państw członkowskich Unii Europejskiej; 12) przekazywanie, w terminie 14 dni od zakończenia danego kwartału, do Pojedynczego Punktu Kontaktowego zestawienia zgłoszonych w poprzednich 3 miesiącach: a) poważnych incydentów, b) incydentów, c) cyberzagrożeń, d) potencjalnych zdarzeń dla cyberbezpieczeństwa”,

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				art. 34: 1. CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT sektorowe oraz dostawcy usług zarządzanych w zakresie cyberbezpieczeństwa współpracują z organami ścigania i wymiaru sprawiedliwości oraz służbami specjalnymi przy realizacji ich ustawowych zadań.”, b) w ust. 2 wyrazy „i CSIRT GOV” zastępuje się wyrazami „CSIRT GOV i CSIRT sektorowe”. 3. CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT sektorowe oraz dostawcy usług zarządzanych z zakresu cyberbezpieczeństwa współpracują z Prezesem Urzędu Lotnictwa Cywilnego, Prezesem Urzędu Komunikacji Elektronicznej oraz Komisją Nadzoru Finansowego. 4. CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT sektorowe współpracują z Narodowym Bankiem Polskim w zakresie wymiany informacji o incydentach, podatnościach i cyberzagrożeniach, które mają wpływ na systemy płatności.
Art. 13	2. Państwa członkowskie zapewniają, aby ich CSIRT lub, w stosownych przypadkach, ich właściwe organy odbierały zgłoszenia o poważnych incydentach zgodnie z art. 23 oraz incydentach, cyberzagrożeniach i potencjalnych zdarzeniach dla cyberbezpieczeństwa zgodnie z art. 30.	TAK		Wdrożone przez przepisy o podłączeniu zespołów CSIRT do systemu S46.
Art. 13	3. Państwa członkowskie zapewniają, aby ich CSIRT lub, w stosownych przypadkach, właściwe organy informowały ich pojedyncze punkty kontaktowe o zgłoszeniach incydentów, cyberzagrożeń i potencjalnych zdarzeń dla cyberbezpieczeństwa dokonywanych na podstawie niniejszej dyrektywy.	TAK	Art. 1 pkt 28 (art. 26 ust. 3)	Art. 26.3: „11) przekazywanie do innych państw, w tym państw członkowskich Unii Europejskiej, i przyjmowanie z tych państw informacji o incydentach poważnych dotyczących dwóch lub większej liczby państw, a także przekazywanie do Pojedynczego Punktu Kontaktowego zgłoszenia

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				incydentu poważnego dotyczącego dwóch lub większej liczby państw członkowskich Unii Europejskiej; 12) przekazywanie, w terminie 14 dni od zakończenia danego kwartału, do Pojedynczego Punktu Kontaktowego zestawienia zgłoszonych w poprzednich 3 miesiącach: a) poważnych incydentów, b) incydentów, c) cyberzagrożeń, d) potencjalnych zdarzeń dla cyberbezpieczeństwa”;
Art. 13	4. Aby zapewnić skuteczne wykonywanie zadań i obowiązków właściwych organów, pojedynczych punktów kontaktowych i CSIRT, państwa członkowskie zapewniają w miarę możliwości odpowiednią współpracę między tymi podmiotami a organami ścigania, organami ochrony danych, organami krajowymi na mocy rozporządzeń (WE) nr 300/2008 i (UE) 2018/1139, organami nadzoru na mocy rozporządzenia (UE) nr 910/2014, właściwymi organami na mocy rozporządzenia (UE) 2022/2554, krajowymi organami regulacyjnymi na mocy dyrektywy (UE) 2018/1972, właściwymi organami na mocy dyrektywy (UE) 2022/2557, a także właściwymi organami na mocy innych sektorowych aktów prawnych Unii w tym państwie członkowskim.	TAK	Art. 1 pkt 4 (art. 2 pkt 11b i 11i) i 28 (art. 26 ust. 12-16)	Art. 2: 11b) podmiot finansowy – podmiot, o którym mowa w art. 2 ust. 1 lit. a-t rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniającego rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (Dz. Urz. UE L 333 z 27.12.2022, str. 1), zwanego dalej „rozporządzeniem 2022/2554”; 11i) poważny incydent związany z ICT – poważny incydent związany z technologiami informacyjno-komunikacyjnymi w rozumieniu art. 3 pkt 10 rozporządzenia 2022/2554; art. 26: 12. CSIRT MON, CSIRT NASK i CSIRT GOV mogą uczestniczyć w procesie wzajemnej oceny, o którym mowa w art. 40a. 13. Przepisy ust. 2 i 3 stosuje się odpowiednio do zadań realizowanych przez CSIRT NASK lub CSIRT GOV w sektorze bankowym i infrastruktury rynków finansowych, w

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				szczegółności w zakresie poważnych incydentów związanych z ICT zgłaszanych przez podmioty kluczowe lub podmioty ważne z tego sektora. 14. CSIRT NASK lub CSIRT GOV może również realizować swoje zadania w odniesieniu do podmiotów finansowych niebędących podmiotami kluczowymi lub podmiotami ważnymi, gdy nie stanowi to dla tego zespołu nieproporcjonalnego czy nadmiernego obciążenia, z uwzględnieniem priorytetowego traktowania poważnych incydentów związanych z ICT zgłaszanych przez podmioty finansowe będące podmiotami kluczowymi lub podmiotami ważnymi, oraz z uwzględnieniem odpowiedniego stosowania ust. 2 i 3 do realizacji zadań przez CSIRT NASK lub CSIRT GOV. 15. CSIRT NASK lub CSIRT GOV współpracują i wymieniają informacje z właściwym organem w rozumieniu rozporządzenia 2022/2554, gdy jest to niezbędne dla realizacji zadań CSIRT NASK lub CSIRT GOV bądź realizacji zadań tego właściwego organu. 16. CSIRT MON, CSIRT NASK i CSIRT GOV informują organ właściwy do spraw podmiotów krytycznych o poważnych incydentach, cyberzagrożeniach i potencjalnych zdarzeniach dla cyberbezpieczeństwa zgłoszonych przez podmiot krytyczny.
Art. 13	5. Państwa członkowskie zapewniają, aby ich właściwe organy na mocy niniejszej dyrektywy oraz ich właściwe organy na mocy dyrektywy (UE) 2022/2557 współpracowały i regularnie wymieniały się informacjami dotyczącymi identyfikacji podmiotów krytycznych, ryzyka, cyberzagrożeń i incydentów, a także ryzyka, zagrożeń i incydentów poza cyberprzestrzenią mających wpływ na podmioty kluczowe wskazane jako podmioty krytyczne na podstawie dyrektywy (UE) 2022/2557, oraz na temat środków	TAK	Art. 1 pkt 46 (art. 42 ust. 1)	Art. 42.1: 13) współpracuje oraz wymienia informacje i dokumenty z organem właściwym do spraw podmiotów krytycznych w zakresie nadzoru nad podmiotem kluczowym będącym podmiotem krytycznym.

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

	podjętych w odpowiedzi na takie ryzyko, zagrożenia i incydenty. Państwa członkowskie zapewniają również, aby ich właściwe organy na mocy niniejszej dyrektywy oraz ich właściwe organy na mocy rozporządzenia (UE) nr 910/2014, rozporządzenia (UE) 2022/2554 i dyrektywy (UE) 2018/1972 regularnie wymieniały się odpowiednimi informacjami, w tym dotyczącymi poważnych incydentów i cyberzagrożeń.			Uwaga – w większości przypadków będą to te same organy zgodnie z projektem ustawy o zmianie ustawy o zarządzaniu kryzysowym oraz niektórych innych ustaw (UC47).
Art. 13	6. Państwa członkowskie upraszczają za pomocą środków technicznych sprawozdawczość dotyczącą zgłoszeń, o których mowa w art. 23 i 30.	TAK	Art. 1 pkt 19 (art. 11 ust. 2) i pkt 33 (art. 31)	Art. 11. 2. Wczesne ostrzeżenie, o którym mowa w ust. 1 pkt 4, zgłoszenie, o którym mowa w ust. 1 pkt 4a, sprawozdanie okresowe, o którym mowa w ust. 1 pkt 4b, sprawozdanie końcowe, o którym mowa w ust. 1 pkt 4c, oraz sprawozdanie z postępu obsługi incydentu poważnego, o którym mowa w art. 12b ust. 1, są przekazywane za pomocą systemu teleinformatycznego, o którym mowa w art. 46 ust. 1. Art. 31. 1. CSIRT MON, CSIRT NASK, CSIRT GOV oraz CSIRT sektorowe określą sposób przekazywania informacji i zgłoszeń, o których mowa w art. 11 i w art. 13, w przypadku braku możliwości przekazania ich za pomocą systemu teleinformatycznego, o którym mowa w art. 46 ust. 1. Art. 31. 2. CSIRT NASK określi sposób dokonywania zgłoszeń, o których mowa w art. 30 ust. 1. 3. Komunikat zawierający informacje o sposobie dokonywania zgłoszeń, o których mowa odpowiednio w art. 11, art. 13 i art. 30 ust. 1, CSIRT MON, CSIRT NASK, CSIRT GOV oraz CSIRT sektorowe publikuje odpowiednio na stronie podmiotowej Biuletynu Informacji Publicznej Ministra Obrony Narodowej, Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego, Agencji

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				Bezpieczeństwa Wewnętrznego lub organu właściwego do spraw cyberbezpieczeństwa.
Art. 14	Artykuł 14 Grupa Współpracy 1. Aby wspierać i ułatwiać strategiczną współpracę i wymianę informacji między państwami członkowskimi, a także aby zwiększać zaufanie między nimi, ustanawia się Grupę Współpracy.	TAK	Art. 1 pkt 50 (art. 45 ust. 1 pkt 1a, 1b, 3 i 6-12 oraz ust. 2)	Art. 45.1: 1a) monitorowanie wdrażania Krajowego planu reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę, zwanego dalej „Krajowym planem”, oraz realizację działań 1b) prowadzenie wykazu podmiotów kluczowych i podmiotów w 3) opracowywanie rocznych sprawozdań dotyczących incydentów poważnych zgłaszanych przez podmioty kluczowe lub podmioty ważne mających wpływ na ciągłość świadczenia usług przez te podmioty w Rzeczypospolitej Polskiej oraz ciągłość świadczenia usług w państwach 6) udostępnianie informacji i dobrych praktyk uzyskanych z Grupy Współpracy podmiotom krajowego systemu cyberbezpieczeństwa w celu usprawnienia działań krajowego systemu 7) rekomendowanie i wspieranie przy wykorzystywaniu europejskich lub międzynarodowych standardów, a także specyfikacji technicznych mających znaczenie dla 8) zachęcanie do korzystania z produktów ICT, usług ICT i procesów ICT certyfikowanych w ramach europejskich lub krajowych programów 9) ustanowienie odpowiednich struktur komunikacyjnych na potrzeby wczesnego wykrywania kryzysów w cyberbezpieczeństwie, reagowania kryzysowego w cyberbezpieczeństwie i zarządzania kryzysowego

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				w cyberbezpieczeństwie, a także koordynacji współpracy w celu ochrony bezpieczeństwa technologii informacyjnej aktywów o krytycznym znaczeniu we współpracy z sektorem prywatnym; 10) współpracę w obszarze cyberbezpieczeństwa z partnerami; 11) koordynację działań organów państwa w przypadku wystąpienia sytuacji kryzysowej w cyberbezpieczeństwie nie dotyczącej wymiaru militarnego; 12) uczestniczenie w pracach Europejskiej sieci organizacji łącznikowych do spraw kryzysów cyberbezpieczeństwa. 2. Przez Grupę Współpracy rozumie się grupę, o której mowa w art. 14 dyrektywy 2022/2555.
Art. 14	2. Grupa Współpracy wykonuje swoje zadania na podstawie dwuletnich programów prac, o których mowa w ust. 7.	NIE		
	3. Grupa Współpracy składa się z przedstawicieli państw członkowskich, Komisji i ENISA. W działaniach Grupy Współpracy uczestniczy w charakterze obserwatora Europejska Służba Działań Zewnętrznych. Europejskie Urzędy Nadzoru i organy właściwe na mocy rozporządzenia (UE) 2022/2554 mogą uczestniczyć w działaniach Grupy Współpracy zgodnie z art. 47 ust. 1 tego rozporządzenia. W stosownych przypadkach Grupa Współpracy może zapraszać Parlament Europejski i przedstawicieli odpowiednich zainteresowanych stron do udziału w swoich pracach. Komisja zapewnia obsługę sekretariatu.	NIE		
Art. 14	4. Grupa Współpracy ma następujące zadania: a) udzielanie wskazówek właściwym organom w związku z transpozycją i wdrażaniem dyrektywy; b) udzielanie wskazówek właściwym organom w związku z tworzeniem i wdrażaniem polityki skoordynowanego ujawniania podatków, o którym mowa w art. 7 ust. 2 lit. d); c) wymianę najlepszych praktyk i informacji w związku z wdrażaniem niniejszej dyrektywy, w tym w odniesieniu do	NIE		

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

	cyberzagrożeń, incydentów, podatności, potencjalnych zdarzeń dla cyberbezpieczeństwa, inicjatyw na rzecz podnoszenia świadomości, szkoleń, ćwiczeń i umiejętności, budowania zdolności, norm i specyfikacji technicznych, a także wskazywania podmiotów kluczowych i ważnych na podstawie art. 2 ust. 2 lit. b)–d); d) wymianę porad i współpracę z Komisją w zakresie nowych inicjatyw dotyczących polityki cyberbezpieczeństwa oraz całościowej spójności sektorowych wymogów dotyczących cyberbezpieczeństwa; e) wymianę porad i współpracę z Komisją w zakresie projektów aktów delegowanych lub wykonawczych przyjmowanych na podstawie rozporządzenia Rady w sprawie dyrektywy; f) wymianę najlepszych praktyk i informacji z odpowiednimi instytucjami, organami, urzędami i agencjami Unii; g) wymianę opinii na temat wdrażania sektorowych aktów prawnych Unii w sprawie jej polityki dotyczącej cyberbezpieczeństwa; h) w stosownych przypadkach omawianie sprawozdań z oceny wzajemnej, o których mowa w art. 19 ust. 9, oraz formułowanie wniosków i zaleceń; i) prowadzenie skoordynowanych oszacowań ryzyka dla bezpieczeństwa krytycznych łańcuchów dostaw zgodnie z art. 22 ust. 1; j) omawianie przypadków wzajemnej pomocy, w tym doświadczeń ze wspólnych transgranicznych działań nadzorczych, o których mowa w art. 37, i wytyków tych działań; k) na wniosek co najmniej jednego zainteresowanego państwa członkowskiego – omawianie konkretnych wniosków o wzajemną pomoc o której mowa w art. 37; l) zapewnianie sieci CSIRT i EU-CyCLONe wskazówek i informacji dotyczących koordynacji ich powołania i ich funkcjonowania; m) wymianę opinii na temat polityki działań następczych po incydentach i sytuacjach kryzysowych w cyberbezpieczeństwie na dużą skalę, na podstawie doświadczeń zdobytych w sieci CSIRT i EU-CyCLONe; n) wkład w rozwój zdolności w zakresie cyberbezpieczeństwa w całej Unii przez ułatwianie wymiany urzędników krajowych w			

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

	programie budowania zdolności z udziałem pracowników właściwych organów lub CSIRT; o) organizowanie regularnych wspólnych spotkań z odpowiednimi prywatnymi zainteresowanymi stronami z całej Unii w celu omawiania działań Grupy Współpracy i zbierania informacji o powstawaniu i skutkach polityki; p) omawianie działań podjętych w związku z ćwiczeniami z zakresu cyberbezpieczeństwa, w tym próby wykończenia przerw ENISA; q) ustalenie metodyki i aspektów organizacyjnych ocen wzajemnych, o których mowa w art. 19 ust. 1, a także – z pomocą Komisji i ENISA – określenie zgodnie z art. 19 ust. 5 metodyki oceny własnej dla państw członkowskich oraz – we współpracy z Komisją i ENISA – opracowanie zgodnie z art. 19 ust. 6 kodeksów postępowania jako podstawy metod pracy wyznaczonych ekspertów do cyberbezpieczeństwa; r) przygotowywanie – na potrzeby przeglądu, o którym mowa w art. 40 – sprawozdań z doświadczeń zdobytych na poziomie międzynarodowym i w ramach współpracy; s) omawianie i regularne ocenianie sytuacji pod względem cyberzagrożeń lub incydentów, na przykład w postaci oprogramowania typu „ransomware”. Grupa Współpracy przedkłada Komisji, Parlamentowi Europejskiemu i Radzie sprawozdania, o których mowa w akapicie pierwszym lit. r).			
Art. 14	5. Państwa członkowskie zapewniają efektywną, skuteczną i bezpieczną współpracę swoich przedstawicieli w Grupie Współpracy.	NIE		
Art. 14	6. Grupa Współpracy może zwracać się do sieci CSIRT o sporządzenie sprawozdania technicznego na wybrane tematy.	NIE		
Art. 14	7. Do 1 lutego 2024 r., a następnie co dwa lata Grupa Współpracy opracowuje program prac przedstawiający działania, które należy podjąć, by osiągnąć jej cele i wykonać jej zadania.	NIE		
Art. 14	8. Komisja może przyjąć akty wykonawcze określające ustalenia proceduralne kluczowe do funkcjonowania Grupy Współpracy. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 39 ust. 2.	NIE		

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

	Komisja dzieli się poradami i współpracuje z Grupą Współpracy, tworząc projekty aktów wykonawczych, o których mowa w akapicie pierwszym niniejszego ustępu, zgodnie z ust. 4 lit. e).			
Art. 14	9. Grupa Współpracy spotyka się regularnie, w każdym razie co najmniej raz w roku, z Grupą ds. Odporności Podmiotów Krytycznych utworzoną na podstawie dyrektywy (UE) 2022/2557, by propagować i ułatwiać współpracę strategiczną i wymianę informacji.	NIE		
Art. 15	Artykuł 15 Sieć CSIRT 1. Ustanawia się sieć krajowych CSIRT, aby przyczyniać się do wzrostu wzajemnego zaufania oraz promować szybką i skuteczną współpracę operacyjną między państwami członkowskimi. 2. Sieć CSIRT składa się z przedstawicieli CSIRT wyznaczonych lub utworzonych zgodnie z art. 10 oraz zespołu reagowania na incydenty komputerowe w instytucjach, organach i agencjach Unii (CERT-EU). Komisja uczestniczy w pracach sieci CSIRT jako obserwator. ENISA zapewnia sekretariat oraz aktywnie wspiera współpracę między CSIRT. 3. Do zadań sieci CSIRT należy: a) wymiennymi formami i metodami doświadczeń CSIRT; b) ułatwianie udostępniania, przekazywania i wymiany między CSIRT technologii i odpowiednich środków, polityki, narzędzi, procedur, dobrych praktyk i ról; c) wymiana stosownych informacji na temat incydentów, potencjalnych zdarzeń dla cyberbezpieczeństwa, cyberzagrożeń, ryzyka i podmiotów; d) wymiana informacji o publikacjach i rekomendacjach dotyczących cyberbezpieczeństwa; e) zapewnienie interoperacyjności w specyfikacjach i protokołach wymiennych informacji; f) na wniosek członka sieci CSIRT, na którego potencjalnie może mieć wpływ incydent – wymiana i omówienie informacji o tym incydencie i związanych z nim cyberzagrożeniach, ryzyku i podmiotach;	NIE		

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

g) na wniosek członka sieci CSIRT – omówienie oraz, w miarę możliwości, wdrożenie skoordynowanej reakcji na incydent wykryty w grani jurysdykcji danego państwa członkowskiego; h) pomaganie państwom członkowskim w reagowaniu na incydenty transgraniczne zgodnie z dyrektywą; i) współpraca i wymiana dobrych praktyk z CSIRT wyznaczonymi na koordynatorów zgodnie z art. 12 ust. 1 oraz pomaganie im w związku z zarządzaniem skoordynowanym ujawnianiem podatności mogących mieć znaczny wpływ na podmioty w więcej niż jednym państwie członkowskim; j) omawianie i wskazywanie dalszych form współpracy operacyjnej, w tym w związku z: (i) kategoryzacji ryzyka groźń i incydentów; (ii) wdrożeniem odpowiednich środków; (iii) wdrożeniem pomocy; (iv) zasadami i trybem koordynacji w reagowaniu na ryzyka i incydenty transgraniczne; (v) wkładem w krajowy plan reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę, o którym mowa w art. 9 ust. 4, państwa członkowskiego; k) informowanie Grupy Współpracy o działaniach sieci i o dalszych formach współpracy operacyjnej omawianych zgodnie z lit. j) oraz wytycznych w ramach potrzeby o współpracy w tym zakresie; l) omawianie wniosków z ćwiczeń z zakresu cyberbezpieczeństwa, w tym ćwiczeń organizowanych przez ENISA; m) na wniosek danego CSIRT – omawianie jego zdolności i gotowości; n) współpraca i wymiana informacji z regionalnymi i unijnymi centrami monitorowania bezpieczeństwa (SOC) w celu poprawy wspólnej świadomości sytuacyjnej pod kątem incydentów i ryzyka groźń w tej Unii; o) w stosownych przypadkach omawianie sprawozdań z oceny wdrożenia, o których mowa w art. 19 ust. 9; p) podawanie wytycznych mających ułatwić konwergencję praktyk operacyjnych w stosowaniu przepisów niniejszego artykułu dotyczących współpracy operacyjnej.			

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

	4. Na potrzeby przeglądu, o którym mowa w art. 40, sieć CSIRT do 17 stycznia 2025 r., a następnie co dwa lata ocenia postępy we współpracy operacyjnej i przyjmuje sprawozdanie. Sprawozdanie to zawiera w szczególności wnioski i zalecenia wynikające z ocen wzajemnych, o których mowa w art. 19, przeprowadzanych w odniesieniu do krajowych CSIRT. Sprawozdanie to przedkłada się Grupie Współpracy. 5. Sieć CSIRT przyjmuje swój regulamin. 6. Sieć CSIRT i EU-CyCLONe uzgadniają procedury i współpracują na ich podstawie.			
Art. 16	Artykuł 16 Europejska sieć organizacji łącznikowych do spraw kryzysów cyberbezpieczeństwa (EU-CyCLONe) 1. Ustanawia się EU-CyCLONe, aby pomagać w skoordynowanym zarządzaniu na szczeblu operacyjnym incydentami i zarządzaniu kryzysowym w cyberbezpieczeństwie na dużą skalę oraz zapewniać regularną wymianę odpowiednich informacji między państwami członkowskimi a instytucjami, organami, urzędami i agencjami Unii.	TAK	Art. 1 pkt 50 (art. 45 ust. 1 pkt 9-12)	Art. 45.1: 9) ustanowienie odpowiednich struktur komunikacyjnych na potrzeby wczesnego wykrywania kryzysów w cyberbezpieczeństwie, reagowania kryzysowego w cyberbezpieczeństwie i zarządzania kryzysowego w cyberbezpieczeństwie, a także koordynacji współpracy w celu ochrony bezpieczeństwa technologii informacyjnej aktywów o krytycznym znaczeniu w współpracy państw w interesie bezpieczeństwa; 10) współpracę w obszarze cyberbezpieczeństwa państw członkowskich; 11) koordynację działań organów państwa w przypadku wystąpienia sytuacji kryzysowej w cyberbezpieczeństwie niedotyczącej wymiaru militarnego; 12) uczestniczenie w pracach Europejskiej sieci organizacji łącznikowych do spraw kryzysów cyberbezpieczeństwa.
Art. 16	2. EU-CyCLONe składa się z przedstawicieli organów państw członkowskich ds. zarządzania kryzysowego w cyberbezpieczeństwie, a jeśli potencjalny lub trwający incydent w cyberbezpieczeństwie na dużą skalę ma lub może mieć znaczny wpływ na usługi i działania objęte zakresem stosowania niniejszej dyrektywy – także Komisji. W pozostałych przypadkach Komisja uczestniczy w działaniach EU-CyCLONe jako obserwator.	TAK	Art. 1 pkt 50 (art. 45 ust. 1 pkt 9-12)	Art. 45.1: 9) ustanowienie odpowiednich struktur komunikacyjnych na potrzeby wczesnego wykrywania kryzysów w cyberbezpieczeństwie, reagowania kryzysowego w cyberbezpieczeństwie i zarządzania kryzysowego w cyberbezpieczeństwie, a także koordynacji

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

	ENISA zapewnia obsługę sekretariatu EU-CyCLONe i pomaga w bezpiecznej wymianie informacji, a także dostarcza narzędzia kluczowe do wsparcia współpracy między państwami członkowskimi przez zapewnienie bezpiecznej wymiany informacji. W stosownych przypadkach EU-CyCLONe może zapraszać przedstawicieli odpowiednich zainteresowanych stron, by uczestniczyli w jej pracach w charakterze obserwatorów.			współpracy w celu ochrony bezpieczeństwa technologii informacyjnej aktywów o krytycznym znaczeniu w państwie; 10) współpracę w obszarze cyberbezpieczeństwa państwa z państwami trzecimi; 11) koordynację działań organów państwa w przypadku wystąpienia sytuacji kryzysowej w cyberbezpieczeństwie nie dotyczącej wymiaru militarnego; 12) uczestniczenie w pracach Europejskiej sieci organizacji łącznikowych do spraw kryzysów cyberbezpieczeństwa.
Art. 16	3. EU-CyCLONe ma następujące zadania: a) podnoszenie poziomu gotowości do zarządzania incydentami i nadzoru nad cyberbezpieczeństwem państwa na dużą skalę; b) rozwijanie wspólnej świadomości sytuacyjnej pod kątem incydentów i sytuacji kryzysowych w cyberbezpieczeństwie na dużą skalę; c) ocenę konsekwencji i wpływu istotnych incydentów i sytuacji kryzysowych w cyberbezpieczeństwie na dużą skalę oraz proponowanie możliwych środków ograniczających ryzyko; d) koordynowanie zarządzania incydentami i zarządzania kryzysowego w cyberbezpieczeństwie na dużą skalę oraz wspieranie procesu decyzyjnego na szczeblu politycznym w odniesieniu do tych incydentów i sytuacji kryzysowych; e) na wniosek zainteresowanego państwa członkowskiego – omawianie krajowych planów reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę, o których mowa w art. 9 ust. 4.	NIE		
Art. 16	4. EU-CyCLONe przyjmuje swój regulamin.	NIE		
Art. 16	5. EU-CyCLONe regularnie składa Grupie Współpracy sprawozdania na temat zarządzania incydentami i zarządzania kryzysowego w cyberbezpieczeństwie na dużą skalę, a także na temat tendencji w tej dziedzinie, koncentrując się zwłaszcza na ich wpływie na podmioty kluczowe i ważne.	NIE		

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

Art. 16	6. EU-CyCLONe współpracuje z siecią CSIRT na podstawie uzgodnionych ustaleń proceduralnych określonych w art. 15 ust. 6.	NIE		
Art. 16	7. Do dnia 17 lipca 2024 r., a następnie co 18 miesięcy EU-CyCLONe przedkłada Parlamentowi Europejskiemu i Radzie sprawozdanie, w którym ocenia swoją pracę.	NIE		
Art. 17	Artykuł 17 Współpraca międzynarodowa Unia może w stosownych przypadkach zawierać zgodnie z art. 218 TFUE umowy międzynarodowe z państwami trzecimi lub organizacjami międzynarodowymi, umożliwiające i organizujące ich udział w niektórych działaniach Grupy Współpracy oraz sieci CSIRT i EU-CyCLONe. Umowy takie są zgodne z unijnymi przepisami o ochronie danych.	NIE		
Art. 18	Artykuł 18 Sprawozdanie o stanie cyberbezpieczeństwa w Unii 1. Co dwa lata ENISA przyjmuje we współpracy z Komisją i Grupą Współpracy sprawozdanie o stanie cyberbezpieczeństwa w Unii oraz przedkłada i przedstawia to sprawozdanie Parlamentowi Europejskiemu. Sprawozdanie udostępnia się m.in. jako dane nadające się do odczytu maszynowego i zawiera ono następujące elementy: a) oszacowanie ryzyka w cyberbezpieczeństwie na poziomie Unii, z uwzględnieniem kryteriów ryzyka i zagrożeń; b) ocenę rozwoju zdolności w zakresie cyberbezpieczeństwa w sektorach publicznym i prywatnym w całej Unii; c) ocenę ogólnego poziomu wiedzy o cyberbezpieczeństwie i cyberhigieny wśród obywateli i podmiotów, w tym małych i średnich przedsiębiorstw; d) zbiorczą ocenę wyników ocen wzajemnych, o których mowa w art. 19; e) zbiorczą ocenę poziomu dojrzałości zdolności i zasobów w zakresie cyberbezpieczeństwa w całej Unii, w tym na poziomie sektorowym, a także stopnia wzajemnego dostosowania krajowych strategii cyberbezpieczeństwa państw członkowskich. 2. Sprawozdanie zawiera konkretne zalecenia polityczne dotyczące usuwania braków i zwiększenia poziomu cyberbezpieczeństwa w	NIE		

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

	całej Unii oraz streszczenie ustaleń za dany okres zawartych w raportach technicznych o stanie cyberbezpieczeństwa w UE dotyczących incydentów i cyberzagrożeń, przygotowanych przez ENISA zgodnie z art. 7 ust. 6 rozporządzenia (UE) 2019/881. 3. We współpracy z Komisją, Grupą Współpracy i siecią CSIRT ENISA opracowuje metodykę zbiorczej oceny, o której mowa w ust. 1 lit. e), w tym odpowiednie zmienne – np. wskaźniki ilościowe i jakościowe.			
Art. 19	Artykuł 19 Oceny wzajemne 1. Do 17 stycznia 2025 r. Grupa Współpracy ustala – z pomocą Komisji i ENISA oraz, w stosownych przypadkach, sieci CSIRT – metodykę i aspekty organizacyjne ocen wzajemnych, by wyciągać wnioski ze wspólnych doświadczeń, zwiększać wzajemne zaufanie, osiągnąć wysoki wspólny poziom cyberbezpieczeństwa, a także zwiększać kluczowe do wdrożenia niniejszej dyrektywy zdolności państw członkowskich w zakresie cyberbezpieczeństwa i doskonalić ich politykę w tej dziedzinie. Udział w ocenach wzajemnych jest dobrowolny. Oceny wzajemne przeprowadzą eksperci ds. cyberbezpieczeństwa. Ekspertów ds. cyberbezpieczeństwa wyznaczają co najmniej dwa państwa członkowskie inne niż państwo członkowskie poddawane ocenie. Oceny wzajemne dotyczą co najmniej jednej z następujących kwestii: a) stopień wdrożenia środków zarządzania ryzykiem w cyberbezpieczeństwie oraz obowiązków dotyczących zgłaszania incydentów określonych w art. 21 i 23; b) poziom zdolności, w tym dostępne zasoby finansowe, techniczne i ludzkie, oraz skuteczność wykonywania zadań przez właściwe organy; c) zdolność operacyjną CSIRT; d) poziom wdrożenia i wdrożenia pomocy, o której mowa w art. 37; e) poziom wdrożenia ustaleń dotyczących mechanizmów wymiany informacji, o których mowa w art. 29; f) szczególne zagadnienia transgraniczne lub międzysektorowe.	TAK	Art. 1 pkt 43 (art. 40a ust. 1–3)	Art. 40a. 1. CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT sektorowy i organy właściwe do spraw cyberbezpieczeństwa mogą, w porozumieniu z Pełnomocnikiem, uczestniczyć w procesie oceny wzajemnej, w celu wymiany doświadczeń, zwiększania wzajemne zaufanie pomiędzy organami z różnych państw, osiągnięcia wysokiego, wspólnego poziomu cyberbezpieczeństwa, a także zwiększenia kluczowych zdolności państw członkowskich Unii Europejskiej w zakresie cyberbezpieczeństwa i doskonalenia ich polityki w tej dziedzinie. 2. Ocena wzajemna jest przeprowadzana przez ekspertów do spraw cyberbezpieczeństwa wyznaczonych na podstawie metodyki obejmującej obiektywne, niedyskryminacyjne, sprawiedliwe i przejrzyste kryteria, jako uprawnionych do prowadzenia ocen wzajemnych. 3. Ocena wzajemna może obejmować: 1) stopień wdrożenia środków zarządzania ryzykiem w cyberbezpieczeństwie oraz obowiązków dotyczących określonych incydentów; 2) poziom zdolności, w tym dostępne zasoby finansowe, techniczne i ludzkie, oraz skuteczność wykonywania i wdrożenia praw właściwych organów; 3) zdolność operacyjną CSIRT; 4) poziom wdrożenia i wdrożenia pomocy;

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				5) poziom wdrożenia ustaleń dotyczących mechanizmów wymiany informacji na temat cyberbezpieczeństwa; 6) szczególne zagadnienia transgraniczne lub międzysektorowe.
Art. 19	2. Metodyka, o której mowa w ust. 1, obejmuje obiektywne, niedyskryminacyjne, sprawiedliwe i przejrzyste kryteria, na podstawie których państwa członkowskie wyznaczają ekspertów ds. cyberbezpieczeństwa uprawnionych do prowadzenia ocen wzajemnych. Komisja i ENISA uczestniczą w ocenach wzajemnych w charakterze obserwatorów.	TAK	Art. 1 pkt 43 (art. 40a ust. 2)	Art. 40a. 2. Ocena wzajemna jest przeprowadzana przez ekspertów do spraw cyberbezpieczeństwa wyznaczonych na podstawie metodyki obejmującej obiektywne, niedyskryminacyjne, sprawiedliwe i przejrzyste kryteria, jako uprawnionych do prowadzenia ocen wzajemnych.
Art. 19	3. Państwa członkowskie mogą wskazać do oceny wzajemnej konkretne zagadnienia, o których mowa w ust. 1 lit. f).	TAK	Art. 1 pkt 43 (art. 40a ust. 5)	Art. 40a. 5. Pełnomocnik może wskazać innym państwom członkowskim Unii Europejskiej uczestniczącym w ocenie wzajemnej szczególne zagadnienia transgraniczne lub międzysektorowe, które należy uwzględnić w ocenie wzajemnej.
Art. 19	4. Przed rozpoczęciem oceny wzajemnej, o której mowa w ust. 1, państwa członkowskie powiadamiają uczestniczące państwa członkowskie o jej zakresie, w tym o konkretnych zagadnieniach wskazanych na podstawie ust. 3.	TAK	Art. 1 pkt 43 (art. 40a ust. 6)	Art. 40a. 6. Pełnomocnik informuje inne państwa członkowskie Unii Europejskiej uczestniczące w ocenie wzajemnej o zakresie oceny wzajemnej przeprowadzanej w Rzeczypospolitej Polskiej.
Art. 19	5. Przed rozpoczęciem oceny wzajemnej państwa członkowskie mogą przeprowadzić ocenę własną aspektów poddawanych ocenie i przekazać jej wyniki wyznaczonym ekspertom ds. cyberbezpieczeństwa. Grupa Współpracy z pomocą Komisji i ENISA określa metodykę oceny własnej prowadzonej przez państwa członkowskie.	TAK	Art. 1 pkt 43 (art. 40a ust. 7)	Art. 40a. 7. W porozumieniu z Pełnomocnikiem podmioty, o których mowa w ust. 1, mogą przeprowadzić ocenę, o której mowa w ust. 3 dotyczącą krajowego systemu cyberbezpieczeństwa i przedstawić jej wyniki ekspertom z innych państw uczestniczących w ocenie wzajemnej. Ocenę tę przeprowadza się zgodnie z metodyką przyjętą przez Grupę współpracy.
Art. 19	6. Oceny wzajemne wiążą się z fizycznymi lub zdalnymi kontrolami na miejscu i zdalną wymianą informacji. Zgodnie z zasadą dobrej współpracy państwo członkowskie poddane ocenie wzajemnej dostarcza wyznaczonym ekspertom ds. cyberbezpieczeństwa informacji potrzebnych do oceny, bez uszczerbku dla unijnych lub krajowych przepisów o ochronie informacji poufnych lub	TAK	Art. 1 pkt 43 (art. 40a ust. 4)	Art. 40a. 4. W ramach procesu oceny wzajemnej podmioty, o których mowa w ust. 1, mogą przekazywać wyznaczonym przez inne państwa członkowskie Unii Europejskiej ekspertom do spraw cyberbezpieczeństwa informacje dotyczące funkcjonowania tych podmiotów,

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

	niejawnych oraz dla zagwarantowania podstawowych funkcji państwa, takich jak bezpieczeństwo narodowe. Grupa Współpracy we współpracy z Komisją i ENISA opracowuje odpowiednie kodeksy postępowania jako podstawę metod pracy wyznaczonych ekspertów ds. cyberbezpieczeństwa. Informacje uzyskane w trakcie oceny wzajemnej wykorzystuje się wyłącznie na potrzeby tej oceny. Eksperci ds. cyberbezpieczeństwa uczestniczący w ocenie wzajemnej nie ujawniają osobom trzecim informacji szczególnie chronionych lub poufnych uzyskanych w trakcie tej oceny.			z uwzględnieniem przepisów o tajemnicach prawnie chronionych.
Art. 19	7. Aspektów poddanych ocenie wzajemnej i ocenionych w danym państwie członkowskim nie poddaje się dalszej ocenie wzajemnej w tym państwie członkowskim przez dwa lata od zakończenia oceny wzajemnej, chyba że to państwo członkowskie zwróci się o przeprowadzenie takiej oceny lub zostanie ona uzgodniona na wniosek Grupy Współpracy.	TAK	Art. 1 pkt 43 (art. 40a ust. 8)	Art. 40a. 8. Oceny wzajemnej nie przeprowadza się w terminie 2 lat od sporządzenia sprawozdania z poprzedniej oceny wzajemnej, jeżeli dotyczy tego samego zakresu. Ocena wzajemna dotycząca tego samego zakresu może być przeprowadzona, jeżeli Pełnomocnik zwróci się o to do innego państwa członkowskiego Unii Europejskiej lub państwa członkowskie Unii Europejskiej uzgodnią to w ramach Grupy współpracy.
Art. 19	8. Państwa członkowskie zapewniają ujawnienie pozostałym państwom członkowskim, Grupie Współpracy, Komisji i ENISA – przed rozpoczęciem oceny wzajemnej – ryzyka konfliktu interesów dotyczącego wyznaczonych ekspertów ds. cyberbezpieczeństwa. Państwo członkowskie poddane ocenie wzajemnej może sprzeciwić się wyznaczeniu konkretnych ekspertów ds. cyberbezpieczeństwa z należycie uzasadnionych powodów, o których informuje się Grupę Współpracy.	TAK	Art. 1 pkt 43 (art. 40a ust. 9)	Art. 40a. 9. Pełnomocnik może sprzeciwić się przeprowadzeniu oceny wzajemnej przez konkretnych ekspertów z innego państwa członkowskiego Unii Europejskiej, jeżeli występuje konflikt interesów.
Art. 19	9. Eksperci ds. cyberbezpieczeństwa uczestniczący w ocenach wzajemnych sporządzają sprawozdania zawierające ustalenia i wnioski z tych ocen. Państwa członkowskie poddane ocenie wzajemnej mogą zgłaszać uwagi do projektów sprawozdań, które ich dotyczą, a uwagi te załącza się do sprawozdań. Sprawozdania te zawierają zalecenia umożliwiające poprawę w aspektach objętych oceną wzajemną. W stosownych przypadkach sprawozdania przedkłada się Grupie Współpracy i sieci CSIRT. Państwo członkowskie poddane ocenie wzajemnej może podjąć decyzję o	TAK	Art. 1 pkt 43 (art. 40a ust. 10 i 11)	Art. 40a. 10. Eksperci do spraw cyberbezpieczeństwa wyznaczeni przez podmioty, o których mowa w ust. 1, uczestniczący w ocenie wzajemnej sporządzają sprawozdanie z oceny wzajemnej, które zatwierdza Pełnomocnik. Sprawozdanie zawiera podsumowanie czynności podjętych w ramach oceny wzajemnej, oraz zalecenia. Sprawozdanie udostępnia się innym państwom członkowskim Unii Europejskiej uczestniczącym w ocenie wzajemnej oraz

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

	podaniu do wiadomości publicznej sprawozdania z oceny wzajemnej lub jego zredagowanej wersji.			organom właściwym do spraw cyberbezpieczeństwa, CSIRT MON, CSIRT NASK i CSIRT GOV. 11. Pełnomocnik może udostępnić sprawozdanie Grupie Współpracy lub Sieci CSIRT. Sprawozdanie to może zostać opublikowane w Biuletynie Informacji Publicznej Pełnomocnika w zakresie w jakim nie zawiera informacji stanowiących tajemnice prawnie chronione.
Art. 20	Artykuł 20 Zarządzanie 1. Państwa członkowskie zapewniają, aby organy zarządzające podmiotów kluczowych i ważnych zatwierdzały środki zarządzania ryzykiem w cyberbezpieczeństwie przyjęte przez te podmioty w celu zapewnienia zgodności z art. 21, nadzorowały ich wdrażanie i mogły być pociągnięte do odpowiedzialności za naruszanie przez te podmioty tego artykułu. Stosowanie niniejszego ustępu nie narusza przepisów krajowych dotyczących zasad odpowiedzialności instytucji publicznych oraz odpowiedzialności urzędników publicznych oraz urzędników wybranych lub mianowanych.	TAK	Art. 1 pkt 4 (art. 2 pkt 8a) i pkt 17 (art. 8a, art. 8c i art. 8d)	Art. 2: 8a) kierownik podmiotu kluczowego lub podmiotu ważnego – kierownik jednostki w rozumieniu art. 3 ust. 1 pkt 6 ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2023 r. poz. 120, z późn. zm.) kierujący podmiotem kluczowym lub podmiotem w tym; w przypadku podmiotu kluczowego lub podmiotu ważnego będącego jednostką sektora finansów publicznych kierownikiem podmiotu jest kierownik, o którym mowa w art. 53 ust. 1 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2024 r. poz. 1530, z późn. zm.); Art. 8a. Rada Ministrów może określić, w drodze rozporządzenia, odrębnie dla danego rodzaju działalności wykonywanej przez podmioty kluczowe lub podmioty ważne szczegółowe wymagania dla systemu zarządzania bezpieczeństwem informacji, o którym mowa w art. 8 ust. 1, biorąc pod uwagę rekomendacje międzynarodowe o charakterze specjalistycznym, w tym rekomendacje Agencji Unii Europejskiej do spraw Cyberbezpieczeństwa, zwanej dalej „ENISA”, wielkość podmiotu, skalę działalności wykonywanej przez te podmioty oraz potrzebę

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				podejmowania przez te podmioty działań zapewniających cyberbezpieczeństwo. Art. 8c. 1. Kierownik podmiotu kluczowego lub podmiotu ważnego ponosi odpowiedzialność za wykonywanie obowiązków w zakresie cyberbezpieczeństwa przez podmiot kluczowy lub podmiot ważny, o których mowa w art. 7b ust. 4, art. 7c, art. 7f ust. 3, art. 8, art. 8d, art. 8e, art. 8f ust. 1 i 2, art. 9–12b, art. 14 i art. 15. 2. W przypadku gdy kierownikiem podmiotu kluczowego lub podmiotu ważnego jest organ wieloosobowy i nie została wskazana osoba odpowiedzialna, odpowiedzialność ponoszą wszyscy członkowie tego organu. 3. Kierownik podmiotu kluczowego lub podmiotu ważnego ponosi odpowiedzialność także wtedy, gdy niektóre z obowiązków albo wszystkie obowiązki zostały powierzone innej osobie za jej zgodą. Art. 8d. Kierownik podmiotu kluczowego lub podmiotu ważnego: 1) podejmuje decyzje w zakresie przygotowania, wdrażania, stosowania, przeglądu i nadzoru systemu zarządzania bezpieczeństwem informacji w podmiocie; 2) planuje adekwatne środki finansowe na realizację obowiązków z zakresu cyberbezpieczeństwa; 3) przydziela zadania z zakresu cyberbezpieczeństwa w tym podmiocie i nadzoruje ich wykonanie; 4) zapewnia, że personel podmiotu jest świadomy obowiązków z zakresu

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				cyberbezpieczeństwa i zna wewnętrzne regulacje podmiotu w tym zakresie; 5) zapewnia zgodność działania tego podmiotu z przepisami prawa oraz z wewnętrznymi regulacjami podmiotu.
Art. 20	2. Państwa członkowskie zapewniają, aby członkowie organu zarządzającego podmiotów kluczowych i ważnych mieli obowiązek odbywać regularne szkolenia w celu zdobycia wystarczającej wiedzy i umiejętności pozwalających im rozpoznać ryzyko i ocenić praktyki zarządzania ryzykiem w cyberbezpieczeństwie oraz ich wpływ na usługi świadczone przez dany podmiot, a także zachęcają podmioty kluczowe i ważne do oferowania podobnych szkoleń ich pracownikom.	TAK	Art. 1 pkt 17 (art. 8e)	Art. 8e. 1. Kierownik podmiotu kluczowego lub podmiotu ważnego oraz osoba, której powierzono obowiązki kierownika w zakresie cyberbezpieczeństwa, raz w roku kalendarzowym przechodzi szkolenie. 2. Zakres szkolenia obejmuje wykonywania obowiązków, o których mowa w art. 7b ust. 4, art. 7c, art. 7f ust. 3, art. 8, art. 8d, art. 8f ust. 1 i 2, art. 9–12b, art. 14 i art. 15. 3. Udział w szkoleniu jest udokumentowany.
Art. 21	Artykuł 21 Środki zarządzania ryzykiem w cyberbezpieczeństwie 1. Państwa członkowskie zapewniają, aby podmioty kluczowe i ważne wprowadzały odpowiednie i proporcjonalne środki techniczne, operacyjne i organizacyjne w celu zarządzania ryzykiem dla bezpieczeństwa sieci i systemów informatycznych wykorzystywanych przez te podmioty do prowadzenia działalności lub świadczenia usług oraz w celu zapobiegania wpływowi incydentów na odbiorców ich usług lub na inne usługi bądź minimalizowania takiego wpływu. Przy uwzględnieniu najnowszego stanu wiedzy oraz, w stosownych przypadkach, odpowiednich norm europejskich i międzynarodowych, a także kosztów wdrożenia środków, o których mowa w akapicie pierwszym, zapewniają poziom bezpieczeństwa sieci i systemów informatycznych odpowiedni do istniejącego ryzyka. Oceniając proporcjonalność tych środków, należyć uwzględnić stopień narażenia podmiotu na ryzyko, wielkość podmiotu i prawdopodobieństwo wystąpienia incydentów oraz ich dotkliwość, w tym ich skutki społeczne i gospodarcze.	TAK	Art 1 pkt 16 (art. 8), pkt 18 (art. 9 i art. 10) i pkt 76 (art. 67c) oraz art. 33	Art. 8. 1. Podmiot kluczowy lub podmiot ważny wdraża system zarządzania bezpieczeństwem informacji w systemie informacyjnym wykorzystywanym w procesach wpływających na świadczenie usługi przez ten podmiot, zapewniający: 1) prowadzenie systematycznego szacowania ryzyka wystąpienia incydentu oraz zarządzanie tym ryzykiem; 2) wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, uwzględniających najnowszy stan wiedzy, koszty wdrożenia, wielkość podmiotu, prawdopodobieństwo wystąpienia incydentów, narażenie podmiotu na ryzyko, skutki społeczne i gospodarcze, w szczególności:

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				a) polityki szacowania ryzyka oraz bezpieczeństwa systemu informacyjnego, w tym polityki tematyczne, b) bezpieczeństwo w procesie nabywania, rozwoju, utrzymania i eksploatacji systemu informacyjnego, w tym testowanie systemu informacyjnego, c) bezpieczeństwo fizyczne i środowiskowe uwzględniające kontrole dostępu, d) bezpieczeństwo zasobów ludzkich, e) bezpieczeństwo i ciągłość łańcucha dostaw produktów ICT, usług ICT i procesów ICT, od których zależy świadczenie usługi, z uwzględnieniem związków pomiędzy bezpośrednim dostawcą sprzętu lub oprogramowania a podmiotem kluczowym lub podmiotem ważnym, f) wdrażanie, dokumentowanie, testowanie i utrzymywanie planów ciągłości działania umożliwiających ciągłe i niezakłócone świadczenie usługi oraz zapewniających poufność, integralność, dostępność i autentyczność informacji, planów awaryjnych oraz planów odtworzenia działalności umożliwiających odtworzenie systemu informacyjnego po zdarzeniu, które spowodowało straty przekraczające zdolności podmiotu do odbudowy za pomocą własnych środków,

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				g) objęcie systemu informacyjnego wykorzystywanego do świadczenia usługi systemem monitorowania w trybie ciągłym, h) polityki i procedury oceny skuteczności środków technicznych i organizacyjnych, i) edukację z zakresu cyberbezpieczeństwa dla personelu podmiotu, j) podstawowe zasady cyberhigieny, k) polityki i procedury stosowania kryptografii, w tym w stosownych przypadkach szyfrowania, l) stosowanie bezpiecznych środków komunikacji elektronicznej w ramach krajowego systemu cyberbezpieczeństwa oraz wewnątrz podmiotu, uwzględniających uwierzytelnianie wieloskładnikowe w stosownych przypadkach, m) zarządzanie aktywami, n) polityki kontroli dostępu; 3) zbieranie informacji o cyberzagrożeniach i podatnościach na incydenty systemu informacyjnego wykorzystywanego do świadczenia usługi; 4) zarządzanie incydentami; 5) stosowanie środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego wykorzystywanego do świadczenia usługi, w tym: a) stosowanie mechanizmów zapewniających poufność, integralność, dostępność

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				i autentyczność danych przetwarzanych w systemie informacyjnym, b) regularne przeprowadzanie aktualizacji oprogramowania, stosownie do zaleceń producenta, z uwzględnieniem analizy wpływu aktualizacji na bezpieczeństwo świadczonej usługi oraz poziomu krytyczności poszczególnych aktualizacji, c) ochronę przed nieuprawnioną modyfikacją w systemie informacyjnym, d) niezwłoczne podejmowanie działań po dostrzeżeniu podatności lub cyberzagrożeń, w tym również czasowe ograniczenie ruchu sieciowego przychodzącego do infrastruktury podmiotu kluczowego lub podmiotu ważnego, które może skutkować zakłóceniem usług świadczonych przez ten podmiot, mając na uwadze konieczność minimalizacji skutków ograniczenia dostępności tych usług, z uwagi na podjęte działania. 2. Wdrażając środki, o których mowa w ust. 1 pkt 2 lit. e, podmiot kluczowy lub podmiot ważny uwzględnia: 1) podatności związane z dostawcą sprzętu lub oprogramowania; 2) ogólną jakość produktów ICT, usług ICT i procesów ICT pochodzących od dostawcy sprzętu lub oprogramowania;

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				3) wyniki skoordynowanej oceny bezpieczeństwa przeprowadzonej przez Grupę współpracy, o której mowa w art. 22 ust. 1 dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniającej rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającą dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz. Urz. UE L 333 z 27.12.2022, str. 80), zwanej dalej „dyrektywą 2022/2555”; 4) wyniki postępowania, o którym mowa w art. 67b. 3. Podmiot ważny będący podmiotem publicznym nie stosuje przepisu ust. 1. Podmiot ważny będący podmiotem publicznym opracowuje, wdraża, realizuje, monitoruje i utrzymuje w systemach informacyjnych kontrolowanych przez ten podmiot system zarządzania bezpieczeństwem informacji spełniający wymogi określone w załączniku nr 4 do ustawy. 4. Podmiot publiczny uwzględnia w systemie zarządzania bezpieczeństwem informacji system informacyjny dostarczany przez inny podmiot publiczny, w tym na podstawie przepisów ustawy, w szczególności system informacyjny zapewniający działanie rejestru publicznego w zakresie odpowiadającym zakresowi kompetencji tego podmiotu, wynikającym z polityki bezpieczeństwa danego systemu informacyjnego lub przepisów prawa regulujących sposób działania tego systemu

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				Art. 9. 1. Podmiot kluczowy lub podmiot ważny: 1) wyznacza co najmniej dwie osoby odpowiedzialne za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa; 2) zapewnia użytkownikowi usługi dostępu do wiedzy pozwalającej na zrozumienie cyberzagrożeń i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami w zakresie związanym ze świadczonymi usługami, w szczególności przez udostępnianie informacji na ten temat na swojej stronie internetowej; 3) zapewnia użytkownikowi usługi możliwość zgłoszenia cyberzagrożenia, incydentu lub podjęcia działań świadczonych usług; 4) po uzyskaniu wpisu podmiotu do wykazu rozpoczyna korzystanie z systemu teleinformatycznego, o którym mowa w art. 46 ust. 1. 2. Podmiot kluczowy lub podmiot ważny będący mikro- lub małym przedsiębiorcą, o którym mowa w art. 2 ust. 1 załącznika I do rozporządzenia 651/2014/UE, wyznacza co najmniej jedną osobę odpowiedzialną za utrzymywanie kontaktów z innymi podmiotami kluczowymi lub podmiotami ważnymi. 3. Podmiot ważny będący podmiotem publicznym wyznacza co najmniej jedną osobę odpowiedzialną za utrzymywanie kontaktów z innymi podmiotami kluczowymi lub podmiotami ważnymi. 4. Obowiązek, o którym mowa w ust. 1 pkt 2, może być zrealizowany przez zamieszczenie na stronie internetowej podmiotu hiperłącza do stron

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				internetowych organu właściwego do spraw cyberbezpieczeństwa, CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT sektorowego. Art. 10. 1. Podmiot kluczowy lub podmiot ważny opracowuje, stosuje i aktualizuje dokumentację dotyczącą bezpieczeństwa systemu informacyjnego wykorzystywanego w procesie świadczenia usługi. 2. Do dokumentacji dotyczącej bezpieczeństwa systemu informacyjnego wykorzystywanego w procesie świadczenia usługi, o której mowa, zalicza się: 1) dokumentację formacyjną; 2) dokumentację operacyjną. 3. Dokumentację normatywną stanowią: 1) dokumentacja systemu zarządzania bezpieczeństwem informacji; 2) dokumentacja ochrony infrastruktury, z wykorzystaniem której świadczona jest usługa, obejmująca: a) charakterystykę usługi oraz infrastruktury, w której świadczona jest usługa, b) ocenę aktualnego stanu ochrony infrastruktury, c) szacowanie ryzyka dla obiektów infrastruktury, d) plan postępowania z ryzykiem, e) opis zabezpieczeń technicznych obiektów infrastruktury, f) zasady organizacji i wykonywania ochrony fizycznej infrastruktury, g) dane o specjalistycznej uzbrojonej formacji ochronnej, o której mowa w art. 2 pkt 7 ustawy z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz. U. z 2025 r. poz. 532), chroniącej infrastrukturę – jeżeli występuje; 3) dokumentacja systemu zarządzania ciągłością działalności;

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				4) dokumentacja techniczna systemu informacyjnego wykorzystywanego w procesie świadczenia usługi; 5) dokumentacja wynikająca ze specyfiki świadczonej usługi w danym sektorze lub podsektorze. 4. Dokumentację operacyjną stanowią zapisy poświadczające wykonywanie czynności wymaganych przez postanowienia zawarte w dokumentacji normatywnej, w tym automatycznie generowane w dyktando systemów informacyjnych. 5. Dokumentacja dotycząca bezpieczeństwa systemu informacyjnego wykorzystywanego w procesie świadczenia usługi może być prowadzona w postaci papierowej lub w postaci elektronicznej. 6. Podmiot kluczowy lub podmiot ważny jest obowiązany do ustanowienia nadzoru nad dokumentacją dotyczącą bezpieczeństwa systemu informacyjnego wykorzystywanego w procesie świadczenia usługi, zapewniającego: 1) dostępność dokumentów wyłącznie dla osób upoważnionych, zgodnie z realizowanymi przez nimi; 2) ochronę dokumentów przed uszkodzeniem, zniszczeniem, utratą, nieuprawnionym dostępem, niewłaściwym użyciem lub utratą integritasu; 3) oznaczanie kolejnych wersji dokumentów umożliwiające określenie zmian dokonanych w tych dokumentach. 7. Podmiot kluczowy lub podmiot ważny przechowuje dokumentację dotyczącą bezpieczeństwa systemu informacyjnego wykorzystywanego w procesie świadczenia usługi przez okres co najmniej 2 lat od dnia jej

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				wycofania z użytkowania lub zakończenia świadczenia usługi, liczony od dnia 1 stycznia roku następującego po roku, w którym wygasa okres jej przechowywania. Przepisu nie stosuje się do podmiotów podlegających ustawie z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i rękopiśmiennemu (Dz.U. 2020 r. poz. 164). 8. Zniszczenie wycofanej z użytkowania dokumentacji dotyczącej bezpieczeństwa systemu informacyjnego wykorzystywanego w procesie świadczenia usługi potwierdza się protokołem brakowania zawierającym w szczególności: datę protokołu, oznaczenie niszczonej dokumentacji, opis sposobu zniszczenia, dane osoby zatwierdzające protokół. Protokoły brakowania dokumentacji dotyczącej bezpieczeństwa systemu informacyjnego wykorzystywanego w procesie świadczenia usługi są przechowywane w sposób trwały. Art. 67c. 1. W przypadku wydania decyzji, o której mowa w art. 67b ust. 15, podmioty, o których mowa w art. 67b ust. 1: 1) nie wprowadzają do użytkowania typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT w zakresie objętym decyzją, dostarczanych przez dostawcę wysokiego ryzyka; 2) wycofują z użytkowania typy produktów ICT, rodzaje usług ICT i konkretne procesy ICT w zakresie objętym decyzją dostarczanych przez dostawcę wysokiego ryzyka nie później niż 7 lat od dnia ogłoszenia decyzji, o której mowa w art. 67b ust. 15, w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski”.

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				2. Przedsiębiorcy telekomunikacyjni, o których mowa w art. 67b ust. 1 pkt 2, wycofują w ciągu 4 lat od dnia ogłoszenia decyzji, o której mowa w art. 67b ust. 15, typy produktów ICT, rodzaje usług ICT, konkretne procesy ICT wskazane w decyzji i określone w wykazie kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług w załączniku nr 3 do ustawy. 3. Do czasu wycofania sprzętu lub oprogramowania, o którym mowa w ust. 1 pkt 2 oraz w ust. 2, dopuszcza się użytkowanie dotychczas posiadanych typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT w zakresie objętym decyzją, dostarczanych przez dostawcę wysokiego ryzyka, w zakresie naprawy, modernizacji, wymiany elementu lub aktualizacji, jeżeli jest to niezbędne dla zapewnienia odpowiedniej jakości i ciągłości świadczonych usług, w szczególności dokonywania niezbędnych napraw awarii lub uszkodzeń. 4. Podmioty, o których mowa w art. 67b ust. 1, do których stosuje się ustawę z dnia 11 września 2019 r. – Prawo zamówień publicznych (Dz. U. z 2024 r. poz. 1320), nie mogą nabywać typów produktów ICT, rodzajów usług ICT lub konkretnych procesów ICT określonych w decyzji, o której mowa w art. 67b ust. 15. 5. W przypadku gdy podmioty, o których mowa w art. 67b ust. 1, do których stosuje się ustawę z dnia 11 września 2019 r. – Prawo zamówień publicznych, nabyły, w drodze zamówienia publicznego, przed dniem ogłoszenia, o której mowa w art. 67b ust. 15, produkt ICT, usługę ICT lub proces ICT określone w tej decyzji, mogą korzystać z tych produktów, usług lub procesów nie dłużej niż 7 lat od dnia ogłoszenia decyzji,

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				o której mowa w art. 67b ust. 15, w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski”, a w przypadku produktów ICT, usług ICT lub procesów ICT wykorzystywanych do wykonywania funkcji krytycznych określonych w załączniku nr 3 do ustawy, nie dłużej niż 4 lat od dnia ogłoszenia decyzji, o której mowa w art. 67b ust. 15. Art. 33. 1. Podmioty, które z dniem wejścia w życie niniejszej ustawy spełniają przesłanki uznania ich za podmiot kluczowy albo za podmiot ważny realizują obowiązki określone w rozdziale 3 ustawy zmienianej w art. 1, w brzmieniu nadanym niniejszą ustawą, w terminie 6 miesięcy od dnia wejścia w życie niniejszej ustawy. 2. Podmioty, które z dniem wejścia w życie niniejszej ustawy spełniają przesłanki uznania ich za podmiot kluczowy przeprowadzają pierwszy audyt, o którym mowa w art. 15 ust. 1 ustawy zmienianej w art. 1, w brzmieniu nadanym niniejszą ustawą, w terminie 24 miesięcy od dnia wejścia w życie niniejszej ustawy. 3. Podmioty, które z dniem wejścia w życie niniejszej ustawy spełniają przesłanki uznania ich za podmiot kluczowy albo za podmiot ważny są obowiązane zarejestrować się w wykazie podmiotów kluczowych i podmiotów ważnych zgodnie z harmonogramem określonym w art. 34 ust. 3 pkt 1 niniejszej ustawy. 4. Podmioty kluczowe lub podmioty ważne, które przed dniem wejścia w życie ustawy były operatorami usług kluczowych zgłaszają incydenty poważne zgodnie z art. 11-art. 12b ustawy zmienianej w art. 1 w brzmieniu nadanym

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				niniejszą ustawą w terminie 6 miesięcy od dnia wejścia w życie niniejszej ustawy. 5. Przedsiębiorcy telekomunikacyjni, którzy przed dniem wejścia w życie niniejszej ustawy realizowali obowiązki określone w dziale VIIa ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2024 r. poz. 34, 731 i 834), realizują te obowiązki na podstawie dotychczasowych przepisów do czasu rozpoczęcia realizacji obowiązków określonych w rozdziale 3 ustawy zmienianej w art. 1 w brzmieniu nadanym niniejszą ustawą. 6. Podmioty kluczowe lub podmioty ważne, które przed dniem wejścia w życie niniejszej ustawy były operatorami usług kluczowych do czasu wdrożenia systemu zarządzania bezpieczeństwem informacji zgodnego z art. 8 ustawy zmienianej w art. 1 w brzmieniu nadanym niniejszą ustawą stosują system zarządzania bezpieczeństwem informacji zgodny z art. 8 ustawy zmienianej w art. 1 w brzmieniu dotychczasowym.
Art. 21	2. Środki, o których mowa w ust. 1, bazują na podejściu uwzględniającym wszystkie zagrożenia i mającym na celu ochronę sieci i systemów informatycznych oraz środowiska fizycznego tych systemów przed incydentami, i obejmują co najmniej następujące elementy: a) politykę analizy ryzyka i bezpieczeństwa systemów i formacji;	TAK	Art 1 pkt 16 (art. 8 ust. 1 pkt 1 i 2 lit. a)	Art. 8. 1. Podmiot kluczowy lub podmiot ważny wdraża system zarządzania bezpieczeństwem informacji w systemie informacyjnym wykorzystywanym w procesach wpływających na świadczenie usługi przez ten podmiot, zapewniający: 1) prowadzenie systematycznego szacowania ryzyka wystąpienia incydentu oraz zarządzanie tym ryzykiem; 2) wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, uwzględniających najnowszy stan wiedzy, koszty wdrożenia, wielkość podmiotu, prawdopodobieństwo wystąpienia

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				incydentów, narażenie podmiotu na ryzyka, skutki społeczne i gospodarcze, w szczególności: a) polityki szacowania ryzyka oraz bezpieczeństwa systemu informacyjnego, w tym polityki tematyczne,
Art. 21	2. Środki, o których mowa w ust. 1, bazują na podejściu uwzględniającym wszystkie zagrożenia i mającym na celu ochronę sieci i systemów informatycznych oraz środowiska fizycznego tych systemów przed incydentami, i obejmują co najmniej następujące elementy: b) obsługę i wydanie;	TAK	Art 1 pkt 16 (art. 8 ust. 1)	Art. 8. 1. Podmiot kluczowy lub podmiot ważny wdraża system zarządzania bezpieczeństwem informacji w systemie informacyjnym wykorzystywanym w procesach wpływających na świadczenie usługi przez ten podmiot, zapewniający: 4) zarządzanie i wydanie;
Art. 21	2. Środki, o których mowa w ust. 1, bazują na podejściu uwzględniającym wszystkie zagrożenia i mającym na celu ochronę sieci i systemów informatycznych oraz środowiska fizycznego tych systemów przed incydentami, i obejmują co najmniej następujące elementy: c) ciągłość działania, np. zarządzanie kopiami zapasowymi i przywracanie normalnego działania po wystąpieniu sytuacji awaryjnej, i zarządzanie i krytyczność;	TAK	Art 1 pkt 16 (art. 8 ust. 1)	Art. 8. 1. Podmiot kluczowy lub podmiot ważny wdraża system zarządzania bezpieczeństwem informacji w systemie informacyjnym wykorzystywanym w procesach wpływających na świadczenie usługi przez ten podmiot, zapewniający: 2) wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, uwzględniających najnowszy stan wiedzy, koszty wdrożenia, wielkość podmiotu, prawdopodobieństwo wystąpienia incydentów, narażenie podmiotu na ryzyka, skutki społeczne i gospodarcze, w szczególności: f) wdrażanie, dokumentowanie, testowanie i utrzymywanie planów ciągłości działania umożliwiających ciągłe i niezakłócone świadczenie usługi oraz zapewniających poufność, integralność, dostępność i autentyczność informacji, planów awaryjnych oraz planów odtworzenia działalności umożliwiających odtworzenie systemu informacyjnego po zdarzeniu, które spowodowało straty przekraczające zdolności podmiotu do odbudowy za pomocą własnych środków

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

Art. 21	2. Środki, o których mowa w ust. 1, bazują na podejściu uwzględniającym wszystkie zagrożenia i mającym na celu ochronę sieci i systemów informatycznych oraz środowiska fizycznego tych systemów przed incydentami, i obejmują co najmniej następujące elementy: d) bezpieczeństwo łańcucha dostaw, w tym aspekty związane z bezpieczeństwem dotyczące stosunków między każdym podmiotem 1) jego bezpośrednimi doświadczeniami lub usługodawcami;	TAK	Art. 1 pkt 4 (art. 2 lit. 4c) i pkt 16 (art. 8 ust. 1 pkt 4 lit. e)	Art. 2: 4c) dostawca sprzętu lub oprogramowania – producenta, upoważnionego przedstawiciela, importera lub dystrybutora, w rozumieniu odpowiednio art. 2 pkt 3–6 rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 765/2008 z dnia 9 lipca 2008 r. ustanawiającego wymagania w zakresie akredytacji i uchylającego rozporządzenie (EWG) nr 339/93 (Dz. Urz. UE L 218 z 13.08.2008, str. 30, z późn. zm.³⁾), produktu ICT, usługi ICT lub produktu ICT; Art. 8. 1. Podmiot kluczowy lub podmiot ważny wdraża system zarządzania bezpieczeństwem informacji w systemie informacyjnym wykorzystywanym w procesach wpływających na świadczenie usługi przez ten podmiot, zapewniający: 2) wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, uwzględniających najnowszy stan wiedzy, koszty wdrożenia, wielkość podmiotu, prawdopodobieństwo wystąpienia incydentów, narażenie podmiotu na ryzyka, skutki społeczne i gospodarcze, w szczególności: e) bezpieczeństwo i ciągłość łańcucha dostaw produktów ICT, usług ICT i procesów ICT, od których zależy świadczenie usługi, z uwzględnieniem związków pomiędzy bezpośrednim dostawcą sprzętu lub oprogramowania a podmiotem kluczowym lub podmiotem ważnym,

³⁾ Zmiany wymienionego rozporządzenia zostały ogłoszone w Dz. Urz. UE L 169 z 25.06.2019, str. 1.

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

Art. 21	2. Środki, o których mowa w ust. 1, bazują na podejściu uwzględniającym wszystkie zagrożenia i mającym na celu ochronę sieci i systemów informatycznych oraz środowiska fizycznego tych systemów przed incydentami, i obejmują co najmniej następujące elementy: e) bezpieczeństwo w procesie nabywania, rozwoju i utrzymania sieci i systemów informatycznych, w tym postępowanie w przypadku pod	TAK	Art. 1 pkt 16 (art. 8 ust. 1 pkt 2 lit. b i g, pkt 3 i 5)	Art. 8. 1. Podmiot kluczowy lub podmiot ważny wdraża system zarządzania bezpieczeństwem informacji w systemie informacyjnym wykorzystywanym w procesach wpływających na świadczenie usługi przez ten podmiot, zapewniający: 2) wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, uwzględniających najnowszy stan wiedzy, koszty wdrożenia, wielkość podmiotu, prawdopodobieństwo wystąpienia incydentów, narażenie podmiotu na ryzyka, skutki społeczne i gospodarcze, w szczególności: b) bezpieczeństwo w procesie nabywania, rozwoju, utrzymania i eksploatacji systemu informacyjnego, w tym testowanie systemu informacyjnego, g) objęcie systemu informacyjnego wykorzystywanego do świadczenia usługi systemem monitorowania w trybie ciągłym, 3) zbieranie informacji o cyberzagrożeniach i podatnościach na incydenty systemu informacyjnego wykorzystywanego do świ 5) stosowanie środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego wykorzystywanego do świadczenia usługi, w tym: a) stosowanie mechanizmów zapewniających poufność, integralność, dostępność i autentyczność danych przetwarzanych w systemie informacyjnym, b) regularne przeprowadzanie aktualizacji oprogramowania, stosownie do zaleceń producenta, z uwzględnieniem analizy wpływu aktualizacji na bezpieczeństwo świadczonej

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				usługi oraz poziomu krytyczności poszczególnych aktualizacji, c) ochronę przed nieuprawnioną modyfikacją w systemie informacyjnym, d) niezwłoczne podejmowanie działań po dostrzeżeniu podatności lub cyberzagrożeń, w tym również czasowe ograniczenie ruchu sieciowego przychodzącego do infrastruktury podmiotu kluczowego lub podmiotu ważnego, które może skutkować zakłóceniem usług świadczonych przez ten podmiot, mając na uwadze konieczność minimalizacji skutków ograniczenia dostępności tych usług, z uwagi na podjęte działania.
Art. 21	2. Środki, o których mowa w ust. 1, bazują na podejściu uwzględniającym wszystkie zagrożenia i mającym na celu ochronę sieci i systemów informatycznych oraz środowiska fizycznego tych systemów przed incydentami, i obejmują co najmniej następujące elementy: f) polityki i procedury służące ocenie skuteczności środków <u>informatycznych w cyberbezpieczeństwie</u> ;	TAK	Art. 1 pkt 16 (art. 8 ust. 1 pkt 2 lit. h)	Art. 8. 1. Podmiot kluczowy lub podmiot ważny wdraża system zarządzania bezpieczeństwem informacji w systemie informacyjnym wykorzystywanym w procesach wpływających na świadczenie usługi przez ten podmiot, zapewniający: 2) wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, uwzględniających najnowszy stan wiedzy, koszty wdrożenia, wielkość podmiotu, prawdopodobieństwo wystąpienia incydentów, narażenie podmiotu na ryzyka, skutki społeczne i gospodarcze, w szczególności: h) polityki i procedury oceny skuteczności środków technicznych i organizacyjnych,
Art. 21	2. Środki, o których mowa w ust. 1, bazują na podejściu uwzględniającym wszystkie zagrożenia i mającym na celu ochronę sieci i systemów informatycznych oraz środowiska fizycznego tych systemów przed incydentami, i obejmują co najmniej następujące elementy: g) podstawowe praktyki cyberhigieny i szkolenia w zakresie <u>cyberbezpieczeństwa</u> ;	TAK	Art. 1 pkt 16 (art. 8 ust. 1 pkt 2 lit. i oraz j)	Art. 8. 1. Podmiot kluczowy lub podmiot ważny wdraża system zarządzania bezpieczeństwem informacji w systemie informacyjnym wykorzystywanym w procesach wpływających na świadczenie usługi przez ten podmiot, zapewniający:

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				2) wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, uwzględniających najnowszy stan wiedzy, koszty wdrożenia, wielkość podmiotu, prawdopodobieństwo wystąpienia incydentów, narażenie podmiotu na ryzyka, skutki społeczne i gospodarcze, w szczególności: i) edukację z zakresu cyberbezpieczeństwa dla personelu podmiotu, j) podstawowe zasady cyberhigieny.
Art. 21	2. Środki, o których mowa w ust. 1, bazują na podejściu uwzględniającym wszystkie zagrożenia i mającym na celu ochronę sieci i systemów informatycznych oraz środowiska fizycznego tych systemów przed incydentami, i obejmują co najmniej następujące elementy: h) polityki i procedury stosowania kryptografii i, w stosownych przypadkach, szyfrowania;	TAK	Art 1 pkt 16 (art. 8 ust. 1 pkt 2 lit. k)	Art. 8. 1. Podmiot kluczowy lub podmiot ważny wdraża system zarządzania bezpieczeństwem informacji w systemie informacyjnym wykorzystywanym w procesach wpływających na świadczenie usługi przez ten podmiot, zapewniający: 2) wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, uwzględniających najnowszy stan wiedzy, koszty wdrożenia, wielkość podmiotu, prawdopodobieństwo wystąpienia incydentów, narażenie podmiotu na ryzyka, skutki społeczne i gospodarcze, w szczególności: k) polityki i procedury stosowania kryptografii, w tym w stosownych przypadkach szyfrowania,
Art. 21	2. Środki, o których mowa w ust. 1, bazują na podejściu uwzględniającym wszystkie zagrożenia i mającym na celu ochronę sieci i systemów informatycznych oraz środowiska fizycznego tych systemów przed incydentami, i obejmują co najmniej następujące elementy: i) bezpieczeństwo zasobów ludzkich, politykę kontroli dostępu i zarządzania identyfikacją;	TAK	Art. 1 pkt 16 (art. 8 ust. 1 pkt 2 lit. d-n i art. 8f)	Art. 8. 1. Podmiot kluczowy lub podmiot ważny wdraża system zarządzania bezpieczeństwem informacji w systemie informacyjnym wykorzystywanym w procesach wpływających na świadczenie usługi przez ten podmiot, zapewniający: 2) wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, uwzględniających najnowszy stan wiedzy, koszty wdrożenia, wielkość podmiotu, prawdopodobieństwo wystąpienia

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				incydentów, narażenie podmiotu na ryzyka, skutki społeczne i gospodarcze, w szczególności: d) bezpieczeństwo zasobów ludzkich, m) zarządzanie aktywami, □ polityki kontroli dostępu; Art. 8f. 1. Przed rozpoczęciem realizacji zadań, o których mowa w art. 8 lub art. 11, osoba przedstawia podmiotowi kluczowemu lub podmiotowi ważnemu informację o osobie z Krajowego Rejestru Karnego stwierdzającą niekaralność za przestępstwa przeciwko ochronie informacji. Kierownik podmiotu kluczowego lub podmiotu ważnego dopuszcza osobę do realizacji zadań, o których mowa w art. 8 lub art. 11, po otrzymaniu informacji, o której mowa w zdaniu pierwszym. 2. Podmiot kluczowy lub podmiot ważny wzywa osobę realizującą zadania, o których mowa w art. 8 lub art. 11, do ponownego przedstawienia informacji o osobie z Krajowego Rejestru Karnego, jeżeli poweźmie uzasadnione podejrzenie, że osoba ta została skazana za przestępstwo przeciwko ochronie informacji. 3. Wymagania, o których mowa w ust. 1 i 2, uznaje się za spełnione, jeżeli osoba realizująca zadania, o których mowa w art. 8 i art. 11, posiada ważne poświadczenie bezpieczeństwa upoważniające do dostępu do informacji niejawnych o klauzuli „poufne” lub wyższej. 4. Osoba skazana prawomocnym wyrokiem sądu za przestępstwa przeciwko ochronie informacji nie może realizować zadań, o których mowa w art. 8 lub art. 11.

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

Art. 21	2. Środki, o których mowa w ust. 1, bazują na podejściu uwzględniającym wszystkie zagrożenia i mającym na celu ochronę sieci i systemów informatycznych oraz środowiska fizycznego tych systemów przed incydentami, i obejmują co najmniej następujące elementy: j) w stosownych przypadkach – stosowanie uwierzytelniania wieloskładnikowego lub ciągłego, zabezpieczonych połączeń głosowych, tekstowych i wideo oraz zabezpieczonych systemów łączności wewnątrz podmiotu w sytuacjach nadzwyczajnych.	TAK	Art. 1 pkt 16 (art. 8 ust. 1 pkt 2 lit. 1)	Art. 8. 1. Podmiot kluczowy lub podmiot ważny wdraża system zarządzania bezpieczeństwem informacji w systemie informacyjnym wykorzystywanym w procesach wpływających na świadczenie usługi przez ten podmiot, zapewniający: 2) wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, uwzględniających najnowszy stan wiedzy, koszty wdrożenia, wielkość podmiotu, prawdopodobieństwo wystąpienia incydentów, narażenie podmiotu na ryzyka, skutki społeczne i gospodarcze, w szczególności: 1) stosowanie bezpiecznych środków komunikacji elektronicznej w ramach krajowego systemu cyberbezpieczeństwa oraz wewnątrz podmiotu, uwzględniających uwierzytelnianie wieloskładnikowe w towarach i usługach; 2) wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, uwzględniających najnowszy stan wiedzy, koszty wdrożenia, wielkość podmiotu, prawdopodobieństwo wystąpienia incydentów, narażenie podmiotu na ryzyka, skutki społeczne i gospodarcze, w szczególności: 1) stosowanie bezpiecznych środków komunikacji elektronicznej w ramach krajowego systemu cyberbezpieczeństwa oraz wewnątrz podmiotu, uwzględniających uwierzytelnianie wieloskładnikowe w towarach i usługach;
Art. 21	3. Państwa członkowskie zapewniają, aby rozważając które ze środków, o których mowa w ust. 2 lit. d) niniejszego artykułu, są odpowiednie, podmioty uwzględniały podatności charakterystyczne dla każdego bezpośredniego dostawcy i usługodawcy oraz ogólną jakość produktów i praktyk cyberbezpieczeństwa dostawców i usługodawców, w tym ich procedury bezpiecznego opracowywania. Państwa członkowskie zapewniają również, aby rozważając, które ze środków, o których mowa w tej literze, są odpowiednie, podmioty musiały uwzględniać wyniki skoordynowanych oszacowań ryzyka dla bezpieczeństwa krytycznych łańcuchów dostaw przeprowadzonych zgodnie z art. 22 ust. 1.	TAK	Art. 1 pkt 16 (art. 8 ust. 2)	Art. 8. 2. Wdrażając środki, o których mowa w ust. 1 pkt 2 lit. e, podmiot kluczowy lub podmiot ważny uwzględnia: 1) podatności związane z dostawcą sprzętu lub oprogramowania; 2) ogólną jakość produktów ICT, usług ICT i procesów ICT pochodzących od dostawcy sprzętu lub oprogramowania; 3) wyniki skoordynowanej oceny bezpieczeństwa przeprowadzonej przez Grupę współpracy, o której mowa w art. 22 ust. 1 dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniającej rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającą dyrektywę (UE) 2016/1148 (dyrektywa NIS 2)

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				(Dz. Urz. UE L 333 z 27.12.2022, str. 80), zwanej dalej „dyrektywą 2022/2555”; 4) wyniki postępowania, o którym mowa w art. 67b.
Art. 21	4. Państwa członkowskie zapewniają, aby podmiot, który stwierdzi, że nie spełnia środków określonych w ust. 2, bez zbędnej zwłoki wprowadził wszelkie istotne, odpowiednie i proporcjonalne środki naprawcze.	NIE		Z uwagi na inne przepisy dotyczące różnych środków nadzoru nie ma potrzeby wdrożenia tego przepisu.
Art. 21	5. Do 17 października 2024 r. Komisja przyjmuje akty wykonawcze określające wymogi techniczne i metodykę dotyczącą środków, o których mowa w ust. 2, w odniesieniu do dostawców usług DNS, rejestrów nazw TLD, dostawców usług chmurowych, dostawców usług ośrodka przetwarzania danych, dostawców sieci dostarczania treści, dostawców usług zarządzanych, dostawców usług zarządzanych w zakresie bezpieczeństwa, dostawców internetowych platform handlowych, wyszukiwarek internetowych oraz platform sieci społecznościowych i dostawców usług zaufania. Komisja może przyjąć akty wykonawcze określające wymogi techniczne i metodykę, a w razie potrzeby również wymogi sektorowe dotyczące środków, o których mowa w ust. 2, w odniesieniu do podmiotów kluczowych i ważnych innych niż te, o których mowa w akapicie pierwszym niniejszego ustępu. Przygotowując akty wykonawcze, o których mowa w akapitach pierwszym i drugim niniejszego ustępu, Komisja na tyle, na ile to możliwe stosuje się do norm międzynarodowych i europejskich, a także odpowiednich specyfikacji technicznych. Komisja wymienia się poradami i wraz z Grupą Współpracy i ENISA współpracuje nad projektami aktów wykonawczych zgodnie z art. 14 ust. 4 lit. e). Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 39 ust. 2.	TAK	Art. 1 pkt 17 (art. 8b ust. 1 i 2)	Art. 8b. 1. Dostawcy usług DNS, rejestry nazw domen najwyższego poziomu (TLD), dostawcy usług chmurowych, dostawcy usługi centrum przetwarzania danych, dostawcy sieci dostarczania treści, dostawcy usług zarządzanych, dostawcy usług zarządzanych w zakresie cyberbezpieczeństwa, dostawcy internetowych platform handlowych, dostawcy wyszukiwarek internetowych oraz dostawcy platform usług sieci społecznościowych stosują, w ramach systemu, o którym mowa w art. 8 ust. 1 środki zarządzania ryzykiem określone w rozporządzeniu wykonawczym Komisji (UE) 2024/2690 z dnia 17 października 2024 r. ustanawiającym zasady stosowania dyrektywy (UE) 2022/2555 w odniesieniu do wymogów technicznych i metodycznych dotyczących środków zarządzania ryzykiem w cyberbezpieczeństwie oraz doprecyzowujące przypadki, w których incydent uznaje się za poważny w odniesieniu do dostawców usług DNS, rejestrów nazw TLD, dostawców usług chmurowych, dostawców usług ośrodka przetwarzania danych, dostawców sieci dostarczania treści, dostawców usług zarządzanych, dostawców usług zarządzanych w zakresie bezpieczeństwa, dostawców internetowych platform handlowych, wyszukiwarek internetowych i platform usług

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				sieci społecznościowych oraz dostawców usług zaufania (Dz. Urz. UE L 2024/2690 z 18.10.2024). 2. W ramach systemu, o którym mowa w art. 8 ust. 1, podmioty kluczowe lub podmioty ważne, inne niż określone w ust. 1, stosują środki zarządzania ryzykiem dla danego rodzaju podmiotu określone w aktach wykonawczych Komisji Europejskiej, wydanych na podstawie art. 21 ust. 5 dyrektywy 2022/2555.
Art. 22	Artykuł 22 Skoordynowane na poziomie Unii szacowanie ryzyka krytycznych łańcuchów dostaw 1. Grupa Współpracy we współpracy z Komisją i ENISA może przeprowadzać skoordynowane szacowanie ryzyka dla bezpieczeństwa określonych krytycznych łańcuchów dostaw usług ICT, systemów ICT lub produktów ICT, z uwzględnieniem technicznych i, w stosownych przypadkach, pozatechnicznych czynników ryzyka. 2. Po konsultacji z Grupą Współpracy i ENISA oraz w razie potrzeby z odpowiednimi zainteresowanymi stronami Komisja wskazuje konkretne krytyczne usługi ICT, systemy ICT lub produkty ICT, które można poddać skoordynowanemu oszacowaniu ryzyka dla bezpieczeństwa, o którym mowa w ust. 1.	NIE		
Art. 23	Artykuł 23 Obowiązki w zakresie zgłaszania incydentów 1. Każde państwo członkowskie zapewnia, aby podmioty kluczowe i ważne bez zbędnej zwłoki zgłaszały swojemu właściwemu CSIRT lub, jeżeli ma to zastosowanie, swojemu właściwemu organowi, zgodnie z ust. 4, incydent mający istotny wpływ na świadczenie przez nie usług, o którym mowa w ust. 3 (poważny incydent). W stosownych przypadkach dane podmioty bez zbędnej zwłoki powiadamiają odbiorców swoich usług o poważnych incydentach, które mogą mieć niekorzystny wpływ na świadczenie tych usług. Każde państwo członkowskie zapewnia, aby podmioty te zgłaszały m.in. informacje umożliwiające CSIRT lub, jeżeli ma to	TAK	Art. 1 pkt 19 (art. 11), pkt 30 (art. 28) i pkt 33 (art. 31)	Art. 11: a) w ust. 1: – wprowadzenie do wyliczenia otrzymuje brzmienie: „Podmiot kluczowy lub podmiot ważny:”, – pkt 5 otrzymuje brzmienie: „5) współdziała podczas obsługi incydentu poważnego i incydentu krytycznego z właściwym CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT sektorowym, przekazując niezbędne dane, w tym d[]o[]obow[]”, e) uchyla się ust. 3,

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

	zastosowanie, właściwemu organowi ustalenie transgranicznego wpływu incydentu. Samo zgłoszenie nie nakłada na podmiot zgłaszający zwiększonej odpowiedzialności. Jeżeli dane podmioty zgłoszą poważny incydent właściwemu organowi na podstawie akapitu pierwszego, państwo członkowskie zapewnia, aby ten właściwy organ po otrzymaniu zgłoszenia przekazał je CSIRT. W razie wystąpienia transgranicznego lub międzysektorowego poważnego incydentu państwa członkowskie zapewniają, aby ich pojedyncze punkty kontaktowe w stosownym czasie otrzymały ważne informacje zgłoszone zgodnie z ust. 4.			Art. 28: a) w ust. 1 wyrazy „operatora usługi kluczowej” zastępuje się wyrazami „podmiot kluczowy lub podmiot ważny”, b) w ust. 2 wyrazy „operatorowi usługi kluczowej” zastępuje się wyrazami „podmiotowi kluczowemu lub podmiotowi węższemu”; Art. 31. 1. CSIRT MON, CSIRT NASK, CSIRT GOV oraz CSIRT sektorowe określają sposób przekazywania informacji i zgłoszeń, o których mowa w art. 11 i w art. 13, w przypadku braku możliwości przekazania ich za pomocą systemu teleinformatycznego, o którym mowa w art. 46 ust 1. 2. CSIRT NASK określi sposób dokonywania zgłoszeń, o których mowa w art. 30 ust. 1. 3. Komunikat zawierający informacje o sposobie dokonywania zgłoszeń, o których mowa odpowiednio w art. 11, art. 13 i art. 30 ust. 1, CSIRT MON, CSIRT NASK, CSIRT GOV oraz CSIRT sektorowe publikuje odpowiednio na stronie podmiotowej Biuletynu Informacji Publicznej Ministra Obrony Narodowej, Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego, Agencji Bezpieczeństwa Wewnętrznego lub organu właściwego do spraw cyberbezpieczeństwa.
Art. 23	2. Jeżeli ma to zastosowanie, państwa członkowskie zapewniają, aby podmioty kluczowe i ważne bez zbędnej zwłoki powiadamiały odbiorców swoich usług, których potencjalnie dotyczy poważne cyberzagrożenie, o środkach zaradczych lub innych środkach, które ci odbiorcy mogą zastosować w reakcji na to zagrożenie. W stosownych przypadkach podmioty te informują również tych odbiorców o samym poważnym cyberzagrożeniu.	TAK	Art. 1 pkt 19 (art. 11 ust. 2a)	Art. 11. 2a. W przypadku zaistnienia poważnego cyberzagrożenia podmiot kluczowy lub podmiot ważny informuje użytkowników swoich usług, na których takie cyberzagrożenie może mieć wpływ, o możliwych środkach zapobiegawczych, które użytkownicy ci mogą podjąć. Podmiot kluczowy lub podmiot ważny informuje tych użytkowników o samym poważnym cyberzagrożeniu, jeżeli nie

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				spowoduje to zwiększenia poziomu ryzyka dla bezpieczeństwa systemów informacyjnych. 2b. Podmiot kluczowy lub podmiot ważny informuje użytkowników swoich usług o incydencie poważnym, jeżeli ma on niekorzystny wpływ na świadczenie tych usług..”
Art. 23	3. Incydent uznaje się za poważny, jeżeli: a) spowodował lub może spowodować dotkliwe zakłócenia operacyjności usług lub trwały finansowy dla danego podmiotu; b) wpłynął lub jest w stanie wpłynąć na inne osoby fizyczne lub prawne, powodując znaczne szkody majątkowe i niemajątkowe.	TAK	Art. 1 pkt 4 (art. 2 pkt 7)	Art. 2: „7) incydent poważny – incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi przez podmiot kluczowy lub podmiot ważny, straty finansowe dla tego podmiotu lub wpływa na inne osoby fizyczne, osoby prawne, jednostki organizacyjne nieposiadające osobowości prawnej poprzez wywołanie poważnej szkody materialnej lub imaterialnej;
Art. 23	4. Państwa członkowskie zapewniają, aby do celów zgłoszenia na podstawie ust. 1 dane podmioty przedkładały CSIRT lub, jeżeli ma to zastosowanie, właściwemu organowi: a) bez zbędnej zwłoki, a w każdym razie w ciągu 24 godzin od powzięcia wiedzy o poważnym incydencie – wczesne ostrzeżenie, w którym w stosownych przypadkach wskazuje się, czy poważny incydent został przypuszczalnie wywołany działaniem bezprawnym lub działaniem w złym zamiarze lub czy mógł wywrzeć wpływ trwały; b) bez zbędnej zwłoki, a w każdym razie w ciągu 72 godzin od powzięcia wiedzy o poważnym incydencie – zgłoszenie incyduentu, w stosownych przypadkach z aktualizacją informacji, o których mowa w lit. a), i wskazaniem wstępnej oceny poważnego incyduentu, w tym jego dotkliwości i skutków, a w stosownych przypadkach także wskazówek i informacji o jego skutkach; c) na wniosek CSIRT lub, jeżeli ma to zastosowanie, właściwego organu – sprawozdanie okresowe na temat odpowiednich skutków i skutku; d) sprawozdanie końcowe nie później niż miesiąc po zgłoszeniu incyduentu na podstawie lit. b), zawierające następujące elementy:	TAK	Art. 1 pkt 19-21 (art. 11 ust 1 i 2, art. 12, art. 12a-art. 12c)	Art. 11: a) w ust. 1: – wprowadzenie do wyliczenia otrzymuje brzmienie: „Podmiot kluczowy lub podmiot ważny:”, – pkt 2 otrzymuje brzmienie: „2) zapewnia dostęp do informacji o rejestrowanych incydentach właściwemu CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT sektorowemu w zakresie niezbędnym do realizacji jego zadań;”, – pkt 4 otrzymuje brzmienie: „4) zgłasza wczesne ostrzeżenie o incydencie poważnym niezwłocznie, nie później niż w ciągu 24 godzin od momentu jego wykrycia, do właściwego CSIRT sektorowego;”, – po pkt 4 dodaje się pkt 4a–4c w brzmieniu: „4a) zgłasza incydent poważny niezwłocznie, nie później niż w ciągu 72 godzin od momentu jego wykrycia, do właściwego CSIRT sektorowego;

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

	(i) ogólny opis incydentu, w tym jego dotkliwość i skutków; (ii) rodzaj zagrożenia lub pierwotną przyczynę, która prawdopodobnie była źródłem incydentu; (iii) tożsamość i wdrożone środki ograniczające ryzyko; (iv) w toku wykonywania pracy przez pracowników tego skutki incydentu; e) jeżeli incydent nie zakończył się w terminie składania sprawozdania końcowego, o którym mowa w lit. d), państwa członkowskie zapewniają, aby zainteresowane podmioty przedstawiły w tym momencie sprawozdanie z postępu prac, a sprawozdanie końcowe – w ciągu miesiąca od zakończenia przez nich obsługi incydentu. Na zasadzie odstępstwa od akapitu pierwszego lit. b) dostawca usług zaufania zgłasza poważne incydenty, które mają wpływ na świadczenie jego usług zaufania CSIRT lub, w stosownych przypadkach, właściwemu organowi, bez zbędnej zwłoki, a w każdym razie w ciągu 24 godzin od powzięcia informacji o takim poważnym incydencie.			4b) przekazuje, na wniosek właściwego CSIRT sektorowego, sprawozdanie okresowe z obsługi incydentu powziętego; 4c) przekazuje właściwemu CSIRT sektorowemu sprawozdanie końcowe z obsługi incydentu poważnego, nie później niż w ciągu miesiąca od daty zgłoszenia, o którym mowa w pkt 4; b) po ust. 1 dodaje się ust. 1a w brzmieniu: „1a. Dostawca usług zaufania zgłasza incydent poważny niezwłocznie, nie później niż w ciągu 24 godzin od momentu jego wykrycia do właściwego CSIRT sektorowego.”; c) ust. 2 otrzymuje brzmienie: „2. Wczesne ostrzeżenie, o którym mowa w ust. 1 pkt 4, zgłoszenie, o którym mowa w ust. 1 pkt 4a, sprawozdanie okresowe, o którym mowa w ust. 1 pkt 4b, sprawozdanie końcowe, o którym mowa w ust. 1 pkt 4c oraz sprawozdanie z postępu obsługi incydentu poważnego, o którym mowa w art. 12b ust. 1, są przekazywane za pomocą systemu teleinformatycznego, o którym mowa w art. 46 ust. 1.”; Art. 12. 1. Wczesne ostrzeżenie, o którym mowa w art. 11 ust. 1 pkt 4, zawiera: 1) dane podmiotu zgłaszającego, w tym firmę przedsiębiorcy, numer z właściwego rejestru, adres i adres; 2) imię i nazwisko, numer telefonu służbowego oraz adres służbowej poczty elektronicznej osoby uprawnionej do składania informacji; 3) imię i nazwisko, numer telefonu służbowego oraz adres służbowej poczty elektronicznej osoby uprawnionej do składania informacji;

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				4) wskazanie momentu wystąpienia i wykrycia incydentu poważnego oraz czas jego trwania; 5) wskazanie, czy incydent poważny został wywołany działaniem bezprawnym lub działaniem w złej wierze, jeżeli możliwe jest dokończenie opisu; 6) określenie, czy incydent dotyczy innych państw członkowskich Unii Europejskiej. 2. Wczesne ostrzeżenie, o którym mowa w art. 11 ust. 1 pkt 4, może zawierać wniosek o wskazanie wytycznych dotyczących możliwych do wdrożenia środków ograniczających skutki incydentu poważnego lub o dodatkowe wsparcie techniczne przy obsłudze incydentu. CSIRT sektorowy nie później niż w ciągu 24 godzin przekazuje podmiotowi zgłaszającemu wytyczne dotyczące wdrożenia środków lub udziela dodatkowego wsparcia technicznego, a w przypadku incydentu poważnego wyczerpującego znamiona przestępstwa również informacje o sposobie zgłoszenia organom ścigania. 3. Zgłoszenie, o którym mowa w art. 11 ust. 1 pkt 4a, zawiera: 1) opis wpływu incydentu poważnego na świadczenie usługi, w tym: a) wskazanie usługi zgłaszającego, na które incydent poważny miał wpływ, b) liczbę użytkowników usługi, na których incydent poważny miał wpływ, c) zasięg geograficzny obszaru, którego dotyczy incydent poważny, d) wpływ incydentu poważnego na świadczenie usługi przez podmioty; 2) opis przyczyn tego incydentu, sposób jego przebiegu oraz prawdopodobne skutki

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				oddziaływania na systemy informacyjne lub świadczenia usług; 3) informacje o podjętych działaniach naprawczych; 4) informacje o podjętych działaniach prewencyjnych; 5) aktualizację informacji, o których mowa w ust. 1, jeżeli nastąpiła ich zmiana. 4. Zgłoszenie, o którym mowa w art. 11 ust. 1 pkt 4a, może zawierać także inne istotne informacje związane z przebiegiem incydentu poważnego lub podjętymi działaniami. 5. Podmiot kluczowy lub podmiot ważny przekazuje informacje znane mu w chwili dokonywania zgłoszenia, o którym mowa w art. 11 ust. 1 pkt 4a, które uzupełnia w trakcie obsługi incydentu poważnego. 6. Podmiot kluczowy lub podmiot ważny przekazuje, w niezbędnym zakresie, we wczesnym ostrzeżeniu, o którym mowa w art. 11 ust. 1 pkt 4, lub zgłoszeniu, o którym mowa w art. 11 ust. 1 pkt 4a, informacje stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa, gdy jest to konieczne do realizacji zadań właściwego CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT sektorowego. 7. Właściwy CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT sektorowy może zwrócić się do podmiotu kluczowego lub podmiotu ważnego o uzupełnienie wczesnego ostrzeżenia, o którym mowa w art. 11 ust. 1 pkt 4, lub zgłoszenia, o którym mowa w art. 11 ust. 1 pkt 4a, o informacje, w tym informacje stanowiące tajemnice prawnie chronione, w zakresie niezbędnym do realizacji zadań, o których mowa w ustawie.

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				8. We wczesnym ostrzeżeniu, o którym mowa w art. 11 ust. 1 pkt 4, lub w zgłoszeniu, o którym mowa w art. 11 ust. 1 pkt 4a, podmiot kluczowy lub podmiot ważny oznacza informacje stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa. Art. 12a. Sprawozdanie końcowe, o którym mowa w art. 11 ust. 1 pkt 4c, zawiera: 1) szczegółowy opis incydentu poważnego, w tym powodów i skutków; 2) rodzaj zagrożenia lub przyczynę, która prawdopodobnie była źródłem incydentu; 3) zastosowane i wdrażane środki ograniczające ryzyko; 4) w odpowiednich przypadkach transgraniczne skutki incydentu. Art. 12b. 1. W przypadku gdy obsługa incydentu poważnego nie zakończyła się w terminie składania sprawozdania końcowego, o którym mowa w art. 11 ust. 1 pkt 4c, podmiot kluczowy lub podmiot ważny przekazuje właściwemu CSIRT sektorowemu sprawozdanie z postępu obsługi tego incydentu. 2. W przypadku gdy obsługa incydentu poważnego nie zakończyła się w terminie składania sprawozdania końcowego, o którym mowa w art. 11 ust. 1 pkt 4c, podmiot kluczowy lub podmiot ważny przekazuje właściwemu CSIRT sektorowemu sprawozdanie końcowe nie później niż w ciągu miesiąca od zakończenia obsługi incydentu poważnego. Art. 12c. Do podmiotu ważnego będącego podmiotem publicznym stosuje się przepisy art. 11–12 z wyjątkiem przepisów o przekazywaniu wczesnego ostrzeżenia, sprawozdania

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				okresowego, sprawozdania z postępu obsługi incydentu i sprawozdania końcowego.
Art. 23	5. CSIRT lub właściwy organ bez zbędnej zwłoki i w miarę możliwości w ciągu 24 godzin od otrzymania wczesnego ostrzeżenia, o którym mowa w ust. 4 lit. a), odpowiada podmiotowi zgłaszającemu, w tym przekazuje mu wstępne informacje zwrotne na temat poważnego incydentu oraz, na wniosek podmiotu, wytyczne lub porady operacyjne dotyczące wdrożenia możliwych środków ograniczających ryzyko. Jeżeli CSIRT nie jest pierwszym odbiorcą zgłoszenia, o którym mowa w ust. 1, wytyczne przedstawia właściwy organ we współpracy z CSIRT. Na wniosek zainteresowanego podmiotu CSIRT zapewnia dodatkowe wsparcie techniczne. Jeżeli zachodzi podejrzenie, że poważny incydent ma cechy przestępstwa, CSIRT lub właściwy organ przedstawia również wytyczne dotyczące zgłaszania poważnego incydentu organom ścigania.	TAK	Art. 1 pkt 33 (art. 32)	Art. 32. 1. CSIRT MON, CSIRT NASK i CSIRT GOV mogą wykonywać niezbędne działania techniczne związane z analizą zagrożeń, koordynacją obsługi incydentu poważnego i incydentu krytycznego. 2. CSIRT MON, CSIRT NASK lub CSIRT GOV może wystąpić do organu właściwego do spraw cyberbezpieczeństwa z wnioskiem o wezwanie podmiotu kluczowego lub podmiotu ważnego, aby w wyznaczonym terminie usunął podatności, które doprowadziły lub mogłyby doprowadzić do incydentu poważnego lub krytycznego. 3. Podmiot kluczowy lub podmiot ważny na wniosek CSIRT MON, CSIRT NASK lub CSIRT GOV udostępnia informacje techniczne związane z incydentem, które będą niezbędne do przeprowadzenia analizy lub koordynacji obsługi incydentu. 4. CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT sektorowe na podstawie informacji, o których mowa w art. 13 ust. 1 pkt 3 i 5, uzyskanych od podmiotu kluczowego lub podmiotu ważnego, mogą przekazywać im informacje o podatnościach i sposobie usunięcia podatności w wykorzystywanych technologiach.”;
Art. 23	6. W stosownych przypadkach, zwłaszcza gdy poważny incydent dotyczy co najmniej dwóch państw członkowskich, CSIRT, właściwy organ lub pojedynczy punkt kontaktowy bez zbędnej zwłoki informują o tym poważnym incydencie pozostałe państwa członkowskie, których on dotyczy, i ENISA. Takie informacje obejmują informacje otrzymane zgodnie z ust. 4. W działaniach tych CSIRT, właściwy organ lub pojedynczy punkt kontaktowy zgodnie z prawem Unii lub prawem krajowym chronią bezpieczeństwo i	TAK	Art. 1 pkt 28 (art. 26 ust. 3 pkt 11)	Art. 26. 3: „11) przekazywanie do innych państw, w tym państw członkowskich Unii Europejskiej, i przyjmowanie z tych państw informacji o incydentach poważnych dotyczących dwóch lub większej liczby państw członkowskich, a także przekazywanie do Pojedynczego Punktu Kontaktowego zgłoszenia incydentu poważnego

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

	interesy handlowe podmiotu oraz poufność przekazanych informacji.			dotyczącego dwóch lub większej liczby państw członkowskich Unii Europejskiej;
Art. 23	7. Jeżeli świadomość społeczeństwa jest niezbędna, żeby zapobiec wystąpieniu poważnego incydentu lub poradzić sobie z trwającym poważnym incydem, lub jeżeli ujawnienie poważnego incydentu z innych względów leży w interesie publicznym, CSIRT państwa członkowskiego lub, jeżeli ma to zastosowanie, jego właściwy organ, a w stosownych przypadkach CSIRT lub właściwe organy innych zainteresowanych państw członkowskich mogą, po konsultacji z zainteresowanym podmiotem, poinformować społeczeństwo o poważnym incydencie lub zobowiązać do tego ten podmiot.	TAK	Art. 1 pkt 40 (art. 37 ust. 2-4)	Art. 37. 2. Właściwy CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT sektorowy może, po konsultacji ze zgłaszającym podmiotem kluczowym lub podmiotem ważnym, opublikować na stronie podmiotowej Biuletynu Informacji Publicznej odpowiednio Ministra Obrony Narodowej, Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego, Agencji Bezpieczeństwa Wewnętrznego lub organu właściwego do spraw cyberbezpieczeństwa informacje o incydentach poważnych, gdy jest to niezbędne, aby zapobiec wystąpieniu incydentu albo zapewnić obsługę incydentu.”, c) uchyla się ust. 3, d) w ust. 4 kręśli się wyraz „i 3”;
Art. 23	8. Na wniosek CSIRT lub właściwego organu pojedynczy punkt kontaktowy przekazuje zgłoszenia otrzymane zgodnie z ust. 1 pojedynczym punktom kontaktowym w innych państwach członkowskich, których dotyczy incydent.	TAK	Art. 1 pkt 56 (art. 48 pkt 2)	Art. 48: 2) przekazywanie, na wniosek właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV, zgłoszenia incydentu dotyczącego więcej niż jednego sektora lub innych państw członkowskich Unii Europejskiej do Pojedynczych Punktów Kontaktowych w innych państwach członkowskich Unii Europejskiej”;
Art. 23	9. Pojedynczy punkt kontaktowy co trzy miesiące przedkłada ENISA sprawozdanie podsumowujące zawierające zanonimizowane i zagregowane dane o poważnych incydentach, incydentach, cyberzagrożeniach i potencjalnych zdarzeniach dla cyberbezpieczeństwa zgłoszonych zgodnie z ust. 1 niniejszego artykułu oraz art. 30. Aby przyczynić się do dostarczania porównywalnych informacji, ENISA może przyjąć wytyczne techniczne dotyczące parametrów informacji, jakie należy zawrzeć w sprawozdaniu podsumowującym. Co sześć miesięcy ENISA	TAK	Art. 1 pkt 57 (art. 49 ust. 6)	Art. 49. 6. Pojedynczy punkt kontaktowy, co trzy miesiące, przedkłada ENISA sprawozdanie podsumowujące zawierające dane o: 1) powziętych i wydatkach; 2) incydentach; 3) cyberzagrożeniach; 4) potencjalnych zdarzeniach dla cyberbezpieczeństwa.

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

	informuje Grupę Współpracy i sieć CSIRT o ustaleniach wynikających z otrzymanych zgłoszeń.			
Art. 23	10. CSIRT lub, w stosownych przypadkach, właściwe organy przekazują właściwym organom zgodnie z dyrektywą (UE) 2022/2557 informacje o poważnych incydentach, incydentach, cyberzagrożeniach i potencjalnych zdarzeniach dla cyberbezpieczeństwa zgłoszonych zgodnie z ust. 1 niniejszego artykułu i z art. 30 przez podmioty wskazane jako podmioty krytyczne na mocy dyrektywy (UE) 2022/2557.	TAK	Art. 1 pkt 28 (art. 26 ust. 16)	Art. 26. 16. CSIRT MON, CSIRT NASK i CSIRT informują organ właściwy do spraw podmiotów krytycznych o poważnych incydentach, cyberzagrożeniach i potencjalnych zdarzeniach dla cyberbezpieczeństwa zgłoszonych przez podmiot krytyczny.
Art. 24	Artykuł 24 Stosowanie europejskich programów certyfikacji cyberbezpieczeństwa 1. Aby wykazać zgodność ze szczególnymi wymogami art. 21, państwa członkowskie mogą wymagać od podmiotów kluczowych i ważnych stosowania konkretnych produktów ICT, usług ICT i procesów ICT opracowanych przez dany podmiot kluczowy lub ważny lub nabytych od osób trzecich, certyfikowanych zgodnie z europejskimi programami certyfikacji cyberbezpieczeństwa przyjętymi na podstawie art. 49 rozporządzenia (UE) 2019/881. Ponadto państwa członkowskie zachęcają podmioty kluczowe i ważne do korzystania z kwalifikowanych usług zaufania. 2. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 38 w celu uzupełnienia niniejszej dyrektywy przez określenie, od których kategorii podmiotów kluczowych i ważnych należy wymagać stosowania certyfikowanych produktów ICT, usług ICT i procesów ICT lub uzyskania certyfikacji dla swoich własnych produktów ICT, usług ICT i procesów ICT na podstawie europejskiego programu certyfikacji cyberbezpieczeństwa przyjętego zgodnie z art. 49 rozporządzenia (UE) 2019/881. Te akty delegowane przyjmuje się w razie stwierdzenia niewystarczających poziomów cyberbezpieczeństwa i określa się w nich termin wdrażania. Przed przyjęciem takich aktów delegowanych Komisja przeprowadza ocenę skutków i prowadzi konsultacje zgodnie z art. 56 rozporządzenia (UE) 2019/881.	NIE		

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

	3. Jeżeli do celów ust. 2 żaden z europejskich programów certyfikacji cyberbezpieczeństwa nie jest odpowiedni, Komisja może – po zasięgnięciu opinii Grupy Współpracy i Europejskiej Grupy ds. Certyfikacji Cyberbezpieczeństwa – zwrócić się do ENISA o przygotowanie propozycji programu zgodnie z art. 48 ust. 2 rozporządzenia (UE) 2019/881.			
Art. 25	Artykuł 25 Normalizacja 1. Aby wspierać spójne wdrażanie art. 21 ust. 1 i 2, państwa członkowskie, nie narzucając ani nie faworyzując stosowania określonego rodzaju technologii, zachęcają do stosowania europejskich i międzynarodowych norm i specyfikacji technicznych istotnych z punktu widzenia bezpieczeństwa sieci i systemów informatycznych.	TAK	Art. 1 pkt 50 (art. 45 ust. 1 pkt 7 i 8, ust. 3-5)	Art. 45. 1: 7) rekomendowanie i wspieranie przy wykorzystywaniu europejskich lub międzynarodowych standardów, a także specyfikacji technicznych mających znaczenie dla bezpieczeństwa i formacji; 8) zachęcanie do korzystania z produktów ICT, usług ICT i procesów ICT certyfikowanych w ramach europejskich lub krajowych programów certyfikacji cyberbezpieczeństwa; 3. Minister właściwy do spraw informatyzacji może opublikować na swojej stronie podmiotowej Biuletynu Informacji Publicznej zestawienie wymogów dokumentów normalizacyjnych, o których mowa w art. 2 pkt 3 ustawy z dnia 12 września 2002 r. o normalizacji (Dz. U. z 2015 r. poz. 1483), których wykonywanie realizuje obowiązki wynikające z przepisów ustawy oraz z przepisów wydanych na podstawie art. 8a. 4. Projekt zestawienia, o którym mowa w ust. 3, minister właściwy do spraw informatyzacji kieruje do 30-dniowych konsultacji publicznych, z których sporządza raport, w którym wskazuje główne tezy zawarte w stanowiskach zgłoszonych do projektu zestawienia oraz odniesienie się do nich. 5. Projekt zestawienia, o którym mowa w ust. 3, uwagi zgłoszone w ramach konsultacji publicznych oraz raport ministra właściwego do

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				spraw informatyzacji publikuje się na stronie podmiotowej Biuletynu Informacji Publicznej ministra właściwego do spraw informatyzacji, z wyłączeniem danych osobowych osób fizycznych biorących udział w konsultacjach publicznych.
Art. 25	2. ENISA we współpracy z państwami członkowskimi i – w stosownych przypadkach – po zasięgnięciu opinii odpowiednich zainteresowanych stron opracowuje porady i wytyczne dotyczące obszarów technicznych, które należy wziąć pod uwagę w związku z ust.1, a także już istniejących norm, w tym norm krajowych, które pozwoliłyby uwzględnić te obszary.	NIE		
Art. 26	Artykuł 26 Jurysdykcja i terytorialność 1. Podmioty objęte zakresem stosowania niniejszej dyrektywy uznaje się za podlegające jurysdykcji państwa członkowskiego, w którym mają miejsce prowadzenia działalności, z następującymi wyjątkami: a) dostawców publicznych sieci łączności elektronicznej lub dostawców publicznie dostępnych usług łączności elektronicznej uznaje się za podlegających jurysdykcji państwa członkowskiego, w którym świadcą usługi; b) dostawców usług DNS, rejestry nazw TLD, podmioty świadczące usługi rejestracji nazw domen, dostawców usług chmurowych, dostawców usług ośrodka przetwarzania danych, dostawców sieci dostarczania treści, dostawców usług zarządzanych, dostawców usług zarządzanych w zakresie bezpieczeństwa, a także dostawców internetowych platform handlowych, wyszukiwarek internetowych lub platform usług sieci społecznościowych uznaje się za podlegających jurysdykcji państwa członkowskiego, w której mają główne miejsce prowadzenia działalności w Unii zgodnie z art. 2; c) podmioty administracji publicznej uznaje się za podlegające jurysdykcji państwa członkowskiego, które je ustanowiło.	TAK	Art. 1 pkt 11 (art. 5a ust. 1, 2 i 10)	Art. 5a. 1. Podmiot kluczowy lub podmiot ważny podlega obowiązkom wynikającym z ustawy, jeżeli mają miejsce zamieszkania na terytorium Rzeczypospolitej Polskiej lub prowadzą działalność na terytorium Rzeczypospolitej Polskiej przez swoje siedziby, oddziały lub w ramach działalności transgranicznej. 2. Przedsiębiorca komunikacji elektronicznej podlega obowiązkom wynikającym z ustawy, jeżeli świadczy usługi na terytorium Rzeczypospolitej Polskiej. 10. Ustawę stosuje się do podmiotów publicznych niezależnie od miejsca ich siedziby.
Art. 26	2. Do celów niniejszej dyrektywy uznaje się, że podmiot, o którym mowa w ust. 1 lit. b), ma swoje główne miejsce prowadzenia działalności w Unii w tym państwie członkowskim, w którym przeważnie podejmuje decyzje związane ze środkami zarządzania	TAK	Art. 1 pkt 11 (art. 5a ust. 3-6)	Art. 5a. 3. Dostawca usług DNS, rejestr nazw domen najwyższego poziomu (TLD), podmiot świadczący usługi rejestracji nazw domen, dostawca chmury obliczeniowej, dostawca usługi

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

	ryzykiem w cyberbezpieczeństwie. Jeżeli nie można ustalić takiego państwa członkowskiego lub jeżeli takich decyzji nie podejmuje się w Unii, uznaje się, że główne miejsce prowadzenia działalności znajduje się w państwie członkowskim, w którym prowadzone są działania w zakresie cyberbezpieczeństwa. Jeżeli nie można ustalić takiego państwa członkowskiego, uznaje się, że główne miejsce prowadzenia działalności znajduje się w państwie członkowskim, w którym dany podmiot ma miejsce prowadzenia działalności o największej liczbie pracowników w Unii.			centrum przetwarzania danych, dostawca sieci dostarczania treści, dostawca usług zarządzanych, dostawca usług zarządzanych w zakresie cyberbezpieczeństwa, dostawca internetowej platformy handlowej, dostawca wyszukiwarki internetowej oraz dostawca platformy usług sieci społecznościowych świadczący usługi na terytorium Rzeczypospolitej Polskiej podlega obowiązkom wynikającym z ustawy, jeżeli Rzeczypospolita Polska jest głównym miejscem prowadzenia działalności przez ten podmiot. 4. Głównym miejscem prowadzenia działalności jest państwo członkowskie Unii Europejskiej w którym ma siedzibę kierownik podmiotu podejmujący decyzje w sprawie systemu zarządzania bezpieczeństwem informacji, o którym mowa w art. 8 ust. 1. 5. W przypadku gdy nie można ustalić, czy kierownik podmiotu podejmujący decyzje w sprawie systemu zarządzania bezpieczeństwem informacji ma siedzibę w państwie członkowskim Unii Europejskiej to głównym miejscem prowadzenia działalności jest państwo członkowskie Unii Europejskiej, w którym są realizowane zadania związane z systemem zarządzania bezpieczeństwem informacji, o których mowa w art. 8 ust. 1. 6. W przypadku gdy informacji, o której mowa w ust. 5, również nie można ustalić, to głównym miejscem prowadzenia działalności jest państwo członkowskie Unii Europejskiej, w którym podmiot, o którym mowa w ust. 3, ma największą liczbę osób zatrudnionych w odniesieniu do innych państw członkowskich Unii Europejskiej.
Art. 26	3. Jeżeli podmiot, o którym mowa w ust. 1 lit. b), nie ma miejsca prowadzenia działalności w Unii, ale oferuje usługi w Unii,	TAK	Art. 1 pkt 11 (art. 5a ust. 7-9)	Art. 5a. 7. Podmiot, o którym mowa w ust. 3, który nie posiada jednostki organizacyjnej w jednym z

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

	wyznacza przedstawiciela w Unii. Przedstawiciel musi mieć miejsce prowadzenia działalności w jednym z tych państw członkowskich, w których oferowane są usługi. Uznaje się, że taki podmiot podlega jurysdykcji państwa członkowskiego, w którym przedstawiciel ma miejsce prowadzenia działalności. W razie niewyznaczenia przedstawiciela w Unii na podstawie niniejszego artykułu państwo członkowskie, w którym dany podmiot świadczy usługi, może podjąć wobec tego podmiotu działania prawne w związku z naruszeniem niniejszej dyrektywy.			państw członkowskich Unii Europejskiej, ale oferuje swoje usługi na terytorium Rzeczypospolitej Polskiej, wyznacza przedstawiciela posiadającego jednostkę organizacyjną na terytorium Rzeczypospolitej Polskiej, o ile nie wyznaczył przedstawiciela posiadającego jednostkę organizacyjną w innym państwie członkowskim Unii Europejskiej. 8. Przedstawicielem, o którym mowa w ust. 7, może być osoba fizyczna, osoba prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej, ustanowiona na terytorium Rzeczypospolitej Polskiej lub w innym państwie członkowskim Unii Europejskiej, wyznaczona do występowania w imieniu podmiotu wskazanego w ust. 1, który nie posiada jednostki organizacyjnej w jednym z państw członkowskich Unii Europejskiej, do którego organ właściwy do spraw cyberbezpieczeństwa, CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT sektorowy może się zwrócić w związku z obowiązkami podmiotu wynikającymi z ustawy. 9. Podmiot, o którym mowa w ust. 3, który nie posiada jednostki organizacyjnej w jednym z państw członkowskich Unii Europejskiej, ale oferuje swoje usługi na terytorium Rzeczypospolitej Polskiej, podlega właściwości polskiego organu właściwego do spraw cyberbezpieczeństwa, jeżeli wyznaczył przedstawiciela posiadającego jednostkę organizacyjną na terytorium Rzeczypospolitej Polskiej.
Art. 26	4. Wyznaczenie przedstawiciela przez podmiot, o którym mowa w ust. 1 lit. b), pozostaje bez uszczerbku dla działań, które mogą zostać podjęte przeciwko samemu podmiotowi.	NIE		

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

Art. 26	5. Państwa członkowskie, które otrzymały wniosek o wzajemną pomoc w odniesieniu do podmiotu, o którym mowa w ust. 1 lit. b), mogą – nie wykraczając poza zakres tego wniosku – zastosować odpowiednie środki nadzoru i egzekwowania przepisów w odniesieniu do danego podmiotu świadczącego usługi lub mającego sieć i system informatyczny na ich terytorium.	NIE		
Art. 27	Artykuł 27 Rejestr podmiotów 1. ENISA tworzy i prowadzi rejestr dostawców usługi DNS, rejestrów nazw TLD, dostawców usług chmurowych, dostawców usług ośrodka przetwarzania danych, dostawców sieci dostarczania treści, dostawców usług zarządzanych, dostawców usług zarządzanych w zakresie bezpieczeństwa, jak również dostawców internetowych platform handlowych, wyszukiwarek internetowych i platform usług sieci społecznościowych, na podstawie informacji otrzymanych z pojedynczych punktów kontaktowych, zgodnie z ust. 4. Na wniosek ENISA zezwala właściwym organom na dostęp do rejestru, w stosownych przypadkach zapewniając jednocześnie gwarancje niezbędne do ochrony poufności informacji.	TAK	Art. 1 pkt 57 (art. 49 ust. 4 i 7)	Art. 49. 4. Pojedynczy punkt kontaktowy przekazuje ENISA aktualne dane z wykazu podmiotów kluczowych i podmiotów ważnych dotyczące dostawców usług DNS, rejestrów nazw domen najwyższego poziomu (TLD), dostawców chmury obliczeniowej, dostawców usług ośrodka przetwarzania danych, dostawców sieci dostarczania treści, dostawców usług zarządzanych, dostawców usług zarządzanych w zakresie cyberbezpieczeństwa, jak również dostawców internetowych platform handlowych, wyszukiwarek internetowych i platform usług sieci społecznościowych. 7. Organ właściwy do spraw cyberbezpieczeństwa dla sektora infrastruktury cyfrowej, CSIRT sektorowy dla tego sektora oraz CSIRT MON, CSIRT NASK, CSIRT GOV może, za pośrednictwem Pojedynczego Punktu Kontaktowego, złożyć wniosek do ENISA o udostępnienie danych z rejestru dostawców usług DNS, rejestrów nazw domen najwyższego poziomu (TLD), dostawców chmury obliczeniowej, dostawców usług ośrodka przetwarzania danych, dostawców sieci dostarczania treści, dostawców usług zarządzanych, dostawców usług zarządzanych w zakresie cyberbezpieczeństwa, jak również dostawców internetowych platform handlowych, wyszukiwarek internetowych i platform usług

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				sieci społecznościowych. We wniosku wskazuje się zakres żądanych danych.
Art. 27	2. Do dnia 17 stycznia 2025 r. państwa członkowskie wymagają od podmiotów, o których mowa w ust. 1, przedłożenia właściwym organom następujących informacji: a) nazwy podmiotu; b) odpowiedniego sektora, podsektora i rodzaju podmiotu, o których mowa w załączniku I lub II, w których prowadzi działalność; c) adresu głównego miejsca prowadzenia działalności podmiotu oraz jego innych prawnych miejsc prowadzenia działalności w Unii lub – jeżeli nie ma on miejsca prowadzenia działalności w Unii – przedstawiciela w Unii; d) aktualnych danych kontaktowych, w tym adresów poczty elektronicznej i numerów telefonów podmiotu oraz, w stosownych przypadkach, przedstawiciela wyznaczonego zgodnie z art. 26 ust. 3; e) państwa członkowskiego, w którym podmiot świadczy usługi; oraz f) zakresów IP podmiotu.	TAK	Art. 1 pkt 57 (art. 49 ust. 5)	Art. 49. 5. Dane, o których mowa w ust. 4, obejmują: 1) nazwę (firmę) podmiotu; 2) sektor, podsektor i rodzaj podmiotu; 3) identyfikator i adres; 4) adres pocztowy i adres e-mail; 5) numer telefonu przyporządkowany do wykonywanej działalności; 6) informację o wyznaczeniu przedstawiciela wraz z danymi kontaktowymi, o których mowa w art. 7 ust. 2 pkt 17 lit. a lub b; 7) adresy innych miejsc prowadzenia działalności w Unii; 8) adres wyznaczonego przedstawiciela, jeżeli jest inny niż adres podmiotu; 9) wskazanie państw członkowskich Unii Europejskiej, w których podmiot świadczy usługi; 10) główne miejsce prowadzenia działalności ustalone zgodnie z art. 5a ust. 3–6.
Art. 27	3. Państwa członkowskie zapewniają, aby podmioty, o których mowa w ust. 1, powiadamiały właściwy organ o zmianach w danych przedłożonych na podstawie ust. 2 niezwłocznie, a w każdym razie w ciągu trzech miesięcy od dnia, w którym nastąpiła zmiana.	TAK	Art. 1 pkt 14 (art. 7c ust. 3 i 4)	Art. 7c. 3. Podmiot kluczowy lub podmiot ważny składa wniosek o zmianę wpisu w wykazie w zakresie danych, o których mowa w art. 7 ust. 3 pkt 1–18, w terminie 14 dni od dnia ich zmiany. 4. Wniosek o zmianę wpisu w wykazie zawiera wskazanie zmienianych danych oraz numer podmiotu w tym wykazie.
Art. 27	4. Po otrzymaniu informacji, o których mowa w ust. 2 i 3, z wyjątkiem informacji, o których mowa w ust. 2 lit. f), pojedynczy punkt kontaktowy danego państwa członkowskiego przekazuje te informacje, bez zbędnej zwłoki, ENISA.	TAK	Art. 1 pkt 57 (art. 49 ust. 4)	Art. 49. 4. Pojedynczy Punkt Kontaktowy przekazuje ENISA aktualne dane z wykazu podmiotów kluczowych i podmiotów ważnych dotyczące dostawców usług DNS, rejestrów nazw domen najwyższego poziomu (TLD), dostawców chmury obliczeniowej, dostawców usług centrum przetwarzania danych, dostawców sieci

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				dostarczania treści, dostawców usług zarządzanych, dostawców usług zarządzanych w zakresie cyberbezpieczeństwa, jak również dostawców internetowych platform handlowych, wyszukiwarek internetowych i platform usług sieci społecznościowych.
Art. 27	5. W stosownych przypadkach informacje, o których mowa w ust. 2 i 3 niniejszego artykułu, przedkłada się z wykorzystaniem mechanizmu krajowego, o którym mowa w art. 3 ust. 4 akapit czwarty.	TAK	Art. 1 pkt 13 i 14 (art. 7 i następne)	Wdrożony poprzez przepisy dotyczące wykazu podmiotów kluczowych i podmiotów ważnych.
Art. 28	Artykuł 28 Baza danych dotyczących rejestracji nazw domen 1. By przyczynić się do bezpieczeństwa, stabilności i odporności DNS, państwa członkowskie wymagają by rejestrów nazw TLD i podmioty świadczące usługi rejestracji nazw domen gromadziły i zachowywały z należytą starannością w specjalnej bazie danych dokładne i kompletne dane dotyczące rejestracji nazw domen zgodnie z unijnymi przepisami o ochronie danych w odniesieniu do danych będących danymi osobowymi.	TAK	Art. 1 pkt 4 (art. 2 pkt 3b) i pkt 26 (rozdział 3a art. 16b ust. 1 i 3)	Art. 2: 3b) abonent nazwy domeny – podmiot będący stroną umowy o utrzymywanie nazwy domeny zawartej z rejestrem nazw domen najwyższego poziomu (TLD) za pośrednictwem podmiotu świadczącego usługi rejestracji nazw domen; Rozdział 3a Obowiązki rejestrów nazw domen najwyższego poziomu oraz zadania i obowiązki podmiotów świadczących usługi rejestracji nazw domen Art. 16b. 1. Rejestr nazw domen najwyższego poziomu (TLD) i podmioty świadczące usługi rejestracji nazw domen z należytą starannością zbierają i zachowują dokładne i kompletne dane dotyczące rejestracji nazw domen. 3. W odniesieniu do danych będących danymi osobowymi przetwarzanie w zakresie, o którym mowa w ust. 1 i 2, następuje zgodnie z przepisami dotyczącymi ochrony danych osobowych.
Art. 28	2. Do celów ust. 1 państwa członkowskie wymagają, by baza danych dotycząca rejestracji nazw domen zawierała informacje kluczowe do zidentyfikowania posiadaczy nazw domen i punktów kontaktowych zarządzających nazwami domen TLD oraz do skontaktowania się z nimi. Informacje te obejmują:)) nazwę domeny;	TAK	Art. 1 pkt 26 (art. 16b ust. 4)	Art. 16b. 4. Baza danych dotyczących rejestracji nazw domen zawiera: 1)) nazwę domeny; 2)) dane rejestracji;

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

	b) dane rejestracji; c) imię i nazwisko lub nazwę osoby rejestrującej oraz adres poczty elektronicznej i numer telefonu; d) adres poczty elektronicznej i numer telefonu, pod którymi można skontaktować się z punktem kontaktowym zarządzającym nazwą domeny, w przypadku gdy różnią się od adresu poczty elektronicznej i numeru telefonu osoby rejestrującej.			3) imię i nazwisko lub nazwę abonenta nazwy domeny oraz adres poczty elektronicznej i numer telefonu; 4) adres poczty elektronicznej i numer telefonu, pod którymi można skontaktować się z punktem kontaktowym zarządzającym nazwą domeny, w przypadku gdy różnią się od adresu poczty elektronicznej i numeru telefonu abonenta nazwy domeny, a w przypadku gdy usługi punktu kontaktowego zarządzającego nazwą domeny nie są dopuszczone dla konkretnej domeny najwyższego poziomu (TLD), należy podać co najmniej dane identyfikujące podmiot świadczący usługi rejestracji nazw domen.
Art. 28	3. Państwa członkowskie wymagają, by rejestry nazw TLD i podmioty świadczące usługi rejestracji nazw domen wdrożyły polityki i procedury, w tym procedury weryfikacji, służące zapewnieniu, aby bazy danych, o których mowa w ust. 1, zawierały dokładne i kompletne dane. Państwa członkowskie wymagają podania takich polityk i procedur do wiadomości publicznej.	TAK	Art. 1 pkt 26 (art. 16b ust. 5 i 6)	Art. 16b. 5. Rejestry nazw domen najwyższego poziomu (TLD) i podmioty świadczące usługi rejestracji nazw domen opracowują i wdrażają polityki i procedury, w tym procedury weryfikacji, służące zapewnieniu, aby bazy danych, o których mowa w ust. 1, zawierały dokładne i kompletne dane. Procedury weryfikacji danych: 1) obejmują działania weryfikacyjne na etapie rejestracji nazwy domeny lub po takiej rejestracji; 2) są wywołane i proponowane; 3) prowadzą do zweryfikowania co najmniej jednego ze sposobów kontaktu, o których mowa w u.f. 4 pkt 3 i 4; 4) obejmują uprawnienie rejestru nazw domen najwyższego poziomu (TLD) lub podmiotów świadczących usługi rejestracji nazw domen do żądania, w uzasadnionych przypadkach, udokumentowania danych identyfikacyjnych innych niż wymienione w ust. 3 i 4, w szczególności numeru lub innego

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				oznaczenia identyfikacyjnego abonenta nazwy domeny zawartego w rejestrach publicznych, o ile obowiązek jego posiadania wynika z przepisów prawa krajowego obowiązującego takiego abonenta. 6. Polityki i procedury, o których mowa w ust. 5, rejestr nazw domen najwyższego poziomu (TLD) i podmioty świadczące usługi rejestracji nazw domen publikują na swoich stronach internetowych. Polityki i procedury podmiotów świadczących usługi rejestracji nazw w konkretnej domenie najwyższego poziomu (TLD) są zgodne z politykami i procedurami opublikowanymi przez rejestr nazw tej domeny najwyższego poziomu (TLD).
Art. 28	4. Państwa członkowskie wymagają, aby po rejestracji nazwy domeny rejestry nazw TLD i podmioty świadczące usługi rejestracji nazw domen bez zbędnej zwłoki podawały do wiadomości publicznej dane dotyczące rejestracji nazwy domeny niebędące danymi osobowymi.	TAK	Art. 1 pkt 26 (art. 16b ust. 7 i 8)	Art. 16b. 7. Po rejestracji nazwy domeny rejestr nazw domen najwyższego poziomu (TLD) i podmioty świadczące usługi rejestracji nazw domen niezwłocznie publikują na stronie internetowej dane dotyczące rejestracji nazwy domeny z wyłączeniem danych osobowych. 8. Obowiązek, o którym mowa w ust. 7, może zostać zrealizowany w szczególności przez zamieszczenie danych w ogólnodostępnej bazie abonentów upublicznianej przez rejestr nazw domen najwyższego poziomu (TLD).
Art. 28	5. Państwa członkowskie wymagają, by rejestry nazw TLD i podmioty świadczące usługi rejestracji nazw domen na zgodny z prawem i należycie uzasadniony wniosek o prawnie uzasadniony dostęp udzielały dostępu do konkretnych danych dotyczących rejestracji nazw domen zgodnie z unijnymi przepisami o ochronie danych. Państwa członkowskie wymagają, by rejestry nazw TLD i podmioty świadczące usługi rejestracji nazw domen udzielały odpowiedzi bez zbędnej zwłoki, a w każdym razie w ciągu nie więcej niż 72 godzin od otrzymania wniosku o dostęp. Państwa	TAK	Art. 1 pkt 26 (art. 16c)	Art. 16c. 1. Rejestry nazw domen najwyższego poziomu (TLD) oraz podmioty świadczące usługi rejestracji nazw domen na żądanie: 1) sądu – w celu przeprowadzenia dowodu w postępowaniu karnym, postępowaniu w sprawach o wykroczenia lub w postępowaniu cywilnym, 2) prokuratora – w celu przeprowadzenia dowodu w postępowaniu karnym lub postępowaniu w sprawach o wykroczenia,

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

	członkowskie wymagają podania do wiadomości publicznej polityk i procedur ujawniania takich danych.		3) Policji oraz innych upoważnionych organów w postępowaniu karnym lub czynnościach wyjaśniających w sprawie o wykroczenie i postępowaniu w sprawach o wykroczenia, w celu przeprowadzenia dowodu w postępowaniu karnym lub czynnościach wyjaśniających w sprawie o wykroczenie i postępowaniu w sprawach o wykroczenia, 4) CSIRT sektorowego – w celu przeprowadzenia obsługi incydentu poważnego przez CSIRT sektorowy związanego z daną domeną, 5) CSIRT GOV, CSIRT MON lub CSIRT NASK – w celu przeprowadzenia obsługi incydentu poważnego lub incydentu krytycznego związanego z daną domeną, 6) podmiotu wykonującego postanowienie sądu w przedmiocie zabezpieczenia środka dowodowego, o którym mowa w art. 479¹⁰⁰ §1 ustawy z dnia 17 listopada 1964 r. – Kodeks postępowania cywilnego (Dz. U. z 2024 r. poz. 1568 i 1841 oraz z 2025 r. poz. 620 oraz z 2025 r. poz. 620, 1172 i 1302), 7) Prezesa Urzędu Komunikacji Elektronicznej – w celu weryfikacji czy podmiot składający sprzeciw wobec wpisania domeny na listę ostrzeżeń, o którym mowa w art. 21 ust. 1 ustawy z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej (Dz. U. z 2024 r. poz. 1803) dysponuje do tej domeny tytułem prawnym – udzielają dostępu do konkretnych danych dotyczących rejestracji nazw domen, które mają znaczenie dla prowadzonego postępowania lub czynności wyjaśniających w sprawie o

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				wykroczenie z zachowaniem przepisów dotyczących ochrony danych osobowych. 2. Żądanie udostępnienia danych, o których mowa w ust. 1, składa się w postaci elektronicznej i opatruje kwalifikowanym podpisem elektronicznym, podpisem zaufanym, podpisem osobistym albo kwalifikowaną pieczęcią elektroniczną. Żądanie zawiera uzasadnienie. 3. Rejestry nazw domen najwyższego poziomu (TLD) oraz podmioty świadczące usługi rejestracji nazw domen udzielają odpowiedzi nie później niż w terminie 72 godzin od dnia otrzymania żądania udostępnienia danych, o którym mowa w ust. 1, w sposób określony w opracowanej przez siebie i podanej do publicznej wiadomości polityce i procedurze ujawniania takich danych.
Art. 28	6. Wypełnianie obowiązków określonych w ust. 1–5 nie prowadzi do powielania gromadzenia danych dotyczących rejestracji nazw domen. W tym celu państwa członkowskie wymagają wzajemnej współpracy od rejestrów nazw TLD i podmiotów świadczących usługi rejestracji nazw domen.	TAK	Art. 1 pkt 26 (art. 16b ust. 2 i 9)	Art. 16b. 2. Podmioty świadczące usługi rejestracji nazw w konkretnej domenie najwyższego poziomu współpracują z rejestrem nazw tej domeny. Baza danych dotycząca rejestracji nazw domen może funkcjonować w szczególności przez umożliwianie podmiotom świadczącym usługi rejestracji nazw domen przez rejestr nazw domen najwyższego poziomu (TLD) na podstawie umów, zautomatyzowanego wprowadzania i aktualizowania danych oraz inicjowanie związanych z tym czynności administracyjnych i technicznych. W takim przypadku przetwarzanie danych przez podmioty świadczące usługi rejestracji nazw domen nie jest uznawane za powielanie zadań rejestru nazw domen najwyższego poziomu (TLD). 9. W przypadku gdy podanie danych, w tym adresu poczty elektronicznej abonenta nazwy domeny, wymaga uzyskania zgody, obowiązek jej

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				uzyskania obciąża podmiot przetwarzający te dane jako pierwszy.
Art. 29	Artykuł 29 Mechanizmy wymiany informacji na temat cyberbezpieczeństwa 1. Państwa członkowskie zapewniają, aby podmioty objęte zakresem stosowania niniejszej dyrektywy, a w stosownych przypadkach również inne podmioty nieobjęte zakresem niniejszej dyrektywy mogły dobrowolnie wymieniać się odpowiednimi informacjami na temat cyberbezpieczeństwa, w tym informacjami o cyberzagrożeniach, potencjalnych zdarzeniach dla cyberbezpieczeństwa, podatnościach, technikach i procedurach, oznakach naruszenia integralności systemu, wrogich taktykach, a także informacjami o grupach przestępczych, ostrzeżeniach dotyczących cyberbezpieczeństwa i zaleceniami dotyczącymi konfiguracji narzędzi bezpieczeństwa mających wykrywać cyberataki, jeżeli wymiana takich informacji: a) ma na celu zapobieganie incydom, ich wykrywanie, reagowanie na nie, przywracanie normalnego działania po i yd t h lub ł god i h k t k ó w; b) zwiększa poziom cyberbezpieczeństwa, zwłaszcza przez podnoszenie świadomości na temat cyberzagrożeń, ograniczanie lub utrudnianie rozprzestrzeniania się cyberzagrożeń, wspieranie różnorodnych zdolności do obrony przed nimi, eliminowanie i ujawnianie podatności, techniki wykrywania zagrożeń, ograniczania ich zasięgu i zapobiegania im, strategię ograniczania ryzyka, etapy reagowania i przywracania normalnego działania lub sprzyjanie współpracy między podmiotami publicznymi i prywatnymi w badaniach nad cyberzagrożeniami.	TAK	Art. 1 pkt 17 (art. 8h ust. 1 i 2)	Art. 8h. 1. Podmioty kluczowe, podmioty ważne CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT sektorowy, dostawcy sprzętu lub oprogramowania dla tych podmiotów lub organizacje społeczne zrzeszające podmioty kluczowe lub podmioty ważne mogą wymieniać między sobą informacje dotyczące cyberbezpieczeństwa, w tym informacje o cyberzagrożeniach, potencjalnych zdarzeniach dla cyberbezpieczeństwa, podatnościach, technikach i procedurach, oznakach naruszenia integralności systemu informacyjnego, wrogich taktykach, a także informacje o grupach przestępczych, ostrzeżenia dotyczące cyberbezpieczeństwa i zalecenia dotyczące konfiguracji narzędzi bezpieczeństwa mających wykrywać cyberataki. 2. Wymiana informacji, ostrzeżeń i zaleceń, o których mowa w ust. 1, jest dopuszczalna jeżeli: 1) ma na celu zapobieganie incydom, ich wykrywanie, reagowanie na nie, przywracanie normalnego działania po incydomach lub łagodzenie ich skutków lub 2) zwiększa poziom cyberbezpieczeństwa, w szczególności przez podnoszenie świadomości na temat cyberzagrożeń, ograniczanie lub utrudnianie ich rozprzestrzeniania się, eliminowanie i ujawnianie podatności, techniki wykrywania cyberzagrożeń, ograniczania ich zasięgu i zapobiegania im, strategię ograniczania ryzyka, etapy reagowania i przywracania normalnego działania lub sprzyjanie współpracy między podmiotami publicznymi i prywatnymi w badaniach nad cyberzagrożeniami.

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

Art. 29	2. Państwa członkowskie zapewniają, aby wymiana informacji odbywała się w społecznościach podmiotów kluczowych i ważnych, a w stosownych przypadkach również ich dostawców lub usługodawców. Wymianę taką prowadzi się za pośrednictwem mechanizmów wymiany informacji o cyberbezpieczeństwie ze względu na potencjalnie poufny charakter wymienianych informacji.	TAK	Art. 1 pkt 17 (art. 8h ust. 3-7)	Art. 8h. 3. Wymiana informacji, ostrzeżeń i zaleceń, o których mowa w ust. 1, odbywa się za pomocą systemu teleinformatycznego, o którym mowa w art. 46 ust. 1, systemów teleinformatycznych zapewnianych przez organy właściwe do spraw cyberbezpieczeństwa lub w drodze porozumień, o których mowa w ust. 6. 4. Wymieniając informacje, o których mowa w ust. 1, podmioty kluczowe lub podmioty ważne oznaczają zakres odbiorców tych informacji. Odbiorca informacji może ją udostępniać w zakresie określonym przez wytwórcę informacji. 5. Wymieniając informacje, o których mowa w ust. 1, za pomocą systemu teleinformatycznego, o którym mowa w art. 46 w ust. 1, nie przekazuje się danych osobowych. 6. Podmioty kluczowe, podmioty ważne, CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT sektorowy, dostawcy sprzętu lub oprogramowania dla tych podmiotów lub organizacje społeczne zrzeszające podmioty kluczowe lub podmioty ważne mogą zawierać porozumienia w sprawie wymiany informacji, o których mowa w ust. 1, w szczególności określając sposób wymiany informacji i zachowania informacji w poufności pomiędzy stronami porozumienia. 7. Koszty wykonania porozumień, o których mowa w ust. 6, są ponoszone w równych częściach przez wszystkie strony, chyba że w danym porozumieniu postanowiono inaczej.
Art. 29	3. Państwa członkowskie ułatwiają tworzenie mechanizmów wymiany informacji o cyberbezpieczeństwie, o których mowa w ust. 2 niniejszego artykułu. W mechanizmach tych można określić elementy operacyjne, w tym korzystanie ze specjalnych platform ICT i narzędzi automatyzacji, a także treści i warunki funkcjonowania mechanizmów wymiany informacji. Określając	TAK	Art. 1 pkt 17 (art. 8h ust. 6 i 7)	Art. 8h. 6. Podmioty kluczowe, podmioty ważne, CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT sektorowy, dostawcy sprzętu lub oprogramowania dla tych podmiotów lub organizacje społeczne zrzeszające podmioty kluczowe lub podmioty ważne mogą zawierać

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

	szczegóły udziału organów publicznych w tych mechanizmach, państwa członkowskie mogą ustalać warunki udostępniania informacji przez właściwe organy lub CSIRT. Państwa członkowskie oferują pomoc w stosowaniu takich mechanizmów zgodnie ze swoją polityką, o której mowa w art. 7 ust. 2 lit. h).			porozumienia w sprawie wymiany informacji, o których mowa w ust. 1, w szczególności określając sposób wymiany informacji i zachowania informacji w poufności pomiędzy stronami porozumienia. 7. Koszty wykonania porozumień, o których mowa w ust. 6, ponoszone są w równych częściach przez wszystkie strony, chyba że w danym porozumieniu postanowiono inaczej.
Art. 29	4. Państwa członkowskie zapewniają, by podmioty kluczowe i ważne powiadamiały właściwe organy, że uczestniczą w mechanizmach wymiany informacji, o których mowa w ust. 2, gdy przystępują do tych mechanizmów, lub, w stosownych przypadkach, o wycofaniu się z takich mechanizmów, gdy wycofanie stanie się skuteczne.	TAK	Art. 1 pkt 13 (art. 7)	Przepis art. 7 dotyczący wykazu podmiotów kluczowych i ważnych obejmuje obowiązek podania informacji o zawarciu porozumień w sprawie wymiany informacji.
Art. 29	5. ENISA pomaga w tworzeniu mechanizmów wymiany informacji na temat cyberbezpieczeństwa, o których mowa w ust. 2, przez wymianę najlepszych praktyk i udzielanie wskazówek.	NIE		
Art. 30	Artykuł 30 Dobrowolne zgłaszanie ważnych informacji 1. Państwa członkowskie zapewniają, by w uzupełnieniu obowiązków zgłaszania, o których mowa w art. 23, następujące podmioty mogły dobrowolnie przekazywać zgłoszenia CSIRT lub, w stosownych przypadkach, właściwym organom: a) podmioty kluczowe i ważne w przypadku incydentów, cyberzagrożeń i potencjalnych zdarzeń dla cyberbezpieczeństwa; b) podmioty inne niż te, o których mowa w lit. a), niezależnie od tego, czy są objęte zakresem stosowania niniejszej dyrektywy, w odniesieniu do poważnych incydentów, cyberzagrożeń oraz potencjalnych zdarzeń dla cyberbezpieczeństwa.	TAK	Art. 1 pkt 22 (art. 13)	Art. 13. 1. Podmiot kluczowy lub podmiot ważny mogą przekazywać do właściwego CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT sektorowego informacje: 1) o incydentach i zagrożeniach; 2) o cyberzagrożeniach; 3) dotyczących podmiotów i ryzyka; 4) o podmiotach; 5) o potencjalnych zdarzeniach dla cyberbezpieczeństwa; 6) o wykorzystywanych technologiach. 2. Informacje, o których mowa w ust. 1, są przekazywane w postaci elektronicznej za pomocą systemu teleinformatycznego, o którym mowa w art. 46 ust. 1, a w przypadku braku możliwości przekazania w postaci elektronicznej,

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				przy użyciu innych dostępnych środków komunikacji. 3. Podmiot kluczowy lub podmiot ważny oznacza informacje stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa.
Art. 30	2. Państwa członkowskie rozpatrują zgłoszenia, o których mowa w ust. 1 niniejszego artykułu, zgodnie z procedurą określoną w art. 23. Państwa członkowskie mogą rozpatrywać zgłoszenia obowiązkowe priorytetowo względem zgłoszeń dobrowolnych. W razie potrzeby CSIRT oraz, w stosownych przypadkach, właściwe organy przekazują pojedynczym punktom kontaktowym informacje o zgłoszeniach otrzymanych na podstawie niniejszego artykułu, zapewniając przy tym poufność i odpowiednią ochronę informacji przekazanych przez podmiot zgłaszający. Bez uszczerbku dla zapobiegania, prowadzenia postępowań, wykrywania i ścigania przestępstw dobrowolne zgłaszanie nie może powodować nałożenia na podmiot zgłaszający żadnych dodatkowych obowiązków, którym by nie podlegał, gdyby nie przekazał zgłoszenia.	NIE		Przepis już jest wdrożony w obecnym brzmieniu art. 30 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa
Art. 31	Artykuł 31 Ogólne aspekty nadzoru i egzekwowania przepisów 1. Państwa członkowskie zapewniają, aby ich właściwe organy skutecznie monitorowały przestrzeganie niniejszej dyrektywy i stosowały środki niezbędne do zagwarantowania tego przestrzegania.	TAK	Art. 1 pkt 63 (art. 53 ust. 1) i pkt 65 (art. 53a–53c)	Art. 53. 1. Nadzór dotyczący stosowania przepisów ustawy sprawują organy właściwe do spraw cyberbezpieczeństwa w zakresie wykonywania przez podmioty kluczowe i podmioty ważne wynikających z ustawy obowiązków. Art. 53a. 1. Organy właściwe do spraw cyberbezpieczeństwa mogą tworzyć, samodzielnie lub wspólnie, metodyki nadzoru dotyczące prowadzenia nadzoru nad podmiotami kluczowymi lub podmiotami ważnymi w zakresie stosowania przepisów ustawy. 2. Metodyki nadzoru określają w szczególności: 1) kryterium; 2) sposób przeprowadzenia; 3) kryteria oceny.

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				3. W przypadku stworzenia metodyki nadzoru organy właściwe do spraw cyberbezpieczeństwa co dwa lata oceniają skuteczność stosowania tej metodyki nadzoru, w szczególności na oceniając efektywność sprawowanego nadzoru. 4. Na podstawie oceny skuteczności organy właściwe do spraw cyberbezpieczeństwa dokonują zmian w metodykach nadzoru. Art. 53b. 1. Organy właściwe do spraw cyberbezpieczeństwa mogą ustalać hierarchię priorytetów w sprawowaniu nadzoru w oparciu o metodykę nadzoru, o której mowa w art. 53a ust. 1, uwzględniając w szczególności wyniki analizy ryzyka dla konkretnego podmiotu kluczowego lub podmiotu ważnego. 2. Analiza ryzyka przeprowadzana jest przez organ właściwy do spraw cyberbezpieczeństwa i uwzględnia w szczególności: 1) znaczenie usługi dla bezpieczeństwa środowiska i porządku publicznego; 2) wpływ usługi na podjęcie i połączenie; 3) prawdopodobieństwo wystąpienia incydentu w podmiocie nadzorowanym oraz rodzaj tego incydentu; 4) potencjalne skutki incydentu takie jak straty finansowe, szkody wizerunkowe, utrata danych osobowych lub zakłócenia w funkcjonowaniu systemów i infrastruktury. Art. 53c. 1. Podmiot kluczowy lub podmiot ważny przekazuje na żądanie organu właściwego do spraw cyberbezpieczeństwa dane, informacje i dokumenty niezbędne do wykonywania przez ten organ jego uprawnień i obowiązków z zakresu sprawowania nadzoru i kontroli, określonych w ustawie.

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				2. Żądanie, o którym mowa w ust. 1, powinno być proporcjonalne do celu, jakiemu ma służyć, oraz zawierać: 1) wskazanie podmiotu kluczowego lub podmiotu wewnętrznego, do którego jest skierowane; 2) dany rodzaj; 3) wskazanie żądanych danych, informacji lub dokumentów oraz okresu, który ich dotyczy; 4) wskazanie celu, jakiemu dane, informacje lub dokumenty mają służyć; 5) wskazanie terminu przekazania danych, informacji lub dokumentów adekwatnego do charakteru danego żądania, nie krótszego niż 7 dni; 6) uzasadnienie danego żądania; 7) pouczenie o zagrożeniu karą w przypadku, o którym mowa w art. 73 ust. 1 pkt 16. 3. Żądanie, o którym mowa w ust. 1, sporządza się w postaci elektronicznej i doręcza się w sposób określony w dziale I rozdziale 8 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego albo przez system teleinformatyczny, o którym mowa w art. 46 ust. 1 pkt 6. 4. Przepisy ust. 1–3 stosuje się odpowiednio do żądania udzielenia dostępu do danych, dokumentów i informacji koniecznych do wykonania nadzoru oraz dowodów realizacji wymogów, o których mowa w art. 8 ust. 1.
Art. 31	2. Państwa członkowskie mogą zezwolić ich właściwym organom na wprowadzenie hierarchii priorytetów w odniesieniu do zadań nadzorczych. Taka hierarchia priorytetów bazuje na podejściu uwzględniającym analizę ryzyka. W tym celu, wykonując zadania nadzorcze określone w art. 32 i 33, właściwe organy mogą określić metodykę nadzorczą pozwalającą ustalić hierarchię priorytetów w tych zadaniach na podstawie podejścia uwzględniającego analizę ryzyka.	TAK	Art. 1 pkt 64 (art. 53a i art. 53b)	Art. 53a. 1. Organy właściwe do spraw cyberbezpieczeństwa mogą tworzyć, samodzielnie lub wspólnie, metodyki nadzoru dotyczące prowadzenia nadzoru nad podmiotami kluczowymi lub podmiotami ważnymi w zakresie stosowania przepisów ustawy. 2. Metodyki nadzoru określają w szczególności: 1) kierunek;

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				2) sposób prowadzenia nadzoru; 3) kryteria oceny. 3. W przypadku stworzenia metodyki nadzoru organy właściwe do spraw cyberbezpieczeństwa co dwa lata oceniają skuteczność stosowania tej metodyki nadzoru, w szczególności oceniając efektywność sprawowanego nadzoru. 4. Na podstawie oceny skuteczności organy właściwe do spraw cyberbezpieczeństwa dokonują zmian w metodykach nadzoru. Art. 53b. 1. Organy właściwe do spraw cyberbezpieczeństwa mogą ustalać hierarchię priorytetów w sprawowaniu nadzoru w oparciu o metodykę nadzoru, o której mowa w art. 53a ust. 1, uwzględniając w szczególności wyniki analizy ryzyka dla konkretnego podmiotu kluczowego lub podmiotu ważnego. 2. Analiza ryzyka przeprowadzana jest przez organ właściwy do spraw cyberbezpieczeństwa uwzględniając w szczególności: 1) znaczenie usługi dla bezpieczeństwa środowiska i porządku publicznego; 2) wpływ usługi podatkowej i społeczność; 3) prawdopodobieństwo wystąpienia incydentu w podmiocie nadzorowanym oraz rodzaj tego incydentu; 4) potencjalne skutki incydentu takie jak straty finansowe, szkody wizerunkowe, utrata danych osobowych lub zakłócenia w funkcjonowaniu systemów i infrastruktury.
Art. 31	3. Właściwe organy odpowiadając na incydenty, które doprowadziły do naruszeń danych osobowych, ściśle współpracują z organami nadzorczymi, na mocy rozporządzenia (UE) 2016/679, bez uszczerbku dla właściwości i zadań organów nadzorczych określonych w tym rozporządzeniu.	NIE		Wdrożone w art. 34 ust. 2 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

Art. 31	4. Bez uszczerbku dla krajowych ram ustawodawczych i instytucjonalnych państwa członkowskie zapewniają, aby nadzorując przestrzeganie niniejszej dyrektywy przez podmioty administracji publicznej oraz nakładając środki egzekwowania przepisów w odniesieniu do naruszeń niniejszej dyrektywy, właściwe organy posiadały odpowiednie uprawnienia do podejmowania takich zadań w sposób niezależny pod względem operacyjnym wobec nadzorowanych podmiotów administracji publicznej. Państwa członkowskie mogą podjąć decyzję o nałożeniu na te podmioty odpowiednich, proporcjonalnych i skutecznych środków nadzoru i egzekwowania przepisów zgodnie z krajowymi ramami ustawodawczymi i instytucjonalnymi.	TAK	Art. 1 pkt 62 i 63 i następne	Przepisy dotyczące nadzoru stosują się także do podmiotów publicznych z zastrzeżeniem wynikającym z art. 53 ust. 10.
Art. 32	Artykuł 32 Środki nadzoru i egzekwowania przepisów dla podmiotów kluczowych 1. Państwa członkowskie zapewniają, by środki nadzoru lub egzekwowania przepisów nakładane na podmioty kluczowe w odniesieniu do obowiązków określonych w niniejszej dyrektywie były skuteczne, proporcjonalne i odstraszające, stosownie do okoliczności każdego indywidualnego przypadku.	TAK	Art. 1 pkt 63 (art. 53) i art. 1 pkt 64 (art. 53d i 53e), art. 1 pkt 69 (art. 59c) oraz art. 1 pkt 17 (art. 8c), art. 1 pkt 23 (art. 15 ust. 1–1c) i art. 1 pkt 39 (Rozdział 6a) oraz art. 1 pkt 76 (art. 67g)	Art. 53 1. Nadzór dotyczący stosowania przepisów ustawy sprawują organy właściwe do spraw cyberbezpieczeństwa w zakresie wykonywania przez podmioty kluczowe i podmioty ważne wynikających z ustawy obowiązków. 2. W ramach nadzoru, o którym mowa w ust. 1, organ właściwy do spraw cyberbezpieczeństwa w stosunku do podmiotów kluczowych może: 1) prowadzić kontrole, w tym dorażne, w siedzibie podmiotu, miejscu wykonywania działalności go pod r r lub d r; 2) zobowiązać podmiot, w drodze decyzji, do przeprowadzanie audytu, o którym mowa w art. 15 ust. 1b, w szczególności w sytuacji wystąpienia poważnego incydentu lub naruszenia przepisów u t wy; 3) zlecić CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT sektorowemu, dokonanie oceny bezpieczeństwa systemu informacyjnego podmiotu klu ow go; 4) wystąpić z wnioskiem o udzielenie informacji niezbędnych do oceny środków, o których mowa w art. 8 ust. 1 pkt 2 i 5 , a także zgodności z

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				obowiązkiem przedkładania informacji właściwym organom zgodnie z art. 7; 5) wystąpić z wnioskiem o udzielenie dostępu do danych, dokumentów i informacji koniecznych do wykonywania ich obowiązków; 6) wystąpić z wnioskiem o przedstawienie dowodów realizacji wymogów, o których mowa w art. 8 ust. 1. 3. Organy właściwe do spraw cyberbezpieczeństwa za pomocą działań nadzorczych sprawują nadzór o charakterze: 1) prewencyjnym i następczym nad podmiotami kluczowymi; 2) następczym nad podmiotami ważnymi, w szczególności w przypadku uzasadnionego podejrzenia, że zachodzi możliwość naruszenia przepisów ustawy. 4. W przypadku uzasadnionego podejrzenia, że działania lub zaniechania podmiotu kluczowego mogą naruszać przepisy ustawy, organ właściwy do spraw cyberbezpieczeństwa kieruje do tego podmiotu pismo w formie elektronicznej z ostrzeżeniem, w którym wskazuje czynności, jakie należy podjąć w celu zapobieżenia lub zaprzestania naruszania przepisów ustawy oraz termin na ich wykonanie. 5. W celu egzekwowania przepisów ustawy organ właściwy do spraw cyberbezpieczeństwa w stosunku do podmiotów kluczowych, także wtedy gdy podmiot kluczowy nie zastosował się do pisma z ostrzeżeniem, o którym mowa w ust. 4, może: 1) nakazać podjęcie określonych czynności dotyczących obowiązków; 2) nakazać, w drodze decyzji, zaniechanie określonych przepisów ustawy;

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				3) nakazać, w drodze decyzji, zapewnienie zgodności systemu zarządzania bezpieczeństwem informacji zgodnie z art. 8 ust. 1 pkt 2 lub zgodnie z art. 8 ust. 3 lub realizacji obowiązku zgłaszania incydentów powstających; 4) nakazać, w drodze decyzji, poinformowanie, w określony przez niego sposób, odbiorców swoich usług, których dotyczy poważne cyberzagrożenie, o charakterze tego zagrożenia oraz o możliwych środkach ochronnych lub naprawczych, jakie należy podjąć w reakcji na zagrożenie; 5) nakazać, w drodze decyzji, wdrożenie, w określonym terminie, zaleceń wydanych w wyniku audytu bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usług; 6) wyznaczyć, w drodze decyzji, na określony czas, nie dłuższy niż miesiąc, spośród osób zatrudnionych w urzędzie obsługującym ten organ, urzędnika monitorującego do nadzorowania wykonywania obowiązków, o których mowa w rozdziale 3, wskazując ściśle określone zadania, które urzędnik monitorujący realizuje w tym celu; 7) nakazać, w drodze decyzji, podanie do wiadomości publicznej informacji o naruszeniach prywatności; 8) nakazać, w drodze decyzji wydanej w postępowaniu uproszczonym, o którym mowa w rozdziale 14 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego, podanie do publicznej wiadomości informacji o incydencie poważnym. 6. Organ właściwy do spraw cyberbezpieczeństwa, podejmując działania, o których mowa w ust. 5, wyznacza podmiotowi

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				kluczowemu termin, w którym zobowiązuje ten podmiot do podjęcia określonych czynności, usunięcia uchybień lub zapewnienia zgodności z wymogami określonymi przez organ. 7. Nakaz, o którym mowa w ust. 5 pkt 1, jest inną czynnością z zakresu administracji publicznej, na którą przysługuje skarga do sądu administracyjnego i wymaga uzasadnienia. 8. Postępowanie w sprawach, o którym mowa w ust. 5 pkt 2–8, jest jednoinstancyjne, a na decyzję organu właściwego do spraw cyberbezpieczeństwa przysługuje skarga do sądu administracyjnego. 9. Organ właściwy do spraw cyberbezpieczeństwa, w przypadku gdy podmiot kluczowy nie zastosował się do nakazu, o którym mowa w ust. 5 pkt 1, lub postanowień decyzji, o której mowa w ust. 5 pkt 2–8, może: 1) wstrzymać udzieloną temu podmiotowi koncesję albo ograniczyć jej zakres do czasu usunięcia uchybień lub zaprzestania naruszeń lub 2) wstrzymać w całości albo w części działalność podmiotu kluczowego wpisanego do rejestru działalności regulowanej, do czasu usunięcia uchybień lub zaprzestania naruszeń, lub 3) wstrzymać zezwolenie na prowadzenie działalności gospodarczej wydane podmiotowi kluczowemu albo ograniczyć zakres tego zezwolenia do czasu usunięcia uchybień lub zaprzestania naruszeń, lub 4) wstrzymać w całości albo w części działalność podmiotu kluczowego, wpisanego do Centralnej Ewidencji i Informacji o Działalności Gospodarczej, do czasu usunięcia uchybień lub zaprzestania naruszeń, lub

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				5) wstrzymać w całości albo w części działalność podmiotu kluczowego, wpisanego do rejestru przedsiębiorców Krajowego Rejestru Sądowego do czasu usunięcia uchybień lub zaprzestania naruszeń, lub 6) zakazać pełnienia w podmiocie kluczowym funkcji zarządczych przez kierownika podmiotu do czasu usunięcia uchybień lub zaprzestania naruszeń, o ile nie doprowadzi to do uniemożliwienia funkcjonowania podmiotu kluczowego w zakresie jaki jest niezbędny do usunięcia uchybień lub zaprzestania naruszeń. 10. Środków, o których mowa w ust. 9, nie stosuje się do podmiotów publicznych. 11. W przypadku wniesienia przez podmiot kluczowy skargi do sądu administracyjnego, o której mowa w ust. 7 lub 8, środków, o których mowa w ust. 9, nie stosuje się do czasu rozstrzygnięcia sprawy przez ten sąd. Sąd rozstrzyga sprawę w terminie miesiąca od dnia wniesienia skargi. 12. Organ właściwy do spraw cyberbezpieczeństwa, podejmując działania, o których mowa w ust. 5 i 9, uwzględnia: 1) wagę naruszenia i znaczenie naruszonych przepisów ustawy, przy czym za poważne naruszenie należy uznać: a) powtarzające się naruszenie, b) niezgłoszenie lub nieobsłużenie incydentów poważnych, c) nieusunięcie uchybień zgodnie z wiążącymi nakazami organów właściwych do spraw cyberbezpieczeństwa, d) utrudnianie prowadzenia audytów lub działań monitorujących nakazanych przez organ

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				właściwy do spraw cyberbezpieczeństwa po stwierdzeniu naruszenia, e) dostarczanie nieprawdziwych lub rażąco niedokładnych informacji w odniesieniu do środków zarządzania ryzykiem w cyberbezpieczeństwie lub obowiązków 1) gwarantujących powziętych; 2) utrzymywanych; 3) wcześniejsze poważne naruszenia ze strony danego podmiotu; 4) spowodowane szkody majątkowe i niemajątkowe, w tym straty finansowe lub gospodarcze, wpływ na inne usługi i liczbę użytkowników, których dotyczy; 5) umyślny lub nieumyślny charakter czynu ze strony przewidywanego; 6) środki zastosowane przez podmiot, aby zapobiec szkodom majątkowym i niemajątkowym lub je ograniczyć; 7) stopień współpracy podmiotu z organem właściwym do spraw cyberbezpieczeństwa. 13. Organ właściwy do spraw cyberbezpieczeństwa przed zastosowaniem środków, o których mowa w ust. 4, 5 i 9, oraz przed nałożeniem kary pieniężnej, informuje podmiot kluczowy o wstępnych ustaleniach, które mogą prowadzić do wydania decyzji lub podjęcia działań, o których mowa w ust. 4, 5 i 9, lub do nałożenia kary pieniężnej. Informacja o wstępnych ustaleniach zawiera szczegółowe uzasadnienie, potwierdzające zasadność zamiaru zastosowania środków lub nałożenia kary pieniężnej. 14. Podmiot kluczowy może przedstawić swoje stanowisko niezwłocznie, nie później niż w

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				terminie 7 dni od dnia poinformowania o wstępnych ustaleniach, o których mowa w ust. 13. 15. Organ właściwy do spraw cyberbezpieczeństwa po przedstawieniu przez podmiot kluczowy swojego stanowiska: 1) uwzględnia stanowisko tego podmiotu i odstępuje od zastosowania środków, o których mowa w ust. 4, 5 lub 9, lub od nałożenia kary pieniężnej, orzeka o tym podmiot o tym fakcie wraz ze szczegółowym uzasadnieniem przyczyn odrzucenia stanowiska podmiotu. 2) odrzuca stanowisko tego podmiotu i stosuje środki, o których mowa w ust. 4, 5 lub 9, lub nakłada karę pieniężną, oraz informuje podmiot o tym fakcie wraz ze szczegółowym uzasadnieniem przyczyn odrzucenia stanowiska podmiotu. 16. Organ właściwy do spraw cyberbezpieczeństwa może odstąpić od poinformowania o wstępnych ustaleniach w przypadku gdy utrudniłoby to natychmiastowe działanie w celu zapobieżenia incydentom, reakcji na nie lub mogłoby mieć niekorzystny wpływ na bezpieczeństwo państwa lub porządek publiczny. 17. Organ właściwy do spraw cyberbezpieczeństwa sprawując nadzór w stosunku do podmiotu ważnego stosuje ust. 2, 4, 5 pkt 1–5, 7–8 oraz ust. 6–8 i ust. 12–16. Art. 53d. 1. Urzędnik monitorujący, o którym mowa w art. 53 ust. 5 pkt 6, w zakresie nadzorowania wykonywania przez podmiot kluczowy obowiązków, o których mowa w rozdziale 3, jest uprawniony do: 1) swobodnego wstępu i poruszania się po terenie podmiotu kluczowego po uzyskaniu przepustki, wydanej bezzwłocznie, której wydania nie można odmówić;

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				2) wglądu do dokumentów dotyczących działalności podmiotu kluczowego; 3) przetwarzania danych osobowych w zakresie niezbędnym do realizacji celu nadzoru; 4) żądania złożenia ustnych lub pisemnych wyjaśnień w sprawach dotyczących zakresu nadzoru; 5) przeprowadzania oględzin urządzeń, nośników oraz systemów informacyjnych, po wcześniejszym zawiadomieniu podmiotu kluczowego. 2. Urzędnik monitorujący, o którym mowa w art. 53 ust. 5 pkt 6, realizuje powierzone mu zadania z zachowaniem przepisów o tajemnicy prawnie chronionej. 3. Do nadzorowania przez urzędnika monitorującego, o którym mowa w art. 53 ust. 5 pkt 6, wykonywania przez podmiot kluczowy obowiązków, o których mowa w rozdziale 3, stosuje się art. 58.4. Zawiadomienie, o którym mowa w ust. 1 pkt 5, przekazuje się na adres do doręczeń elektronicznych albo za pomocą systemu teleinformatycznego, o którym mowa w art. 46 ust. 1 w terminie 1 dnia przed przeprowadzeniem oględzin. Art. 53e. 1. Realizując uprawnienie, o którym mowa w art. 53 ust. 9, organ właściwy do spraw cyberbezpieczeństwa wydaje decyzję, która zawiera: 1) dane podmiotu kluczowego lub kierownika podmiotu kluczowego; 2) rodzaj stwierdzonych uchybień lub naruszeń dokonanych przez podmiot kluczowy lub kierownika podmiotu kluczowego;

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				3) podjęte dotychczas środki nadzorcze nad podmiotem kluczowym; 4) podstawę prawną i rodzaj środka określonego w art. 53 ust. 9; 5) termin stosowania tego środka; 6) uzasadnienie. 2. Termin stosowania środków, o których mowa w art. 53 ust. 9, określa się przy uwzględnieniu kryteriów, o których mowa w art. 53 ust. 12. Środek nie może być stosowany dłużej niż 14 dni od daty doręczenia decyzji o jego zastosowaniu. 3. W zależności od zastosowanego środka, jeżeli podmiot kluczowy usunął uchybienia lub zaprzestał naruszania przepisów ustawy przed terminem określonym w decyzji, uchyla się decyzję o zastosowaniu tego środka. 4. W przypadku powzięcia informacji, w szczególności na skutek stosowania innych środków nadzorczych, określonych w art. 53 ust. 1, 4 i 5, że podmiot kluczowy nie usunął wcześniej stwierdzonych uchybień lub w dalszym ciągu narusza przepisy ustawy lub w przypadku gdy podmiot kluczowy nie wykazał w terminie, na jaki został zastosowany środek, że usunął uchybienia lub zaprzestał naruszania przepisów ustawy, organ właściwy do spraw cyberbezpieczeństwa ponownie wydaje decyzję o zastosowaniu środka określonego w art. 53 ust. 9 na kolejny okres, nie dłuższy niż 14 dni. Przepis ten stosuje się do czasu usunięcia uchybień lub zaprzestania naruszeń przez podmiot kluczowy. W stosunku do ponownej decyzji nie stosuje się art. 53 ust. 13–16. 5. Organ właściwy do spraw cyberbezpieczeństwa z urzędu lub na wniosek podmiotu kluczowego uchyla decyzję, o której mowa w ust. 1, po

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				usunięciu uchybień lub zaprzestaniu naruszeń przez podmiot kluczowy. 6. Podmiot kluczowy może złożyć wniosek o którym mowa w ust. 5 po usunięciu uchybień lub zaprzestaniu naruszeń, przedstawiając dowody potwierdzające zastosowanie się odpowiednio do nakazu, o którym mowa w art. 53 ust. 5 pkt 1, lub postanowień decyzji, o której mowa w art. 53 ust. 5 pkt 2–8. 7. Wniosek, o którym mowa w ust. 5, organ właściwy do spraw cyberbezpieczeństwa rozpatruje niezwłocznie, nie później niż w terminie 7 dni od dnia jego otrzymania. 8. Czynności, o których mowa w ust. 3 i 5 organ dokonuje w formie decyzji. 9. Decyzja, o której mowa w ust. 1 jest wykonalna z dniem jej doręczenia podmiotowi kluczowemu. Decyzje, o których mowa w ust. 3, 4 i 5 są natychmiast wykonalne. 10. Postępowanie w sprawie stosowania i uchylania środków, o których mowa w art. 53 ust. 9, jest jednoinstancyjne. Na decyzje, o których mowa w ust. 1 i 3-5 podmiot kluczowy może wnieść skargę do sądu administracyjnego. 11. Organ właściwy do spraw cyberbezpieczeństwa publikuje na swojej stronie podmiotowej Biuletynu Informacji Publicznej informację o zastosowaniu wobec podmiotu kluczowego lub kierownika podmiotu kluczowego środków, o których mowa w art. 53 ust. 9. Informacja zawiera: 1) dane podmiotu kluczowego lub imię i nazwisko kierownika podmiotu kluczowego; 2) podstawę prawną i rodzaj zastosowanego środka, o którym mowa w art. 53 ust. 9;

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				3) wskazanie daty początkowej i końcowej obowiązywania środka; 4) wskazanie, czy wobec podmiotu kluczowego lub kierownika podmiotu kluczowego ponownie zastosowano środek, a jeśli tak, to wskazanie nowej daty końcowej stosowania tego środka. 12. Publikacja, o której mowa w ust. 11, nie obejmuje tajemnicy przedsiębiorstwa, jak również innych informacji podlegających ochronie na podstawie odrębnych przepisów. 13. Organ właściwy do spraw cyberbezpieczeństwa publikuje na swojej stronie internetowej Biuletynu Informacji Publicznej informację o uchyleniu decyzji, o której mowa w ust. 1. 14. Podmiot kluczowy, w okresie stosowania wobec niego środka, o którym mowa w art. 53 ust. 9, nie może wykonywać działalności, której dotyczy ten środek. 15. W okresie stosowania środka, o którym mowa w art. 53 ust. 9, podmiot kluczowy ma obowiązek niezwłocznie podjąć działania zmierzające jedynie do usunięcia uchybień bądź zaprzestania naruszeń. W tym celu w szczególności może składać oświadczenia woli i wiedzy, podejmować czynności procesowe w postępowaniach, przedsięwziąć czynności faktyczne, jeżeli nie stoją one w sprzeczności z celem stosowanego środka lub nie zmierzają do jego obejścia. 16. W zakresie nieuregulowanym, a dotyczącym zawieszania, ograniczania i wznawiania koncesji, zezwolenia na prowadzenie działalności gospodarczej lub wstrzymania prowadzenia działalności gospodarczej zastosowanie mają przepisy odrębne.

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				Art. 59c 1. W przypadkach uzasadnionych charakterem sprawy lub pilnością przeprowadzenia czynności kontrolnych wynikających z ochrony bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego lub w przypadku potrzeby realizacji wzajemnej pomocy, o której mowa w art. 59b ust. 1 lub potrzeby sprawdzenia, czy podmiot kluczowy usunął uchybienia lub zaprzestał dokonywania naruszeń, można zarządzić przeprowadzenie kontroli doraźnej, o której mowa w art. 53 ust. 2 pkt 1. 2. Kontrola doraźna, o której mowa w art. 53 ust. 2 pkt 1, może być zarządzona w szczególności w razie potrzeby: 1) sprawdzenia informacji uzyskanej od urzędnika monitorującego, o którym mowa w art. 53 ust. 5 pkt 6, że podmiot kluczowy może <u>zagrażać</u> <u>prywatności</u> <u>użytkowników</u>; 2) sprawdzenia, w celu podjęcia działań na podstawie art. 53e ust. 4 i 5, czy podmiot kluczowy usunął uchybienia lub zaprzestał dokonywania naruszeń; 3) sprawdzenia wykonania zaleceń pokontrolnych, wykonania decyzji albo postanowień nakazujących usunięcie naruszeń prawa w związku z przeprowadzoną kontrolą. 3. Kontrolę doraźną, o której mowa w art. 53 ust. 2 pkt 1, prowadzi się zgodnie z przepisami dotyczącymi kontroli na zasadach ogólnych. Do podmiotów kontrolowanych niebędących przedsiębiorcami nie stosuje się przepisów dotyczących programu kontroli i sporządzania wystąpienia pokontrolnego. 4. Kontrola doraźna, o której mowa w art. 53 ust. 2 pkt 1, może być prowadzona także wtedy, gdy

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				nie było możliwości wcześniejszego powiadomienia podmiotu kontrolowanego o terminie przeprowadzenia kontroli. Uzasadnienie przyczyny braku powiadomienia o zamiarze wszczęcia kontroli umieszcza się w sprawozdaniu z kontroli albo protokole kontroli. 5. Kontrola doraźna, o której mowa w art. 53 ust. 2 pkt 1, kończy się sporządzeniem: 1) sprawozdania z kontroli – w przypadku jednostek samorządu terytorialnego oraz podmiotów niebędących przedsiębiorcami, 2) protokołu kontroli – w przypadku podmiotów będących przedsiębiorcami - zawierającymi opis ustalonego stanu faktycznego oraz jego ocenę, a także, w razie potrzeby, zalecenia lub wnioski wzywające do usunięcia nieprawidłowości lub usprawnienia funkcjonowania podmiotu kontrolowanego. Sprawozdanie albo protokół podpisuje kierownik komórki do spraw kontroli w organie właściwym do spraw cyberbezpieczeństwa. 6. Kierownik podmiotu kontrolowanego w terminie 3 dni roboczych od dnia otrzymania sprawozdania albo protokołu, o którym mowa w ust. 5, ma prawo przedstawić do niego stanowisko. Nie wstrzymuje to realizacji ustaleń kontroli doraźnej. 7. Jeżeli w toku kontroli doraźnej, o której mowa w art. 53 ust. 2 pkt 1, zostaną ujawnione okoliczności wskazujące na naruszenia przepisów ustawy, które wykraczają poza zakres tej kontroli, kontrolę w dalszej części przeprowadza się na zasadach ogólnych z zastosowaniem art. 54–59b. 8. Do kontroli doraźnej, o której mowa w art. 53 ust. 2 pkt 1, w zakresie nieuregulowanym niniejszą ustawą w stosunku do podmiotów

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				będących przedsiębiorcami stosuje się odpowiednio przepisy ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców, a w przypadku jednostek samorządu terytorialnego oraz podmiotów niebędących przedsiębiorcami – przepisy ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej. Przepisów art. 47 ust. 1 i 2 oraz art. 54 ust. 1 ustawy z dnia 6 marca 2018 r. – Prawo Przedsiębiorców nie stosuje się.”; Art. 8c. 1. Kierownik podmiotu kluczowego lub podmiotu ważnego ponosi odpowiedzialność za wykonywanie obowiązków w zakresie cyberbezpieczeństwa przez podmiot kluczowy lub podmiot ważny, o których mowa w art. 7b ust. 4, art. 7c, art. 7f ust. 3, art. 8, art. 8d, art. 8e, art. 8f ust. 1 i 2, art. 9–12b, art. 14 i art. 15. 2. W przypadku gdy kierownikiem podmiotu kluczowego lub podmiotu ważnego jest organ wieloosobowy i nie została wskazana osoba odpowiedzialna, odpowiedzialność ponoszą wszyscy członkowie tego organu. 3. Kierownik podmiotu kluczowego lub podmiotu ważnego ponosi odpowiedzialność także wtedy, gdy niektóre z obowiązków albo wszystkie obowiązki zostały powierzone innej osobie za jej zgodą. Art. 15. 1. Podmiot kluczowy przeprowadza, na własny koszt, co najmniej raz na 3 lata, audyt bezpieczeństwa systemu informacyjnego wykorzystywanego w procesie świadczenia usługi, zwanego dalej „audytem”, licząc od dnia sporządzenia i podpisania przez audytorów przeprowadzających audyt raportu z ostatniego audytu.

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				1a. Podmiot kluczowy przedstawia w postaci elektronicznej kopię raportu z przeprowadzonego audytu, o którym mowa w ust. 1, organowi właściwemu do spraw cyberbezpieczeństwa, w terminie trzech dni roboczych od dnia jego otrzymania przez podmiot kluczowy lub podmiot ważny. 1b. Organ właściwy do spraw cyberbezpieczeństwa może nakazać podmiotowi kluczowemu w każdym czasie lub podmiotowi ważnemu w przypadku wystąpienia incydentu poważnego lub innego naruszenia przepisów ustawy przez ten podmiot, w drodze decyzji, przeprowadzenie zewnętrznego audytu bezpieczeństwa systemu informacyjnego wykorzystywanego w procesie świadczenia usługi, wraz z określeniem terminu przekazania kopii raportu z przeprowadzonego audytu i wskazaniem rodzaju podmiotów uprawnionych do przeprowadzenia audytu. Organ właściwy do spraw cyberbezpieczeństwa może również określić zakres audytu. 1c. Decyzja, o której mowa w ust. 1b, podlega natychmiastowemu wykonaniu. Rozdział 6a Ocena bezpieczeństwa Art. 36a. 1. CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT sektorowy mogą przeprowadzić ocenę bezpieczeństwa systemów informacyjnych wykorzystywanych przez podmioty krajowego systemu cyberbezpieczeństwa. 2. Ocena bezpieczeństwa polega na przeprowadzeniu testów bezpieczeństwa systemu informacyjnego w celu identyfikacji podatności tego systemu. Wyboru rodzaju testów

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				bezpieczeństwa dokonuje się adekwatnie do systemu informacyjnego i świadczonej usługi z uwzględnieniem specyfiki sektora lub podsektora. 3. Przepisów niniejszego rozdziału nie stosuje się do ocen bezpieczeństwa systemów teleinformatycznych: 1) podmiotów krajowego systemu cyberbezpieczeństwa, które znajdują się w zbiorze organów i podmiotów, o których mowa w art. 32a ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu; 2) akredytowanych na podstawie art. 48 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2024 r. poz. 632 i 1222 oraz z 2025 r. poz. 820). 4. Zespołem właściwym do przeprowadzenia oceny bezpieczeństwa jest: 1) w przypadku podmiotów, o których mowa w art. 26 ust. 5 – CSIRT MON; 2) w przypadku podmiotów, o których mowa w art. 26 ust. 6 pkt 1 lit. a–k – CSIRT NASK; 3) w przypadku podmiotów, o których mowa w art. 26 ust. 7 pkt 1–4d – CSIRT GOV. 5. CSIRT MON, CSIRT NASK albo CSIRT GOV przeprowadza ocenę bezpieczeństwa systemu informacyjnego podmiotu krajowego systemu cyberbezpieczeństwa, po poinformowaniu organu właściwego do spraw cyberbezpieczeństwa o zamiarze przeprowadzenia oceny bezpieczeństwa. 6. CSIRT sektorowy może przeprowadzić ocenę bezpieczeństwa systemu informacyjnego podmiotu kluczowego lub podmiotu ważnego po uzyskaniu zgody CSIRT MON, CSIRT NASK lub CSIRT GOV właściwego dla danego podmiotu

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				kluczowego lub podmiotu ważnego. O zamiarze przeprowadzenia oceny bezpieczeństwa systemu informacyjnego podmiotu krajowego systemu cyberbezpieczeństwa CSIRT sektorowy informuje organ właściwy do spraw cyberbezpieczeństwa dla danego sektora. 7. Przepisów ust. 5 i 6 nie stosuje się, gdy ocena bezpieczeństwa systemu informacyjnego jest przeprowadzana na zlecenie organu właściwego do spraw cyberbezpieczeństwa. Art. 36b. 1. Ocena bezpieczeństwa systemu informacyjnego może być przeprowadzona: 1) za zgodą podmiotu krajowego systemu cyberbezpieczeństwa, wyrażoną w formie pisemnej lub formie elektronicznej pod rygorem nieważności albo 2) na zlecenie organu właściwego do spraw cyberbezpieczeństwa. 2. Ocenę bezpieczeństwa systemów informacyjnych Kancelarii Sejmu, Kancelarii Senatu, Kancelarii Prezydenta Rzeczypospolitej Polskiej, Narodowego Banku Polskiego, Biura Rzecznika Praw Obywatelskich, Biura Rzecznika Praw Dziecka, Instytutu Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu, Państwowej Inspekcji Pracy, Trybunału Konstytucyjnego, Sądu Najwyższego, sądów administracyjnych, Najwyższej Izby Kontroli, Krajowej Rady Radiofonii i Telewizji, Krajowego Biura Wyborczego, Urzędu Ochrony Danych Osobowych przeprowadza się wyłącznie po uzyskaniu zgody tych podmiotów. 3. Organ właściwy do spraw cyberbezpieczeństwa przed zleceniem przeprowadzenia oceny bezpieczeństwa przeprowadza analizę ryzyka, o której mowa w art. 53b ust. 2, i na jej podstawie

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				dokonyuje wyboru podmiotu kluczowego lub podmiotu ważnego, którego system informacyjny będzie podlegał ocenie bezpieczeństwa. 4. Ocenę bezpieczeństwa systemu informacyjnego przeprowadza się z uwzględnieniem zasady minimalizacji zakłócenia pracy systemu informacyjnego lub ograniczenia jego dostępności i nie może prowadzić do nieodwracalnego zniszczenia danych przetwarzanych w systemie informacyjnym podlegającym tej ocenie. 5. Ocena bezpieczeństwa nie może być przeprowadzona, a rozpoczęta przerywa się, jeżeli: 1) podmiot krajowego systemu cyberbezpieczeństwa nie posiada kopii bezpieczeństwa systemu; 2) istnieje zagrożenie nieodwracalnego zniszczenia danych przetwarzanych w systemie; 3) czas potrzebny na przywrócenie systemu z kopii bezpieczeństwa może w istotny sposób zakłócić pracę systemu lub ograniczyć jego dostępność; 4) czynności podejmowane podczas oceny bezpieczeństwa mogą doprowadzić do uszkodzenia produktów ICT wchodzących w skład tego systemu oraz innych systemów informacyjnych podmiotu kluczowego; 5) istnieje zagrożenie ograniczenia dostępności usług świadczonych przez podmiot krajowego systemu cyberbezpieczeństwa. 6. W celu minimalizacji negatywnych następstw oceny bezpieczeństwa systemu informacyjnego CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT sektorowy uzgadnia z podmiotem

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				krajowego systemu cyberbezpieczeństwa, w drodze porozumienia, tryb i ramowe warunki przeprowadzania tej oceny, w szczególności datę rozpoczęcia, harmonogram oraz zakres i rodzaj przeprowadzanych w ramach oceny bezpieczeństwa testów bezpieczeństwa. 7. Podmiot krajowego systemu cyberbezpieczeństwa, którego system informacyjny podlega ocenie bezpieczeństwa, przekazuje CSIRT przeprowadzającemu ocenę niezbędne informacje techniczne i organizacyjne niezbędne do przeprowadzenia oceny bezpieczeństwa oraz wskazuje imię i nazwisko, adres służbowej poczty elektronicznej oraz numer telefonu służbowego osoby upoważnionej do reprezentacji podmiotu, a także osoby upoważnionej do udzielania wyjaśnień CSIRT w trakcie przeprowadzania oceny bezpieczeństwa. 8. CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT sektorowy mogą wytwarzać lub pozyskiwać urządzenia lub programy komputerowe, o których mowa w art. 269b ustawy z dnia 6 czerwca 1997 r. – Kodeks karny (Dz. U. z 2025 r. poz. 383), oraz ich używać w celu określenia podatności ocenianego systemu informacyjnego na możliwość popełnienia przestępstw, o których mowa w art. 165 § 1 pkt 4, art. 267 § 3, art. 268a § 1 albo § 2 w związku z § 1, art. 269 § 1 i 2 albo art. 269a ustawy z dnia 6 czerwca 1997 r. – Kodeks karny. 9. Używając urządzeń lub programów komputerowych, o których mowa w ust. 8, CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT sektorowy mogą uzyskać dostęp do informacji dla nich nieprzeznaczonej, przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				inne szczególne zabezpieczenie, lub mogą uzyskać dostęp do całości lub części tego systemu informacyjnego. 10. Informacje uzyskane przez CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT sektorowy w wyniku przeprowadzania oceny bezpieczeństwa systemu informacyjnego stanowią tajemnicę prawnie chronioną i nie mogą być wykorzystane do realizacji innych zadań ustawowych CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT sektorowego. 11. Materiały zawierające informacje, o których mowa w ust. 10, podlegają niezwłocznemu, trwałemu i nieodwracalnemu, protokolarnemu zniszczeniu, którego dokonuje komisja. Zniszczeniu nie podlegają informacje o czynnościach przeprowadzanych w ramach oceny bezpieczeństwa oraz o wykrytych podatnościach systemu informacyjnego. 12. Komisja, o której mowa w ust. 11, składa się z trzech osób powołanych przez osobę kierującą zespołem CSIRT spośród pracowników, funkcjonariuszy lub żołnierzy realizujących zadania odpowiednio w CSIRT MON, CSIRT NASK, CSIRT GOV albo CSIRT sektorowym. 13. Po przeprowadzeniu oceny bezpieczeństwa systemu informacyjnego CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT sektorowy sporządzają i przekazują podmiotowi, którego system podlegał ocenie bezpieczeństwa, raport zawierający podsumowanie przeprowadzonych w ramach oceny bezpieczeństwa czynności oraz wskazanie wykrytych podatności systemu informacyjnego. Jeżeli ocenę bezpieczeństwa przeprowadza CSIRT sektorowy, to raport

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				przekazywany jest do właściwego CSIRT MON, CSIRT NASK albo CSIRT GOV. Art. 36c. Jeżeli wykryta podatność może wystąpić w innych systemach informacyjnych, CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT sektorowy informują niezwłocznie ministra właściwego do spraw informatyzacji oraz Pełnomocnika o wykrytej podatności oraz o możliwości jej wystąpienia w innych systemach informacyjnych. Art. 36d. Rada Ministrów określi, w drodze rozporządzenia: 1) tryb przeprowadzania oceny bezpieczeństwa, o której mowa w art. 36a, 2) szczegółowe informacje przekazywane do CSIRT niezbędne do przeprowadzenia oceny bezpieczeństwa, 3) rodzaje przeprowadzanych testów bezpieczeństwa w ramach oceny bezpieczeństwa, o których mowa w art. 36a ust. 2, 4) sposób niszczenia materiałów zawierających informacje, o których mowa w art. 36b ust. 10, 5) tryb działania komisji, o której mowa w art. 36b ust. 11, 6) wzór protokołu zniszczenia materiałów zawierających informacje, o których mowa w art. 36b ust. 10 – mając na uwadze konieczność zapewnienia sprawnego przeprowadzenia oceny bezpieczeństwa, bezpieczeństwo systemów informacyjnych podlegających ocenie, rodzaj materiałów podlegających zniszczeniu i konieczność zapewnienia efektywności i przejrzystości prowadzonych działań komisji.

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				Art. 67g. 1. Minister właściwy do spraw informatyzacji w przypadku wystąpienia incydentu krytycznego może, w drodze decyzji, wydać polecenie zabezpieczające. 2. Polecenie zabezpieczające dotyczy nieokreślonej liczby podmiotów kluczowych lub podmiotów ważnych oraz podmiotów finansowych, z wyłączeniem podmiotów określonych w art. 16 rozporządzenia 2022/2554. 3. Do postępowania w sprawie o wydanie polecenia zabezpieczającego nie stosuje się art. 10, art. 34, art. 79, art. 81, art. 81a, art. 107 § 1 pkt 3, art. 145 § 1 pkt 4 i art. 156 § 1 pkt 4 oraz rozdziału 8 działu I ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego, a pozostałe przepisy tej ustawy stosuje się odpowiednio. 4. Stronę zawiadamia się o czynnościach w sprawie przez publiczne opublikowanie informacji na stronie podmiotowej Biuletynu Informacji Publicznej ministra właściwego do spraw informatyzacji. 5. Przed wydaniem polecenia zabezpieczającego minister właściwy do spraw informatyzacji przeprowadza we współpracy z Zespołem, o którym mowa w art. 35 ust. 3, analizę obejmującą: 1) istotność cyberzagrożenia związanego z incydentem krytycznym; 2) szacowanie ryzyka związane z zaistniałym incydentem krytycznym; 3) przewidywane lub zaistniałe skutki incydentu krytycznego; 4) skuteczność obowiązku określonego zachowania zmniejszającego skutki incydentu krytycznego lub zapobiegającego jego rozprzestrzenieniu;

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				5) ocenę stopnia dotkliwości wprowadzanych obowiązków dla podmiotów objętych poleceniem zabezpieczającym oraz proporcjonalności tych obowiązków do celu ich wprowadzania. 6. Do analizy, o której mowa w ust. 5, nie stosuje się art. 106 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego. 7. Pełnomocnik, dyrektor Rządowego Centrum Bezpieczeństwa, Szef Agencji Bezpieczeństwa Wewnętrznego oraz minister właściwy do spraw informatyzacji, może wzywać podmioty, o których mowa w ust. 2, lub organy administracji publicznej do udzielenia informacji niezbędnych do przeprowadzenia analizy. Organy administracji publicznej udzielają informacji, o których mowa w zdaniu pierwszym, niezwłocznie, nie później niż w ciągu 72 godzin od otrzymania wezwania. 8. Przedstawiciele podmiotów, o których mowa w ust. 2, organizacji społecznych zrzeszających podmioty, o których mowa w ust. 2, lub organów administracji publicznej mogą być zapraszani przez Pełnomocnika do udziału w pracach Zespołu, o którym mowa w art. 35 ust. 3, lub w jego posiedzeniach w związku z przygotowywaniem analizy, o której mowa w ust. 5. 9. Polecenie zabezpieczające zawiera: 1) wskazanie rodzaju lub rodzajów podmiotów, których dotyczy; 2) obowiązek określonego zachowania zmniejszającego skutki incydentu krytycznego lub pociągającego jego rozprzestrzenienie; 3) termin jego wdrożenia. 10. Obowiązkiem określonego zachowania, o którym mowa w ust. 9 pkt 2, jest:

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				1) nakaz przeprowadzenia szacowania ryzyka związanego ze stosowaniem określonego produktu ICT, usługi ICT lub procesu ICT i wprowadzenie środków ochrony proporcjonalnych do identyfikowanych ryzyk; 2) nakaz przeglądu planów ciągłości działania, planów awaryjnych i planów odtworzenia działalności pod kątem ryzyka wystąpienia incydentu krytycznego związanego z daną podmiotem; 3) nakaz zastosowania określonej poprawki bezpieczeństwa w produkcie ICT lub usłudze ICT po identyfikacji podatności; 4) nakaz szczególnej konfiguracji produktu ICT lub usługi ICT, zabezpieczającej przed wykorzystaniem określonej podatności; 5) nakaz wzmożonego monitorowania zachowania systemu informatycznego; 6) zakaz korzystania z określonego produktu ICT lub usługi ICT, które posiada podatność, która przyczyniła się do zaistnienia incydentu krytycznego; 7) nakaz wprowadzenia ograniczenia ruchu sieciowego przychodzącego do infrastruktury podmiotu kluczowego lub podmiotu ważnego, który skutkując zakłóceniem usług świadczonych przez ten podmiot został sklasyfikowany przez CSIRT MON, CSIRT NASK lub CSIRT GOV jako przyczyna trwającego incydentu krytycznego; 8) nakaz wstrzymania dystrybucji lub zakaz instalacji określonej wersji oprogramowania; 9) nakaz zabezpieczenia określonych informacji, w tym danych osobowych;

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				10) nakaz wytworzenia obrazów stanu określonych urządzeń zainfekowanych złośliwym oprogramowaniem. 11. Wskazanie obowiązku określonego zachowania, o którym mowa w ust. 9 pkt 2, następuje z uwzględnieniem środków adekwatnych, w szczególności w świetle analizy, o której mowa w ust. 5. 12. Polecenie zabezpieczające wydaje się na czas koordynacji obsługi incydentu krytycznego lub na czas oznaczony, nie dłużej niż na dwa lata. 13. Polecenie zabezpieczające wygasa: 1) z dniem wskazanym w ogłoszeniu o zakończeniu koordynacji obsługi incydentu w dzienniku urzędowym ministra właściwego do spraw informatyzacji, lub 2) po upływie czasu, na który zostało wydane. 14. Polecenie zabezpieczające podlega natychmiastowej wykonalności. 15. Minister właściwy do spraw informatyzacji ogłasza komunikat o wydaniu polecenia zabezpieczającego, w swoim dzienniku urzędowym oraz na stronie internetowej urzędu obsługującego ministra. Załącznikiem do komunikatu jest wydane polecenie zabezpieczające. 16. Polecenie zabezpieczające uznaje się za doręczone z chwilą ogłoszenia komunikatu o wydaniu polecenia zabezpieczającego w dzienniku urzędowym ministra właściwego do spraw informatyzacji. 17. Od polecenia zabezpieczającego nie przysługuje wniosek o ponowne rozpatrzenie sprawy.

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

Art. 32	2. Państwa członkowskie zapewniają, by wykonując uprawnienia nadzorcze wobec podmiotów kluczowych, właściwe organy były uprawnione do objęcia tych podmiotów co najmniej: a) kontrolami na miejscu i nadzorem zdalnym, w tym wyrywkowymi kontrolami prowadzonymi przez przeszkolonych pracowników;	TAK	Art. 1 pkt 63 (art. 53 ust. 2 pkt 1) i pkt 69 (art. 59c)	Art. 53. 2. W ramach nadzoru, o którym mowa w ust. 1, organ właściwy do spraw cyberbezpieczeństwa w stosunku do podmiotów kluczowych może: 1) prowadzić kontrole, w tym doraźne, w siedzibie podmiotu, miejscu wykonywania działalności gospodarczej lub innej; Art. 59c. 1. W przypadkach uzasadnionych charakterem sprawy lub pilnością przeprowadzenia czynności kontrolnych wynikających z ochrony bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego lub w przypadku potrzeby realizacji wzajemnej pomocy, o której mowa w art. 59b ust. 1, lub potrzeby sprawdzenia, czy podmiot kluczowy usunął uchybienia lub zaprzestał dokonywania naruszeń, można zarządzić przeprowadzenie kontroli doraźnej, o której mowa w art. 53 ust. 2 pkt 1. 2. Kontrola doraźna, o której mowa w art. 53 ust. 2 pkt 1, może być zarządzona w szczególności w razie potrzeby: 1) sprawdzenia informacji uzyskanej od urzędnika monitorującego, o którym mowa w art. 53 ust. 5 pkt 6, że podmiot kluczowy może naruszać przepisy ustawy; 2) sprawdzenia, w celu podjęcia działań na podstawie art. 53e ust. 4 i 5, czy podmiot kluczowy usunął uchybienia lub zaprzestał dokonywania naruszeń; 3) sprawdzenia wykonania zaleceń pokontrolnych, wykonania decyzji albo postanowień nakazujących usunięcie naruszeń prawa w związku z przeprowadzoną kontrolą. 3. Kontrolę doraźną, o której mowa w art. 53 ust. 2 pkt 1, prowadzi się zgodnie z przepisami

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				dotyczącymi kontroli na zasadach ogólnych. Do podmiotów kontrolowanych niebędących przedsiębiorcami nie stosuje się przepisów dotyczących programu kontroli i sporządzania wystąpienia pokontrolnego. 4. Kontrola doraźna, o której mowa w art. 53 ust. 2 pkt 1, może być prowadzona także wtedy, gdy nie było możliwości wcześniejszego powiadomienia podmiotu kontrolowanego o terminie przeprowadzenia kontroli. Uzasadnienie przyczyny braku powiadomienia o zamiarze wszczęcia kontroli umieszcza się w sprawozdaniu z kontroli albo protokole kontroli. 5. Kontrola doraźna, o której mowa w art. 53 ust. 2 pkt 1, kończy się sporządzeniem: 1) sprawozdania z kontroli – w przypadku jednostek samorządu terytorialnego oraz podmiotów niebędących przedsiębiorcami, 2) protokołu kontroli – w przypadku podmiotów będących przedsiębiorcami – zawierającymi opis ustalonego stanu faktycznego oraz jego ocenę, a także, w razie potrzeby, zalecenia lub wnioski wzywające do usunięcia nieprawidłowości lub usprawnienia funkcjonowania podmiotu kontrolowanego. Sprawozdanie z kontroli albo protokół kontroli podpisuje kierownik komórki do spraw kontroli w organie właściwym do spraw cyberbezpieczeństwa. 6. Kierownik podmiotu kontrolowanego w terminie 3 dni roboczych od dnia otrzymania sprawozdania z kontroli albo protokołu kontroli, o których mowa w ust. 5, ma prawo przedstawić do niego stanowisko. Nie wstrzymuje to realizacji ustaleń kontroli doraźnej.

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				7. Jeżeli w toku kontroli doraźnej, o której mowa w art. 53 ust. 2 pkt 1, zostaną ujawnione okoliczności wskazujące na naruszenia przepisów ustawy, które wykraczają poza zakres tej kontroli, kontrolę w dalszej części przeprowadza się na zasadach ogólnych z zastosowaniem art. 54–59b. 8. Do kontroli doraźnej, o której mowa w art. 53 ust. 2 pkt 1, w zakresie nieuregulowanym niniejszą ustawą w stosunku do podmiotów będących przedsiębiorcami stosuje się odpowiednio przepisy ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców, a w przypadku jednostek samorządu terytorialnego oraz podmiotów niebędących przedsiębiorcami – przepisy ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej. Przepisów art. 47 ust. 1 i 2 oraz art. 54 ust. 1 ustawy z dnia 6 marca 2018 r. – Prawo Przedsiębiorców „i to jej”;
Art. 32	b) regularnymi ukierunkowanymi audytami bezpieczeństwa prowadzonymi przez podmiot lub właściwy organ;	TAK	Art. 1 pkt 23 (art. 15 ust. 1 i 1a)	Art. 15. 1. Podmiot kluczowy przeprowadza, na własny koszt, co najmniej raz na 3 lata, audyt bezpieczeństwa systemu informacyjnego wykorzystywanego w procesie świadczenia usługi, zwanego dalej „audytem”, licząc od dnia sporządzenia i podpisania przez audytorów przeprowadzających audyt raportu z ostatniego audytu. 1a. Podmiot kluczowy przedstawia w postaci elektronicznej kopię raportu z przeprowadzonego audytu, o którym mowa w ust. 1, organowi właściwemu do spraw cyberbezpieczeństwa, w terminie trzech dni roboczych od dnia jego otrzymania przez podmiot kluczowy lub podmiot ważny.
Art. 32	c) audytami doraźnymi, w tym w uzasadnionych przypadkach w związku z wystąpieniem poważnego incydentu lub z naruszeniem przepisów dyrektywy przez podmiot kluczowy;	TAK	Art. 1 pkt 23 (art. 15 ust. 1b i 1c), pkt 63 (art. 53	Art. 15. 1b. Organ właściwy do spraw cyberbezpieczeństwa może nakazać podmiotowi kluczowemu w każdym czasie lub podmiotowi

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

			ust. 2) i pkt 39 (Rozdział 6a) ważnemu w przypadku wystąpienia incydentu poważnego lub innego naruszenia przepisów ustawy przez ten podmiot, w drodze decyzji, przeprowadzenie zewnętrznego audytu bezpieczeństwa systemu informacyjnego wykorzystywanego w procesie świadczenia usługi, wraz z określeniem terminu przekazania kopii raportu z przeprowadzonego audytu i wskazaniem rodzaju podmiotów uprawnionych do przeprowadzenia audytu. Organ właściwy do spraw cyberbezpieczeństwa może również określić zakres audytu. 1c. Decyzja, o której mowa w ust. 1b, podlega natychmiastowemu wykonaniu, Art. 53 ust. 2: 2) zobowiązać podmiot, w drodze decyzji, do przeprowadzanie audytu, o którym mowa w art. 15 ust. 1b, w sytuacji wystąpienia poważnego incydentu lub naruszenia przepisów ustawy przez podmiot klurowy; Rozdział 6a Ocena bezpieczeństwa Art. 36a. 1. CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT sektorowy mogą przeprowadzić ocenę bezpieczeństwa systemów informacyjnych wykorzystywanych przez podmioty krajowego systemu cyberbezpieczeństwa. 2. Ocena bezpieczeństwa polega na przeprowadzeniu testów bezpieczeństwa systemu informacyjnego w celu identyfikacji podatności tego systemu. Wyboru rodzaju testów bezpieczeństwa dokonuje się adekwatnie do systemu informacyjnego i świadczonej usługi z uwzględnieniem specyfiki sektora lub podsektora.

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				3. Przepisów niniejszego rozdziału nie stosuje się do ocen bezpieczeństwa systemów teleinformatycznych: 1) podmiotów krajowego systemu cyberbezpieczeństwa, które znajdują się w zbiorze organów i podmiotów, o których mowa w art. 32a ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu; 2) akredytowanych na podstawie art. 48 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2024 r. poz. 632 i 1222 oraz z 2025 r. poz. 820). 4. Zespołem właściwym do przeprowadzenia oceny bezpieczeństwa jest: 1) w przypadku podmiotów, o których mowa w art. 26 ust. 5 – CSIRT MON; 2) w przypadku podmiotów, o których mowa w art. 26 ust. 6 pkt 1 lit. a–k – CSIRT NASK; 3) w przypadku podmiotów, o których mowa w art. 26 ust. 7 pkt 1–4d – CSIRT GOV. 5. CSIRT MON, CSIRT NASK albo CSIRT GOV przeprowadza ocenę bezpieczeństwa systemu informacyjnego podmiotu krajowego systemu cyberbezpieczeństwa, po poinformowaniu organu właściwego do spraw cyberbezpieczeństwa o zamiarze przeprowadzenia oceny bezpieczeństwa. 6. CSIRT sektorowy może przeprowadzić ocenę bezpieczeństwa systemu informacyjnego podmiotu kluczowego lub podmiotu ważnego po uzyskaniu zgody CSIRT MON, CSIRT NASK lub CSIRT GOV właściwego dla danego podmiotu kluczowego lub podmiotu ważnego. O zamiarze przeprowadzenia oceny bezpieczeństwa systemu informacyjnego podmiotu krajowego systemu

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				cyberbezpieczeństwa CSIRT sektorowy informuje organ właściwy do spraw cyberbezpieczeństwa dla danego sektora. 7. Przepisów ust. 5 i 6 nie stosuje się, gdy ocena bezpieczeństwa systemu informacyjnego jest przeprowadzana na zlecenie organu właściwego do spraw cyberbezpieczeństwa. Art. 36b. 1. Ocena bezpieczeństwa systemu informacyjnego może być przeprowadzona: 1) za zgodą podmiotu krajowego systemu cyberbezpieczeństwa, wyrażoną w formie pisemnej lub formie elektronicznej pod rygorem nieważności albo 2) na zlecenie organu właściwego do spraw cyberbezpieczeństwa. 2. Ocenę bezpieczeństwa systemów informacyjnych Kancelarii Sejmu, Kancelarii Senatu, Kancelarii Prezydenta Rzeczypospolitej Polskiej, Narodowego Banku Polskiego, Biura Rzecznika Praw Obywatelskich, Biura Rzecznika Praw Dziecka, Instytutu Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu, Państwowej Inspekcji Pracy, Trybunału Konstytucyjnego, Sądu Najwyższego, sądów administracyjnych, Najwyższej Izby Kontroli, Krajowej Rady Radiofonii i Telewizji, Krajowego Biura Wyborczego, Urzędu Ochrony Danych Osobowych przeprowadza się wyłącznie po uzyskaniu zgody tych podmiotów. 3. Organ właściwy do spraw cyberbezpieczeństwa przed zleceniem przeprowadzenia oceny bezpieczeństwa przeprowadza analizę ryzyka, o której mowa w art. 53b ust. 2, i na jej podstawie dokonuje wyboru podmiotu kluczowego lub podmiotu ważnego, którego system informacyjny będzie podlegał ocenie bezpieczeństwa.

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				4. Ocenę bezpieczeństwa systemu informacyjnego przeprowadza się z uwzględnieniem zasady minimalizacji zakłócenia pracy systemu informacyjnego lub ograniczenia jego dostępności i nie może prowadzić do nieodwracalnego zniszczenia danych przetwarzanych w systemie informacyjnym podlegającym tej ocenie. 5. Ocena bezpieczeństwa nie może być przeprowadzona, a rozpoczęta przerywa się, jeżeli: 1) podmiot krajowego systemu cyberbezpieczeństwa nie posiada kopii bazy danych i twórczości; 2) istnieje zagrożenie nieodwracalnego zniszczenia danych przetwarzanych w systemie; 3) czas potrzebny na przywrócenie systemu z kopii bezpieczeństwa może w istotny sposób zakłócić pracę systemu lub ograniczyć jego dostępność; 4) czynności podejmowane podczas oceny bezpieczeństwa mogą doprowadzić do uszkodzenia produktów ICT wchodzących w skład tego systemu oraz innych systemów informacyjnych podmiotu kluczowego; 5) istnieje zagrożenie ograniczenia dostępności usług świadczonych przez podmiot krajowego systemu cyberbezpieczeństwa. 6. W celu minimalizacji negatywnych następstw oceny bezpieczeństwa systemu informacyjnego CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT sektorowy uzgadnia z podmiotem krajowego systemu cyberbezpieczeństwa, w drodze porozumienia, tryb i ramowe warunki przeprowadzania tej oceny, w szczególności datę

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				rozpoczęcia, harmonogram oraz zakres i rodzaj przeprowadzanych w ramach oceny bezpieczeństwa testów bezpieczeństwa. 7. Podmiot krajowego systemu cyberbezpieczeństwa, którego system informacyjny podlega ocenie bezpieczeństwa, przekazuje CSIRT przeprowadzającemu ocenę niezbędne informacje techniczne i organizacyjne niezbędne do przeprowadzenia oceny bezpieczeństwa oraz wskazuje imię i nazwisko, adres służbowej poczty elektronicznej oraz numer telefonu służbowego osoby upoważnionej do reprezentacji podmiotu, a także osoby upoważnionej do udzielania wyjaśnień CSIRT w trakcie przeprowadzania oceny bezpieczeństwa. 8. CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT sektorowy mogą wytwarzać lub pozyskiwać urządzenia lub programy komputerowe, o których mowa w art. 269b ustawy z dnia 6 czerwca 1997 r. – Kodeks karny (Dz. U. z 2025 r. poz. 383), oraz ich używać w celu określenia podatności ocenianego systemu informacyjnego na możliwość popełnienia przestępstw, o których mowa w art. 165 § 1 pkt 4, art. 267 § 3, art. 268a § 1 albo § 2 w związku z § 1, art. 269 § 1 i 2 albo art. 269a ustawy z dnia 6 czerwca 1997 r. – Kodeks karny. 9. Używając urządzeń lub programów komputerowych, o których mowa w ust. 8, CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT sektorowy mogą uzyskać dostęp do informacji dla nich nieprzeznaczonej, przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne zabezpieczenie, lub mogą uzyskać dostęp do całości lub części tego systemu informacyjnego.

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				10. Informacje uzyskane przez CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT sektorowy w wyniku przeprowadzania oceny bezpieczeństwa systemu informacyjnego stanowią tajemnicę prawnie chronioną i nie mogą być wykorzystane do realizacji innych zadań ustawowych CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT sektorowego. 11. Materiały zawierające informacje, o których mowa w ust. 10, podlegają niezwłocznemu, trwałemu i nieodwracalnemu, protokolarnemu zniszczeniu, którego dokonuje komisja. Zniszczeniu nie podlegają informacje o czynnościach przeprowadzanych w ramach oceny bezpieczeństwa oraz o wykrytych podatnościach systemu informacyjnego. 12. Komisja, o której mowa w ust. 11, składa się z trzech osób powołanych przez osobę kierującą zespołem CSIRT spośród pracowników, funkcjonariuszy lub żołnierzy realizujących zadania odpowiednio w CSIRT MON, CSIRT NASK, CSIRT GOV albo CSIRT sektorowym. 13. Po przeprowadzeniu oceny bezpieczeństwa systemu informacyjnego CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT sektorowy sporządzają i przekazują podmiotowi, którego system podlegał ocenie bezpieczeństwa, raport zawierający podsumowanie przeprowadzonych w ramach oceny bezpieczeństwa czynności oraz wskazanie wykrytych podatności systemu informacyjnego. Jeżeli ocenę bezpieczeństwa przeprowadza CSIRT sektorowy, to raport przekazywany jest do właściwego CSIRT MON, CSIRT NASK albo CSIRT GOV. Art. 36c. Jeżeli wykryta podatność może wystąpić w innych systemach informacyjnych, CSIRT

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				MON, CSIRT NASK, CSIRT GOV i CSIRT sektorowy informują niezwłocznie ministra właściwego do spraw informatyzacji oraz Pełnomocnika o wykrytej podatności oraz o możliwości jej wystąpienia w innych systemach informacyjnych. Art. 36d. Rada Ministrów określi, w drodze rozporządzenia: 1) tryb przeprowadzania oceny bezpieczeństwa, o której mowa w art. 36a, 2) szczegółowe informacje przekazywane do CSIRT niezbędne do przeprowadzenia oceny bezpieczeństwa, 3) rodzaje przeprowadzanych testów bezpieczeństwa w ramach oceny bezpieczeństwa, o których mowa w art. 36a ust. 2, 4) sposób niszczenia materiałów zawierających informacje, o których mowa w art. 36b ust. 10, 5) tryb działania komisji, o której mowa w art. 36b ust. 11, 6) wzór protokołu zniszczenia materiałów zawierających informacje, o których mowa w art. 36b ust. 10 – mając na uwadze konieczność zapewnienia sprawnego przeprowadzenia oceny bezpieczeństwa, bezpieczeństwo systemów informacyjnych podlegających ocenie, rodzaj materiałów podlegających zniszczeniu i konieczność zapewnienia efektywności i przejrzystości prowadzonych działań komisji.
Art. 32	d) skanami bezpieczeństwa na podstawie obiektywnych, niedyskryminacyjnych, sprawiedliwych i przejrzystych kryteriów szacowania ryzyka, w razie potrzeby we współpracy z danym podmiotem;	TAK	Art. 1 pkt 63 (art. 53 ust. 2 pkt 3)	Art. 53. 2: 3) zlecić CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT sektorowemu, dokonanie oceny bezpieczeństwa systemu informacyjnego podmiotu klawidowego;

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

Art. 32	e) wnioskami o udzielenie informacji niezbędnych do oceny środków zarządzania ryzykiem w cyberbezpieczeństwie przyjętych przez dany podmiot, w tym udokumentowanej polityki cyberbezpieczeństwa, a także zgodności z obowiązkiem przedkładania informacji właściwym organom zgodnie z art. 27;	TAK	Art. 1 pkt 63 (art. 53 ust. 2 pkt 4)	Art. 53. 2: 4) wystąpić z wnioskiem o udzielenie informacji niezbędnych do oceny środków, o których mowa w art. 8 ust. 1 pkt 2 i 5, a także zgodności z obowiązkiem przedkładania informacji właściwym organom zgodnie z art. 7;
Art. 32	f) wnioskami o udzielenie dostępu do danych, dokumentów i informacji koniecznych do wykonywania ich zadań i obowiązków;	TAK	Art. 1 pkt 63 (art. 53 ust. 2 pkt 5)	Art. 53. 2: 5) wystąpić z wnioskiem o udzielenie dostępu do danych, dokumentów i informacji koniecznych do wykonywania ich zadań i obowiązków;
Art. 32	g) wnioskami o przedstawienie dowodów realizacji polityki cyberbezpieczeństwa, takich jak wyniki audytu bezpieczeństwa przeprowadzonego przez wykwalifikowanego audytora oraz odpowiednie dowody.	TAK	Art. 1 pkt 63 (art. 53 ust. 2 pkt 6)	Art. 53. 2: 6) wystąpić z wnioskiem o przedstawienie dowodów realizacji wymogów, o których mowa w art. 8 ust. 1.
Art. 32	Ukierunkowane audyty bezpieczeństwa, o których mowa w akapicie pierwszym lit. b), opierają się na oszacowaniach ryzyka przeprowadzonych przez właściwy organ lub badany podmiot bądź na innych dostępnych informacjach dotyczących ryzyka. Wyniki ukierunkowanych audytów bezpieczeństwa udostępnia się właściwemu organowi. Koszty takiego ukierunkowanego audytu bezpieczeństwa prowadzonego przez niezależną instytucję pokrywa podmiot poddawany audytowi, z wyjątkiem należycie uzasadnionych przypadków, gdy właściwy organ postanowi inaczej.			
Art. 32	3. Wykonując swoje uprawnienia na mocy ust. 2 lit. e), f) lub g), właściwe organy podają cel wniosku i określają informacje, o które wnoszą.	TAK	Art. 1 pkt 64 (art. 53c ust. 1 i 2 pkt 3 i 4)	Art. 53c. 1. Podmiot kluczowy lub podmiot ważny przekazuje na żądanie organu właściwego do spraw cyberbezpieczeństwa dane, informacje i dokumenty niezbędne do wykonywania przez ten organ jego uprawnień i obowiązków z zakresu sprawowania nadzoru i kontroli określonych w ustawie. 2. Żądanie, o którym mowa w ust. 1, ma być proporcjonalne do celu, jakiemu ma służyć, oraz zawierać: 3) wskazanie żądanych danych, informacji lub dokumentów oraz okresu, który ich dotyczy;

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				4) wskazanie celu, jakiemu dane, informacje lub dokumenty mają służyć;
Art. 32	4. Państwa członkowskie zapewniają, aby wykonując uprawnienia w zakresie egzekwowania przepisów wobec podmiotów kluczowych, ich właściwe organy były uprawnione co najmniej do: a) wydawania ostrzeżeń dotyczących naruszeń przez dane podmioty informacji dyrektorzy;	TAK	Art. 1 pkt 63 (art. 53 ust. 4)	Art. 53. 4. W przypadku uzasadnionego podejrzenia, że działania lub zaniechania podmiotu kluczowego mogą naruszać przepisy ustawy, organ właściwy do spraw cyberbezpieczeństwa kieruje do tego podmiotu pismo w formie elektronicznej z ostrzeżeniem, w którym wskazuje czynności, jakie należy podjąć w celu zapobieżenia lub zaprzestania naruszania przepisów ustawy oraz termin na ich wykonanie.
Art. 32	b) wydawania wiążących poleceń – w tym dotyczących podjęcia środków niezbędnych do zapobieżenia incydentowi lub usunięcia jego skutków oraz określenia terminów wdrożenia takich środków i zgłoszenia ich wdrożenia – lub nakazów zobowiązujących dane podmioty do naprawienia stwierdzonych uchybień lub usunięcia informacji dyrektorzy;	TAK	Art. 1 pkt 63 (art. 53 ust. 5 i 7) i pkt 75 (art. 67g)	Art. 53. 5. W celu egzekwowania przepisów ustawy organ właściwy do spraw cyberbezpieczeństwa w stosunku do podmiotów kluczowych, także wtedy gdy podmiot kluczowy nie zastosował się do pisma z ostrzeżeniem, o którym mowa w ust. 4, może: 1) nakazać podjęcie określonych czynności dotyczących obrotu i wydania; 7. Nakaz, o którym mowa w ust. 5 pkt 1, jest inną czynnością z zakresu administracji publicznej, na którą przysługuje skarga do sądu administracyjnego i wymaga uzasadnienia. Art. 67g. 1. Minister właściwy do spraw informatyzacji w przypadku wystąpienia incydentu krytycznego może, w drodze decyzji, wydać polecenie zabezpieczające. 2. Polecenie zabezpieczające dotyczy nieokreślonej liczby podmiotów kluczowych lub podmiotów ważnych oraz podmiotów finansowych, z wyłączeniem podmiotów określonych w art. 16 rozporządzenia 2022/2554. 3. Do postępowania w sprawie o wydanie polecenia zabezpieczającego nie stosuje się art.

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				10, art. 34, art. 79, art. 81, art. 81a, art. 107 § 1 pkt 3, art. 145 § 1 pkt 4 i art. 156 § 1 pkt 4 oraz rozdziału 8 działu I ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego, a pozostałe przepisy tej ustawy stosuje się odpowiednio. 4. Stronę zawiadamia się o czynnościach w sprawie przez publiczne opublikowanie informacji na stronie podmiotowej Biuletynu Informacji Publicznej ministra właściwego do spraw informatyzacji. 5. Przed wydaniem polecenia zabezpieczającego minister właściwy do spraw informatyzacji przeprowadza we współpracy z Zespołem, o którym mowa w art. 35 ust. 3, analizę obejmującą: 1) istotność cyberzagrożenia związanego z i 2) szacowanie ryzyka związane z zaistniałym i 3) przewidywane lub zaistniałe skutki incydentu krytycznego; 4) skuteczność obowiązku określonego zachowania zmniejszającego skutki incydentu krytycznego lub zapobiegającego jego 5) ocenę stopnia dotkliwości wprowadzanych obowiązków dla podmiotów objętych poleceniem zabezpieczającym oraz proporcjonalności tych obowiązków do celu ich wprowadzania. 6. Do analizy, o której mowa w ust. 5, nie stosuje się art. 106 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego. 7. Pełnomocnik, dyrektor Rządowego Centrum Bezpieczeństwa, Szef Agencji Bezpieczeństwa Wewnętrznego oraz minister właściwy do spraw

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				informatyzacji, może wzywać podmioty, o których mowa w ust. 2, lub organy administracji publicznej do udzielenia informacji niezbędnych do przeprowadzenia analizy. Organy administracji publicznej udzielają informacji, o których mowa w zdaniu pierwszym, niezwłocznie, nie później niż w ciągu 72 godzin od otrzymania wezwania. 8. Przedstawiciele podmiotów, o których mowa w ust. 2, organizacji społecznych zrzeszających podmioty, o których mowa w ust. 2, lub organów administracji publicznej mogą być zapraszani przez Pełnomocnika do udziału w pracach Zespołu, o którym mowa w art. 35 ust. 3, lub w jego posiedzeniach w związku z przygotowaniem analizy, o której mowa w ust. 5. 9. Polecenie zabezpieczające zawiera: 1) wskazanie rodzaju lub rodzajów podmiotów, których dotyczy; 2) obowiązek określonego zachowania zmniejszającego skutki incydentu krytycznego lub zapobiegającego jego rozprzestrzenieniu; 3) termin jego wdrożenia. 10. Obowiązkiem określonego zachowania, o którym mowa w ust. 9 pkt 2, jest: 1) nakaz przeprowadzenia szacowania ryzyka związanego ze stosowaniem określonego produktu ICT, usługi ICT lub procesu ICT i wprowadzenie środków ochrony proporcjonalnych do zidentyfikowanych ryzyk; 2) nakaz przeglądu planów ciągłości działania, planów awaryjnych i planów odtworzenia działalności pod kątem ryzyka wystąpienia

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				incydentu krytycznego związanego z daną podmiotowością; 3) nakaz zastosowania określonej poprawki bezpieczeństwa w produkcie ICT lub usłudze ICT powodującym daną podmiotowość; 4) nakaz szczególnej konfiguracji produktu ICT lub usługi ICT, zabezpieczającej przed wykorzystaniem określonej podmiotowości; 5) nakaz wzmożonego monitorowania oprogramowania i formacji; 6) zakaz korzystania z określonego produktu ICT lub usługi ICT, które posiada podatność, która przyczyniła się do zaistnienia incydentu krytycznego; 7) nakaz wprowadzenia ograniczenia ruchu sieciowego przychodzącego do infrastruktury podmiotu kluczowego lub podmiotu ważnego, który skutkując zakłóceniem usług świadczonych przez ten podmiot został sklasyfikowany przez CSIRT MON, CSIRT NASK lub CSIRT GOV jako przyczyna trwania i wydatku krytycznego; 8) nakaz wstrzymania dystrybucji lub zakaz importacji określonej w rejestrze oprogramowania; 9) nakaz zabezpieczenia określonych informacji, w tym danych i komunikatów; 10) nakaz wytworzenia obrazów stanu określonych urządzeń zainfekowanych złośliwym oprogramowaniem. 11. Wskazanie obowiązku określonego zachowania, o którym mowa w ust. 9 pkt 2, następuje z uwzględnieniem środków adekwatnych, w szczególności w świetle analizy, o której mowa w ust. 5.

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				12. Polecenie zabezpieczające wydaje się na czas koordynacji obsługi incydentu krytycznego lub na czas oznaczony, nie dłużej niż na dwa lata. 13. Polecenie zabezpieczające wygasa: 1) z dniem wskazanym w ogłoszeniu o zakończeniu koordynacji obsługi incydentu w dzienniku urzędowym ministra właściwego do spraw informatyzacji, lub 2) po upływie czasu, na który zostało wydane. 14. Polecenie zabezpieczające podlega natychmiastowej wykonalności. 15. Minister właściwy do spraw informatyzacji ogłasza komunikat o wydaniu polecenia zabezpieczającego w swoim dzienniku urzędowym oraz stronie internetowej urzędu obsługującego ministra. Załącznikiem do komunikatu jest wydane polecenie zabezpieczające. 16. Polecenie zabezpieczające uznaje się za doręczone z chwilą ogłoszenia komunikatu o wydaniu polecenia zabezpieczającego w dzienniku urzędowym ministra właściwego do spraw informatyzacji. 17. Od polecenia zabezpieczającego nie przysługuje wniosek o ponowne rozpatrzenie sprawy.
Art. 32	c) nakazania danym podmiotom, by zaniechały postępowania naruszającego niniejszą dyrektywę i nie powtarzały takiego postępowania;	TAK	Art. 1 pkt 63 (art. 53 ust. 5 i 8)	Art. 53. 5. W celu egzekwowania przepisów ustawy organ właściwy do spraw cyberbezpieczeństwa w stosunku do podmiotów kluczowych, także wtedy gdy podmiot kluczowy nie zastosował się do pisma z ostrzeżeniem, o którym mowa w ust. 4, może: 2) nakazać, w drodze decyzji, zaniechanie przetwarzania danych osobowych; 8. Postępowanie w sprawach, o którym mowa w ust. 5 pkt 2–8, jest jednoinstancyjne, a na decyzję

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				organu właściwego do spraw cyberbezpieczeństwa przysługuje skarga do sądu administracyjnego.
Art. 32	d) nakazania danym podmiotom, by w określony sposób i w określonym terminie zapewniły zgodność swoich środków zarządzania ryzykiem w cyberbezpieczeństwie z art. 21 lub wypłyły obowiązki głównych i wydawców określonych w art. 23;	TAK	Art. 1 pkt 63 (art. 53 ust. 5 pkt 3 i ust. 8)	Art. 53. 5. W celu egzekwowania przepisów ustawy organ właściwy do spraw cyberbezpieczeństwa w stosunku do podmiotów kluczowych, także wtedy gdy podmiot kluczowy nie zastosował się do pisma z ostrzeżeniem, o którym mowa w ust. 4, może: 3) nakazać, w drodze decyzji, zapewnienie zgodności systemu zarządzania bezpieczeństwem informacji zgodnie z art. 8 ust. 1 pkt 2 lub zgodnie z art. 8 ust. 3 lub realizacji obowiązku zgłaszania incydentu powstającego; 8. Postępowanie w sprawach, o którym mowa w ust. 5 pkt 2–8, jest jednoinstancyjne, a na decyzję organu właściwego do spraw cyberbezpieczeństwa przysługuje skarga do sądu administracyjnego.
Art. 32	e) nakazania danym podmiotom, by poinformowały osoby fizyczne lub prawne, w odniesieniu do których świadczą usługi lub prowadzą działania, a których potencjalnie dotyczy poważne cyberzagrożenie, o charakterze tego zagrożenia, a także o możliwych środkach ochronnych lub naprawczych, jakie te osoby fizyczne lub prawne mogą podjąć w reakcji na to zagrożenie;	TAK	Art. 1 pkt 63 (art. 53 ust. 5 pkt 4 i ust. 8)	Art. 53. 5. W celu egzekwowania przepisów ustawy organ właściwy do spraw cyberbezpieczeństwa w stosunku do podmiotów kluczowych, także wtedy gdy podmiot kluczowy nie zastosował się do pisma z ostrzeżeniem, o którym mowa w ust. 4, może: 4) nakazać, w drodze decyzji, poinformowanie, w określony przez niego sposób, odbiorców swoich usług, których dotyczy poważne cyberzagrożenie, o charakterze tego zagrożenia oraz o możliwych środkach ochronnych lub naprawczych, jakie należy podjąć w reakcji na to zagrożenie 8. Postępowanie w sprawach, o którym mowa w ust. 5 pkt 2–8, jest jednoinstancyjne, a na decyzję organu właściwego do spraw cyberbezpieczeństwa przysługuje skarga do sądu administracyjnego.

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

Art. 32	f) nakazania danym podmiotom, by w rozsądnym terminie wdrożyły [] [] [] i [] wyd[] w wy[]ku []dytu b[]pi[]ń[tw];	TAK	Art. 1 pkt 63 (art. 53 ust. 5 pkt 5 i ust. 8)	Art. 53. 5. W celu egzekwowania przepisów ustawy organ właściwy do spraw cyberbezpieczeństwa w stosunku do podmiotów kluczowych, także wtedy gdy podmiot kluczowy nie zastosował się do pisma z ostrzeżeniem, o którym mowa w ust. 4, może: 5) nakazać, w drodze decyzji, wdrożenie, w określonym terminie, zaleceń wydanych w wyniku audytu bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi 8. Postępowanie w sprawach, o którym mowa w ust. 5 pkt 2–8, jest jednoinstancyjne, a na decyzję organu właściwego do spraw cyberbezpieczeństwa przysługuje skarga do sądu administracyjnego.
Art. 32	g) wyznaczenia urzędnika monitorującego – ze ściśle określonymi zadaniami na oznaczony okres – do nadzorowania przestrzegania pr[]d[]podmioty [rt. 21 i 23;	TAK	Art. 1 pkt 63 (art. 53 ust. 5 pkt 6 i ust. 8) i pkt 64 (art. 53d)	Art. 53. 5. W celu egzekwowania przepisów ustawy organ właściwy do spraw cyberbezpieczeństwa w stosunku do podmiotów kluczowych, także wtedy gdy podmiot kluczowy nie zastosował się do pisma z ostrzeżeniem, o którym mowa w ust. 4, może: 6) wyznaczyć, w drodze decyzji, na określony czas, nie dłuższy niż miesiąc, spośród osób zatrudnionych w urzędzie obsługującym ten organ, urzędnika monitorującego do nadzorowania wykonywania obowiązków, o których mowa w rozdziale 3, wskazując ściśle określone zadania, które urzędnik monitorujący r[]li[uj] w tym []i[]; 8. Postępowanie w sprawach, o którym mowa w ust. 5 pkt 2–8, jest jednoinstancyjne, a na decyzję organu właściwego do spraw cyberbezpieczeństwa przysługuje skarga do sądu administracyjnego.

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				Art. 53d. 1. Urzędnik monitorujący, o którym mowa w art. 53 ust. 5 pkt 6, w zakresie nadzorowania wykonywania przez podmiot kluczowy obowiązków, o których mowa w rozdziale 3, jest uprawniony do: 1) swobodnego wstępu i poruszania się po terenie podmiotu kluczowego po uzyskaniu przepustki, wydanej bezzwłocznie, której wydanie może odmówić; 2) wglądu do dokumentów dotyczących działalności podmiotu kluczowego; 3) przetwarzania danych osobowych w zakresie niezbędnym do realizacji celu nadzoru; 4) żądania złożenia ustnych lub pisemnych wyjaśnień w sprawach dotyczących zakresu nadzoru; 5) przeprowadzania oględzin urządzeń, nośników oraz systemów informacyjnych, po wcześniejszym zawiadomieniu podmiotu kluczowego. 2. Urzędnik monitorujący, o którym mowa w art. 53 ust. 5 pkt 6, realizuje powierzone mu zadania z zachowaniem przepisów o tajemnicy prawnie chronionej. 3. Do nadzorowania przez urzędnika monitorującego, o którym mowa w art. 53 ust. 5 pkt 6, wykonywania przez podmiot kluczowy obowiązków, o których mowa w rozdziale 3, stosuje się art. 58. 4. Zawiadomienie, o którym mowa w ust. 1 pkt 5, przekazuje się na adres do doręczeń elektronicznych albo za pomocą systemu teleinformatycznego, o którym mowa w art. 46 ust. 1 w terminie 1 dnia przed przeprowadzeniem oględzin.

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

Art. 32	h) nakazania danym podmiotom, by w określony sposób podały do wiadomości publicznej informacje o naruszeniach niniejszej dyrektywy;	TAK	Art. 1 pkt 63 (art. 53 ust. 5 pkt 7 i 8 i ust. 8)	Art. 53. 5. W celu egzekwowania przepisów ustawy organ właściwy do spraw cyberbezpieczeństwa w stosunku do podmiotów kluczowych, także wtedy gdy podmiot kluczowy nie zastosował się do pisma z ostrzeżeniem, o którym mowa w ust. 4, może: 7) nakazać, w drodze decyzji, podanie do wiadomości publicznej informacji o naruszeniach przepisów ustawy; 8) nakazać, w drodze decyzji wydanej w postępowaniu uproszczonym, o którym mowa w rozdziale 14 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego, podanie do publicznej wiadomości informacji o incydencie poważnym. 8. Postępowanie w sprawach, o którym mowa w ust. 5 pkt 2–8, jest jednoinstancyjne, a na decyzję organu właściwego do spraw cyberbezpieczeństwa przysługuje skarga do sądu administracyjnego.
Art. 32	i) nałożenia lub zwrócenia się o nałożenie przez właściwe organy lub sądy zgodnie z prawem krajowym administracyjnej kary pieniężnej zgodnie z art. 34 niezależnie od środków, o których mowa w lit. a)–h) niniejszego ustępu.	TAK	Art. 1 pkt 82 (art. 73 ust. 1-1c) i pkt 84 (art. 74 ust. 1 i 2)	Art. 73. 1. Karze pieniężnej podlega podmiot kluczowy lub podmiot ważny, który: 1) nie uzupełnił w terminie brakujących danych w wykazie podmiotów kluczowych i podmiotów ważnych pomimo wezwania, o którym mowa w art. 7b ust. 2 albo art. 7j ust. 3, albo art. 7k ust. 2, albo art. 7l ust. 3 pkt 2; 2) nie przeprowadza systematycznego szacowania ryzyka lub nie zarządza ryzykiem wystąpienia incydentu, o których mowa w art. 8 ust. 1 pkt 1; 3) nie wdrożył systemu zarządzania bezpieczeństwem informacji w systemie informacyjnym wykorzystywanym w procesach wpływających na świadczenie usługi albo system

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				ten nie zapewnia funkcjonalności, o których mowa w art. 8 ust. 1 albo art. 8 ust. 3; 4) nie wykonuje obowiązków, o których mowa w art. 10 ust. 1; 5) nie wykonuje obowiązku, o którym mowa w art. 11 ust. 1 pkt 1; 6) nie wykonuje obowiązku, o którym mowa w art. 11 ust. 1 pkt 4; 7) nie wykonuje obowiązku, o którym mowa w art. 11 ust. 1 pkt 4a; 8) nie wykonuje obowiązku, o którym mowa w art. 11 ust. 1 pkt 4b; 9) nie wykonuje obowiązku, o którym mowa w art. 11 ust. 1 pkt 4c; 10) nie wykonuje obowiązku, o którym mowa w art. 11 ust. 1 pkt 5; 11) nie przeprowadza audytu w terminie, o którym mowa w art. 15 ust. 1 lub art. 16 pkt 2; 12) nie usuwa podatności, o których mowa w art. 32 ust. 2; 13) nie korzysta z systemu teleinformatycznego, o którym mowa w art. 46 ust. 1, w celu realizacji obowiązków, o których mowa w art. 11; 14) uniemożliwia lub utrudnia wykonywanie kontroli, o których mowa w art. 53 ust. 2 pkt 1; 15) nie realizuje obowiązku, o którym mowa w art. 53a; 16) uniemożliwia lub utrudnia urzędnikowi monitorującemu, o którym mowa w art. 53 ust. 5 pkt 6, wykonywanie powierzonych mu zadań lub realizację uprawnień, o których mowa w art. 53d ust. 1; 17) nie wykonał w wyznaczonym terminie zaleceń pokontrolnych, o których mowa w art. 59 ust. 1;

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				18) nie wykonuje obowiązków, o których mowa w art. 67 ust. 1 2, 4 i 5; 19) nie wdrożył w terminie określonym w poleceniu zabezpieczającym, o którym mowa w art. 67g ust. 9 pkt 3, określonego zachowania, o którym mowa w art. 67g ust. 10; 20) odstąpił od wykonywania zawartego w poleceniu zabezpieczającym, o którym mowa w art. 67g ust. 9, określonego zachowania, o którym mowa w art. 67g ust. 10, przed wygaśnięciem polecenia zabezpieczającego. 1a. Organ właściwy do spraw cyberbezpieczeństwa, jeżeli przemawia za tym waga i znaczenie naruszonych przepisów, może nałożyć karę pieniężną na podmiot, który: 1) w terminie, o którym mowa w art. 7c ust. 1, nie złożył wniosku o wpis do wykazu podmiotów kluczowych i podmiotów ważnych, o którym mowa w art. 7 ust. 1; 2) nie wykonuje obowiązków, o których mowa w art. 9. 1b. Karze pieniężnej podlega także podmiot kluczowy lub podmiot ważny, którego działanie lub zaniechanie, o którym mowa w ust. 1 pkt 2, 4–12, 14–16 i 18 oraz ust. 1a pkt 2, miało charakter jednorazowy. 1c. Podmiot ważny będący podmiotem publicznym podlega karze pieniężnej, jeżeli nie wykonuje obowiązku, o którym mowa w art. 8 ust. 3. Art. 74.1. Karę pieniężną, o której mowa w art. 73, art. 73a i art. 73b ust. 1 pkt 4, nakłada, w drodze decyzji, organ właściwy do spraw cyberbezpieczeństwa.

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				2. Karę pieniężną, o której mowa w art. 73b ust. 1 pkt 1–3, nakłada, w drodze decyzji, minister właściwy do spraw informatyzacji.
Art. 32	5. Jeżeli środki z zakresu egzekwowania przepisów zastosowane na podstawie ust. 4 lit. a)–d) i f) okażą się nieskuteczne, państwa członkowskie zapewniają, by ich właściwe organy były uprawnione do wyznaczenia terminu, do którego podmiot kluczowy jest zobowiązany podjąć działania konieczne do usunięcia uchybień lub zapewnienia zgodności z wymogami określonymi przez te organy. Jeżeli żądane działanie nie zostanie podjęte w wyznaczonym terminie, państwa członkowskie zapewniają, by właściwe organy były uprawnione do: a) tymczasowego zawieszenia lub zwrócenia się do organu, który przyznał certyfikację lub udzielił zezwolenia, lub do sądu, zgodnie z prawem krajowym, o tymczasowe zawieszenie certyfikacji lub zezwolenia na niektóre lub wszystkie odpowiednie usługi świadczone bądź na część lub całość działalności prowadzonej przez podmiot kluczowy; b) zwrócenia się do właściwych instytucji lub sądów, zgodnie z prawem krajowym, o nałożenie tymczasowego zakazu pełnienia funkcji zarządczych w tym podmiocie kluczowym na osobę fizyczną wykonującą obowiązki zarządcze na poziomie dyrektora generalnego lub przedstawiciela prawnego w tym podmiocie. Tymczasowe zawieszenie lub zakaz pełnienia funkcji na podstawie niniejszego ustępu stosuje się tylko do czasu, gdy dany podmiot podejmie działania niezbędne do usunięcia uchybień lub spełnienia wymogów właściwego organu, w związku z którymi nałożono na niego środki egzekwowania przepisów. Takie tymczasowe zawieszenie lub zakaz stosuje się z zastrzeżeniem odpowiednich gwarancji proceduralnych zgodnych z ogólnymi zasadami prawa Unii i z Kartą, w tym prawa do skutecznej ochrony prawnej i do rzetelnego procesu sądowego, domniemania niewinności oraz prawa do obrony. Środki egzekwowania przepisów określone w niniejszym ustępie nie mają zastosowania do podmiotów administracji publicznej objętych zakresem niniejszej dyrektywy.	TAK	Art. 1 pkt 63 (art. 53 ust. 6 i 9-11), pkt 64 (art. 53e) i pkt 46 (art. 42 ust. 11)	Art. 53. 6. Organ właściwy do spraw cyberbezpieczeństwa podejmując działania, o których mowa w ust. 5, wyznacza podmiotowi kluczowemu termin, w którym zobowiązuje ten podmiot do podjęcia określonych czynności, usunięcia uchybień lub zapewnienia zgodności z wymogami określonymi przez organ. 9. Organ właściwy do spraw cyberbezpieczeństwa, w przypadku gdy podmiot kluczowy nie zastosował się do nakazu, o którym mowa w ust. 5 pkt 1, lub postanowień decyzji, o której mowa w ust. 5 pkt 2–8, może: 1) wstrzymać udzieloną temu podmiotowi koncesję albo ograniczyć jej zakres do czasu usunięcia uchybień lub zaprzestania naruszeń lub 2) wstrzymać w całości albo w części działalność podmiotu kluczowego wpisanego do rejestru działalności regulowanej, do czasu usunięcia uchybień lub zaprzestania naruszeń, lub 3) wstrzymać zezwolenie na prowadzenie działalności gospodarczej wydane podmiotowi kluczowemu albo ograniczyć zakres tego zezwolenia do czasu usunięcia uchybień lub zaprzestania naruszeń, lub 4) wstrzymać w całości albo w części działalność podmiotu kluczowego, wpisanego do Centralnej Ewidencji i Informacji o Działalności Gospodarczej, do czasu usunięcia uchybień lub zaprzestania naruszeń, lub 5) wstrzymać w całości albo w części działalność podmiotu kluczowego, wpisanego do rejestru przedsiębiorców Krajowego Rejestru

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				Sądowego do czasu usunięcia uchybień lub zaprzestania naruszeń, lub 6) zakazać pełnienia w podmiocie kluczowym funkcji zarządczych przez kierownika podmiotu do czasu usunięcia uchybień lub zaprzestania naruszeń, o ile nie doprowadzi to do uniemożliwienia funkcjonowania podmiotu kluczowego w zakresie jaki jest niezbędny do usunięcia uchybień lub zaprzestania naruszeń. 10. Środków, o których mowa w ust. 9, nie stosuje się do podmiotów publicznych. 11. W przypadku wniesienia przez podmiot kluczowy skargi do sądu administracyjnego, o której mowa w ust. 7 lub 8, środków, o których mowa w ust. 9, nie stosuje się do czasu rozstrzygnięcia sprawy przez ten sąd. Sąd rozstrzyga sprawę w terminie miesiąca od dnia wniesienia skargi. Art. 53e. 1. Realizując uprawnienie, o którym mowa w art. 53 ust. 9, organ właściwy do spraw cyberbezpieczeństwa wydaje decyzję, która zawiera: 1) dane podmiotu kluczowego lub kluczkowego podmiotu kluczkowego; 2) rodzaj stwierdzonych uchybień lub naruszeń dokonanych przez podmiot kluczowy lub kluczkowego podmiotu kluczkowego; 3) podjęte dotychczas środki nadzorcze nad podmiotem kluczkowym; 4) podstawę prawną i rodzaj środka określonego w art. 53 ust. 9; 5) terminy i sposób ich wykonania; 6) uzasadnienie. 2. Termin stosowania środków, o których mowa w art. 53 ust. 9, określa się przy uwzględnieniu

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				kryteriów, o których mowa w art. 53 ust. 12. Środek nie może być stosowany dłużej niż 14 dni od daty doręczenia decyzji o jego zastosowaniu. 3. W zależności od zastosowanego środka jeżeli podmiot kluczowy, usunął uchybienia lub zaprzestał naruszania przepisów ustawy przed terminem określonym w decyzji, uchyła się decyzję o zastosowaniu tego środka. 4. W przypadku powzięcia informacji, w szczególności na skutek stosowania innych środków nadzorczych, określonych w art. 53 ust. 1, 4 i 5, że podmiot kluczowy, nie usunął wcześniej stwierdzonych uchybień lub w dalszym ciągu narusza przepisy ustawy lub w przypadku gdy podmiot kluczowy nie wykazał w terminie, na jaki został zastosowany środek, że usunął uchybienia lub zaprzestał naruszania przepisów ustawy, organ właściwy do spraw cyberbezpieczeństwa ponownie wydaje decyzję o zastosowaniu środka określonego w art. 53 ust. 9 na kolejny okres, nie dłuższy niż 14 dni. Przepis ten stosuje się do czasu usunięcia uchybień lub zaprzestania naruszeń przez podmiot kluczowy. W stosunku do ponownej decyzji nie stosuje się art. 53 ust. 13–16. 5. Organ właściwy do spraw cyberbezpieczeństwa z urzędu lub na wniosek podmiotu kluczowego uchyła decyzję, o której mowa w ust. 1, po usunięciu uchybień lub zaprzestaniu naruszeń przez podmiot kluczowy. 6. Podmiot kluczowy może złożyć wniosek o którym mowa w ust. 5 po usunięciu uchybień lub zaprzestaniu naruszeń, przedstawiając dowody potwierdzające zastosowanie się odpowiednio do nakazu, o którym mowa w art. 53 ust. 5 pkt 1, lub

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				postanowień decyzji, o której mowa w art. 53 ust. 5 pkt 2–8. 7. Wniosek, o którym mowa w ust. 5, organ właściwy do spraw cyberbezpieczeństwa rozpatruje niezwłocznie, nie później niż w terminie 7 dni od dnia jego otrzymania. 8. Czynności, o których mowa w ust. 3 i 5 organ dokonuje w formie decyzji. 9. Decyzja, o której mowa w ust. 1 jest wykonalna z dniem jej doręczenia podmiotowi kluczowemu. Decyzje, o których mowa w ust. 3, 4 i 5 są natychmiast wykonalne. 10. Postępowanie w sprawie stosowania i uchylania środków, o których mowa w art. 53 ust. 9, jest jednoinstancyjne. Na decyzje, o których mowa w ust. 1 i 3–5 podmiot kluczowy może wnieść skargę do sądu administracyjnego. 11. Organ właściwy do spraw cyberbezpieczeństwa publikuje na swojej stronie podmiotowej Biuletynu Informacji Publicznej informację o zastosowaniu wobec podmiotu kluczowego lub kierownika podmiotu kluczowego środków, o których mowa w art. 53 ust. 9. Informacja zawiera: 1) dane podmiotu kluczowego lub imię i nazwisko kierownika tego podmiotu kluczowego; 2) podstawę prawną i rodzaj zastosowanego środka, o którym mowa w art. 53 ust. 9; 3) wskazanie daty początkowej i końcowej obowiązywania środka; 4) wskazanie, czy wobec podmiotu kluczowego lub kierownika podmiotu kluczowego ponownie zastosowano środek, a jeśli tak to wskazanie nowej daty końcowej stosowania tego środka.

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				12. Publikacja, o której mowa w ust. 11, nie obejmuje tajemnicy przedsiębiorstwa, jak również innych informacji podlegających ochronie na podstawie odrębnych przepisów. 13. Organ właściwy do spraw cyberbezpieczeństwa publikuje na swojej stronie podmiotowej Biuletynu Informacji Publicznej informację o uchyleniu decyzji, o której mowa w ust. 1. 14. Podmiot kluczowy, w okresie stosowania wobec niego środka, o którym mowa w art. 53 ust. 9, nie może wykonywać działalności, której dotyczy ten środek. 15. W okresie stosowania środka, o którym mowa w art. 53 ust. 9, podmiot kluczowy, ma obowiązek niezwłocznie podjąć działania zmierzające jedynie do usunięcia uchybień bądź zaprzestania naruszeń. W tym celu w szczególności może składać oświadczenia woli i wiedzy, podejmować czynności procesowe w postępowaniach, przedsięwziąć czynności faktyczne, jeżeli nie stoją one w sprzeczności z celem stosowanego środka lub nie zmierzają do jego obejścia. 16. W zakresie nieuregulowanym, a dotyczącym zawieszania, ograniczania i wznawiania koncesji, zezwolenia na prowadzenie działalności gospodarczej lub wstrzymania prowadzenia działalności gospodarczej zastosowanie mają przepisy odrębne. Art. 42. 11. Organ właściwy do spraw cyberbezpieczeństwa prowadzi i regularnie aktualizuje wykaz osób, wobec których wydana została decyzja o zastosowaniu środka nadzorczego, o którym mowa w art. 53 ust. 9 pkt 6, obejmujący: 1) imię (imio□);

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				2) imię i nazwisko; 3) numer PESEL, a w przypadku jego nieposiadania – datę urodzenia; 4) wagę podmiotu kluczowego; 5) datę wydania decyzji; 6) kraj pracy; 7) okoliczności wydania decyzji; 8) podstawę prawną wydania decyzji.
Art. 32	6. Państwa członkowskie zapewniają, aby każda osoba fizyczna odpowiedzialna za podmiot kluczowy lub działająca w charakterze przedstawiciela prawnego tego podmiotu na podstawie uprawnienia do jego reprezentowania, podejmowania decyzji w jego imieniu lub sprawowania nad nim kontroli była uprawniona do zapewnienia przestrzegania przez ten podmiot niniejszej dyrektywy. Państwa członkowskie zapewniają, by te osoby fizyczne mogły być pociągnięte do odpowiedzialności za niewywiązanie się z obowiązku zapewnienia przestrzegania niniejszej dyrektywy. W odniesieniu do podmiotów administracji publicznej niniejszy ustęp pozostaje bez uszczerbku dla przepisów krajowych dotyczących odpowiedzialności urzędników publicznych oraz osób pełniących funkcję z wyboru lub powołania.	TAK	Art. 1 pkt 17 (art. 8c)	Art. 8c. 1. Kierownik podmiotu kluczowego lub podmiotu ważnego ponosi odpowiedzialność za wykonywanie obowiązków w zakresie cyberbezpieczeństwa przez podmiot kluczowy lub podmiot ważny, o których mowa w art. 7b ust. 4, art. 7c, art. 7f ust. 3, art. 8, art. 8d, art. 8e, art. 8f ust. 1 i 2, art. 9–12b, art. 14 i art. 15. 2. W przypadku gdy kierownikiem podmiotu kluczowego lub podmiotu ważnego jest organ wieloosobowy i nie została wskazana osoba odpowiedzialna, odpowiedzialność ponoszą wszyscy członkowie tego organu. 3. Kierownik podmiotu kluczowego lub podmiotu ważnego ponosi odpowiedzialność także wtedy, gdy niektóre z obowiązków albo wszystkie obowiązki zostały powierzone innej osobie za jej zgodą.
Art. 32	7. Przyjmując środki egzekwowania przepisów, o których mowa w ust. 4 lub 5, właściwe organy przestrzegają prawa do obrony oraz biorą pod uwagę okoliczności każdego indywidualnego przypadku i należycie uwzględniają co najmniej: a) wagę naruszenia i znaczenie naruszonych przepisów, przy czym za poważne należy uznać w każdym przypadku m.in. następujące naruszenia: (i) powtarzające się naruszenia; (ii) zagrożenie lub uszkodzenie powołanych i wydanych;	TAK	Art. 1 pkt 63 (art. 53 ust. 12)	Art. 53. 12. Organ właściwy do spraw cyberbezpieczeństwa, podejmując działania, o których mowa w ust. 5 i 9, uwzględnia: 1) wagę naruszenia i znaczenie naruszonych przepisów ustawy, przy czym za poważne naruszenie należy uznać: a) powtarzające się naruszenie, b) niezgłoszenie lub nieobsłużenie incydentów poważnych,

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

	(iii) nieusunięcie uchybień zgodnie z wiążącymi nakazami właściwych organów; (iv) utrudnianie prowadzenia audytów lub działań monitorujących określonych przez właściwe organy po stwierdzeniu naruszenia; (v) dostarczanie nieprawdziwych lub rażąco niedokładnych informacji w odniesieniu do środków zarządzania ryzykiem w cyberbezpieczeństwie lub obowiązków zgłaszania incydentów u odpowiednich w art. 21 i 23; b) otrzymanie informacji; 1) istotne w szczególności informacje dotyczące danego podmiotu; d) spowodowane szkody majątkowe i niemajątkowe, w tym straty finansowe lub gospodarcze, wpływ na inne usługi i liczbę użytkowników, których dotyczy incydent; e) umyślny lub nieumyślny charakter czynu ze strony sprawcy informacji; f) środki zastosowane przez podmiot, aby zapobiec szkodom majątkowym i niemajątkowym lub je ograniczyć; g) stosowanie zatwierdzonych kodeksów postępowania lub stwierdzonej modyfikacji polityki; h) stopień współpracy odpowiedzialnych osób fizycznych lub prawnych z właściwymi organami.			c) nieusunięcie uchybień zgodnie z wiążącymi nakazami organów właściwych do spraw cyberbezpieczeństwa, d) utrudnianie prowadzenia audytów lub działań monitorujących nakazanych przez organ właściwy do spraw cyberbezpieczeństwa po stwierdzeniu naruszenia, e) dostarczanie nieprawdziwych lub rażąco niedokładnych informacji w odniesieniu do środków zarządzania ryzykiem w cyberbezpieczeństwie lub obowiązków określonych w art. 21 i 23; 2) otrzymanie informacji; 3) wcześniejsze poważne naruszenia ze strony danego podmiotu; 4) spowodowane szkody majątkowe i niemajątkowe, w tym straty finansowe lub gospodarcze, wpływ na inne usługi i liczbę użytkowników, których dotyczy incydent; 5) umyślny lub nieumyślny charakter czynu ze strony sprawcy informacji; 6) środki zastosowane przez podmiot, aby zapobiec szkodom majątkowym i niemajątkowym lub je ograniczyć; 7) stopień współpracy podmiotu z organem właściwym do spraw cyberbezpieczeństwa.
Art. 32	8. Właściwe organy przedstawiają szczegółowe uzasadnienie zastosowanych środków z zakresu egzekwowania przepisów. Zanim zastosują takie środki, właściwe organy powiadamiają dane podmioty o swoich wstępnych ustaleniach. Dają im one też rozsądny czas na przedstawienie uwag, z wyjątkiem należycie uzasadnionych przypadków, gdy utrudniłoby to natychmiastowe działanie w celu zapobieżenia incydentom lub reakcji na nie.	TAK	Art. 1 pkt 63 (art. 53 ust. 13, 14 i 16)	Art. 53. 13. Organ właściwy do spraw cyberbezpieczeństwa przed zastosowaniem środków, o których mowa w ust. 4, 5 i 9, oraz przed nałożeniem kary pieniężnej, informuje podmiot kluczowy o wstępnych ustaleniach, które mogą prowadzić do wydania decyzji lub podjęcia działań, o których mowa w ust. 4, 5 i 9, lub do nałożenia kary pieniężnej. Informacja o wstępnych ustaleniach zawiera szczegółowe uzasadnienie, potwierdzające zasadność zamiaru

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				zastosowania środków lub nałożenia kary pieniężnej. 14. Podmiot kluczowy może przedstawić swoje stanowisko niezwłocznie, nie później niż w terminie 7 dni od dnia poinformowania o wstępnych ustaleniach, o których mowa w ust. 13. 16. Organ właściwy do spraw cyberbezpieczeństwa może odstąpić od poinformowania o wstępnych ustaleniach w przypadku gdy utrudniłoby to natychmiastowe działanie w celu zapobieżenia incydentom, reakcji na nie lub mogłoby mieć niekorzystny wpływ na bezpieczeństwo państwa lub porządek publiczny.
Art. 32	9. Państwa członkowskie zapewniają, aby ich właściwe organy na mocy niniejszej dyrektywy informowały odpowiednie właściwe organy w tym samym państwie członkowskim na podstawie dyrektywy (UE) 2022/2557, gdy wykonują uprawnienia w zakresie nadzoru i egzekwowania przepisów, aby zapewnić przestrzeganie niniejszej dyrektywy przez podmiot uznany za krytyczny zgodnie z dyrektywą (UE) 2022/2557. W stosownych przypadkach właściwe organy na podstawie dyrektywy (UE) 2022/2557 mogą zwrócić się do właściwych organów na podstawie niniejszej dyrektywy o wykonanie ich uprawnień z zakresu nadzoru i egzekwowania przepisów w stosunku do podmiotu i wskazanego jako podmiot krytyczny na podstawie dyrektywy (UE) 2022/2557.	TAK	Art. 1 pkt 46 (art. 42 ust. 1 pkt 13) i pkt 64 (art. 53f ust. 4)	Art. 42. 1: 13) współpracuje oraz wymienia informacje i dokumenty z organem właściwym do spraw podmiotów krytycznych w zakresie nadzoru nad podmiotem kluczowym będącym podmiotem krytycznym. Art. 53f. 4. Przepisy ust. 1–3 stosuje się odpowiednio do współpracy organów właściwych do spraw cyberbezpieczeństwa i organów właściwych do spraw podmiotów krytycznych w przypadku, gdy nadzór jest sprawowany nad podmiotem kluczowym będącym podmiotem krytycznym. Uwaga – w większości przypadków będą to te same organy zgodnie z projektem ustawy o zmianie ustawy o zarządzaniu kryzysowym oraz niektórych innych ustaw (UC47).
Art. 32	10. Państwa członkowskie zapewniają, by ich właściwe organy zgodnie z niniejszą dyrektywą współpracowały z odpowiednimi właściwymi organami zainteresowanego państwa członkowskiego zgodnie z rozporządzeniem (UE) 2022/2554. W szczególności	TAK	Art. 1 pkt 69 (art. 59b ust. 6 i 7)	Art. 59b. 6. Organy właściwe do spraw cyberbezpieczeństwa współpracują za pośrednictwem Pojedynczego Punktu Kontaktowego z organami innych państw

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

	państwa członkowskie zapewniają, by ich właściwe organy na mocy niniejszej dyrektywy informowały forum nadzoru, ustanowione zgodnie z art. 32 ust. 1 rozporządzenia (UE) 2022/2554, gdy wykonują uprawnienia w zakresie nadzoru i egzekwowania przepisów, by zapewnić przestrzeganie niniejszej dyrektywy przez podmiot kluczowy, wyznaczony jako kluczowy dostawca usług ICT będący osobą trzecią zgodnie z art. 31 rozporządzenia (UE) 2022/2554.			członkowskich Unii Europejskiej właściwych do stosowania rozporządzenia 2022/2554. 7. Organy właściwe do spraw cyberbezpieczeństwa informują forum nadzoru, o którym mowa w art. 32 ust. 1 rozporządzenia 2022/2554, jeżeli podejmują czynności nadzorcze wobec podmiotu kluczowego, który został wyznaczony jako kluczowy dostawca usług ICT zgodnie z art. 31 rozporządzenia 2022/2554.
Art. 33	Artykuł 33 Środki nadzoru i egzekwowania przepisów w odniesieniu do podmiotów ważnych 1. W przypadku otrzymania dowodu, wskazania lub informacji, że podmiot ważny rzekomo nie stosuje się do niniejszej dyrektywy, w szczególności jej w art. 21 i 23, państwa członkowskie zapewniają, by w razie potrzeby właściwe organy podjęły działania w postaci środków nadzoru ex post. Państwa członkowskie zapewniają, aby środki te były skuteczne, proporcjonalne i odstrasżające stosownie do okoliczności każdego indywidualnego przypadku. 2. Państwa członkowskie zapewniają, by wykonując zadania nadzorcze wobec podmiotów ważnych, właściwe organy były uprawnione do objęcia tych podmiotów co najmniej: a) kontrolami na miejscu i nadzorem zdalnym ex post prowadzonymi przez podmioty odpowiedzialne za bezpieczeństwo; b) ukierunkowanymi audytami bezpieczeństwa prowadzonymi przez podmioty niezależne i tytułujące lub właściwe organy; c) skanami bezpieczeństwa na podstawie obiektywnych, niedyskryminacyjnych, sprawiedliwych i przejrzystych kryteriów szacowania ryzyka, w razie potrzeby we współpracy z danym podmiotem; d) wnioskami o udzielenie informacji niezbędnych do oceny ex post środków zarządzania ryzykiem w cyberbezpieczeństwie przyjętych przez dany podmiot, w tym udokumentowanej polityki cyberbezpieczeństwa, a także wypełnienia obowiązku przedłożenia informacji właściwym organom zgodnie z art. 27;	TAK	Art. 1 pkt 63 (art. 53 ust. 17)	Art. 53. 17. Organ właściwy do spraw cyberbezpieczeństwa sprawując nadzór w stosunku do podmiotu ważnego stosuje ust. 2, 4, 5 pkt 1–5, 7–11 oraz ust. 6–8 i ust. 12–16.

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

	e) wnioskami o udzielenie dostępu do danych, dokumentów i informacji koniecznych do wykonywania ich zadań i obowiązków; f) wnioskami o przedstawienie dowodów realizacji polityki cyberbezpieczeństwa, takich jak wyniki audytu bezpieczeństwa przeprowadzonego przez wykwalifikowanego audytora oraz odpowiednie dowody. Ukierunkowane audyty bezpieczeństwa, o których mowa w akapicie pierwszym lit. b), opierają się na oszacowaniach ryzyka przeprowadzonych przez właściwy organ lub badany podmiot bądź na innych dostępnych informacjach o ryzyku. Wyniki ukierunkowanych audytów bezpieczeństwa udostępnia się właściwemu organowi. Koszty takiego ukierunkowanego audytu bezpieczeństwa prowadzonego przez niezależną instytucję pokrywa podmiot poddany audytowi, z wyjątkiem należycie uzasadnionych przypadków, gdy właściwy organ postanowi inaczej. 3. Wykonując swoje uprawnienia na mocy ust. 2 lit. d), e) lub f), właściwe organy podają cel wniosku i określają informacje, o które wnoszą. 4. Państwa członkowskie zapewniają, by wykonując uprawnienia w zakresie egzekwowania przepisów wobec podmiotów ważnych, właściwe organy były uprawnione co najmniej do: a) wydawania ostrzeżeń dotyczących naruszania przez dane podmioty ich polityki prywatności; b) przyjmowania wiążących poleceń lub nakazów zobowiązujących dane podmioty do naprawienia stwierdzonych uchybień lub uchybień w polityce prywatności; c) nakazania danym podmiotom, by zaniechały postępowania, które naruszają ich politykę prywatności i powstrzymały tego postępowania; d) nakazania danym podmiotom, by w określony sposób i w określonym terminie zapewniły zgodność swoich środków zarządzania ryzykiem w cyberbezpieczeństwie z art. 21 lub wyłożyły obowiązki ogólnych i szczególnych określonych w art. 23; e) nakazania danym podmiotom, by poinformowały osoby fizyczne lub prawne, w odniesieniu do których świadczą usługi lub prowadzą działania, a których potencjalnie dotyczy poważne cyberzagrożenie, o charakterze tego zagrożenia, a także o możliwych środkach			

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

	ochronnych lub naprawczych, jakie te osoby fizyczne lub prawne mogą ponieść w związku z groźbą; f) nakazania danym podmiotom, by w rozsądnym terminie wdrożyły środki wydane w wyniku audytu bezpieczeństwa; g) nakazania danym podmiotom, by w określony sposób podały do wiadomości publicznej informacje o naruszeniach przez nie informacji dotyczących danych; h) zastosowania lub zwrócenia się o zastosowanie przez właściwe organy lub sądy, zgodnie z prawem krajowym, administracyjnej kary pieniężnej na podstawie art. 34 oprócz środków, o których mowa w lit. a)–g) niniejszego ustępu. 5. Art. 32 ust. 6, 7 i 8 stosuje się odpowiednio do środków nadzoru i egzekwowania przepisów określonych w niniejszym artykule w odniesieniu do podmiotów ważnych. 6. Państwa członkowskie zapewniają, by ich właściwe organy zgodnie z niniejszą dyrektywą współpracowały z odpowiednimi właściwymi organami zainteresowanego państwa członkowskiego zgodnie z rozporządzeniem (UE) 2022/2554. W szczególności państwa członkowskie zapewniają, by ich właściwe organy na mocy niniejszej dyrektywy informowały forum nadzoru, ustanowione zgodnie z art. 32 ust. 1 rozporządzenia (UE) 2022/2554, gdy wykonują uprawnienia w zakresie nadzoru i egzekwowania przepisów, by zapewnić przestrzeganie niniejszej dyrektywy przez podmiot ważny, wyznaczony jako kluczowy dostawca usług ICT będący osobą trzecią zgodnie z art. 31 rozporządzenia (UE) 2022/2554.			
Art. 34	Artykuł 34 Ogólne warunki nakładania administracyjnych kar pieniężnych na podmioty kluczowe i ważne 1. Państwa członkowskie zapewniają, by administracyjne kary pieniężne nakładane na podmioty kluczowe i ważne zgodnie z niniejszym artykułem za naruszenia niniejszej dyrektywy były skuteczne, proporcjonalne i odstraszające, stosownie do okoliczności każdego indywidualnego przypadku.	TAK	Art. 1 pkt 82 (art. 73 ust. 1-1d, 3a i 5), pkt 84 (art. 74 ust. 1-5) i pkt 86 (art. 76a, art. 76b, art. 76d i art. 76e)	Art. 73. 1. Karze pieniężnej podlega podmiot kluczowy lub podmiot ważny, który: 1) nie uzupełnił w terminie brakujących danych w wykazie podmiotów kluczowych i podmiotów ważnych pomimo wezwania, o którym mowa w art. 7b ust. 2 albo art. 7j ust. 3, albo art. 7k ust. 2, albo art. 7l ust. 3 pkt 2; 2) nie przeprowadza systematycznego szacowania ryzyka lub nie zarządza ryzykiem wystąpienia incydentu, o którym mowa w art. 8 ust. 1 pkt 1;

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				3) nie wdrożył systemu zarządzania bezpieczeństwem informacji w systemie informacyjnym wykorzystywanym w procesach wpływających na świadczenie usługi albo system ten nie zapewnia funkcjonalności, o których mowa w art. 8 ust. 1 albo art. 8 ust. 3; 4) nie wykonuje obowiązków, o których mowa w art. 10 ust. 1; 5) nie wykonuje obowiązku, o którym mowa w art. 11 ust. 1 pkt 1; 6) nie wykonuje obowiązku, o którym mowa w art. 11 ust. 1 pkt 4; 7) nie wykonuje obowiązku, o którym mowa w art. 11 ust. 1 pkt 4a; 8) nie wykonuje obowiązku, o którym mowa w art. 11 ust. 1 pkt 4b; 9) nie wykonuje obowiązku, o którym mowa w art. 11 ust. 1 pkt 4c; 10) nie wykonuje obowiązku, o którym mowa w art. 11 ust. 1 pkt 5; 11) nie przeprowadza audytu w terminie, o którym mowa w art. 15 ust. 1 lub art. 16 pkt 2; 12) nie usuwa podatności, o których mowa w art. 32 ust. 2; 13) nie korzysta z systemu teleinformatycznego, o którym mowa w art. 46 ust. 1, w celu realizacji obowiązków, o których mowa w art. 11; 14) uniemożliwia lub utrudnia wykonywanie kontroli, o których mowa w art. 53 ust. 2 pkt 1; 15) nie realizuje obowiązku, o którym mowa w art. 53a; 16) uniemożliwia lub utrudnia urzędnikowi monitorującemu, o którym mowa w art. 53 ust. 5 pkt 6, wykonywanie powierzonych mu zadań lub realizację uprawnień, o których mowa w art. 53d ust. 1;

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				17) nie wykonał w wyznaczonym terminie zaleceń pokontrolnych, o których mowa w art. 59 ust. 1. 1a. Organ właściwy do spraw cyberbezpieczeństwa, jeżeli przemawia za tym waga i znaczenie naruszonych przepisów, może nałożyć karę pieniężną na podmiot, który: 1) w terminie, o którym mowa w art. 7c ust. 1, nie złożył wniosku o wpis do wykazu podmiotów kluczowych i podmiotów ważnych, o którym mowa w art. 7 ust. 1; 2) nie wykonuje obowiązków, o których mowa w art. 9. 1b. Karze pieniężnej podlega także podmiot kluczowy lub podmiot ważny, którego działanie lub zaniechanie, o którym mowa w ust. 1 pkt 2, 4–12, 14-16 i 18 oraz ust. 1a pkt 2, miało charakter jednorazowy. 1c. Podmiot ważny będący podmiotem publicznym podlega karze pieniężnej, jeżeli nie wykonuje obowiązku, o którym mowa w art. 8 ust. 3. 1d. Przepis ust. 1 pkt 13 nie stosuje się do Ministra Obrony Narodowej, urzędu go obsługującego oraz podmiotów podległych Ministrowi Obrony Narodowej i przez niego nadzorowanych. 3a. W przypadku gdy okres wykonywania działalności gospodarczej jest krótszy niż 12 miesięcy albo podmiot nie osiągnął przychodu za podstawę wymiaru kary pieniężnej przyjmuje się równowartość kwoty 500 000 euro, wyrażonej w złotych i ustalonej przy zastosowaniu kursu średniego ogłaszanego przez Narodowy Bank Polski obowiązującego w dniu 31 grudnia w roku poprzedzającym rok wydania decyzji o wymierzeniu kary.

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				5. Jeżeli podmiot kluczowy albo podmiot ważny narusza przepisy ustawy, powodując: 1) bezpośrednie i poważne cyberzagrożenie dla obronności, bezpieczeństwa państwa, bezpieczeństwa i porządku publicznego lub życia i zdrowia ludzi, 2) zagrożenie wywołania poważnej szkody majątkowej lub poważnych utrudnień w świadczeniu usług – organ właściwy do spraw cyberbezpieczeństwa nakłada karę w wysokości do 100 000 000 zł. Art. 74.1. Karę pieniężną, o której mowa w art. 73, art. 73a i art. 73b ust. 1 pkt 4, nakłada, w drodze decyzji, organ właściwy do spraw cyberbezpieczeństwa. 2. Karę pieniężną, o której mowa w art. 73b ust. 1 pkt 1–3, nakłada, w drodze decyzji, minister właściwy do spraw informatyzacji. 3. Karę pieniężną, o której mowa w art. 73c ust. 1, nakłada, w drodze decyzji, właściwy organ w rozumieniu rozporządzenia 2022/2554. 4. Organ właściwy do spraw cyberbezpieczeństwa lub właściwy organ w rozumieniu rozporządzenia 2022/2554 może decyzji, o której mowa w ust. 1 lub ust. 3, nadać rygor natychmiastowej wykonalności w całości albo w części, jeżeli wymaga tego ochrona bezpieczeństwa lub porządku publicznego. 5. Wpływy z tytułu kar pieniężnych, o których mowa w art. 73–73c, stanowią przychód Funduszu Cyberbezpieczeństwa, o którym mowa w art. 2 ustawy z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa.

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				Art. 76a. 1. Organ właściwy do spraw cyberbezpieczeństwa, podejmując decyzję o nałożeniu kary pieniężnej i ustalając jej wysokość uwzględnia odpowiednio kryteria określone w art. 53 ust. 12 oraz wysokość przychodu uzyskanego z działalności gospodarczej w roku obrotowym poprzedzającym wymierzenie kary pieniężnej, możliwości finansowe podmiotu kluczowego lub podmiotu ważnego będącego podmiotem publicznym albo możliwości finansowe kierownika podmiotu kluczowego lub podmiotu ważnego. Art. 189a §2 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego nie stosuje się. 2. W przypadku gdy podmiot kluczowy lub podmiot ważny powstał w wyniku połączenia lub przekształcenia innych podmiotów, obliczając wysokość jego przychodu organ właściwy do spraw cyberbezpieczeństwa uwzględnia przychód osiągnięty przez te podmioty w roku obrotowym poprzedzającym rok nałożenia kary pieniężnej. Przepisy art. 73 ust. 3–4 stosuje się odpowiednio. 3. W związku z toczącym się postępowaniem w sprawie nałożenia kary pieniężnej, podmiot, wobec którego wszczęto to postępowanie lub podmiot zatrudniający kierownika podmiotu kluczowego lub podmiotu ważnego jest obowiązany do dostarczenia organowi uprawnionemu do nałożenia kary pieniężnej na każde jego żądanie, w terminie wskazanym w wezwaniu, nie dłuższym niż 1 miesiąc od dnia otrzymania żądania, danych niezbędnych do określenia podstawy wymiaru kary pieniężnej. 4. W przypadku niedostarczenia danych lub dostarczenia danych uniemożliwiających

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				ustalenie podstawy wymiaru kary pieniężnej, organ właściwy do spraw cyberbezpieczeństwa ustala podstawę wymiaru kary pieniężnej w sposób szacunkowy, uwzględniając w szczególności wielkość danego podmiotu kluczowego lub podmiotu ważnego, specyfikę działalności tego podmiotu lub ogólnodostępne dane finansowe. 5. Karę pieniężną uiszcza się w terminie 14 dni od dnia, w którym decyzja o jej wymierzeniu stała się ostateczna, lub od dnia doręczenia decyzji z rygiorem natychmiastowej wykonalności, na rachunek bankowy organu właściwego do spraw cyberbezpieczeństwa, wskazany w decyzji o wymierzeniu kary pieniężnej. 6. Kary pieniężne nieuiszczone w terminie wraz z odsetkami podlegają ściągnięciu przez organ właściwy do spraw cyberbezpieczeństwa, który wymierzył karę pieniężną, w trybie określonym w przepisach o postępowaniu egzekucyjnym w administracji. 7. Organ właściwy do spraw cyberbezpieczeństwa przekazuje na rachunek Funduszu Cyberbezpieczeństwa środki pochodzące z kar pieniężnych w terminie 14 dni od dnia ich uiszczenia albo pobrania. W tym samym terminie przekazuje ministrowi właściwemu do spraw informatyzacji kopię decyzji o wymierzeniu kary pieniężnej lub innego dokumentu stanowiącego podstawę naliczenia, pobrania i przekazania na rachunek Funduszu Cyberbezpieczeństwa kary pieniężnej lub odsetek od nieterminowej wpłaty. 8. Organ właściwy do spraw cyberbezpieczeństwa w terminie 14 dni od dnia wystąpienia zdarzenia mogącego skutkować zmianą lub uchyleniem decyzji lub dokumentu stanowiącego podstawę do

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				naliczenia, pobrania i przekazania na rachunek Funduszu Cyberbezpieczeństwa środków pochodzących z kar pieniężnych, informuje ministra właściwego do spraw informatyzacji o tym zdarzeniu, a w szczególności o wniesieniu skargi do sądu administracyjnego, skargi kasacyjnej, wydaniu prawomocnego wyroku, wszczęciu lub zakończeniu postępowania administracyjnego w zakresie wznowienia postępowania, uchylenia, zmiany lub stwierdzenia nieważności decyzji. 9. Organ właściwy do spraw cyberbezpieczeństwa może odstąpić od nałożenia kary pieniężnej, jeżeli waga naruszenia i znaczenie naruszonych przepisów są znikome, a podmiot albo kierownik podmiotu kluczowego lub podmiotu ważnego zaprzestał naruszania prawa lub naprawił wyrządzoną szkodę. 10. Do postępowania w sprawie nałożenia kar pieniężnych, o których mowa w art. 73b ust. 1 i art. 73c ust. 1, stosuje się odpowiednio ust. 1–9. Art. 76b. 1. Niezależnie od kary pieniężnej nałożonej na podstawie art. 73 ust. 1, organ właściwy do spraw cyberbezpieczeństwa, w celu przymuszenia podmiotu kluczowego albo podmiotu ważnego do wykonania nałożonych na niego obowiązków, może nałożyć na ten podmiot, w drodze decyzji, okresową karę pieniężną w wysokości od 500 zł do 100 000 złotych za każdy dzień opóźnienia, w wykonaniu decyzji wydanych na podstawie art. 53 ust. 5 pkt 2–8. 2. Okresową karę pieniężną nakłada się, licząc od daty wskazanej w decyzji o nałożeniu tej kary. 3. Do okresowej kary pieniężnej stosuje się przepisy art. 74 ust. 4 i 5.

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				Art. 76d. 1. W przypadku, o którym mowa w art. 73 ust. 1 pkt 3, kara pieniężna może być nakładana w sposób określony w art. 14 § 1b ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego. 2. Do postępowania w sprawie nałożenia kary pieniężnej stosuje się przepisy działu II rozdziału 14 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego, z wyjątkiem przepisów o milczącym załatwieniu sprawy. Art. 76e. W zakresie nieuregulowanym w niniejszym rozdziale stosuje się odpowiednio przepisy działu IVa ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego.
Art. 34	2. Administracyjne kary pieniężne nakłada się niezależnie od środków, o których mowa w art. 32 ust. 4 lit. a)–h), art. 32 ust. 5 i art. 33 ust. 4 lit. a)–g).	TAK		
Art. 34	3. Podejmując decyzję o nałożeniu administracyjnej kary pieniężnej i o jej wysokości, w każdym indywidualnym przypadku należyte uwzględnia się co najmniej elementy wymienione w art. 32 ust. 7.	TAK	Art. 1 pkt 86 (art. 76a ust. 1)	Art. 76a. 1. Organ właściwy do spraw cyberbezpieczeństwa, podejmując decyzję o nałożeniu kary pieniężnej i ustalając jej wysokość uwzględnia odpowiednio kryteria określone w art. 53 ust. 12 oraz wysokość przychodu uzyskanego z działalności gospodarczej w roku obrotowym poprzedzającym wymierzenie kary pieniężnej, możliwości finansowe podmiotu kluczowego lub podmiotu ważnego będącego podmiotem publicznym albo możliwości finansowe kierownika podmiotu kluczowego lub podmiotu ważnego. Art. 189a §2 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego nie stosuje się.
Art. 34	4. Państwa członkowskie zapewniają, by podmioty kluczowe dokonujące naruszeń art. 21 lub 23 podlegały zgodnie z ust. 2 i 3 niniejszego artykułu administracyjnym karom pieniężnym w	TAK	Art. 1 pkt 82 (art. 73 ust. 3)	Art. 73. 3. Wysokość kary pieniężnej nie może przekroczyć 10 000 000 euro, wyrażonej w złotych i ustalonej przy zastosowaniu kursu

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

	maksymalnej wysokości co najmniej 10 000 000 EUR lub co najmniej 2 % łącznego rocznego światowego obrotu w poprzednim roku obrotowym przedsiębiorstwa, do którego należy podmiot kluczowy, przy czym zastosowanie ma kwota wyższa.			średniego ogłaszanego przez Narodowy Bank Polski obowiązującego w dniu 31 grudnia w roku poprzedzającym rok wydania decyzji o wymierzeniu kary lub 2% przychodów osiągniętych przez podmiot kluczowy z działalności gospodarczej w roku obrotowym poprzedzającym wymierzenie kary, przy czym zastosowanie ma kwota wyższa. Kara ta nie może być jednak niższa niż 20 000 zł.
Art. 34	5. Państwa członkowskie zapewniają, by podmioty ważne dokonujące naruszeń art. 21 lub 23 podlegały zgodnie z ust. 2 i 3 niniejszego artykułu administracyjnym karom pieniężnym w maksymalnej wysokości co najmniej 7 000 000 EUR lub 1,4 % łącznego rocznego światowego obrotu w poprzednim roku obrotowym przedsiębiorstwa, do którego należy podmiot ważny, przy czym zastosowanie ma kwota wyższa.	TAK	Art. 1 pkt 82 (art. 73 ust. 4)	Art. 73. 4. Wysokość kary pieniężnej nie może przekroczyć 7 000 000 euro, wyrażonej w złotych i ustalonej przy zastosowaniu kursu średniego ogłaszanego przez Narodowy Bank Polski obowiązującego w dniu 31 grudnia w roku poprzedzającym rok wydania decyzji o wymierzeniu kary lub 1,4% przychodów osiągniętych przez podmiot ważny z działalności gospodarczej w roku obrotowym poprzedzającym wymierzenie kary. Kara ta nie może być jednak niższa niż 15 000 zł. Przepis ust. 3a stosuje się odpowiednio z zastrzeżeniem, że za podstawę wymiaru kary pieniężnej przyjmuje się równowartość kwoty 250 000 euro.
Art. 34	6. Państwa członkowskie mogą przewidzieć uprawnienie do nakładania okresowych kar pieniężnych w celu przymuszenia podmiotu kluczowego lub ważnego do zaprzestania naruszenia niniejszej dyrektywy zgodnie z wcześniejszą decyzją właściwego organu.	TAK	Art. 1 pkt 76 (art. 76b)	Art. 76b. 1. Niezależnie od kary pieniężnej nałożonej na podstawie art. 73 ust. 1, organ właściwy do spraw cyberbezpieczeństwa, w celu przymuszenia podmiotu kluczowego albo podmiotu ważnego do wykonania nałożonych na niego obowiązków, może nałożyć na ten podmiot, w drodze decyzji, okresową karę pieniężną w wysokości od 500 zł do 100 000 złotych za każdy dzień opóźnienia, w wykonaniu decyzji wydanych na podstawie art. 53 ust. 5 pkt 2–8. 2. Okresową karę pieniężną nakłada się, licząc od daty wskazanej w decyzji o nałożeniu tej kary.

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				3. Do okresowej kary pieniężnej stosuje się przepisy art. 74 ust. 4 i 5.
Art. 34	7. Bez uszczerbku dla uprawnień właściwych organów na mocy art. 32 i 33, każde państwo członkowskie może ustanowić przepisy określające, czy i w jakim zakresie administracyjne kary pieniężne można nakładać na podmioty administracji publicznej.	TAK		Podmioty administracji publicznej sklasyfikowane jako podmioty kluczowe lub podmioty ważne podlegają administracyjnym karom pieniężnym.
Art. 34	8. Jeżeli system prawny danego państwa członkowskiego nie przewiduje administracyjnych kar pieniężnych, to państwo członkowskie zapewnia takie stosowanie niniejszego artykułu, by o nałożenie kary pieniężnej wnosił właściwy organ, a nakładał ją właściwy sąd krajowy, przy zapewnieniu skuteczności tych rozwiązań prawnych i równoważności ich skutku względem administracyjnej kary pieniężnej nakładanej przez właściwe organy. W każdym przypadku nakładane kary pieniężne muszą być skuteczne, proporcjonalne i odstraszające. Do dnia 17 października 2024 r. państwo członkowskie powiadamia Komisję o przepisach, które przyjęło zgodnie z niniejszym ustępem, oraz niezwłocznie powiadamia o późniejszych przepisach zmieniających lub zmianach mających na nie wpływ.	NIE		
Art. 35	Artykuł 35 Naruszenia pociągające za sobą naruszenie ochrony danych osobowych 1. Jeżeli w czasie nadzoru lub egzekwowania przepisów właściwe organy powzięły wiedzę, że naruszenie przez podmiot kluczowy lub ważny obowiązków określonych w art. 21 i 23 niniejszej dyrektywy może pociągać za sobą naruszenie ochrony danych osobowych zdefiniowane w art. 4 pkt 12 rozporządzenia (UE) 2016/679, które podlega zgłoszeniu na podstawie art. 33 tego rozporządzenia, bez zbędnej zwłoki informują o tym organy nadzorcze, o których mowa w art. 55 i 56 tego rozporządzenia.	TAK	Art. 1 pkt 69 (art. 59a ust. 1)	Art. 59a. 1. W przypadku stwierdzenia podczas sprawowania nadzoru, podejrzenia naruszenia ochrony danych osobowych organ właściwy do spraw cyberbezpieczeństwa informuje o tym Prezesa Urzędu Ochrony Danych Osobowych w terminie 7 dni od dnia stwierdzenia podejrzenia tego naruszenia.
Art. 35	2. Jeżeli organy nadzorcze, o których mowa w art. 55 lub 56 rozporządzenia (UE) 2016/679, nałożą administracyjną karę pieniężną na podstawie art. 58 ust. 2 lit. i) tego rozporządzenia, właściwe organy nie nakładają na podstawie art. 34 niniejszej dyrektywy administracyjnej kary pieniężnej za naruszenie, o którym	TAK	Art. 1 pkt 86 (art. 76c)	Art. 76c. 1. Jeżeli za czyn zagrożony karą określoną w art. 73 lub art. 73a została nałożona prawomocnie kara pieniężna przez Prezesa Urzędu Ochrony Danych Osobowych w związku z naruszeniem ochrony danych osobowych, organ

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

	mowa w ust. 1 niniejszego artykułu, wynikające z tego samego zachowania, za które nałożono administracyjną karę pieniężną na podstawie art. 58 ust. 2 lit. i) rozporządzenia (UE) 2016/679. Właściwe organy mogą jednak zastosować środki egzekwowania przepisów, określone w art. 32 ust. 4 lit. a)–h), art. 32 ust. 5 i art. 33 ust. 4 lit. a)–g) niniejszej dyrektywy.			właściwy do spraw cyberbezpieczeństwa nie wszczyna postępowania w sprawie nałożenia kary i poprzestaje na pouczeniu. Jeżeli zostało wszczęte postępowanie w sprawie nałożenia kary pieniężnej, stosuje się odpowiednio art. 189f ust. 1 pkt 2 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego. 2. W przypadku, o którym mowa w ust. 1, organ właściwy do spraw cyberbezpieczeństwa może stosować środki nadzoru określone w art. 53 ust. 4, 5 i 9.
Art. 35	3. Jeżeli organ nadzorczy właściwy na mocy rozporządzenia (UE) 2016/679 jest ustanowiony w innym państwie członkowskim niż właściwy organ, właściwy organ informuje organ nadzorczy ustanowiony w jego państwie członkowskim o naruszeniu ochrony danych osobowych, o którym mowa w ust. 1.	NIE		
Art. 36	Artykuł 36 Kary Państwa członkowskie ustanawiają przepisy dotyczące kar mających zastosowanie w przypadku naruszeń przepisów i środków krajowych przyjętych na podstawie niniejszej dyrektywy i wprowadzają wszelkie środki niezbędne do zapewnienia wykonywania tych sankcji. Przewidziane kary muszą być skuteczne, proporcjonalne i odstraszające. Państwa członkowskie najpóźniej do dnia 17 stycznia 2025 r. powiadamiają Komisję o tych przepisach i środkach, a następnie niezwłocznie powiadamiają ją o zmianach mających na nie wpływ.	TAK	Art. 1 pkt 82 (art. 73 ust. 1-1b i 3–5), pkt 83 i 84 (art. 73a-74 ust. 1-5) oraz pkt 86 (art. 76a–76e)	Art. 73. 1. Karze pieniężnej podlega podmiot kluczowy lub podmiot ważny, który: 1) nie uzupełnił w terminie brakujących danych w wykazie podmiotów kluczowych i podmiotów ważnych pomimo wezwania, o którym mowa w art. 7b ust. 2 albo art. 7j ust. 3, albo art. 7k ust. 2, albo art. 7l ust. 3 pkt 2; 2) nie przeprowadza systematycznego szacowania ryzyka lub nie zarządza ryzykiem wystąpienia incydentu, o których mowa w art. 8 ust. 1 pkt 1; 3) nie wdrożył systemu zarządzania bezpieczeństwem informacji w systemie informacyjnym wykorzystywanym w procesach wpływających na świadczenie usługi albo system ten nie zapewnia funkcjonalności, o których mowa w art. 8 ust. 1; 4) nie wykonuje obowiązków, o których mowa w art. 10 ust. 1;

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				5) nie wykonuje obowiązku, o którym mowa w art. 11 ust. 1 pkt 1; 6) nie wykonuje obowiązku, o którym mowa w art. 11 ust. 1 pkt 4; 7) nie wykonuje obowiązku, o którym mowa w art. 11 ust. 1 pkt 4; 8) nie wykonuje obowiązku, o którym mowa w art. 11 ust. 1 pkt 4b; 9) nie wykonuje obowiązku, o którym mowa w art. 11 ust. 1 pkt 4; 10) nie wykonuje obowiązku, o którym mowa w art. 11 ust. 1 pkt 5; 11) nie przeprowadza audytu w terminie, o którym mowa w art. 15 ust. 1 lub art. 16 pkt 2; 12) nie usuwa podatności, o których mowa w art. 32 ust. 2; 13) nie korzysta z systemu teleinformatycznego, o którym mowa w art. 46 ust. 1, w celu realizacji obowiązków, o których mowa w art. 11; 14) uniemożliwia lub utrudnia wykonywanie kontroli, o której mowa w art. 53 ust. 2 pkt 1; 15) nie realizuje obowiązku, o którym mowa w art. 53; 16) uniemożliwia lub utrudnia urzędnikowi monitorującemu, o którym mowa w art. 53 ust. 5 pkt 6, wykonywanie powierzonych mu zadań lub realizację uprawnień, o których mowa w art. 53d ust. 1; 17) nie wykonał w wyznaczonym terminie zaleceń pokontrolnych, o których mowa w art. 59 ust. 1. 1a. Organ właściwy do spraw cyberbezpieczeństwa, jeżeli przemawia za tym waga i znaczenie naruszonych przepisów, może nałożyć karę pieniężną na podmiot, który:

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				1) w terminie, o którym mowa w art. 7c ust. 1, nie złożył wniosku o wpis do wykazu podmiotów kluczowych i podmiotów ważnych, o którym mowa w art. 7 ust. 1; 2) nie wykonuje obowiązków, o których mowa w art. 9. 1b. Karze pieniężnej podlega także podmiot kluczowy lub podmiot ważny, którego działanie lub zaniechanie, o którym mowa w ust. 1 pkt 2, 4–12, 14-16 i 18 oraz ust. 1a pkt 2, miało charakter jednorazowy. 3. Wysokość kary pieniężnej nie może przekroczyć 10 000 000 euro, wyrażonej w złotych i ustalonej przy zastosowaniu kursu średniego ogłaszanego przez Narodowy Bank Polski obowiązującego w dniu 31 grudnia w roku poprzedzającym rok wydania decyzji o wymierzeniu kary lub 2% przychodów osiągniętych przez podmiot kluczowy z działalności gospodarczej w roku obrotowym poprzedzającym wymierzenie kary, przy czym zastosowanie ma kwota wyższa. Kara ta nie może być jednak niższa niż 20 000 zł. 3a. W przypadku gdy okres wykonywania działalności gospodarczej jest krótszy niż 12 miesięcy albo podmiot nie osiągnął przychodu za podstawę wymiaru kary pieniężnej przyjmuje się równowartość kwoty 500 000 euro, wyrażonej w złotych i ustalonej przy zastosowaniu kursu średniego ogłaszanego przez Narodowy Bank Polski obowiązującego w dniu 31 grudnia w roku poprzedzającym rok wydania decyzji o wymierzeniu kary. 4. Wysokość kary pieniężnej nie może przekroczyć 7 000 000 euro, wyrażonej w złotych i ustalonej przy zastosowaniu kursu średniego

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				ogłaszanego przez Narodowy Bank Polski obowiązującego w dniu 31 grudnia w roku poprzedzającym rok wydania decyzji o wymierzeniu kary lub 1,4% przychodów osiągniętych przez podmiot ważny z działalności gospodarczej w roku obrotowym poprzedzającym wymierzenie kary. Kara ta nie może być jednak niższa niż 15 000 zł. Przepis ust. 3a stosuje się odpowiednio z zastrzeżeniem, że za podstawę wymiaru kary pieniężnej przyjmuje się równowartość kwoty 250 000 euro. 5. Jeżeli podmiot kluczowy albo podmiot ważny narusza przepisy ustawy, powodując: 1) bezpośrednie i poważne cyberzagrożenie dla obronności, bezpieczeństwa państwa, bezpieczeństwa i porządku publicznego lub życia i zdrowia ludzi, 2) zagrożenie wywołania poważnej szkody majątkowej lub poważnych utrudnień w świadczeniu usług – organ właściwy do spraw cyberbezpieczeństwa nakłada karę w wysokości do 100 000 000 zł. Art. 73a. 1. Karze pieniężnej może podlegać kierownik podmiotu kluczowego lub podmiotu ważnego, który: 1) nie wykonuje co najmniej jednego z obowiązków, o których mowa w art. 7c ust. 1, art. 7b, art. 7c ust. 6 lub art. 7f ust. 3, 2) nie wykonuje co najmniej jednego z obowiązków, o których mowa w art. 8 ust. 1 3) nie wykonuje co najmniej jednego z obowiązków, o których mowa w art. 8d, 4) nie wykonuje obowiązku, o którym mowa w art. 8e,

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				5) nie wykonał obowiązku, o którym mowa w art. 8f ust. 2 lub 3, 6) nie wyznaczył co najmniej dwóch osób do kontaktu z podmiotami kluczowymi lub podmiotami ważnymi, albo w przypadku kierowania mikro- lub małym przedsiębiorcą, o którym mowa w art. 2 ust. 1 załącznika I do rozporządzenia 651/2014/UE, co najmniej jednej osoby do kontaktu z podmiotami krajowego systemu cyberbezpieczeństwa, 7) nie zapewnił użytkownikowi możliwości zgłoszenia cyberzagrożenia, incydentu lub podatności związanych ze świadczoną usługą 8) nie wykonuje co najmniej jednego z obowiązków, o których mowa w art. 10 ust. 1 i 6–8, 9) nie wykonuje co najmniej jednego z obowiązków, o których mowa w art. 11, 10) nie wykonuje co najmniej jednego z obowiązków, o których mowa w art. 12, 11) przekazał sprawozdanie końcowe, o którym mowa w art. 11 ust. 1 pkt 4c, niezawierające elementów określonych w art. 12a, 12) nie wykonuje co najmniej jednego z obowiązków, o których mowa w art. 12b, 13) nie wykonuje obowiązku, o którym mowa w art. 14, 14) nie wykonuje co najmniej jednego z obowiązków, o których mowa w art. 15 – jeżeli przemawia za tym czas, zakres lub charakter naruszenia. 2. Karze pieniężnej może także podlegać kierownik podmiotu kluczowego lub podmiotu ważnego, którego zaniechanie w realizacji obowiązków, o których mowa w ust. 1, miało charakter jednorazowy.

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				3. Niezależnie od kary pieniężnej, o której mowa w art. 73 ust. 1, karę pieniężną można nałożyć również na kierownika podmiotu kluczowego lub podmiotu ważnego za niedokonanie obowiązków wskazanych w tym przepisie. 4. Kara pieniężna, o której mowa w ust. 1–3, może być wymierzona w kwocie nie większej niż 300% otrzymywanego przez ukaranego wynagrodzenia obliczanego według zasad obowiązujących przy ustalaniu ekwiwalentu pieniężnego za urlop. 5. Kara pieniężna, o której mowa w ust. 1–3, może być wymierzona kierownikowi podmiotu kluczowego lub podmiotu ważnego będącym podmiotem publicznym w kwocie nie większej niż 100% otrzymywanego przez ukaranego wynagrodzenia obliczanego według zasad obowiązujących przy ustalaniu ekwiwalentu pieniężnego za urlop. W przypadku gdy podmiot kluczowy lub podmiot ważny będący podmiotem publicznym jest zobowiązany do stosowania ustawy również na podstawie innego sektora wskazanego w załączniku nr 1 lub 2, do kar pieniężnych wymierzanych kierownikowi tego podmiotu stosuje się ust. 4. Art. 73b. 1. Karze pieniężnej podlega: 1) podmiot świadczący usługi rejestracji nazw domen, który nie wykonuje obowiązków, o których mowa w art. 16b i art. 16c; 2) rejestr domen najwyższego poziomu (TLD), który nie wykonuje obowiązków, o których mowa w art. 16b i art. 16c; 3) producent lub dostawca, który nie przekazał dokumentacji badanego produktu ICT lub usługi ICT na wezwanie CSIRT MON, CSIRT NA ☐ K lub ☐ IRT GOV;

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				4) podmiot, który nie przekazał informacji, o którym mowa w art. 43 ust. 1; 5) dostawca usług DNS, rejestr nazw domen najwyższego poziomu (TLD), podmiot świadczący usługi rejestracji nazw domen, dostawca chmury obliczeniowej, dostawca usług centrum przetwarzania danych, dostawca sieci dostarczania treści, dostawca usług zarządzanych, dostawca usług zarządzanych w zakresie cyberbezpieczeństwa, dostawca internetowej platformy handlowej, dostawca wyszukiwarki internetowej oraz dostawca platformy usług sieci społecznościowych świadczący usługi na terytorium Rzeczypospolitej Polskiej, który nie wyznaczył przedstawiciela zgodnie z art. 5a ust. 7. 2. Do wysokości kary pieniężnej, o której mowa w ust. 1 pkt 1 i pkt 5, jeżeli dostawca usług DNS, rejestr nazw domen najwyższego poziomu (TLD), podmiot świadczący usługi rejestracji nazw domen, dostawca chmury obliczeniowej, dostawca usług centrum przetwarzania danych, dostawca sieci dostarczania treści, dostawca usług zarządzanych, dostawca usług zarządzanych w zakresie cyberbezpieczeństwa, dostawca internetowej platformy handlowej, dostawca wyszukiwarki internetowej oraz dostawca platformy usług sieci społecznościowych jest: 1) podmiotem kluczowym – stosuje się art. 73 ust. 3; 2) podmiotem ważnym – stosuje się art. 73 ust. 4. 3. Do wysokości kary pieniężnej, o której mowa w ust. 1 pkt 2, stosuje się art. 73 ust. 3. 4. Kara pieniężna, o której mowa w ust. 1 pkt 3 i 4, wynosi 50 000 zł.

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				Art. 73c. 1. Podmiot finansowy, który nie jest podmiotem kluczowym lub podmiotem ważnym oraz nie jest podmiotem określonym w art. 16 ust. 1 rozporządzenia 2022/2554, podlega karze pieniężnej, jeżeli: 1) nie wykonuje co najmniej jednego z obowiązków, o których mowa w art. 67c ust. 1, 2, 4 i 5; 2) nie wdrożył w terminie określonym w poleceniu zabezpieczającym, o którym mowa w art. 67g ust. 9 pkt 3, określonego zachowania, o którym mowa w art. 67g ust. 10; 3) odstąpił od wykonywania zawartego w poleceniu zabezpieczającym, o którym mowa w art. 67g ust. 9, określonego zachowania, o którym mowa w art. 67g ust. 10, przed wygaśnięciem polecenia zabezpieczającego. 2. Do wysokości kary pieniężnej, o której mowa w ust. 1, stosuje się art. 73 ust. 3. Art. 74.1. Karę pieniężną, o której mowa w art. 73, art. 73a i art. 73b ust. 1 pkt 4, nakłada, w drodze decyzji, organ właściwy do spraw cyberbezpieczeństwa. 2. Karę pieniężną, o której mowa w art. 73b ust. 1 pkt 1–3, nakłada, w drodze decyzji, minister właściwy do spraw informatyzacji. 3. Karę pieniężną, o której mowa w art. 73c ust. 1, nakłada, w drodze decyzji, właściwy organ w rozumieniu rozporządzenia 2022/2554. 4. Organ właściwy do spraw cyberbezpieczeństwa lub właściwy organ w rozumieniu rozporządzenia 2022/2554 może decyzji, o której mowa w ust. 1 lub ust. 3, nadać rygor natychmiastowej wykonalności w całości albo w części, jeżeli

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				wymaga tego ochrona bezpieczeństwa lub porządku publicznego. 5. Wpływy z tytułu kar pieniężnych, o których mowa w art. 73–73c, stanowią przychód Funduszu Cyberbezpieczeństwa, o którym mowa w art. 2 ustawy z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa. Art. 76a. 1. Organ właściwy do spraw cyberbezpieczeństwa, podejmując decyzję o nałożeniu kary pieniężnej i ustalając jej wysokość, uwzględnia odpowiednio kryteria określone w art. 53 ust. 12 oraz wysokość przychodu uzyskanego z działalności gospodarczej w roku obrotowym poprzedzającym wymierzenie kary pieniężnej, możliwości finansowe podmiotu kluczowego lub podmiotu ważnego będącego podmiotem publicznym albo możliwości finansowe kierownika podmiotu kluczowego lub podmiotu ważnego. Art. 189a §2 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego nie stosuje się. 2. W przypadku gdy podmiot kluczowy lub podmiot ważny powstał w wyniku połączenia lub przekształcenia innych podmiotów, obliczając wysokość jego przychodu organ właściwy do spraw cyberbezpieczeństwa uwzględnia przychód osiągnięty przez te podmioty w roku obrotowym poprzedzającym rok nałożenia kary pieniężnej. Przepisy art. 73 ust. 3–4 stosuje się odpowiednio. 3. W związku z toczącym się postępowaniem w sprawie nałożenia kary pieniężnej, podmiot, wobec którego wszczęto to postępowanie lub podmiot zatrudniający kierownika podmiotu

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				kluczowego lub podmiotu ważnego jest obowiązany do dostarczenia organowi uprawnionemu do nałożenia kary pieniężnej na każde jego żądanie, w terminie wskazanym w wezwaniu, nie dłuższym niż 1 miesiąc od dnia otrzymania żądania, danych niezbędnych do określenia podstawy wymiaru kary pieniężnej. 4. W przypadku niedostarczenia danych lub dostarczenia danych uniemożliwiających ustalenie podstawy wymiaru kary pieniężnej, organ właściwy do spraw cyberbezpieczeństwa ustala podstawę wymiaru kary pieniężnej w sposób szacunkowy, uwzględniając w szczególności wielkość danego podmiotu kluczowego lub podmiotu ważnego, specyfikę działalności tego podmiotu lub ogólnodostępne dane finansowe. 5. Karę pieniężną uiszcza się w terminie 14 dni od dnia, w którym decyzja o jej wymierzeniu stała się ostateczna, lub od dnia doręczenia decyzji z rygiorem natychmiastowej wykonalności, na rachunek bankowy organu właściwego do spraw cyberbezpieczeństwa, wskazany w decyzji o wymierzeniu kary pieniężnej. 6. Kary pieniężne nieuiszczone w terminie wraz z odsetkami podlegają ściągnięciu przez organ właściwy do spraw cyberbezpieczeństwa, który wymierzył karę pieniężną w trybie określonym w przepisach o postępowaniu egzekucyjnym w administracji. 7. Organ właściwy do spraw cyberbezpieczeństwa przekazuje na rachunek Funduszu Cyberbezpieczeństwa środki pochodzące z kar pieniężnych w terminie 14 dni od dnia ich uiszczenia albo pobrania. W tym samym terminie przekazuje ministrowi

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				właściwemu do spraw informatyzacji kopię decyzji o wymierzeniu kary pieniężnej lub innego dokumentu stanowiącego podstawę naliczenia, pobrania i przekazania na rachunek Funduszu Cyberbezpieczeństwa kary pieniężnej lub odsetek od nieterminowej wpłaty. 8. Organ właściwy do spraw cyberbezpieczeństwa w terminie 14 dni od dnia wystąpienia zdarzenia mogącego skutkować zmianą lub uchynieniem decyzji lub dokumentu stanowiącego podstawę do naliczenia, pobrania i przekazania na rachunek Funduszu Cyberbezpieczeństwa środków pochodzących z kar pieniężnych, informuje ministra właściwego do spraw informatyzacji o tym zdarzeniu, a w szczególności o wniesieniu skargi do sądu administracyjnego, skargi kasacyjnej, wydaniu prawomocnego wyroku, wszczęciu lub zakończeniu postępowania administracyjnego w zakresie wznowienia postępowania, uchylenia, zmiany lub stwierdzenia nieważności decyzji. 9. Organ właściwy do spraw cyberbezpieczeństwa może odstąpić od nałożenia kary pieniężnej, jeżeli waga naruszenia i znaczenie naruszonych przepisów są znikome, a podmiot albo kierownik podmiotu kluczowego lub podmiotu ważnego zaprzestał naruszania prawa lub naprawił wyrządzoną szkodę. 10. Do postępowania w sprawie nałożenia kar pieniężnych, o których mowa w art. 73b ust. 1 i art. 73c ust. 1, stosuje się odpowiednio ust. 1–9. Art. 76b. 1. Niezależnie od kary pieniężnej nałożonej na podstawie art. 73 ust. 1, organ właściwy do spraw cyberbezpieczeństwa, w celu przymuszenia podmiotu kluczowego albo

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				podmiotu ważnego do wykonania nałożonych na niego obowiązków, może nałożyć na ten podmiot, w drodze decyzji, okresową karę pieniężną w wysokości od 500 zł do 100 000 złotych za każdy dzień opóźnienia, w wykonaniu decyzji wydanych na podstawie art. 53 ust. 5 pkt 2–8. 2. Okresową karę pieniężną nakłada się, licząc od daty wskazanej w decyzji o nałożeniu tej kary. 3. Do okresowej kary pieniężnej stosuje się przepisy art. 74 ust. 4 i 5. Art. 76c. 1. Jeżeli za czyn zagrożony karą określoną w art. 73 lub art. 73a została nałożona prawomocnie kara pieniężna przez Prezesa Urzędu Ochrony Danych Osobowych w związku z naruszeniem ochrony danych osobowych, organ właściwy do spraw cyberbezpieczeństwa nie wszczyna postępowania w sprawie nałożenia kary i przestaje na pouczeniu. Jeżeli zostało wszczęte postępowanie w sprawie nałożenia kary pieniężnej, stosuje się odpowiednio art. 189f ust. 1 pkt 2 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego. 2. W przypadku o którym mowa w ust. 1, organ właściwy do spraw cyberbezpieczeństwa może stosować środki nadzoru określone w art. 53 ust. 4, 5 i 9. Art. 76d. 1. W przypadku, o którym mowa w art. 73 ust. 1 pkt 3, kara pieniężna może być nakładana w sposób określony w art. 14 § 1b ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego. 2. Do postępowania w sprawie nałożenia kary pieniężnej stosuje się przepisy działu II rozdziału 14 ustawy z dnia 14 czerwca 1960 r. – Kodeks

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				postępowania administracyjnego, z wyjątkiem przepisów o milczącym załatwieniu sprawy. Art. 76e. W zakresie nieuregulowanym w niniejszym rozdziale stosuje się odpowiednio przepisy działu IVa ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego.
Art. 37	Artykuł 37 Wzajemna pomoc 1. Jeżeli podmiot świadczy usługi w więcej niż jednym państwie członkowskim lub świadczy usługi w co najmniej jednym państwie członkowskim, a jego sieć i systemy informatyczne są zlokalizowane w co najmniej jednym innym państwie członkowskim, właściwe organy zainteresowanych państw członkowskich współpracują ze sobą i udzielają sobie wzajemnie pomocy, odpowiednio do potrzeb. Współpraca ta obejmuje co najmniej następujące kwestie: a) właściwe organy stosujące środki nadzoru lub egzekwowania przepisów w państwie członkowskim informują – za pośrednictwem pojedynczego punktu kontaktowego – właściwe organy w pozostałych zainteresowanych państwach członkowskich o zastosowanych środkach nadzoru i egzekwowania przepisów i koordynują je z tymi właściwymi organami w tej sprawie; b) właściwy organ może zwrócić się do innego właściwego organu o udzielenie środków nadzoru lub egzekwowania przepisów; c) właściwy organ po otrzymaniu uzasadnionego wniosku od innego właściwego organu udziela temu innemu właściwemu organowi pomocy współmiernej do swoich zasobów, tak by można było skutecznie, wydajnie i spójnie wdrożyć środki nadzoru lub egzekwowania przepisów. Wzajemna pomoc, o której mowa w akapicie pierwszym lit. c), może obejmować wnioski o udzielenie informacji i zastosowanie środków nadzoru, w tym wnioski o przeprowadzenie kontroli na miejscu lub nadzoru zewnętrznego lub ukierunkowanych audytów bezpieczeństwa. Właściwy organ, do którego skierowany jest	TAK	Art. 1 pkt 69 (art. 59b ust. 1-4)	Art. 59b. 1. Organ właściwy do spraw cyberbezpieczeństwa udziela pomocy organom innych państw członkowskich Unii Europejskiej w sprawowaniu nadzoru nad podmiotami kluczowymi lub podmiotami ważnymi, których systemy informacyjne znajdują się na terytorium Rzeczypospolitej Polskiej. 2. Organ właściwy do spraw cyberbezpieczeństwa może, za pośrednictwem Pojedynczego Punktu Kontaktowego, zwracać się do organów innych państw członkowskich Unii Europejskiej o przeprowadzenie czynności nadzorczych nad podmiotami kluczowymi lub podmiotami ważnymi, świadczącymi usługi na terytorium Rzeczypospolitej Polskiej, których siedziba, zarząd lub systemy informacyjne znajdują się na terytorium innego państwa członkowskiego Unii Europejskiej. 3. Organ właściwy do spraw cyberbezpieczeństwa odmawia udzielenia pomocy, o której mowa w ust. 1, jeżeli: 1) nie jest właściwy w sprawie; 2) żądana pomoc jest nieproporcjonalna do realizowanych przez organ zadań z zakresu nadzoru; 3) organ innego państwa członkowskiego Unii Europejskiej żąda udostępnienia informacji lub dokumentów, których udostępnienie narusza

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

	wniosek o pomoc, nie może odmówić wykonania tego wniosku, chyba że zostanie ustalone, że organ ten nie jest organem właściwym do udzielenia pomocy, której dotyczy wniosek, że pomoc ta jest niewspółmierna do zadań nadzorczych właściwego organu lub że wniosek dotyczy informacji lub obejmuje działania, których ujawnienie lub wykonanie byłoby sprzeczne z podstawowymi interesami państwa członkowskiego w zakresie bezpieczeństwa narodowego, bezpieczeństwa publicznego lub obronnością. Zanim właściwy organ odmówi wykonania wniosku, zasięga opinii innych zainteresowanych właściwych organów, a na wniosek jednego z zainteresowanych państw członkowskich – także opinii Komisji i ENISA.			podstawowy interes bezpieczeństwa państwa, bezpieczeństwa i porządku publicznego lub obronności. 4. Przed odmową udzielenia pomocy organ właściwy do spraw cyberbezpieczeństwa konsultuje się z wnioskującym o udzielenie pomocy organem innego państwa, a także z Komisją Europejską i ENISA, jeśli żąda tego państwo członkowskie Unii Europejskiej.
	2. W stosownych przypadkach i za obopólnym porozumieniem właściwe organy z różnych państw członkowskich mogą prowadzić wspólne działania nadzorcze.	TAK	Art. 1 pkt 69 (art. 59b ust. 5)	Art. 59b. 5. Organ właściwy do spraw cyberbezpieczeństwa może prowadzić wspólne czynności nadzorcze z organem innego państwa członkowskiego Unii Europejskiej.
Art. 38	Artykuł 38 Wykonywanie przekazanych uprawnień 1. Powierzenie Komisji uprawnień do przyjmowania aktów delegowanych podlega warunkom określonym w niniejszym artykule. 2. Uprawnienia do przyjmowania aktów delegowanych, o których mowa w art. 24 ust. 2, powierza się Komisji na okres pięciu lat od 16 stycznia 2023 r. 3. Przekazanie uprawnień, o którym mowa w art. 24 ust. 2, może zostać odwołane w dowolnym momencie przez Parlament Europejski lub przez Radę. Decyzja o odwołaniu kończy przekazanie określonych w niej uprawnień. Decyzja o odwołaniu staje się skuteczna następnego dnia po jej opublikowaniu w Dzienniku Urzędowym Unii Europejskiej lub w późniejszym terminie określonym w tej decyzji. Nie wpływa ona na ważność już obowiązujących aktów delegowanych. 4. Przed przyjęciem aktu delegowanego Komisja konsultuje się z ekspertami wyznaczonymi przez każde państwo członkowskie zgodnie z zasadami określonymi w Porozumieniu	NIE		

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

	międzyinstytucjonalnym w sprawie lepszego stanowienia prawa z dnia 13 kwietnia 2016 r. 5. Niezwłocznie po przyjęciu aktu delegowanego Komisja przekazuje go równocześnie Parlamentowi Europejskiemu i Radzie. 6. Akt delegowany przyjęty na podstawie art. 24 ust. 2 wchodzi w życie tylko wówczas, gdy ani Parlament Europejski, ani Rada nie wyraziły sprzeciwu w terminie dwóch miesięcy od przekazania tego aktu Parlamentowi Europejskiemu i Radzie, lub gdy, przed upływem tego terminu, zarówno Parlament Europejski, jak i Rada poinformowały Komisję, że nie wniosą sprzeciwu. Termin ten przedłuża się o dwa miesiące z inicjatywy Parlamentu Europejskiego lub Rady.			
Art. 39	Artykuł 39 Procedura komitetowa 1. Komisję wspomaga komitet. Komitet ten jest komitetem w rozumieniu rozporządzenia (UE) nr 182/2011. 2. W przypadku odesłania do niniejszego ustępu stosuje się art. 5 rozporządzenia (UE) nr 182/2011. 3. W przypadku gdy opinia komitetu ma zostać uzyskana w drodze procedury pisemnej, procedura ta kończy się bez osiągnięcia rezultatu, gdy – przed upływem terminu na wydanie opinii – zdecyduje o tym przewodniczący komitetu lub wniesie o to członek komitetu.	NIE		
Art. 40	Artykuł 40 Przegląd Do dnia 17 października 2027 r., a następnie co 36 miesięcy Komisja przeprowadza przegląd funkcjonowania niniejszej dyrektywy i składa Parlamentowi Europejskiemu i Radzie sprawozdanie na ten temat. W sprawozdaniu ocenia się w szczególności znaczenie wielkości danych podmiotów oraz sektorów, podsektorów, rodzaju podmiotu, o którym mowa w załącznikach I i II, dla funkcjonowania gospodarki i społeczeństwa w kontekście cyberbezpieczeństwa. W tym celu oraz z myślą o dalszym rozwijaniu współpracy strategicznej i operacyjnej Komisja bierze pod uwagę sprawozdania Grupy Współpracy i sieci CSIRT na temat doświadczeń zdobytych	NIE		

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

	na poziomie strategicznym i operacyjnym. Sprawozdaniu towarzyszy w razie potrzeby wniosek ustawodawczy.			
Art. 41	Artykuł 41 Transpozycja 1. Do dnia 17 października 2024 r. państwa członkowskie przyjmują i publikują przepisy niezbędne do wykonania niniejszej dyrektywy. Niezwłocznie powiadamiają one o tym Komisję. Państwa członkowskie stosują te przepisy od dnia 18 października 2024 r.	TAK	Art. 47	Art. 47. Ustawa wchodzi w życie po upływie miesiąca od dnia ogłoszenia.
Art. 41	2. Przepisy, o których mowa w ust. 1, przyjęte przez państwa członkowskie zawierają odniesienie do niniejszej dyrektywy lub odniesienie takie towarzyszy ich urzędowej publikacji. Sposób dokonywania takiego odniesienia określany jest przez państwa członkowskie.	TAK	Odnośnik przy tytule ustawy	Odnośnik przy tytule ustawy Niniejsza ustawa wdraża dyrektywę Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniającą rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającą dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz. Urz. UE L 333 z 27.12.2022, str. 80).
Art. 42	Artykuł 42 Zmiana rozporządzenia (UE) nr 910/2014 W rozporządzeniu (UE) nr 910/2014 uchyla się art. 19 ze skutkiem od dnia 18 października 2024 r.	TAK	Art. 15	Art. 15. W ustawie z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. z 2024 r. poz. 1725) wprowadza się następujące zmiany: 1) w art. 4 po ust. 5 dodaje się ust. 5a i 5b w brzmieniu: „5a. Do wniosku o wpis, o którym mowa w ust. 1, dołącza się dane, o których mowa w art. 7 ust. 3 pkt 1–17 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077, 1222 oraz z 2025 r. poz. 1017, 1069 i ...). 5b. Po wpisie do rejestru, minister właściwy do spraw informatyzacji dane, o których mowa w art. 7 ust. 2 pkt 1–17 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, wpisuje do wykazu podmiotów kluczowych i

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

				podmiotów ważnych, o którym mowa w art. 7 ust. 1 tej ustawy. Danych tych nie zamieszcza się w rejestrze.”; 2) w art. 15 w ust. 2 skreśla się wyrazy „oraz informacje o zdarzeniach powodujących naruszenia bezpieczeństwa lub utratę integralności, o których mowa w art. 20a ust. 2”; 3) uchyla się art. 20a; 7) uchyla się art. 30a; 8) uchyla się art. 39; 9) w art. 46 uchyla się pkt 8.
Art. 43	Artykuł 43 Zmiana dyrektywy (UE) 2018/1972 W dyrektywie (UE) 2018/1972 uchyla się art. 40 i 41 ze skutkiem od dnia 18 października 2024 r.	NIE		
Art. 44	Artykuł 44 Uchylenie Dyrektywa (UE) 2016/1148 traci moc ze skutkiem od dnia 18 października 2024 r. Odesłania do uchylonej dyrektywy uznaje się za odesłania do niniejszej dyrektywy i odczytuje się zgodnie z tabelą korelacji w załączniku III.	NIE		
Art. 45	Artykuł 45 Wejście w życie Niniejsza dyrektywa wchodzi w życie dwudziestego dnia po jej opublikowaniu w Dzienniku Urzędowym Unii Europejskiej.	NIE		
Art. 46	Artykuł 46 Adresaci Niniejsza dyrektywa skierowana jest do państw członkowskich.	NIE		
Załącznik III	ZAŁĄCZNIK III TABELA KORELACJI		NIE	
	Dyrektywa (UE) 2016/1148	Niniejsza dyrektywa		

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

	art. 1 ust. 1	art. 1 ust. 1			
	art. 1 ust. 2	art. 1 ust. 2			
	art. 1 ust. 3	–			
	art. 1 ust. 4	art. 2 ust. 12			
	art. 1 ust. 5	art. 2 ust. 13			
	art. 1 ust. 6	art. 2 ust. 6 i 11			
	art. 1 ust. 7	art. 2 ust. 4			
	art. 2	art. 2 ust. 14			
	art. 3	art. 5			
	art. 4	art. 6			
	art. 5	–			
	art. 6	–			
	art. 7 ust. 1	art. 7 ust. 1 i 2			
	art. 7 ust. 2	art. 7 ust. 4			
	art. 7 ust. 3	art. 7 ust. 3			
	art. 8 ust. 1–5	art. 8 ust. 1–5			
	art. 8 ust. 6	art. 13 ust. 4			
	art. 8 ust. 7	art. 8 ust. 6			
	art. 9 ust. 1, 2 i 3	art. 10 ust. 1, 2 i 3			

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

art. 9 ust. 4	art. 10 ust. 9			
art. 9 ust. 5	art. 10 ust. 19			
art. 10 ust. 1, 2 i 3 akapit pierwszy	art. 11 ust. 1–3			
Art. 10 ust. 3 akapit drugi	art. 23 ust. 9			
art. 11 ust. 1	art. 14 ust. 1 i 2			
art. 11 ust. 2	art. 14 ust. 3			
art. 11 ust. 3	art. 14 ust. 4 i 6 akapit pierwszy lit. a)–q) i lit. s) oraz ust. 7			
art. 11 ust. 4	art. 14 ust. 4 akapit pierwszy lit. r) i akapit drugi			
art. 11 ust. 5	art. 14 ust. 8			
art. 12 ust. 1–5	art. 15 ust. 1–5			
art. 13	art. 17			
art. 14 ust. 1 i 2	art. 21 ust. 1–4			
art. 14 ust. 3	art. 23 ust. 1			
art. 14 ust. 4	art. 23 ust. 3			
art. 14 ust. 5	art. 23 ust. 5, 6 i 8			
art. 14 ust. 6	art. 23 ust. 7			
art. 14 ust. 7	art. 23 ust. 11			
art. 15 ust. 1	art. 31 ust. 1			

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

art. 15 ust. 2 akapit pierwszy lit. a)	art. 32 ust. 2 lit. e)			
art. 15 ust. 2 akapit pierwszy lit. b)	art. 32 ust. 2 lit. g)			
art. 15 ust. 2 akapit drugi	art. 32 ust. 3			
art. 15 ust. 3	art. 32 ust. 4 lit. b)			
art. 15 ust. 4	art. 31 ust. 3			
art. 16 ust. 1	art. 21 ust. 1–4			
art. 16 ust. 3	art. 23 ust. 1			
art. 16 ust. 4	art. 23 ust. 3			
art. 16 ust. 5	–			
art. 16 ust. 6	art. 23 ust. 6			
art. 16 ust. 7	art. 23 ust. 7			
art. 16 ust. 8 i 9	art. 21 ust. 5 i art. 23 ust. 11			
art. 16 ust. 10	–			
art. 16 ust. 11	art. 2 ust. 1, 2 i 3			
art. 17 ust. 1	art. 33 ust. 1			
art. 17 ust. 2 lit. a)	art. 32 ust. 2 lit. e)			
art. 17 ust. 2 lit. b)	art. 32 ust. 4 lit. b)			
art. 17 ust. 3	art. 37 ust. 1 lit. a) i b)			

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

	art. 18 ust. 1	art. 26 ust. 1–2			
	art. 18 ust. 2	art. 26 ust. 3			
	art. 18 ust. 3	art. 26 ust. 4			
	art. 19	art. 25			
	art. 20	art. 30			
	art. 21	art. 36			
	art. 22	art. 39			
	art. 23	art. 40			
	art. 24	–			
	art. 25	art. 41			
	art. 26	art. 45			
	art. 27	art. 46			
	załącznik I pkt 1	art. 11 ust. 1			
	załącznik I pkt 2 lit. a) ppkt (i)–(iv)	art. 11 ust. 2 lit. a)–d)			
	załącznik I pkt 2 lit. a) ppkt (v)	art. 11 ust. 2 lit. f)			
	załącznik I pkt 2 lit. b)	art. 11 ust. 4			
	załącznik I pkt 2 lit. c) ppkt (i) i(ii)	art. 11 ust. 5 lit. a)			
	załącznik II	załącznik I			

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

	załącznik III pkt 1, 2	załącznik II pkt 6			
	załącznik III pkt 3	załącznik I pkt 8			

SEKTORY KLUCZOWE

Dyrektywa NIS 2			Nowelizacja			
Sektor	Podsektor	Rodzaj podmiotu	Sektor	Podsektor	Rodzaj podmiotu	Komentarz
Artykuł 3 Podmioty kluczowe i ważne 1. Do celów niniejszej dyrektywy następujące podmioty uznaje się za podmioty kluczowe: g) jeżeli państwo członkowskie tak postanowi, podmioty, które to państwo członkowskie wskazało przed 16 stycznia 2023 r. jako operatorów usług kluczowych zgodnie z dyrektywą (UE) 2016/1148 lub prawem krajowym.			Energia	Wydobywanie kopalin	Podmioty prowadzące działalność gospodarczą w zakresie wydobywania gazu ziemnego na podstawie koncesji, o której mowa w art. 22 ust. 1 ustawy z dnia 9 czerwca 2011 r. – Prawo geologiczne i górnicze (Dz. U. z 2024 r. poz. 1290 oraz z 2025 r. poz. 769 i 1023).	
					Podmioty prowadzące działalność gospodarczą w zakresie wydobywania ropy naftowej na podstawie koncesji, o której mowa w art. 22 ust. 1 ustawy z dnia 9 czerwca 2011 r. – Prawo geologiczne i górnicze.	
					Podmioty prowadzące działalność gospodarczą w zakresie wydobywania węgla brunatnego na podstawie koncesji, o której mowa w art. 22 ust. 1 ustawy z dnia 9 czerwca 2011 r. – Prawo geologiczne i górnicze.	
					Podmioty prowadzące działalność gospodarczą w zakresie wydobywania węgla kamiennego na podstawie koncesji, o której mowa w art. 22 ust. 1 ustawy z dnia 9 czerwca 2011 r. – Prawo geologiczne i górnicze.	
					Podmioty prowadzące działalność gospodarczą w zakresie wydobywania pozostałych kopalin na podstawie koncesji, o której mowa w art. 22 ust. 1 ustawy z dnia 9 czerwca 2011 r. – Prawo geologiczne i górnicze.	
1. Energetyka	a) energia elektryczna	— przedsiębiorstwa energetyczne zgodnie z definicją w art. 2 pkt 57 dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/944, wykonujące funkcję dostaw zgodnie z definicją w art. 2 pkt 12 tej dyrektywy		Energia elektryczna	Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne (Dz. U. z 2024 r. poz. 266, z późn. zm.), posiadające koncesję na wykonywanie działalności gospodarczej w zakresie obrotu energią elektryczną.	

		— operatorzy systemów dystrybucyjnych zgodnie z definicją w art. 2 pkt 29 dyrektywy (UE) 2019/944			Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 25 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie dystrybucji energii elektrycznej.		
		— operatorzy systemów przesyłowych zgodnie z definicją w art. 2 pkt 35 dyrektywy (UE) 2019/944			Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 24 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie przesyłania energii elektrycznej.		
		— wytwórcy zgodnie z definicją w art. 2 pkt 38 dyrektywy (UE) 2019/944			Przedsiębiorstwo energetyczne, o którym w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne posiadające koncesję na wykonywanie działalności gospodarczej w zakresie wytwarzania energii elektrycznej.		
		- wyznaczeni operatorzy rynku energii elektrycznej zgodnie z definicją w art. 2 pkt 8 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/943			Podmioty, o których mowa w art. 3 pkt 28b ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne.		
		- uczestnicy rynku zgodnie z definicją w art. 2 pkt 25 rozporządzenia (UE) 2019/943 świadczący usługi agregacji, odpowiedzi odbioru lub magazynowania energii zgodnie z definicją w art. 2 pkt 18, 20 i 59 dyrektywy (UE) 2019/944			Uczestnicy rynku świadczący usługę o której mowa w art. 3 pkt 6e ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne.		
					Uczestnicy rynku świadczący usługę, o której mowa w art. 3 pkt 11j ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne.		
					Uczestnicy rynku świadczący usługę, o której mowa w art. 3 pkt 59 i art. 3 pkt 59a ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne		
		- operatorzy punktów ładowania odpowiedzialni za zarządzanie punktem ładowania i jego obsługę, świadczący usługę ładowania użytkownikom końcowym, w tym w imieniu i na rzecz dostawcy usług w zakresie mobilności			Przedsiębiorcy odpowiedzialni za zarządzanie punktem ładowania i jego obsługę, świadczący usługę ładowania na rzecz użytkowników końcowych, w tym w imieniu i na rzecz dostawcy usług w zakresie mobilności		
	b) system ciepłowniczy	— operatorzy systemów ciepłowniczych lub chłodniczych zgodnie z definicją			Ciepło	Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie	

	lub chłodniczy	w art. 2 pkt 19 dyrektywy Parlamentu Europejskiego i Rady (UE) 2018/2001			działalności gospodarczej w zakresie wytwarzania ciepła.	
					Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie obrotu ciepłem.	
					Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie przesyłania ciepła.	
					Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie dystrybucji ciepła.	
	c) ropa naftowa	— operatorzy ropociągów		Ropa i paliwa	Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie wytwarzania paliw ciekłych, o której mowa w art. 32 ust. 1 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne.	
		— operatorzy instalacji służących do produkcji, rafinacji, przetwarzania, magazynowania i przesyłu ropy naftowej			Podmioty prowadzące działalność gospodarczą w zakresie przesyłania ropy naftowej.	
					Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie przesyłania paliw ciekłych siecią rurociągów, o której mowa w art. 32 ust. 1 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne.	
				Podmiot prowadzący działalność gospodarczą w zakresie magazynowania ropy naftowej, w tym w zakresie bezzbiornikowego podziemnego		

					magazynowania ropy naftowej, o którym mowa w art. 22 ust. 1 ustawy z dnia 9 czerwca 2011 r. – Prawo geologiczne i górnicze. Podmioty prowadzące działalność gospodarczą w zakresie przeładunku ropy naftowej. Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, wykonujące działalność gospodarczą w zakresie magazynowania paliw ciekłych, o którym mowa w art. 32 ust. 1 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, oraz podmiot prowadzący działalność w zakresie bezzbiornikowego podziemnego magazynowania paliw ciekłych, o którym mowa w art. 22 ust. 1 ustawy z dnia 9 czerwca 2011 r. –Prawo geologiczne i górnicze. Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, wykonujące działalność gospodarczą w zakresie przeładunku paliw ciekłych, o którym mowa w art. 32 ust. 1 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne. Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, wykonujące działalność gospodarczą w zakresie obrotu paliwami ciekłymi lub w zakresie obrotu paliwami ciekłymi z zagranicą, o którym mowa w art. 32 ust. 1 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne. Podmioty prowadzące działalność gospodarczą w zakresie wytwarzania paliw syntetycznych.	
		— krajowe centrale zapasów zgodnie z definicją w art. 2 lit. f dyrektywy Rady 2009/119/WE			Agencja wykonawcza utworzona na podstawie ustawy z dnia 17 grudnia 2020 r. o rezerwach strategicznych (Dz. U. z 2024 r. poz. 1598 i 1907).	

d)	gaz	— przedsiębiorstwa dostarczające gaz zgodnie z definicją w art. 2 pkt 8 dyrektywy Parlamentu Europejskiego i Rady 2009/73/WE			Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie obrotu gazem ziemnym z zagranicą lub na wykonywanie działalności gospodarczej w zakresie obrotu paliwami gazowymi.	
		— operatorzy systemów dystrybucyjnych zgodnie z definicją w art. 2 pkt 6 dyrektywy 2009/73/WE			Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 25 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, będące wyznaczonym przez Prezesa Urzędu Regulacji Energetyki operatorem systemu dystrybucyjnego gazowego.	
		— operatorzy systemów przesyłowych zgodnie z definicją w art. 2 pkt 4 dyrektywy 2009/73/WE			Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 24 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, będące wyznaczonym przez Prezesa Urzędu Regulacji Energetyki operatorem systemu przesyłowego gazowego.	
		— operatorzy systemów magazynowania zgodnie z definicją w art. 2 pkt 10 dyrektywy 2009/73/WE			Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 26 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, będące wyznaczonym przez Prezesa Urzędu Regulacji Energetyki operatorem systemu magazynowania paliw gazowych.	
		— operatorzy systemów LNG zgodnie z definicją w art. 2 pkt 12 dyrektywy 2009/73/WE			Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 27 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, będące wyznaczonym przez Prezesa Urzędu Regulacji Energetyki operatorem systemu skraplania gazu ziemnego.	
		— przedsiębiorstwa gazowe zgodnie z definicją w art. 2 pkt 1 dyrektywy 2009/73/WE			Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, prowadzące działalność w zakresie wytwarzania paliw gazowych, o którym mowa w art. 3 pkt 45 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne.	
					Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie	

					działalności gospodarczej w zakresie przesyłania paliw gazowych.	
				Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie obrotu gazem ziemnym z zagranicą lub na wykonywanie działalności gospodarczej w zakresie obrotu paliwami gazowymi.		
		— operatorzy instalacji służących do rafinacji i przetwarzania gazu ziemnego		Przedsiębiorstwa energetyczne prowadzące działalność gospodarczą w zakresie rafinacji i przetwarzania gazu ziemnego.		
	BRAK			Energetyka jądrowa	Podmiot będący operatorem obiektu energetyki jądrowej, określonego w art. 2 pkt 2 ustawie z dnia 29 czerwca 2011 r. o przygotowaniu i realizacji inwestycji w zakresie obiektów energetyki jądrowej oraz inwestycji towarzyszących (Dz. U. z 2025 r. poz. 1156).	
	e) wodór	— operatorzy instalacji służących do produkcji, magazynowania i przesyłu wodoru		Wodór	Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, prowadzące działalność w zakresie przesyłania wodoru.	
					Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, prowadzące działalność w zakresie magazynowania wodoru.	
					Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, prowadzące działalność w zakresie wytwarzania wodoru.	
					Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, prowadzące działalność w zakresie dystrybucji wodoru.	
2. Transport		— przewoźnicy lotniczy zgodnie z definicją w art. 3 pkt 4 rozporządzenia	Transport	Transport lotniczy	Przewoźnik lotniczy, o którym mowa w art. 3 pkt 4 rozporządzenia Parlamentu	

	a) transport lotniczy	(WE) nr 300/2008, wykorzystywani do celów komercyjnych			Europejskiego i Rady (WE) nr 300/2008 z dnia 11 marca 2008 r. w sprawie wspólnych zasad w dziedzinie ochrony lotnictwa cywilnego i uchylającego rozporządzenie (WE) nr 2320/2002 (Dz. Urz. UE L 97 z 09.04.2008, str. 72).	
		— zarządzający portem lotniczym zgodnie z definicją w art. 2 pkt 2 dyrektywy Parlamentu Europejskiego i Rady 2009/12/WE, porty lotnicze zgodnie z definicją w art. 2 pkt 1 tej dyrektywy, w tym porty bazowe wymienione w sekcji 2 załącznika II do rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1315/2013; oraz jednostki obsługujące urządzenia pomocnicze znajdujące się w portach lotniczych			Zarządzający lotniskiem, o którym mowa w art. 2 pkt 7 ustawy z dnia 3 lipca 2002 r. – Prawo lotnicze (Dz. U. z 2025 r. poz.1431).	
		— operatorzy zarządzający ruchem lotniczym zapewniający służbę kontroli ruchu lotniczego (ATC) zgodnie z definicją w art. 2 pkt 1 rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 549/2004			Przedsiębiorca, o którym mowa w art. 177 ust. 2 ustawy z dnia 3 lipca 2002 r. – Prawo lotnicze, wykonujący dla przewoźników lotniczych oraz innych użytkowników statków powietrznych jedną lub więcej kategorii usług, o których mowa w art. 176 tej ustawy, oraz przedsiębiorca, o którym mowa w art. 186b ust. 1 pkt 2 ustawy z dnia 3 lipca 2002 r. – Prawo lotnicze, wykonujący dla przewoźników lotniczych zadania związane z kontrolą bezpieczeństwa.	
	b) transport kolejowy	— zarządcy infrastruktury zgodnie z definicją w art. 3 pkt 2 dyrektywy Parlamentu Europejskiego i Rady 2012/34/UE		Transport kolejowy	Instytucja zapewniająca służby żeglugi powietrznej, o której mowa w art. 127 ust. 1 ustawy z dnia 3 lipca 2002 r. – Prawo lotnicze.	
		— przedsiębiorstwa kolejowe zgodnie z definicją w art. 3 pkt 1 dyrektywy 2012/34/UE, w tym operatorzy infrastruktury kolejowej zdefiniowanej w art. 3 pkt 12 tej dyrektywy			Zarządca infrastruktury kolejowej w rozumieniu art. 4 pkt 7 ustawy z dnia 28 marca 2003 r. o transporcie kolejowym (Dz. U. z 2025 r. poz. 1234), z wyłączeniem zarządców wyłącznie infrastruktury nieczynnej, o której mowa w art. 4 pkt 1b tej ustawy, infrastruktury prywatnej, o której mowa w art. 4 pkt 1c, oraz infrastruktury kolei wąskotorowej, o której mowa w art. 4 pkt 1d tej ustawy.	
					Przewoźnik kolejowy, o którym mowa w art. 4 pkt 9 ustawy z dnia 28 marca 2003 r. o transporcie kolejowym, którego działalność podlega licencjonowaniu, oraz operator obiektu infrastruktury usługowej, o którym mowa w art. 4 pkt 52 ustawy z dnia 28 marca 2003 r. o transporcie	

					kolejowym, jeżeli przedsiębiorca wykonujący funkcję operatora jest jednocześnie przewoźnikiem kolejowym.	
	c) transport wodny	— armatorzy śródlądowego, morskiego i przybrzeżnego wodnego transportu pasażerów i towarów zgodnie z definicją dla transportu morskiego w załączniku I do rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 725/2004, z wyłączeniem poszczególnych statków, na których prowadzą działalność ci armatorzy		Transport wodny	Armator w transporcie morskim pasażerów i towarów zgodnie z definicją dla transportu morskiego w załączniku I do rozporządzenia (WE) nr 725/2004 Parlamentu Europejskiego i Rady z dnia 31 marca 2004 r. w sprawie podniesienia ochrony statków i obiektów portowych (Dz. Urz. UE L 129 z 29.04.2004, str. 6, z późn. zm.), z wyłączeniem poszczególnych statków, na których prowadzą działalność ci armatorzy.	
					Armator, o którym mowa w art. 5 ust. 1 pkt 2 ustawy z dnia 21 grudnia 2000 r. o żegludze śródlądowej (Dz. U. z 2025 r. poz. 18.).	
		— organy zarządzające portami zgodnie z definicją w art. 3 pkt 1 dyrektywy Parlamentu Europejskiego i Rady 2005/65/WE, w tym ich obiekty portowe zgodnie z definicją w art. 2 pkt 11 rozporządzenia (WE) nr 725/2004; orędkoiki wykonujące prace i operujące sprzętem znajdującym się w tych portach			Podmiot zarządzający portem morskim, o którym mowa w art. 3 ust. 1 pkt 2 ustawy z dnia 4 września 2008 r. o ochronie żeglugi i portów morskich (Dz. U. z 2024 r. poz. 597).	
					Podmiot zarządzający obiektem portowym, o którym mowa w art. 2 pkt 11 rozporządzenia (WE) 725/2004 Parlamentu Europejskiego i Rady z dnia 31 marca 2004 r. w sprawie podniesienia ochrony statków i obiektów portowych.	
					Podmioty prowadzące na terenie portu działalność wspomagającą transport morski ujęte w klasie 52.22 klasyfikacji NACE Rev. 2, ujętej w załączniku I do rozporządzenia (WE) nr 1893/2006 Parlamentu Europejskiego i Rady z dnia 20 grudnia 2006 r. w sprawie statystycznej klasyfikacji działalności gospodarczej NACE Rev. 2 i zmieniającego rozporządzenie Rady (EWG) nr 3037/90 oraz niektóre rozporządzenia WE w sprawie określonych dziedzin statystycznych (Dz. Urz. UE L 393 z 30.12.2006, str. 1, z późn. zm.).	
		— operatorzy systemów ruchu statków (SRS) zgodnie z definicją w art. 3 lit. o)			VTS (Służba Kontroli Ruchu Statków) — aparat pomocniczy dyrektora urzędu	

		dyrektywy 2002/59/WE Parlamentu Europejskiego i Rady			morskiego powołany w celu monitorowania ruchu statków i przekazywania informacji, stanowiący część składową Narodowego Systemu SafeSeaNet, o którym mowa w art. 91 ustawy z dnia 18 sierpnia 2011 r. o bezpieczeństwie morskim (Dz. U. z 2025 r. poz. 883).	
	d) transport drogowy	— organy administracji drogowej zgodnie z definicją w art. 2 pkt 12 rozporządzenia delegowanego Komisji (UE) 2015/962 odpowiedzialne za zarządzanie ruchem drogowym, z wyłączeniem podmiotów publicznych, dla których zarządzanie ruchem lub obsługa inteligentnych systemów transportowych jest inną niż istotna częścią ich ogólnej działalności		Transport drogowy	Zarządca drogi, o którym mowa w art. 19 ust. 2 pkt 1 ustawy z dnia 21 marca 1985 r. o drogach publicznych (Dz. U. z 2025 r. poz. 889)	
		— operatorzy inteligentnych systemów transportowych zgodnie z definicją w art. 4 pkt 1 dyrektywy Parlamentu Europejskiego i Rady 2010/40/UE			Podmioty świadczące usługę ITS, o której mowa w art. 4 pkt 36 ustawy z dnia 21 marca 1985 r. o drogach publicznych.	
3. Bankowość		— instytucje kredytowe zgodnie z definicją w art. 4 pkt 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 575/2013	Bankowość i infrastruktura rynków finansowych		Instytucja kredytowa, o której mowa w art. 4 ust. 1 pkt 17 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe (Dz. U. z 2024 r. poz. 1646, z późn. zm.).	
					Bank krajowy, o którym mowa w art. 4 ust. 1 pkt 1 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe.	
					Oddział banku zagranicznego, o którym mowa w art. 4 ust. 1 pkt 20 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe.	
					Spółdzielcze kasy oszczędnościowo-kredytowe w rozumieniu ustawy z dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych (Dz. U. z 2025 r. poz. 379, 820, 1069, 1170 i 1191).	
4. Infrastruktura rynków finansowych		— operatorzy systemów obrotu zgodnie z definicją w art. 4 pkt 24 dyrektywy Parlamentu Europejskiego i Rady 2014/65/UE			Podmiot prowadzący rynek regulowany, o którym mowa w art. 14 ust. 1 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi (Dz. U. z 2024 r. poz. 722, z późn. zm.).	

		— kontrahenci centralni (CCP) zgodnie z definicją w art. 2 pkt 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 648/2012			Podmiot, o którym mowa w art. 3 pkt 49 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi.			
					Podmiot, o którym mowa w art. 48 ust. 7 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi.			
					Podmiot prowadzący ASO w rozumieniu art. 3 pkt 2 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi.			
					Podmiot prowadzący OTF w rozumieniu art. 3 pkt 10b ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi.			
					Podmiot, o którym mowa w art. 3 pkt 49 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi.			
	BRAK							
5. Opieka zdrowotna		— świadczeniodawcy zgodnie z definicją w art. 3 lit. g dyrektywy Parlamentu Europejskiego i Rady 2011/24/UE	Ochrona zdrowia	Udzielanie świadczeń zdrowotnych i zdrowie publiczne	Podmiot leczniczy, o którym mowa w art. 4 ust. 1 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej (Dz. U. z 2025 r. poz. 450, 620, 637 i 1211). Podmioty udzielające świadczeń opieki zdrowotnej będące podwykonawcą dla podmiotów kluczowych lub ważnych w sektorze ochrona zdrowia, w rozumieniu art. 133 ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (Dz. U. z 2025 r. poz. 1461). Świadczeniodawcy posiadający w swojej strukturze organizacyjnej Szpitalny Oddział Ratunkowy, Centrum Urazowe lub Centrum Urazowe dla Dzieci.	Kolejność nazw podmiotów zmieniona względem projektu dla wykazania zgodności z dyrektywą.		

		Brak w dyrektywie			Jednostka podległa ministrowi właściwemu do spraw zdrowia albo przez niego nadzorowana, właściwa w zakresie systemów informacyjnych ochrony zdrowia.	
		Brak w dyrektywie			Urzędy obsługujące organy Państwowej Inspekcji Sanitarnej.	
		Brak w dyrektywie			Krajowe Centrum Monitorowania Ratownictwa Medycznego, o którym mowa w art. 27a ustawy z dnia 8 września 2006 r. o Państwowym Ratownictwie Medycznym (Dz. U. z 2025 r. poz. 91 i 637).	
		Brak w dyrektywie			Jednostki organizacyjne publicznej służby krwi, o których mowa w art. 4 ust. 3 pkt 2 ustawy z dnia 22 sierpnia 1997 r. o publicznej służbie krwi (Dz. U. z 2024 r. poz. 1782).	
		— laboratoria referencyjne UE, o których mowa w art. 15 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2371			Laboratoria referencyjne UE, o których mowa w art. 15 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2371 z dnia 23 listopada 2022 r. w sprawie poważnych transgranicznych zagrożeń zdrowia oraz uchylenia decyzji nr 1082/2013/UE (Dz. Urz. UE L 314 z 06.12.2022, str. 1).	
		- podmioty prowadzące działalność badawczo-rozwojową w zakresie produktów leczniczych zdefiniowanych w art. 1 pkt 2 dyrektywy Parlamentu Europejskiego i Rady 2001/83/WE	Produkcja i dystrybucja substancji czynnych, produktów leczniczych i wyrobów medycznych	Podmioty prowadzące działalność badawczo-rozwojową w zakresie produktów leczniczych zdefiniowanych w art. 1 pkt 2 dyrektywy 2001/83/WE Parlamentu Europejskiego i Rady z dnia 6 listopada 2001 r. w sprawie wspólnotowego kodeksu odnoszącego się do produktów leczniczych stosowanych u ludzi (Dz. Urz. UE L 311 z 28.11.2001, str. 67, z późn. zm.).		
			— podmioty produkujące podstawowe substancje farmaceutyczne oraz leki i pozostałe wyroby farmaceutyczne, o których mowa w sekcji C dział 21 klasyfikacji NACE Rev. 2			Podmioty produkujące podstawowe substancje farmaceutyczne oraz leki i pozostałe wyroby farmaceutyczne, o których mowa w sekcji C dział 21 klasyfikacji NACE Rev. 2.
		— podmioty produkujące wyroby medyczne uznane za mające krytyczne znaczenie podczas danego stanu			Podmioty produkujące wyroby medyczne uznane za mające krytyczne znaczenie podczas danego stanu zagrożenia zdrowia	

		zagrożenia zdrowia publicznego („wykaz wyrobów medycznych o krytycznym znaczeniu w przypadku stanu zagrożenia zdrowia publicznego”) w rozumieniu art. 22 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/123			publicznego („wykaz wyrobów medycznych o krytycznym znaczeniu w przypadku stanu zagrożenia zdrowia publicznego”) w rozumieniu art. 22 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/123 z dnia 25 stycznia 2022 r. w sprawie wzmocnienia roli Europejskiej Agencji Leków w zakresie gotowości na wypadek sytuacji kryzysowej i zarządzania kryzysowego w odniesieniu do produktów leczniczych i wyrobów medycznych (Dz. Urz. UE L 20 z 31.01.2022, str. 1, z późn. zm.).	
		Brak w dyrektywie			Urząd Rejestracji Produktów Leczniczych, Wyrobów Medycznych i Produktów Biobójczych	
					Urzędy obsługujące organy Inspekcji Farmaceutycznej	
Artykuł 3 Podmioty kluczowe i ważne					Przedsiębiorca prowadzący działalność polegającą na prowadzeniu hurtowni farmaceutycznej w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne (Dz. U. z 2025 r. poz. 750, 905, 924 i 1416).	
1. Do celów niniejszej dyrektywy następujące podmioty uznaje się za podmioty kluczowe: g) jeżeli państwo członkowskie tak postanowi, podmioty, które to państwo członkowskie wskazało przed 16 stycznia 2023 r. jako operatorów usług kluczowych zgodnie z dyrektywą (UE) 2016/1148 lub prawem krajowym.					Przedsiębiorca lub podmiot prowadzący działalność gospodarczą w państwie członkowskim Unii Europejskiej lub państwie członkowskim Europejskiego Porozumienia o Wolnym Handlu (EFTA) - stronie umowy o Europejskim Obszarze Gospodarczym, który uzyskał pozwolenie na dopuszczenie do obrotu produktu leczniczego.	
					Importer produktu leczniczego lub substancji czynnej w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne.	
					Wytwórca produktu leczniczego lub substancji czynnej w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne.	

					Importer równoległy w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne.	
					Dystrybutor substancji czynnej w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne.	
					Przedsiębiorca prowadzący działalność w formie apteki ogólnodostępnej w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne	
6. Woda pitna		- dostawcy i dystrybutorzy „wody przeznaczonej do spożycia przez ludzi” zdefiniowanej w art. 2 pkt 1 lit. a) dyrektywy Parlamentu Europejskiego i Rady (UE) 2020/2184, z wyłączeniem dystrybutorów, dla których dystrybucja wody przeznaczonej do spożycia przez ludzi jest inną niż istotną częścią ich ogólnej działalności polegającej na dystrybucji innych produktów i towarów	Zaopatrzenie w wodę pitną i jej dystrybucja		Podmiot dostarczający wodę przeznaczoną do spożycia przez ludzi, w tym przedsiębiorstwo wodociągowo-kanalizacyjne o którym mowa w art. 2 pkt 4 ustawy z dnia 7 czerwca 2001 r. o zbiorowym zaopatrzeniu w wodę i zbiorowym odprowadzaniu ścieków (Dz. U. z 2024 r. poz. 757), z wyłączeniem podmiotów, dla których dostarczanie wody przeznaczonej do spożycia przez ludzi jest inną niż istotną częścią ich ogólnej działalności.	
7. Ścieki		- przedsiębiorstwa zbierające, odprowadzające lub oczyszczające ścieki komunalne, bytowe lub przemysłowe zgodnie z definicją w art. 2 pkt 1, 2 i 3 dyrektywy Rady 91/271/EWG, z wyłączeniem przedsiębiorstw, dla których zbieranie, odprowadzanie lub oczyszczanie ścieków komunalnych, bytowych lub przemysłowych jest inną niż istotną częścią ich ogólnej działalności	Zbiorowe odprowadzanie ścieków		Podmiot odprowadzający lub oczyszczający ścieki, w tym przedsiębiorstwo wodociągowo-kanalizacyjne, o którym mowa w art. 2 pkt 4 ustawy z dnia 7 czerwca 2001 r. o zbiorowym zaopatrzeniu w wodę i zbiorowym odprowadzaniu ścieków, z wyłączeniem podmiotów, dla których odprowadzanie lub oczyszczanie ścieków jest inną niż istotną częścią ich ogólnej działalności.	
8. Infrastruktura cyfrowa		— dostawcy punktu wymiany ruchu internetowego	Infrastruktura cyfrowa	Infrastruktura cyfrowa z wyłączeniem komunikacji elektronicznej	Dostawca punktu wymiany ruchu internetowego.	
		— dostawcy usług DNS, z wyłączeniem operatorów głównych serwerów nazw			Dostawca usług DNS, z wyłączeniem operatorów głównych serwerów nazw.	
		— rejestry nazw TLD			Rejestr nazw domen najwyższego poziomu (TLD).	
		— dostawcy usług chmurowych			Dostawca chmury obliczeniowej.	
		— dostawcy usług ośrodka przetwarzania danych			Dostawca usług centrum przetwarzania danych.	

		— dostawcy sieci dostarczania treści			Dostawca sieci dostarczania treści.	
		— dostawcy usług zaufania			Dostawca usług zaufania.	
					Podmiot świadczący usługę rejestracji nazw domen.	
		— dostawcy publicznych sieci łączności elektronicznej		Komunikacja elektroniczna	Przedsiębiorca komunikacji elektronicznej.	
		— dostawcy publicznie dostępnych usług łączności elektronicznej				
9. Zarządzanie usługami ICT (między przedsiębiorstwami)		- dostawcy usług zarządzanych	Zarządzanie usługami ICT		Dostawca usług zarządzanych.	
		- dostawcy usług zarządzanych w zakresie bezpieczeństwa			Dostawca usług zarządzanych w zakresie cyberbezpieczeństwa.	
10. Podmioty administracji publicznej		- podmioty administracji publicznej w ramach instytucji rządowych na szczeblu centralnym zdefiniowane przez państwo członkowskie zgodnie z prawem krajowym — podmioty administracji publicznej na szczeblu regionalnym zdefiniowane przez państwo członkowskie zgodnie z prawem krajowym	Podmioty publiczne	—	1) Podmioty z uwzględnieniem pkt 2-4: a) jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 1 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych oraz urzędy je obsługujące, b) jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 3, 5-6, 8, 9 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych, c) państwowe instytucje kultury, d) instytuty badawcze, e) Narodowy Bank Polski, f) Bank Gospodarstwa Krajowego, g) Urząd Dozoru Technicznego, h) Polska Agencja Żeglugi Powietrznej, i) Polskie Centrum Akredytacji, j) Urząd Komisji Nadzoru Finansowego, k) Polska Agencja Prasowa, l) Państwowe Gospodarstwo Wodne Wody Polskie, o którym mowa w ustawie	

					z dnia 20 lipca 2017 r. – Prawo wodne (Dz. U. z 2025 r. poz. 960). m) Polski Fundusz Rozwoju i inne instytucje rozwoju, o których mowa w art. 2 ust. 1 pkt 1 i 3–6 ustawy z dnia 4 lipca 2019 r. o systemie instytucji rozwoju. n) Narodowy Fundusz Ochrony Środowiska i Gospodarki Wodnej, o) wojewódzkie fundusze ochrony środowiska i gospodarki wodnej, p) Państwowy Fundusz Rehabilitacji Osób Niepełnosprawnych, q) Zakład Unieszkodliwiania Odpadów Promieniotwórczych z siedzibą w Otwocku-Świerku, r) państwowa osoba prawna, wobec której wydano decyzję, o której mowa w art. 7m s) spółka, o której mowa w art. 2 ust. 1 ustawy z dnia 29 kwietnia 2016 r. o szczególnych zasadach wykonywania niektórych zadań dotyczących informatyzacji w zakresie działów administracji rządowej budżet i finanse publiczne.	
					2) w odniesieniu do samorządu województwa: jednostki budżetowe oraz zakłady budżetowe z wyłączeniem: a) jednostek organizacyjnych, o których mowa w art. 2 ustawy z dnia 14 grudnia 2016 r. – Prawo oświatowe oraz ich zespołów, b) jednostek organizacyjnych wspierania rodziny i systemu pieczy zastępczej, o których mowa dnia 9 czerwca 2011 r. o wspieraniu rodziny i systemie pieczy zastępczej, c) jednostek organizacyjnych, o których mowa w art. 6 pkt 5 ustawy z dnia 12 marca 2004 r. o pomocy społecznej,	

					oprócz regionalnych ośrodków polityki społecznej, d) wojewódzkich urzędów pracy, e) parków krajobrazowych i ich zespołów, f) jednostek obsługujących, o których mowa 8d ustawy z dnia 5 czerwca 1998 r. o samorządzie województwa, w zakresie w jakim prowadzą wspólną obsługę jednostek, o których mowa w lit. a-□;	
					3) w odniesieniu do samorządu powiatu: starostwo powiatowe.	
					4) w odniesieniu do samorządu gminy: urząd gminy, jeżeli zatrudnia na dzień 1 stycznia danego roku w przeliczeniu na pełny wymiar czasu pracy na podstawie umowy o pracę co najmniej 50 osób.	
11. Przestrzeń kosmiczna		- operatorzy infrastruktury naziemnej należącej do, zarządzanej i obsługiwanej przez państwa członkowskie lub podmioty prywatne, które wspierają świadczenie usług kosmicznych, z wyjątkiem dostawców publicznych sieci łączności elektronicznej	Przestrzeń kosmiczna		Operator infrastruktury naziemnej, który wspiera świadczenie usług kosmicznych, z operatora, o którym mowa w art. 2 pkt 40 lit. b ustawy z dnia 12 lipca 2024 r. – Prawo komunikacji elektronicznej	
		Brak			Polska Agencja Kosmiczna	Polska Agencja Kosmiczna jest podmiotem publicznym na szczeblu centralnym. Przeniesiono ją do tego sektora ze względu na to, że jej działalność jest związana z przestrzenią kosmiczną.

SEKTORY WAŻNE

Dyrektywa NIS 2			Nowelizacja			Komentarz
Sektor	Podsektor	Sektor	Podsektor	Sektor	Podsektor	
1. Usługi pocztowe i kurierskie		operatorzy świadczący usługi pocztowe zgodnie z definicją w art. 2 pkt 1a dyrektywy 97/67/WE, w tym dostawcy usług kurierskich	Usługi pocztowe		Operator pocztowy, o którym mowa w art. 3 pkt 12 ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe (Dz. U. z 2025 r. poz. 366, 820 i 1456).	
Brak			Inwestycje energetyki jądrowej		Podmiot będący inwestorem obiektu energetyki jądrowej określonego w art. 2 pkt 2 ustawy z	

					dnia 29 czerwca 2011 r. o przygotowaniu i realizacji inwestycji w zakresie obiektów energetyki jądrowej oraz inwestycji towarzyszących, który uzyskał decyzję zasadniczą, o której mowa w art. 3a ust. 1 tej ustawy.	
2. Gospodarowanie odpadami		- przedsiębiorstwa zajmujące się gospodarowaniem odpadami zgodnie z definicją w art. 3 pkt 9 dyrektywy Parlamentu Europejskiego i Rady 2008/98/WE, z wyłączeniem przedsiębiorstw, dla których gospodarowanie odpadami nie stanowi głównej działalności gospodarczej	Gospodarowanie odpadami	Zbieranie odpadów	Przedsiębiorstwa świadczące usługi w rozumieniu ustawy z dnia 14 grudnia 2012 r. o odpadach (Dz. U. z 2023 r. poz. 1587, z późn. zm.), polegające na zbieraniu odpadów, zobowiązane do uzyskania wpisu w rejestrze, o którym mowa w art. 49 ust. 1 ustawy o odpadach, z wyłączeniem przedsiębiorstw, dla których usługi te nie stanowią podstawowej działalności gospodarczej określonej zgodnie z przepisami wydanymi na podstawie art. 40 ust. 2 ustawy z dnia 29 czerwca 1995 r. o statystyce publicznej (Dz. U. z 2024 r. poz. 1799).	
				Transport odpadów	Przedsiębiorstwa świadczące usługi w rozumieniu ustawy z dnia 14 grudnia 2012 r. o odpadach, polegające na transporcie odpadów, zobowiązane do uzyskania wpisu w rejestrze, o którym mowa w art. 49 ust. 1 ustawy o odpadach, z wyłączeniem przedsiębiorstw, dla których usługi te nie stanowią podstawowej działalności gospodarczej określonej zgodnie z przepisami wydanymi na podstawie art. 40 ust. 2 ustawy z dnia 29 czerwca 1995 r. o statystyce publicznej.	
				Przetwarzanie odpadów, w tym sortowanie, wraz z nadzorem nad wymienionymi działaniami, a także późniejsze postępowanie z miejscami unieszkodliwiania odpadów	Przedsiębiorstwa świadczące usługi w rozumieniu ustawy z dnia 14 grudnia 2012 r. o odpadach, polegające na przetwarzaniu odpadów w tym sortowaniu, wraz z nadzorem nad wymienionymi działaniami, a także podmioty	

					świadczące usługi z późniejszym postępowaniem z miejscami unieszkodliwiania odpadów, zobowiązane do uzyskania wpisu w rejestrze, o którym mowa w art. 49 ust. 1 ustawy z dnia 14 grudnia 2012 r. o odpadach, z wyłączeniem przedsiębiorstw, dla których usługi te nie stanowią podstawowej działalności gospodarczej określonej zgodnie z przepisami wydanymi na podstawie art. 40 ust. 2 ustawy z dnia 29 czerwca 1995 r. o statystyce publicznej.	
				Działania wykonywane w charakterze sprzedawcy odpadów lub pośrednika w obrocie odpadami	Przedsiębiorstwa świadczące usługi w rozumieniu ustawy z dnia 14 grudnia 2012 r. o odpadach, polegające na działaniach wykonywanych w charakterze sprzedawcy odpadów lub pośrednika w obrocie odpadami, zobowiązane do uzyskania wpisu w rejestrze, o którym mowa w art. 49 ust. 1 ustawy z dnia 14 grudnia 2012 r. o odpadach, z wyłączeniem przedsiębiorstw, dla których usługi te nie stanowią podstawowej działalności gospodarczej określonej zgodnie z przepisami wydanymi na podstawie art. 40 ust. 2 ustawy z dnia 29 czerwca 1995 r. o statystyce publicznej.	
3. Produkcja, wytwarzanie i dystrybucja chemikaliów		- przedsiębiorstwa zajmujące się produkcją substancji oraz wytwarzaniem i dystrybucją substancji lub mieszanin, o których mowa w art. 3 pkt 9 i 14 rozporządzenia (WE) nr 1907/2006 Parlamentu Europejskiego i Rady, a także przedsiębiorstwa zajmujące się wytwarzaniem z substancji lub mieszanin wyrobów zgodnie z definicją w art. 3 pkt 3 tego rozporządzenia	Produkcja, wytwarzanie i dystrybucja chemikaliów		Przedsiębiorstwo zajmujące się produkcją substancji oraz wytwarzaniem i dystrybucją substancji lub mieszanin, o których mowa w art. 3 pkt 9 i 14 rozporządzenia (WE) nr 1907/2006 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2006 r. w sprawie rejestracji, oceny, udzielania zezwoleń i stosowanych ograniczeń w zakresie chemikaliów (REACH) i utworzenia Europejskiej Agencji Chemikaliów, zmieniające dyrektywę 1999/45/WE oraz uchylające rozporządzenie Rady	

					(EWG) nr 793/93 i rozporządzenie Komisji (WE) nr 1488/94, jak również dyrektywę Rady 76/769/EWG i dyrektywy Komisji 91/155/EWG, 93/67/EWG, 93/105/WE i 2000/21/WE (Dz. Urz. UE L 396 z 30.12.2006, str.1, z późn. zm.). Przedsiębiorstwa zajmujące się wytwarzaniem z substancji lub mieszanin wyrobów o których mowa w art. 3 pkt 3 rozporządzenia (WE) nr 1907/2006 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2006 r. w sprawie rejestracji, oceny, udzielania zezwoleń i stosowanych ograniczeń w zakresie chemikaliów (REACH) i utworzenia Europejskiej Agencji Chemikaliów, zmieniające dyrektywę 1999/45/WE oraz uchylające rozporządzenie Rady (EWG) nr 793/93 i rozporządzenie Komisji (WE) nr 1488/94, jak również dyrektywę Rady 76/769/EWG i dyrektywy Komisji 91/155/EWG, 93/67/EWG, 93/105/WE i 2000/21/WE.	
4. Produkcja, przetwarzanie i dystrybucja żywności		- przedsiębiorstwa spożywcze zgodnie z definicją w art. 3 pkt 2 rozporządzenia (WE) nr 178/2002 Parlamentu Europejskiego i Rady, zajmujące się dystrybucją hurtową oraz przemysłowymi produkcją i przetwarzaniem	Produkcja, przetwarzanie i dystrybucja żywności		Przedsiębiorstwa spożywcze w rozumieniu art. 3 pkt 2 rozporządzenia (WE) nr 178/2002 Parlamentu Europejskiego i Rady z dnia 28 stycznia 2002 r. ustanawiające ogólne zasady i wymagania prawa żywnościowego, powołujące Europejski Urząd ds. Bezpieczeństwa Żywności oraz ustanawiające procedury w zakresie bezpieczeństwa żywności, zajmujące się dystrybucją hurtową oraz przemysłowymi produkcją i przetwarzaniem (Dz. Urz. UE L 31 z 01.02.2002, str. 1, z późn. zm.).	
5. Produkcja	a) produkcja wyrobów medycznych i wyrobów	- podmioty produkujące wyroby medyczne zdefiniowane w art. 2 ust. 1 rozporządzenia Parlamentu	Produkcja	Produkcja wyrobów medycznych i wyrobów medycznych do diagnostyki in vitro	Podmioty produkujące wyroby medyczne w rozumieniu art. 2 ust. 1 rozporządzenia Parlamentu	

	medycznych do diagnostyki in vitro	Europejskiego i Rady (UE) 2017/745 oraz podmioty produkujące wyroby medyczne do diagnostyki in vitro zdefiniowane w art. 2 ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2017/746, z wyjątkiem podmiotów produkujących wyroby medyczne wymienione w załączniku I pkt 5 tiret piąte niniejszej dyrektywy			Europejskiego i Rady (UE) 2017/745 z dnia 5 kwietnia 2017 r. w sprawie wyrobów medycznych, zmiany dyrektywy 2001/83/WE, rozporządzenia (WE) nr 178/2002 i rozporządzenia (WE) nr 1223/2009 oraz uchylecia dyrektyw Rady 90/385/EWG i 93/42/EWG (Dz. Urz. UE L 117 z 05.05.2017, str. 1, z późn. zm.). Podmioty produkujące wyroby medyczne do diagnostyki in vitro w rozumieniu art. 2 ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2017/746 z dnia 5 kwietnia 2017 r. w sprawie wyrobów medycznych do diagnostyki in vitro oraz uchylecia dyrektywy 98/79/WE i decyzji Komisji 2010/227/UE (Dz. Urz. UE L 117 z 05.05.2017, str. 176, z późn. zm.), z wyjątkiem podmiotów produkujących wyroby medyczne uznane za mające krytyczne znaczenie podczas danego stanu zagrożenia zdrowia publicznego.	
	b) produkcja komputerów, wyrobów elektronicznych i optycznych	- przedsiębiorstwa prowadzące którykolwiek z rodzajów działalności gospodarczej, o których mowa w sekcji C dział 26 klasyfikacji NACE Rev. 2		Produkcja komputerów, wyrobów elektronicznych i optycznych	Przedsiębiorca prowadzący którykolwiek z rodzajów działalności gospodarczej, o których mowa w sekcji C dział 26 klasyfikacji NACE Rev. 2, ujętej w załączniku I do rozporządzenia (WE) nr 1893/2006 Parlamentu Europejskiego i Rady z dnia 20 grudnia 2006 r. w sprawie statystycznej klasyfikacji działalności gospodarczej NACE Rev. 2 i zmieniającego rozporządzenie Rady (EWG) nr 3037/90 oraz niektóre rozporządzenia WE w sprawie określonych dziedzin statystycznych (Dz. Urz. UE L 393 z 30.12.2006, str. 1, z późn. zm.).	

	c) produkcja urządzeń elektrycznych	- przedsiębiorstwa prowadzące którykolwiek z rodzajów działalności gospodarczej, o których mowa w sekcji C dział 27 klasyfikacji NACE Rev. 2		Produkcja urządzeń elektrycznych	Przedsiębiorca prowadzący którykolwiek z rodzajów działalności gospodarczej, o których mowa w sekcji C dział 27 klasyfikacji NACE Rev. 2.	
	d) Produkcja maszyn i urządzeń, gdzie indziej niesklasyfikowana	- przedsiębiorstwa prowadzące którykolwiek z rodzajów działalności gospodarczej, o których mowa w sekcji C dział 28 klasyfikacji NACE Rev. 2		Produkcja maszyn i urządzeń, gdzie indziej niesklasyfikowana	Przedsiębiorca prowadzący którykolwiek z rodzajów działalności gospodarczej, o których mowa w sekcji C dział 28 klasyfikacji NACE Rev. 2.	
	e) produkcja pojazdów samochodowych, przyczep i naczep	- przedsiębiorstwa prowadzące którykolwiek z rodzajów działalności gospodarczej, o których mowa w sekcji C dział 29 klasyfikacji NACE Rev. 2		Produkcja pojazdów samochodowych, przyczep i naczep	Przedsiębiorca prowadzący którykolwiek z rodzajów działalności gospodarczej, o których mowa w sekcji C dział 29 klasyfikacji NACE Rev. 2.	
	f) produkcja pozostałego sprzętu transportowego	- przedsiębiorstwa prowadzące którykolwiek z rodzajów działalności gospodarczej, o których mowa w sekcji C dział 30 klasyfikacji NACE Rev. 2		Produkcja pozostałego sprzętu transportowego	Przedsiębiorca prowadzący którykolwiek z rodzajów działalności gospodarczej, o których mowa w sekcji C dział 30 klasyfikacji NACE Rev. 2.	
6. Dostawcy usług cyfrowych		— dostawcy internetowych platform handlowych	Dostawcy usług cyfrowych		Dostawca internetowej platformy handlowej.	
		— dostawcy wyszukiwarek internetowych			Dostawca wyszukiwarki internetowej.	
		— dostawcy platform usług sieci społecznościowych			Dostawca platformy sieci usług społecznościowych.	
7. Badania naukowe		organizacje badawcze	Badania naukowe		Organizacja badawcza. Podmioty, o których mowa w art. 7 ust. 1 pkt 1–4, 6-7 ustawy z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce.	
BRAK			Podmioty publiczne		Samorządowe jednostki budżetowe; samorządowe zakłady budżetowe; samorządowe instytucje kultury; spółki prawa handlowego wykonujące zadania o charakterze użyteczności publicznej w rozumieniu art. 1 ust. 2 ustawy z dnia 20 grudnia 1996 r. o gospodarce komunalnej (Dz. U. z 2021 r. poz. 679)	

JEDN. RED.	TREŚĆ PRZEPISU / PRZEPISÓW PROJEKTU	UZASADNIENIE WPROWADZENIA PRZEPISU
Art. 1 pkt 3	3) w art. 1: a) w ust. 1 w pkt 3 kropkę zastępuje się średnikiem i dodaje pkt 4 w brzmieniu: „4) zakres Krajowego planu reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę.”, b) w ust. 2 uchyla się pkt 1 i 2;	Dostosowanie przepisu ogólnego zawierającego zakres podmiotowy i przedmiotowy ustawy do zmian wprowadzonych w projektowanej ustawie.
Art. 1 pkt 5	5) po art. 2 dodaje się art. 2a w brzmieniu: „Art. 2a. W przypadku podmiotu publicznego pod pojęciem usługi rozumie się także zadanie publiczne realizowane przez ten podmiot.”;	Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniającą rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającą dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz. Urz. UE L 333 z 27.12.2022, str. 80), zwanej dalej „dyrektywą NIS2”, posługuje się pojęciem usług w szerokim znaczeniu – odnosi się ona także do podmiotów publicznych. W polskim systemie prawnym podmioty publiczne realizują zadania publiczne. Aby uniknąć wątpliwości w przepisach ogólnych wskazuje się wprost, że w przypadku podmiotu publicznego pod pojęciem usługi rozumie się także zadanie publiczne realizowane przez ten podmiot. Oczywiście zdarza się, że podmiot publiczny, np. instytucja gospodarki budżetowej, świadczy komercyjne usługi, które nie są zadaniami publicznymi, jednakże dla celów niniejszej ustawy to uogólnienie jest konieczne, w przeciwnym razie konieczne byłoby utrzymanie dotychczasowego pojęcia „incydentu w podmiocie publicznym” czy też wprowadzenia odrębnych progów dla incydentu związanego z zadaniami publicznymi.
Art. 1 pkt 6	6) w art. 3 wyrazy „kluczowych i usług cyfrowych” zastępuje się wyrazami „przez podmioty kluczowe lub podmioty ważne”;	W przepisie art. 3 zawierającym cel krajowego systemu cyberbezpieczeństwa dostosowano terminologię do terminologii wynikającej z dyrektywy NIS 2.
Art. 1 pkt 7	7) po art. 3 dodaje się art. 3a w brzmieniu: „Art. 3a. W ramach obsługi incydentów podmiot krajowego systemu cyberbezpieczeństwa może w szczególności podejmować działania	Projektowany przepis ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077 i 1222 oraz z 2025 r. poz. 1017 i 1069), zwanej

	w celu wykrywania źródła lub dokonywania analizy aktywności, w tym ruchu sieciowego, powodujących wystąpienie incydentu zakłócającego świadczenie usług przez ten podmiot.”;	dalej „ustawą o KSC” przesądza, że w ramach obsługi incydentu dotknięty nim podmiot może wykrywać źródło ataku oraz czasowo ograniczyć ruch sieciowy z adresów IP lub adresów URL. Uprawnienia te są niezbędne dla zapewnienia skutecznej reakcji na incydent, a w praktyce sprawiają one problemy praktyczne. Wykrycie źródła ataku często jest niezbędne do jego powstrzymania i przywrócenia normalnego funkcjonowania systemów. Równocześnie te działania mogą prowadzić do ewentualnego naruszenia uprawnień innych podmiotów. Do tej pory istniały wątpliwości na ile takie działania mogą być podejmowane. W związku z tym konieczne jest wprowadzenie wyraźnej podstawy prawnej do takich działań.
Art. 1 pkt 8	8) w art. 4: a) pkt 1 i 2 otrzymują brzmienie: „1) podmioty kluczowe; 2) podmioty ważne;”, b) pkt 6 otrzymuje brzmienie: „6) CSIRT sektorowe;”, c) uchyla się pkt 7–16, d) po pkt 17 dodaje się pkt 17a w brzmieniu: „17a) Połączone Centrum Operacyjne Cyberbezpieczeństwa, zwane dalej „PCOC”;	Zmienia się przepis wskazujący podmioty krajowego systemu cyberbezpieczeństwa w ten sposób, aby dostosować go do nowej terminologii wynikającej z dyrektywy NIS2. Przepis nie nakłada dodatkowych obowiązków na przedsiębiorców ponad to, co jest wymagane prawem unijnym.
Art. 1 pkt 9	9) w tytule rozdziału 2 wyrazy „operatorów usług kluczowych” zastępuje się wyrazami „podmiotów kluczowych lub podmiotów ważnych”;	Tytuł rozdziału dostosowuje się do nowej terminologii wynikającej z dyrektywy NIS2. Przepis nie nakłada dodatkowych obowiązków na przedsiębiorców ponad to, co jest wymagane prawem unijnym.
Art. 1 pkt 12	12) uchyla się art. 6;	Uchyla się podstawę prawną do wydania przez Radę Ministrów rozporządzenia w sprawie wykazu usług kluczowych. Dyrektywa NIS 2 nakazuje podmiotom kluczowym i podmiotom ważnym wdrożyć środki zarządzania ryzykiem dotyczące usług świadczonych przez te podmioty, a nie jednej konkretnej usługi.

		Usługi kluczowe występują w przypadku dyrektywy CER – ich wykaz został ustalony w rozporządzeniu delegowanym Komisji (UE) 2023/2450 z dnia 25 lipca 2023 r. uzupełniającym dyrektywę Parlamentu Europejskiego i Rady (UE) 2022/2557 przez ustanowienie wykazu usług kluczowych (Dz. Urz. UE L 2023/2450 z 30.10.2023). Tym bardziej prawodawca krajowy nie może precyzować usług kluczowych w rozporządzeniu. Przepis nie nakłada dodatkowych obowiązków na przedsiębiorców ponad to, co jest wymagane prawem unijnym.
Art. 1 pkt 17 (w zakresie dodawanego art. 8a)	„Art. 8a. Rada Ministrów może określić, w drodze rozporządzenia, odrębnie dla danego rodzaju działalności wykonywanej przez podmioty kluczowe lub podmioty ważne, szczegółowe wymagania dla systemu zarządzania bezpieczeństwem informacji, o którym mowa w art. 8 ust. 1, biorąc pod uwagę rekomendacje międzynarodowe o charakterze specjalistycznym, w tym rekomendacje Agencji Unii Europejskiej do spraw Cyberbezpieczeństwa, zwanej dalej „ENISA”, wielkość podmiotu, skalę działalności wykonywanej przez te podmioty oraz potrzebę podejmowania przez te podmioty działań zapewniających cyberbezpieczeństwo.”.	Zgodnie z dodawanym przepisem Rada Ministrów będzie mogła ustalać, w drodze rozporządzenia, odrębnie dla danego rodzaju działalności wykonywanej przez podmioty kluczowe lub podmioty ważne, szczegółowe wymagania dla systemu zarządzania bezpieczeństwem informacji. Przepis ten pozwoli uwzględnić specyfikę poszczególnych sektorów i przedstawić rozwiązania dostosowane do tej specyfiki. Będzie to fakultatywne upoważnienie ustawowe. Minimalne wymagania dla systemu zarządzania bezpieczeństwem informacji będą musiały być zgodne z nowym brzmieniem art. 8 ust. 1a, a przez to również z art. 21 dyrektywy NIS 2.
Art. 1 pkt 17 (w zakresie dodawanego art. 8g)	„Art. 8g. Podmiot kluczowy będący dostawcą usług zarządzanych w zakresie cyberbezpieczeństwa świadczącym usługę obsługi incydentów udostępnia na swojej stronie internetowej co najmniej następujące informacje na temat swojej działalności:	Nawiązując do powszechnej międzynarodowej praktyki (publikowanie informacji na podstawie wzoru zawartego w pkt. 3.3 dokumentu RFC 2350 ¹), wprowadza się dla dostawców usług zarządzanych z zakresu

¹<https://datatracker.ietf.org/doc/html/rfc2350>

Jako przykłady praktyki można wskazać:

<https://www.knf.gov.pl/knf/pl/komponenty/img/RFC2350.pdf>

<https://www.csirt.gov.sk/csirt-sk-description-document-according-to-rfc-2350.html>

<https://www.ncsc.gov.ie/pdfs/RFC2350%20NCSC-IE.txt>.

	1) nazwę (firmę); 2) zakres działania, w tym: a) oferowany rodzaj wsparcia, b) zasady współpracy i wymiany informacji, c) politykę komunikacji; 3) oferowane usługi oraz politykę obsługi incydentów i koordynacji incydentów; 4) dane kontaktowe, w tym: a) adres ze wskazaniem strefy czasowej, b) numer telefonu, adres poczty elektronicznej oraz wskazanie innych dostępnych środków komunikacji elektronicznej z dostawcą, c) dane o wykorzystywanych kluczach publicznych i sposobach szyfrowania komunikacji z dostawcą, d) sposoby kontaktu z dostawcą, w tym sposób zgłaszania incydentów.”.	cyberbezpieczeństwa obowiązek udostępniania na stronie internetowej podstawowych informacji o swojej działalności. W celu zrealizowania tego obowiązku wystarczy zamieścić krótki plik tekstowy na stronie internetowej dostawcy usług zarządzanych z zakresu cyberbezpieczeństwa. Przepis ten nie wprowadza ograniczeń co do świadczenia usług przez dostawców usług zarządzanych w zakresie cyberbezpieczeństwa.
Art. 1 pkt 19 (w zakresie zmienianego art. 11 ust. 4)	„4. Rada Ministrów określi, w drodze rozporządzenia, progi uznania incydentu za poważny według rodzaju zdarzenia w poszczególnych sektorach i podsektorach określonych w załączniku nr 1 i 2 do ustawy, z wyłączeniem progów uznania incydentu za poważny, dla podmiotów, dla których progi te określiła Komisja Europejska w akcie wykonawczym wydanym na podstawie art. 23 ust. 11 dyrektywy 2022/2555, wskazując w zależności od rodzaju zdarzenia czy odnosi się ono do: 1) liczby użytkowników, których dotyczy zakłócenie świadczenia usługi, 2) czasu oddziaływania incydentu na świadczoną usługę, 3) zasięgu geograficznego obszaru, którego dotyczy incydent, 4) innych czynników charakterystycznych dla danego sektora lub podsektora, jeżeli występują – kierując się potrzebą zapewnienia ochrony przed zagrożeniem życia lub zdrowia ludzi, znacznymi stratami majątkowymi oraz obniżeniem jakości świadczonej usługi.	Rozporządzenie ma na celu określenie progów incydentu poważnego, co ułatwi przedsiębiorcom spełnienie wymogów zgłaszania tych incydentów.
Art. 1 pkt 23 lit. c–h	„c) w ust. 2 w pkt 3 wyrazy „sektorowy zespół cyberbezpieczeństwa” zastępuje się wyrazami „CSIRT sektorowy”, d) po ust. 2 dodaje się ust. 2a w brzmieniu:	Dostosowuje się przepisy do zmian terminologicznych - pojęcie „sektorowego zespołu cyberbezpieczeństwa” zastępuje się pojęciem „CSIRT sektorowego”.

	„2a. Audyt nie może być przeprowadzony przez osobę realizującą w podmiocie audytowanym zadania, o których mowa w art. 8 oraz art. 9–13, lub która realizowała te zadania w podmiocie audytowanym w przeciągu roku przed rozpoczęciem audytu.”, e) w ust. 3 uchyla się pkt 3, f) w ust. 5 wyrazy „operatorowi usługi kluczowej” zastępuje się wyrazami „podmiotowi kluczowemu lub podmiotowi ważnemu”, g) uchyla się ust. 6, h) w ust. 7: – wprowadzenie do wyliczenia otrzymuje brzmienie: „Podmiot kluczowy lub podmiot ważny przekazuje kopię raportu z przeprowadzonego audytu na wniosek:”, – uchyla się pkt 1, – w pkt 2 wyrazy „operator usługi kluczowej” zastępuje się wyrazami „podmiot kluczowy lub podmiot ważny”;	Przepis wprowadza wymóg dotyczący audytorów przeprowadzających audyt bezpieczeństwa.
Art. 1 pkt 24	24) art. 16 otrzymuje brzmienie: „Art. 16. Podmiot: 1) kluczowy lub ważny realizuje obowiązki, o których mowa w niniejszym rozdziale, w terminie 6 miesięcy, 2) kluczowy zapewnia przeprowadzenie audytu, o którym mowa w art. 15 ust. 1, po raz pierwszy w terminie 24 miesięcy – od dnia spełnienia przesłanek uznania za podmiot kluczowy lub podmiot ważny.”;	Należało przesądzić, od kiedy podmioty kluczowe i podmioty ważne będą miały obowiązek wdrożenia obowiązków wynikających z ustawy. Obecnie momentem, od którego liczą się terminy na wdrożenie obowiązków przez operatorów usług kluczowych, jest doręczenie decyzji o uznaniu za operatora usługi kluczowej. W projektowanych przepisach wskazano, że podmiot kluczowy i podmiot ważny realizuje swoje obowiązki w terminie 6 miesięcy od dnia spełnienia przesłanek uznania za podmiot kluczowy lub podmiot ważny. Audyt systemu będzie realizowany po raz pierwszy w terminie 24 miesięcy od dnia spełnienia przesłanek uznania za podmiot kluczowy lub podmiot ważny.
Art. 1 pkt 26 (w zakresie rozdziału 3b)	„Rozdział 3b. Wspólne wykonywanie obowiązków z zakresu cyberbezpieczeństwa przez podmioty publiczne Art. 16d. Podmiot publiczny realizuje obowiązki, o których mowa w art. 7b ust. 4, art. 7c, art. 7f ust. 3, art. 8, art. 8c-8f, art. 9–12b i art. 15, jeżeli wykorzystuje system informacyjny w celu realizacji zadania publicznego.	Dodanie rozdziału 3b wynika z uwzględnienia w ramach krajowego systemu cyberbezpieczeństwa podmiotów publicznych, co zgodnie z dyrektywą NIS 2 pozostawiono do decyzji poszczególnym państwom członkowskim. W związku z tym, że w Polsce te podmioty objęte są obowiązkami w zakresie obsługi incydentów od 2018 r., wolą Ministra Cyfryzacji jest utrzymanie ich w obrębie

	Art. 16e. 1. Minister kierujący działem administracji rządowej może wyznaczyć, obsługujący go urząd, jednostkę jemu podległą albo przez niego nadzorowaną jako jednostkę odpowiedzialną za realizację obowiązków, o których mowa w art. 7b ust. 4, art. 7c, art. 7f ust. 3, art. 8, art. 8c-8f, art. 9–12b lub art. 15, w pozostałych jednostkach organizacyjnych lub organach podległych oraz nadzorowanych przez tego ministra, a także w obsługującym go urzędzie. 2. Centralny organ administracji rządowej, niebędący ministrem, może wyznaczyć obsługujący go urząd, jednostkę jemu podległą albo przez niego nadzorowaną jako jednostkę odpowiedzialną za realizację obowiązków, o których mowa w art. 7b ust. 4, art. 7c, art. 7f ust. 3, art. 8, art. 8c-8f, art. 9–12b lub art. 15, w pozostałych jednostkach organizacyjnych lub nadzorowanych przez tego ministra, a także w obsługującym go urzędzie. 3. Wojewoda może wyznaczyć obsługujący go urząd, jednostkę jemu podległą albo przez niego nadzorowaną jako jednostkę odpowiedzialną za realizację obowiązków, o których mowa w art. 7b ust. 4, art. 7c, art. 7f ust. 3, art. 8, art. 8c-8f, art. 9–12b lub art. 15, w pozostałych jednostkach organizacyjnych podległych oraz nadzorowanych przez wojewodę, a także w obsługującym go urzędzie. 4. Prokurator Generalny może spośród powszechnych jednostek organizacyjnych prokuratury wyznaczyć jednostkę odpowiedzialną za realizację obowiązków, o których mowa w art. 7b ust. 4, art. 7c, art. 7f ust. 3, art. 8, art. 8c–8f, art. 9–12b lub art. 15, w pozostałych jednostkach prokuratury. 5. Jednostka samorządu terytorialnego może zapewnić wspólną obsługę realizacji obowiązków, o których mowa w art. 7b ust. 4, art. 7c, art. 7f ust. 3, art. 8, art. 8c–8f, art. 8h, art. 9–12b lub art. 15. Do wyznaczenia jednostki obsługującej i obsługiwanej stosuje się odpowiednio art. 10a–10d ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2024 r. poz. 1465, 1572, 1907 i 1940), art. 6a–6d ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym (Dz. U. z 2024 r. poz. 107 i 1907) oraz art. 8c–8f ustawy z dnia 5 czerwca 1998 r. o samorządzie województwa (Dz. U. z 2025 r. poz. 581).	krajowego systemu cyberbezpieczeństwa. Przedmiotowe przepisy wprowadzają rozwiązania dostosowane do ich specyfiki. W wielu przypadkach organy administracji wykorzystują w swojej pracy systemy administrowane przez ich jednostkę nadrzędną, w takim wypadku optymalnym rozwiązaniem jest, by tylko jedna jednostka odpowiadała za bezpieczeństwo takiego systemu.

	6. Jednostki samorządu terytorialnego mogą zawrzeć porozumienie w sprawie powierzenia jednej z nich realizacji obowiązków, o których mowa w art. 7b ust. 4, art. 7c, art. 7f ust. 3, art. 8, art. 8c–8f, art. 8h, art. 9–12b lub art. 15. 7. W porozumieniu, o którym mowa w ust. 6, wskazuje się jednostki organizacyjne, samorządowe osoby prawne lub spółki prawa handlowego, o których mowa w art. 9 ust. 1 ustawy z dnia 20 grudnia 1996 r. o gospodarce komunalnej jednostki samorządu terytorialnego powierzającej realizacji obowiązków, o których mowa w art. 7b ust. 4, art. 7c, art. 7f ust. 3, art. 8, art. 8c–8f, art. 8h, art. 9–12b lub art. 15, objęte porozumieniem. 8. Jednostka samorządu terytorialnego, której powierzono realizację obowiązków, o których mowa w art. 7b ust. 4, art. 7c, art. 7f ust. 3, art. 8, art. 8c–8f, art. 8h, art. 9–12b lub art. 15, wyznacza jednostkę organizacyjną, samorządową osobę prawną lub spółkę prawa handlowego, o której mowa w art. 9 ust. 1 ustawy z dnia 20 grudnia 1996 r. o gospodarce komunalnej, do realizacji tych obowiązków. 9. Do porozumień, o których mowa w ust. 6, stosuje się odpowiednio art. 74 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym. Art. 16f. Podmioty publiczne, dla których jednostka wyznaczona realizuje obowiązki z zakresu cyberbezpieczeństwa, współpracują z tą jednostką w szczególności przez: 1) przekazywanie informacji o incydentach; 2) wykonywanie decyzji kierownika tej jednostki w zakresie systemu zarządzania bezpieczeństwem informacji; 3) publikowanie na swojej stronie internetowej adresu strony internetowej jednostki wyznaczonej zawierającej informacje o cyberbezpieczeństwie zgodnie z art. 9; 4) uczestnictwo kierownika jednostki w szkoleniach z zakresu cyberbezpieczeństwa, jeżeli są prowadzone przez jednostkę wyznaczoną. Art. 16g. W celu prawidłowego wykonania obowiązków, o których mowa w art. 11 i art. 12, kierownik jednostki wyznaczonej, o której mowa w art. 16e, może wskazać podmiotom publicznym terminy na przekazanie informacji o incydentach.	

	Art. 16h. Jednostka wyznaczona, o której mowa w art. 16e: 1) zgłasza w imieniu podmiotu publicznego wczesne ostrzeżenie, zgłoszenie incydentu poważnego, sprawozdanie okresowe i sprawozdanie końcowe, o których mowa w art. 11 ust. 1 pkt 4-4c, do CSIRT sektorowego; 2) wskazuje osobę kontaktową do podmiotów publicznych, którym realizuje zadania z zakresu cyberbezpieczeństwa; 3) korzysta z systemu teleinformatycznego, o którym mowa w art. 46 ust. 1, w celu realizacji obowiązków, o których mowa w rozdziale 3.”;	
Art. 1 pkt 27	27) uchyla się rozdział 4 i 5;	Ze względu na zmiany w strukturze krajowego systemu cyberbezpieczeństwa uchyla się rozdziały 4 i 5 ustawy o KSC dotyczące dostawców usług cyfrowych oraz podmiotów publicznych. Te podmioty, zgodnie z dyrektywą NIS 2, staną się podmiotami kluczowymi i podmiotami ważnymi, w związku z czym nie jest zasadne utrzymywanie dla nich osobnych regulacji.
Art. 1 pkt 29 (w zakresie dodawanego art. 26c)	„Art. 26c. 1. CSIRT NASK, w celu minimalizacji ryzyka powstania szkód materialnych i niematerialnych związanych z nieuprawnionym upublicznieniem danych osobowych w sieci internet, tworzy i udostępnia usługę online umożliwiającą sprawdzenie przez osobę fizyczną, czy jej dane osobowe nie zostały ujawnione w sieci internet w sposób nieuprawniony, na skutek incydentu lub cyberzagrożenia. 2. Dla realizacji usługi online, o której mowa w ust. 1, CSIRT NASK może gromadzić i przetwarzać następujące dane osobowe: 1) imię i nazwisko; 2) datę urodzenia; 3) adres zamieszkania; 4) płeć; 5) imię i nazwisko nadane podczas urodzenia; 6) miejsce urodzenia; 7) identyfikator użytkownika w Węźle Krajowym nadawany tymczasowo podczas uwierzytelniania; 8) login, który uległ nieuprawnionemu upublicznieniu; 9) adres poczty elektronicznej;	Przepis umożliwia CSIRT NASK tworzenie i udostępnianie usługi online, która umożliwia osobie fizycznej sprawdzenie, czy jej dane osobowe zostały ujawnione w sieci internet w sposób nieuprawniony. W związku z coraz częstszymi wyciekami danych i ich potencjalnie szerokimi skutkami w postaci szkód materialnych i niematerialnych niezwykle istotne jest, aby udostępnić publicznie usługę, która pozwoli osobom fizycznym, których dane zostały udostępnione, na podjęcie odpowiednich kroków zapobiegających szkodzie lub zmierzających do minimalizacji negatywnych skutków.

	10) numer telefonu; 11) numer PESEL.”;	
Art. 1 pkt 34	34) w art. 33: a) w ust. 1 wyrazy „urządzenia informatycznego lub oprogramowania” zastępuje się wyrazami „produktu ICT lub usługi ICT”, b) po ust. 1 dodaje się ust. 1a–1e w brzmieniu: „1a. Badanie, o którym mowa w ust. 1, przeprowadza się także na pisemny wniosek Pełnomocnika lub przewodniczącego Kolegium, skierowany do organu prowadzącego lub nadzorującego właściwy CSIRT. 1b. Badanie, o którym mowa w ust. 1, przeprowadza się w środowisku testowym i nie może ono wpłynąć na ciągłość świadczenia usług przez podmioty kluczowe lub podmioty ważne. 1c. CSIRT MON, CSIRT NASK i CSIRT GOV prowadząc badanie, o którym mowa w ust. 1, są uprawnieni do stosowania technik mających na celu: 1) obserwację i analizę pracy produktu ICT lub usługi ICT; 2) uzyskanie dostępu do przetwarzanych danych; 3) odtworzenie postaci źródłowej produktu ICT lub usługi ICT; 4) zwielokrotnienie (powielenie) kodu programowego oraz tłumaczenie (translacja) jego formy; 5) odtworzenie algorytmu przetwarzania danych; 6) identyfikację realizowanych funkcji; 7) usunięcie lub przełamanie zabezpieczeń przed badaniem; 8) identyfikację podatności lub identyfikację nieudokumentowanych funkcji realizowanych przez produkt ICT lub usługę ICT. 1d. CSIRT MON, CSIRT NASK i CSIRT GOV w czasie prowadzenia badania, o którym mowa w ust. 1, nie są związane postanowieniami umów, w szczególności umów licencyjnych, badanych produktów ICT lub usług ICT, które ograniczyłyby możliwość przeprowadzenia tego badania. 1e. Badanie, o którym mowa w ust. 1: 1) nie narusza autorskich praw osobistych oraz majątkowych, oraz 2) nie wymaga zgody licencjodawcy lub dysponenta produktu ICT lub usługi ICT.	Przepis precyzuje przepisy o badaniu urządzenia informatycznego lub oprogramowania.

	1f. Postanowienia umów sprzeczne z ust. 1–1d są nieważne.”, c) ust. 2 otrzymuje brzmienie: „2. CSIRT MON, CSIRT NASK albo CSIRT GOV, podejmując badanie produktu ICT, usługi ICT lub procesu ICT, informuje pozostałe CSIRT poziomu krajowego o fakcie podjęcia badań oraz o produkcie ICT lub usłudze ICT, których badanie dotyczy.”, d) w ust. 4 i 6–8 wyrazy „urządzeń informatycznych lub oprogramowania” zastępuje się wyrazami „produktów ICT lub usług ICT”, e) w ust. 4a wyrazy „zagrożeniu cyberbezpieczeństwa” zastępuje się wyrazem „cyberzagrożeniu”, f) po ust. 4b dodaje się ust. 4c w brzmieniu: „4c. Rekomendacje, o których mowa w ust. 4, a także informację o ich zmianie lub odwołaniu, Pełnomocnik publikuje na swojej stronie podmiotowej Biuletynu Informacji Publicznej.”, g) ust. 5 otrzymuje brzmienie: „5. Podmiot krajowego systemu cyberbezpieczeństwa może wnieść do Pełnomocnika zastrzeżenia do rekomendacji dotyczących stosowania produktów ICT lub usług ICT, z uwagi na ich negatywny wpływ na świadczoną usługę lub realizowane zadanie publiczne, nie później niż w terminie 14 dni od dnia udostępnienia rekomendacji na stronie podmiotowej Biuletynu Informacji Publicznej Pełnomocnika.”, h) dodaje się ust. 9 w brzmieniu: „9. CSIRT MON, CSIRT NASK lub CSIRT GOV przeprowadzający badanie może zwrócić się do producenta badanego produktu ICT lub dostawcy badanej usługi ICT o przekazanie dokumentacji. Przepis art. 53c stosuje się odpowiednio. O zwróceniu się do producenta, jak również o nieprzekazaniu przez producenta dokumentacji w terminie, CSIRT przeprowadzający badanie informuje ministra właściwego do spraw informatyzacji.”	
Art. 1 pkt 36 pkt a i pkt c–e	a) ust. 1 otrzymuje brzmienie: „1. CSIRT MON, CSIRT NASK i CSIRT GOV przekazują sobie wzajemnie informacje o incydencie krytycznym lub incydencie w cyberbezpieczeństwie na dużą skalę oraz informują o nim Rządowe	Przepis dostosowuje brzmienie przepisu o Zespole do spraw incydentów krytycznych do innych zmian w ustawie o KSC.

	Centrum Bezpieczeństwa, właściwy CSIRT sektorowy oraz ministra właściwego do spraw zagranicznych.”, c) po ust. 2 dodaje się ust 2a w brzmieniu: „2a. Informacja, o której mowa w ust. 1, może zawierać dane osobowe tylko wtedy, gdy jest to niezbędne dla ochrony podmiotów krajowego systemu cyberbezpieczeństwa przed incydentami.”, d) w ust. 4 i 5 wyrazy „zagrożeniach cyberbezpieczeństwa” zastępuje się wyrazem „cyberzagrożeniach”, e) w ust. 5 wyraz „cyberbezpieczeństwa” zastępuje się wyrazem „bezpieczeństwa”;	
Art. 1 pkt 37	37) po art. 35 dodaje się art. 35a w brzmieniu: „Art. 35a. W przypadku wystąpienia incydentu krytycznego Prezes Rady Ministrów może, na podstawie propozycji Rządowego Zespołu Zarządzania Kryzysowego, o której mowa w art. 9 ust. 1 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2023 r. poz. 122, z późn. zm.), zobowiązać Ministra Obrony Narodowej do udzielenia wsparcia CSIRT koordynującemu obsługę tego incydentu przez właściwe jednostki organizacyjne podległe Ministrowi Obrony Narodowej lub przez niego nadzorowane.”;	Dodawany przepis pozwoli jednostkom wojskowym wesprzeć podmioty krajowego systemu cyberbezpieczeństwa przy obsłudze szczególnie groźnych incydentów.
Art. 1 pkt 38	38) w art. 36: a) ust. 2–4 otrzymują brzmienie: „2. W skład Zespołu wchodzi przedstawiciele CSIRT MON, CSIRT NASK, Szefa Agencji Bezpieczeństwa Wewnętrznego realizującego zadania w ramach CSIRT GOV, Rządowego Centrum Bezpieczeństwa oraz ministra właściwego do spraw zagranicznych. 3. Pełnomocnik przewodniczy pracom Zespołu. 4. Obsługę prac Zespołu zapewnia urząd obsługujący Pełnomocnika.”, b) w ust. 6 wyrazy „dyrektor Rządowego Centrum Bezpieczeństwa” zastępuje się wyrazem „Pełnomocnik”;	Dodawane przepisy uzupełniają regulacje dotyczące funkcjonowania Zespołu do spraw Incydentów Krytycznych.
Art. 1 pkt 40	40) w art. 37: a) ust. 1 i 2 otrzymują brzmienie: „1. Do udostępniania informacji o podatnościach, incydentach i cyberzagrożeniach oraz o ryzyku wystąpienia incydentów nie stosuje się przepisów: 1) ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej;	Przepis wyłącza stosowanie ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2022 r. poz. 902) oraz ustawy z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego (Dz. U. z 2023 r. poz. 1524) do udostępniania

	2) ustawy z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego, z wyjątkiem informacji, których udostępnienie nie zagrażałoby bezpieczeństwu państwa lub bezpieczeństwu publicznemu. 2. Właściwy CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT sektorowy może, po konsultacji ze zgłaszającym podmiotem kluczowym lub podmiotem ważnym, opublikować na stronie podmiotowej Biuletynu Informacji Publicznej odpowiednio Ministra Obrony Narodowej, Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego, Agencji Bezpieczeństwa Wewnętrznego lub organu właściwego do spraw cyberbezpieczeństwa informacje o incydentach poważnych, gdy jest to niezbędne, aby zapobiec wystąpieniu incydentu albo zapewnić obsługę incydentu.”, c) uchyla się ust. 3, d) w ust. 4 skreśla się wyrazy „i 3”;	informacji o podatnościach, incydentach i cyberzagrożeniach oraz o ryzyku wystąpienia incydentów.
Art. 1 pkt 42	42) użyte w art. 40, w art. 42 w ust. 1 w pkt 5, w art. 44 w ust. 3 w zdaniu pierwszym i drugim, w art. 49 w ust. 3 we wprowadzeniu do wyliczenia, w art. 64 oraz w art. 93 w ust. 11 w pkt 4, w różnej liczbie i różnym przypadku, wyrazy „sektorowy zespół cyberbezpieczeństwa” zastępuje się użytymi w odpowiedniej liczbie i odpowiednim przypadku wyrazami „CSIRT sektorowy”	W wymienionych przepisach pojęcie „sektorowego zespołu cyberbezpieczeństwa” zastępuje się pojęciem „CSIRT sektorowego”.
Art. 1 pkt 47	47) w art. 43: a) ust. 1 otrzymuje brzmienie „1. Organ właściwy do spraw cyberbezpieczeństwa może, bez wszczynania postępowania, o którym mowa w art. 7j lub art. 7l, wystąpić do podmiotu, o którym mowa w załączniku nr 1 lub nr 2 do ustawy, o udzielenie informacji, które umożliwią wstępną ocenę, czy dany podmiot należy uznać za podmiot kluczowy lub podmiot ważny. Przepis art. 53c ust. 2 i 3 stosuje się odpowiednio. b) uchyla się ust. 2–5, c) ust. 6 otrzymuje brzmienie: „6. Informacje udzielone przez podmiot, o którym mowa w ust. 1, mogą stanowić podstawę do wpisania podmiotu do wykazu na podstawie art. 7j albo wydania decyzji, o której mowa w art. 7l.”;	Przepis wprowadza kompetencje dla organów właściwych do spraw cyberbezpieczeństwa do żądania informacji od podmiotów, które potencjalnie mogą być podmiotami kluczowymi i ważnymi.

Art. 1 pkt 48	48) w art. 44: a) ust. 1 otrzymuje brzmienie: „1. Organ właściwy do spraw cyberbezpieczeństwa zapewnia funkcjonowanie CSIRT sektorowego dla podmiotów kluczowych lub podmiotów ważnych w danym sektorze lub podsektorze wymienionych w załączniku nr 1 i 2 do ustawy, do którego zadań należy: 1) przyjmowanie wczesnych ostrzeżeń, zgłoszeń o incydentach, sprawozdań okresowych i sprawozdań końcowych, o których mowa w art. 11 ust. 1 pkt 4– 4c; 2) przyjmowanie zgłoszeń o potencjalnych zdarzeniach dla cyberbezpieczeństwa; 3) reagowanie na incydenty; 4) gromadzenie informacji o podatnościach i cyberzagrożeniach; 5) współpraca z podmiotem kluczowym lub podmiotem ważnym w zakresie wymiany dobrych praktyk oraz informacji o podatnościach i cyberzagrożeniach, organizacja i uczestniczenie w ćwiczeniach oraz wspieranie inicjatyw szkoleniowych; 6) współpraca z CSIRT MON, CSIRT NASK i CSIRT GOV w koordynowanym przez nie reagowaniu na incydenty, w szczególności w zakresie wymiany informacji o cyberzagrożeniach oraz stosowanych środkach zapobiegających i ograniczających wpływ incydentów; 7) współpraca z innymi CSIRT sektorowymi w zakresie wymiany informacji o podatnościach i cyberzagrożeniach.”, b) po ust. 1 dodaje się ust. 1a–1d w brzmieniu: „1a. CSIRT sektorowy przekazuje, za pomocą systemu teleinformatycznego, o którym mowa w art. 46 ust. 1, wczesne ostrzeżenie, zgłoszenie incydentu, sprawozdanie okresowe i sprawozdanie końcowe, o których mowa w art. 11 ust. 1 pkt 4– 4c, niezwłocznie, nie później niż 8 godzin od jego otrzymania, do właściwego CSIRT MON, CSIRT NASK albo CSIRT GOV. 1b. CSIRT sektorowy może, w szczególności: 1) zapewniać we współpracy z CSIRT MON, CSIRT NASK i CSIRT GOV dynamiczną analizę ryzyka i analizę incydentów oraz wspomagać w podnoszeniu świadomości cyberzagrożeń wśród podmiotów kluczowych lub podmiotów ważnych danego sektora lub podsektora;	Projekt przewiduje utworzenie zespołów CSIRT sektorowych wspierających przedsiębiorców w reagowaniu na incydenty. Przepis nie nakłada na przedsiębiorców dodatkowych obowiązków.

	2) wykonywać niezbędne działania techniczne związane z analizą cyberzagrożeń oraz reagowaniem na incydent poważny; 3) koordynować, w ramach sektora lub podsektora, w uzgodnieniu z podmiotami kluczowymi lub podmiotami ważnymi obsługę incydentów, które ich dotyczą; 4) wspierać, w uzgodnieniu z podmiotem kluczowym lub podmiotem ważnym, wykonywanie przez niego obowiązków określonych w art. 11, art. 12– 12b i art. 13; 5) w ramach reagowania na incydent poważny wystąpić do organu właściwego do spraw cyberbezpieczeństwa z wnioskiem o wezwanie podmiotu kluczowego lub podmiotu ważnego, aby w wyznaczonym terminie usunął podatności, które doprowadziły lub mogłyby doprowadzić do incydentu poważnego; 6) prowadzić działania na rzecz podnoszenia poziomu bezpieczeństwa systemów informacyjnych podmiotów kluczowych lub podmiotów ważnych w danym sektorze lub podsektorze, w szczególności przez: a) wykonywanie oceny bezpieczeństwa, b) identyfikowanie podatności systemów dostępnych w otwartych sieciach teleinformatycznych, a także powiadamianie właścicieli tych systemów o wykrytych podatnościach oraz cyberzagrożeniach; 7) na wniosek podmiotu kluczowego lub ważnego wspierać dany podmiot w zakresie monitorowania ich sieci i systemów informatycznych w czasie rzeczywistym lub zbliżonym do rzeczywistego. 1c. CSIRT sektorowy, który otrzymał zgłoszenie incydentu, a nie jest właściwy do jego przyjęcia, przekazuje niezwłocznie to zgłoszenie do właściwego CSIRT wraz z otrzymanymi informacjami. 1d. CSIRT sektorowy informuje o złożeniu wniosku, o którym mowa w ust. 1b pkt 5, właściwy CSIRT MON, CSIRT NASK albo CSIRT GOV.”, c) uchyla się ust. 2, d) ust. 4 otrzymuje brzmienie: „4. Organ właściwy do spraw cyberbezpieczeństwa informuje podmioty kluczowe lub podmioty ważne w danym sektorze oraz CSIRT MON, CSIRT NASK i CSIRT GOV o ustanowieniu CSIRT sektorowego i zakresie realizowanych zadań. e) po ust. 4 dodaje się ust. 5 i 6 w brzmieniu:	

	5. Przepisy ust. 1–1d, 3 i 4 stosuje się odpowiednio do CSIRT sektorowego ustanowionego w sektorze bankowym i infrastruktury rynków finansowych, w szczególności w zakresie poważnych incydentów związanych z ICT zgłaszanych przez podmioty kluczowe lub podmioty ważne. 6. CSIRT sektorowy ustanowiony w sektorze bankowości i infrastruktury rynków finansowych może również realizować swoje zadania w odniesieniu do podmiotów finansowych niebędących podmiotami kluczowymi lub podmiotami ważnymi, w szczególności w zakresie wsparcia w obsłudze poważnych incydentów związanych z ICT, gdy nie stanowi to dla niego nieproporcjonalnego czy nadmiernego obciążenia, z uwzględnieniem priorytetowego traktowania poważnych incydentów związanych z ICT zgłaszanych przez podmioty finansowe będące podmiotami kluczowymi lub podmiotami ważnymi oraz odpowiedniego stosowania ust. 1–1d, 3 i 4 do realizacji zadań.”;	
Art. 1 pkt 49	49) po art. 44 dodaje się art. 44a–44f w brzmieniu: „Art. 44a. 1. Organ właściwy do spraw cyberbezpieczeństwa może powierzyć realizację zadania lub zadań CSIRT sektorowego: 1) jednostce jemu podległej albo przez niego nadzorowanej; 2) organowi przez niego nadzorowanemu; 3) urzędowi, który obsługuje. 2. Organ właściwy do spraw cyberbezpieczeństwa może powierzyć realizację zadania albo zadań CSIRT sektorowego państwowej osobie prawnej, o której mowa w art. 3 ustawy z dnia 16 grudnia 2016 r. o zasadach zarządzania mieniem państwowym, jeżeli dysponuje ona zdolnościami technicznymi i organizacyjnymi niezbędnymi do wypełniania zadań CSIRT sektorowego w danym sektorze lub podsektorze. 3. Organy właściwe do spraw cyberbezpieczeństwa mogą, w drodze porozumienia, powierzyć realizację zadania lub zadań CSIRT sektorowego dla kilku sektorów lub podsektorów, dla których są właściwe, jednostce podległej jednemu z tych organów albo nadzorowanej przez jeden z tych organów. Stroną tego porozumienia jest również jednostka, której powierzono zadania.	Wprowadza się obowiązek powołania przez organ właściwy do spraw cyberbezpieczeństwa CSIRT sektorowego właściwego dla danego sektora lub podsektora, który będzie wspierał podmioty kluczowe i podmioty ważne tego sektora w obszarze reagowania na incydenty. Do obligatoryjnych zadań CSIRT sektorowego będzie należało przyjmowanie zgłoszeń o incydentach oraz reagowanie na incydenty. Dotychczas sektorowe zespoły cyberbezpieczeństwa miały za zadanie przyjmować zgłoszenia o incydentach poważnych i reagować na nie. Projektowana zmiana pozwoli CSIRT sektorowemu uzyskiwać więcej zgłoszeń o incydentach, dzięki czemu zespół będzie mógł szybciej zdobywać doświadczenie i wiedzę w ciągle zmieniającej się sytuacji w cyberprzestrzeni. Przełoży się to na skuteczną pomoc dla podmiotów kluczowych i podmiotów ważnych zmagających się z incydentami.

	4. Organy właściwe do spraw cyberbezpieczeństwa określają w porozumieniu, o którym mowa w ust. 3, w szczególności zakres powierzonych zadań, weryfikację prawidłowości ich wykonania oraz sposób finansowania powierzonych zadań. Art. 44b. 1. Minister będący organem właściwym do spraw cyberbezpieczeństwa dla kilku sektorów lub podsektorów może powierzyć jednostce jemu podległej albo nadzorowanej przez niego zadanie lub zadania CSIRT sektorowego. 2. Powierzenie odbywa się w drodze decyzji, do której nie stosuje się przepisów ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego. 3. Komunikat o powierzeniu przez ministra będącego organem właściwym do spraw cyberbezpieczeństwa dla kilku sektorów lub podsektorów zadania lub zadań CSIRT sektorowego jednostce podległej albo nadzorowanej przez tego ministra ogłasza się w dzienniku urzędowym organu właściwego do spraw cyberbezpieczeństwa. 4. Ministrowie, którzy przejęli właściwość nadzorczą nad sektorami, dla których dotychczasowy minister wyznaczył wspólny CSIRT sektorowy, zawierają porozumienie, w którym wyznaczają jednostkę, która przejmie zadania CSIRT sektorowego dla poszczególnych sektorów lub podsektorów. Do czasu zawarcia porozumienia decyzja, o której mowa w ust. 2, zachowuje moc. Art. 44c. 1. Organ właściwy do spraw cyberbezpieczeństwa może powierzyć CSIRT MON, CSIRT NASK albo CSIRT GOV realizację zadania albo zadań CSIRT sektorowego. 2. Powierzenie, o którym mowa w ust. 1, następuje na podstawie porozumienia organu właściwego do spraw cyberbezpieczeństwa: 1) w przypadku powierzenia zadań CSIRT NASK – za zgodą ministra właściwego do spraw informatyzacji – z Dyrektorem Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego; 2) w przypadku powierzenia zadań CSIRT GOV – z Szefem Agencji Bezpieczeństwa Wewnętrznego; 3) w przypadku powierzenia zadań CSIRT MON – z Ministrem Obrony Narodowej.	

	3. Do porozumienia, o którym mowa w ust. 2, stosuje się przepis art. 44a ust. 4. 4. Minister Obrony Narodowej, jako organ właściwy do spraw cyberbezpieczeństwa, może powierzyć CSIRT MON realizację zadań CSIRT sektorowego w drodze decyzji niepodlegającej ogłoszeniu. Art. 44d. 1. Zadania CSIRT sektorowego: 1) są finansowane z części budżetu państwa, której dysponentem jest minister albo centralny organ administracji rządowej, będący organem właściwym do spraw cyberbezpieczeństwa; 2) mogą być dofinansowywane: a) ze środków pochodzących z budżetu Unii Europejskiej, b) ze środków przeznaczonych na realizację programów finansowanych z udziałem środków pochodzących z budżetu Unii Europejskiej. 2. Jednostka, której powierzono zadania CSIRT sektorowego dla danego sektora lub podsektora, może otrzymać na realizację tych zadań dotację celową, z części budżetowej, której dysponentem jest minister będący organem właściwym do spraw cyberbezpieczeństwa dla danego sektora lub podsektora. 3. W przypadku, gdy jednostce budżetowej powierzono realizację zadania lub zadań CSIRT sektorowego dla kilku sektorów lub podsektorów, otrzymuje ona środki z części budżetowych, których dysponentami są organy właściwe do spraw cyberbezpieczeństwa dla danego sektora lub podsektora, które zawarły porozumienie, o którym mowa w art. 44a ust. 3. 4. CSIRT sektorowy dla sektora bankowości i infrastruktury rynków finansowych otrzymuje dotację celową na realizację swoich zadań, o których mowa w art. 44, z części budżetowej, której dysponentem jest Szef Kancelarii Prezesa Rady Ministrów. Art. 44e. 1. Komunikat o zawarciu porozumienia, o którym mowa w art. 44a ust. 3, art. 44b ust. 3 lub art. 44c ust. 2, ogłasza się w dzienniku urzędowym organu właściwego do spraw cyberbezpieczeństwa i wskazuje się: 1) adres strony internetowej, na której zostanie zamieszczona treść porozumienia wraz ze stanowiącymi jego integralną treść załącznikami; 2) termin, od którego porozumienie będzie obowiązywało.	

	2. Organ właściwy do spraw cyberbezpieczeństwa informuje Pełnomocnika o zawarciu porozumienia, o którym mowa w art. 44a ust. 3, art. 44b ust. 3 lub art. 44c ust. 2. Pełnomocnik publikuje komunikat o zawarciu porozumienia na swojej stronie podmiotowej Biuletynu Informacji Publicznej. Art. 44f. Organ właściwy do spraw cyberbezpieczeństwa raz w roku, w terminie do dnia 31 stycznia, przedkłada Pełnomocnikowi sprawozdanie z funkcjonowania CSIRT sektorowego za rok poprzedni.”	
Art. 1 pkt 51 i 52	51) art. 45a otrzymuje brzmienie: „Art. 45a. 1. Minister właściwy do spraw informatyzacji może udzielić wsparcia finansowego w ramach programów rządowych lub innych programów finansowanych w całości albo w części z udziałem środków, o których mowa w art. 5 ust. 3 pkt 6 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych, na realizację projektów, których celem jest: 1) tworzenie i rozwój produktów ICT, usług ICT oraz procesów ICT z zakresu cyberbezpieczeństwa; 2) rozwój kompetencji w obszarze cyberbezpieczeństwa; 3) zapewnianie cyberbezpieczeństwa w danej jednostce organizacyjnej; 4) promocja dobrych praktyk, programów edukacyjnych, kampanii i szkoleń na rzecz poszerzania wiedzy i budowania świadomości z zakresu cyberbezpieczeństwa; 5) wsparcie w obszarze standaryzacji i certyfikacji cyberbezpieczeństwa; 6) rozwój infrastruktury służącej zapewnianiu cyberbezpieczeństwa; 7) wsparcie badań naukowych, rozwoju technologicznego i projektów pilotażowych związanych z cyberbezpieczeństwem; 8) wsparcie w obsłudze incydentów; 9) identyfikacja i mitygacja podatności produktów ICT, usług ICT i procesów ICT, 10) zwiększenie rozpoznawalności produktów lub usług z zakresu cyberbezpieczeństwa; 11) inne działania służące rozwojowi cyberbezpieczeństwa. 2. Wsparcie finansowe, o którym mowa w ust. 1, może być udzielane podmiotom publicznym, jak i prywatnym, i może stanowić: 1) pomoc publiczną dla podmiotów prywatnych; 2) pomoc <i>de minimis</i> dla podmiotów prywatnych;	Przepis umożliwia udzielanie wsparcia finansowego z zakresu cyberbezpieczeństwa podmiotom publicznym oraz prywatnym przez ministra właściwego do spraw informatyzacji.

	3) dofinansowanie dla podmiotów publicznych. 3. Wsparcie finansowe, o którym mowa w ust. 1, jest udzielane podmiotom, które mają zdolność do realizacji projektu, o którym mowa w ust. 1. 4. Wsparcie finansowe, o którym mowa w ust. 1, może mieć charakter zwrotny albo bezzwrotny. 5. Wybór projektów, na które jest udzielane wsparcie finansowe, o którym mowa w ust. 1, następuje w trybie konkursowym albo pozakonkursowym. 6. Minister właściwy do spraw informatyzacji określi, odrębnie dla danego programu, o którym mowa w ust. 1, w drodze rozporządzenia, szczegółowe warunki, formę oraz tryb udzielania wsparcia finansowego, o którym mowa w ust. 1, a także podmioty go udzielające, uwzględniając konieczność realizacji celów określonych w tych programach, efektywność i skuteczność wykorzystania tego wsparcia oraz przejrzystość jego udzielania, a także zapewnienie jego zgodności z rynkiem wewnętrznym. 52) po art. 45a dodaje się art. 45b i art. 45c w brzmieniu: „Art. 45b. Wsparcie finansowe, o którym mowa w art. 45a ust. 1, może być udzielane w imieniu ministra właściwego do spraw informatyzacji przez podmiot mu podległy albo przez niego nadzorowany. Art. 45c. 1. Wyboru projektów dokonuje się w sposób przejrzysty, rzetelny i bezstronny na podstawie obiektywnych kryteriów oceny biorąc pod uwagę w szczególności wpływ projektu na realizację celów określonych w art. 45a ust. 1 oraz na krajowy system cyberbezpieczeństwa. 2. Podstawę dofinansowania projektu stanowi umowa o dofinansowanie projektu zawarta z beneficjentem przez podmiot udzielający wsparcia finansowego, o którym mowa w art. 45a ust. 1. 3. Beneficjent może wykorzystywać otrzymane wsparcie tylko na wydatki służące realizacji celów wskazanych w art. 45a ust. 1. 4. Beneficjent jest obowiązany zwrócić wsparcie wykorzystane niezgodnie z ust. 3, w terminie nie dłuższym niż 15 dni od określonego w umowie dnia wykonania zadania.	

	5. Beneficjent informuje podmiot udzielający wsparcie o postępach w realizacji projektu w terminach wskazanych w umowie, o której mowa w ust. 2. 6. Do umowy, o której mowa w ust. 2, stosuje się odpowiednio art. 150 ustawy o finansach publicznych. 3.”	
Art. 1 pkt 53 lit. a	53) w art. 46: a) w ust. 1: – w pkt 5 wyrazy „zagrożeniach cyberbezpieczeństwa” zastępuje się wyrazem „cyberzagrożeniach”, - kropkę zastępuje się średnikiem i dodaje się pkt 6–8 w brzmieniu: „6) czynności nadzorcze organów właściwych do spraw cyberbezpieczeństwa; 7) dokonywanie zgłoszenia naruszenia ochrony danych osobowych, o którym mowa w art. 33 rozporządzenia 2016/679 i art. 44 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2023 r. poz. 1206) przez podmioty kluczowe lub podmioty ważne; 8) wymianę informacji o aktach prawnych ministra właściwego do spraw informatyzacji, Pełnomocnika, organów właściwych do spraw cyberbezpieczeństwa oraz Prezesa Rady Ministrów, o których mowa w art. 33 ust. 4, art. 42 ust. 1 pkt 5, art. 45 ust. 3, art. 67, art. 67a, art. 67b ust. 15, art. 67g ust. 1 i art. 67l ust. 1.”,	Przepis umożliwia wprowadzenie w systemie S46 wspierania czynności nadzorczych organów właściwych do spraw cyberbezpieczeństwa oraz dokonywanie zgłoszenia naruszenia ochrony danych osobowych.
Art. 1 pkt 55	55) w art. 47: a) ust. 1 otrzymuje brzmienie: „1. Minister właściwy do spraw informatyzacji może realizować zadania, o których mowa w art. 45 ust. 1, 45a ust. 1 i art. 46 ust. 1 i 1a, jednostkom jemu podległym lub przez niego nadzorowanym.”, b) dodaje się ust. 3 w brzmieniu: „3. Minister właściwy do spraw informatyzacji może udostępniać jednostkom, o których mowa w ust. 1, dane z wykazu podmiotów kluczowych i podmiotów ważnych w zakresie i w celu realizacji zadań im powierzonych, z uwzględnieniem poufności, integralności, dostępności i autentyczności tych danych.”;	Wprowadza się przepis umożliwiający powierzenie jednostkom podległym albo nadzorowanym przez ministra właściwego do spraw informatyzacji prowadzenie wykazu podmiotów kluczowych i podmiotów ważnych oraz umożliwi przekazanie potrzebnych danych tym jednostkom.

Art. 1 pkt 57 lit. b tiret pierwsze	57) w art. 49: b) w ust. 3: – w pkt 2 wyrazy „Agencji Unii Europejskiej do spraw Bezpieczeństwa Sieci i Informacji (ENISA)” zastępuje się wyrazem „ENISA”,	Przepis dostosowuje dotychczasową nazwę ENISA do skrótu ujętego we wcześniejszych przepisach.
Art. 1 pkt 59	59) w art. 51 w ust. 1: a) w pkt 2 wyrazy „zagrożenia cyberbezpieczeństwa” zastępuje się wyrazem „cyberzagrożenia”, b) pkt 5–8 otrzymują brzmienie: „5) koordynację działań związanych z obsługą incydentów w czasie stanu wojennego lub w czasie wojny, z zastrzeżeniem kompetencji Naczelnego Dowódcy Sił Zbrojnych; 6) ocenę wpływu incydentów poważnych i krytycznych na system obronny państwa; 7) ocenę cyberzagrożeń, w zakresie ich wpływu na system obronny państwa oraz przedstawianie właściwym organom, w przypadku wprowadzenia stanu wojennego lub stanu wojny, propozycji dotyczących działań obronnych z zastrzeżeniem kompetencji Naczelnego Dowódcy Sił Zbrojnych; 8) koordynację, we współpracy z ministrem właściwym do spraw wewnętrznych i ministrem właściwym do spraw informatyzacji, realizacji zadań organów administracji rządowej i jednostek samorządu terytorialnego w czasie stanu wojennego lub w czasie wojny dotyczących działań obronnych w przypadku cyberzagrożenia z zastrzeżeniem kompetencji Naczelnego Dowódcy Sił Zbrojnych.”;	Przepis uzupełnia kompetencje Ministra Obrony Narodowej w zakresie zapewnienia bezpieczeństwa w cyberprzestrzeni w wymiarze militarnym. Przepis nie nakłada na przedsiębiorców dodatkowych obowiązków.
Art. 1 pkt 61 w zakresie dodawanego rozdziału 10a	61) po rozdziale 10 dodaje się rozdział 10a–10c w brzmieniu: „Rozdział 10a. Zadania ministra właściwego do spraw energii Art. 52a. 1. Organem właściwym, o którym mowa w art. 4 ust. 1 rozporządzenia 2024/1366, jest minister właściwy do spraw energii. 2. Właściwy organ, określony w ust. 1, identyfikuje podmioty o dużym wpływie i podmioty o krytycznym wpływie zgodnie z art. 24 rozporządzenia 2024/1366. Identyfikacja podmiotu o dużym wpływie lub podmiotu o krytycznym wpływie jest inną czynnością z zakresu administracji publicznej, na którą przysługuje skarga do sądu administracyjnego i wymaga uzasadnienia.	Przepisy te służą zapewnieniu wykonania szczególnych zadań związanych z sektorem energii, które należą do kompetencji ministra właściwego do spraw energii.

	3. Minister właściwy do spraw energii może wystąpić do podmiotu kluczowego lub podmiotu ważnego z podsektora energii elektrycznej, o udzielenie informacji, które umożliwią wstępną ocenę, czy dany podmiot należy uznać za podmiot o dużym wpływie lub podmiot o krytycznym wpływie zgodnie z art. 24 rozporządzenia 2024/1366. Przepis art. 53c ust. 1–3 stosuje się odpowiednio. Art. 52b. 1. Minister właściwy do spraw energii prowadzi kontrole podmiotów zidentyfikowanych jako podmioty o krytycznym wpływie, o których mowa w rozporządzeniu 2024/1366. 2. W przypadku kontroli, o której mowa w ust. 1, przepisy art. 54 stosuje się.”	
Art. 1 pkt 61 w zakresie dodawanego rozdziału 10b	„Rozdział 10b Zadania ministra właściwego do spraw zagranicznych Art. 52c. Minister właściwy do spraw zagranicznych prowadzi i koordynuje działalność dyplomatyczną w zakresie cyberbezpieczeństwa w stosunkach z państwami trzecimi i organizacjami międzynarodowymi. Art. 52d. Minister właściwy do spraw informatyzacji przekazuje ministrowi właściwemu do spraw zagranicznych, z wyłączeniem danych osobowych: 1) informacje, odebrane i wysyłane przez Pojedynczy Punkt Kontaktowy, o wystąpieniu incydentu dotyczącego innych państw wraz z krótkim opisem i wskazaniem wszystkich państw, których dotyczył incydent; 2) sprawozdanie, o którym mowa w art. 49 ust. 6; 3) informacje pochodzące z Grupy Współpracy, o których mowa w art. 49 ust. 3 pkt 4–6; 4) informacje, o których mowa w art. 49 ust. 1; 5) informacje, odebrane i wysyłane przez Pojedynczy Punkt Kontaktowy, dotyczące sytuacji kryzysowych w cyberprzestrzeni.	Przepisy te określają zadania ministra właściwego do spraw zagranicznych.
Art. 1 pkt 65	65) art. 54 otrzymuje brzmienie: „Art. 54. Do kontroli realizowanej wobec podmiotów kluczowych lub podmiotów ważnych: 1) będących przedsiębiorcami stosuje się przepisy rozdziału 5 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców; 2) nie będących przedsiębiorcami stosuje się przepisy ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej;	Zmiany w art. 54 mają charakter dostosowujący i są konsekwencją zmian wprowadzonych w pozostałych przepisach.

	3) będących jednostkami samorządu terytorialnego stosuje się przepisy ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej.”	
Art. 1 pkt 66	66) w art. 56 dodaje się ust. 3 i 4 w brzmieniu: „3. Organ przeprowadzający kontrolę może żądać od podmiotu kontrolowanego przedstawienia tłumaczenia na język polski sporządzonej w języku obcym dokumentacji przedłożonej przez podmiot kontrolowany. Tłumaczenie dokumentacji podmiot kontrolowany jest obowiązany wykonać na własny koszt. Zlecenie tłumaczenia dokumentacji podmiotom trzecim odbywa się z poszanowaniem tajemnicy prawnie chronionej na podstawie odrębnych przepisów. 4. Organ przeprowadzający kontrolę, występując do podmiotu kontrolowanego z żądaniem, o którym mowa w ust. 3, wskazuje zakres dokumentów, które mają zostać przetłumaczone, ich związek z przeprowadzaną kontrolą oraz określa termin na przedstawienie tłumaczenia dokumentacji, uwzględniający zakres koniecznego tłumaczenia.”;	Przepisy te regulują zasady przygotowywania tłumaczeń na potrzeby prowadzonych postępowań kontrolnych, co jest niezbędne dla zapewnienia organom realnej możliwości zapoznania się z kluczowymi dokumentami.
Art. 1 pkt 67	67) w art. 58: a) ust. 4–8 otrzymują brzmienie: „4. W przypadku zastrzeżeń dotyczących ustaleń zawartych w protokole kontroli, kontrolowany ma prawo odmówić podpisania protokołu kontroli oraz złożyć umotywowane pisemne zastrzeżenia do tego protokołu w terminie 7 dni od dnia przedstawienia mu go do podpisu. 5. Odmowę podpisania protokołu kontroli osoba prowadząca czynności kontrolne odnotowuje w protokole wraz ze wskazaniem daty tej odmowy. 6. W razie złożenia zastrzeżeń do protokołu kontroli kierownik komórki organizacyjnej do spraw kontroli dokonuje ich analizy. 7. Kierownik komórki organizacyjnej do spraw kontroli: 1) odrzuca zastrzeżenia do protokołu kontroli wniesione przez osobę nieuprawnioną lub wniesione po upływie terminu i informuje o tym na piśmie zgłaszającego zastrzeżenia, podając przyczyny, albo 2) uwzględnia zastrzeżenia do protokołu kontroli w całości albo w części lub je oddala. 8. W razie potrzeby, w związku ze zgłoszeniem zastrzeżeń do protokołu, osoba prowadząca czynności kontrolne podejmuje dodatkowe czynności kontrolne, a w przypadku stwierdzenia przez kierownika komórki	W zmienianym art. 58 wskazano wyraźnie, że kontrolowany w przypadku zastrzeżeń co do ustaleń zawartych w protokole kontroli ma prawo odmówić jego podpisania, a także złożyć umotywowane pisemne zastrzeżenia do tego protokołu w terminie 7 dni od dnia przedstawienia mu protokołu kontroli do podpisu. Nie tylko podkreślono zatem uprawnienie kontrolowanego do odmowy podpisania protokołu, ale również postanowiono, że pisemne zastrzeżenia powinny być umotywowane. Obowiązek analizy zastrzeżeń przekazano na kierownika komórki do spraw kontroli jednocześnie zdejmując ten obowiązek z osoby prowadzącej czynności kontrolne. Kierownik komórki do spraw kontroli po analizie odrzuca zastrzeżenia i informuje, o tym fakcie podmiot kontrolowany albo uwzględnia zastrzeżenia w całości lub w części lub je oddala. Kierownik komórki obowiązany jest również do sporządzenia stanowiska wobec złożonych zastrzeżeń.

	organizacyjnej do spraw kontroli zasadności zastrzeżeń do protokołu kontroli zmienia lub uzupełnia odpowiednią część protokołu kontroli w formie aneksu do protokołu.”, b) po ust. 8 dodaje się ust. 9–11 w brzmieniu: „9. Kierownik komórki organizacyjnej do spraw kontroli, po rozpatrzeniu zastrzeżeń do protokołu kontroli, sporządza stanowisko wobec tych zastrzeżeń. 10. O nieuwzględnieniu zastrzeżeń do protokołu kontroli w całości albo w części kierownik komórki organizacyjnej do spraw kontroli informuje podmiot kontrolowany na piśmie. 11. Protokół kontroli: 1) w postaci papierowej sporządza się w dwóch egzemplarzach, z których jeden pozostawia się podmiotowi kontrolowanemu; 2) w postaci elektronicznej doręcza się podmiotowi kontrolowanemu na adres do doręczeń elektronicznych.”;	Osoba prowadząca czynności kontrole w razie potrzeby podejmuje dodatkowe czynności kontrolne, a w przypadku stwierdzenia przez kierownika komórki do spraw kontroli zasadności zastrzeżeń zmienia lub uzupełnia odpowiednią część protokołu w formie aneksu.
Art. 1 pkt 68	68) w art. 59: a) ust. 1 otrzymuje brzmienie: „1. Jeżeli na podstawie informacji zgromadzonych w toku kontroli organ właściwy do spraw cyberbezpieczeństwa uzna, że mogło dojść do naruszenia przepisów ustawy przez podmiot kontrolowany, przekazuje zalecenia pokontrolne wzywające do usunięcia nieprawidłowości. Organ właściwy do spraw cyberbezpieczeństwa wskazuje termin usunięcia tych nieprawidłowości, uwzględniając zakres i rodzaj naruszeń.”, b) w ust. 3 skreśla się wyrazy „lub ministra właściwego do spraw informatyzacji”;	Zmiana procedury w przypadku zastrzeżeń do protokołu w zaproponowanym brzmieniu pozwoli na zapewnienie większej efektywności i obiektywności.
Art. 1 pkt 70	70) w art. 61 ust. 3 otrzymuje brzmienie: „3. Pełnomocnikiem jest minister właściwy do spraw informatyzacji, sekretarz stanu albo podsekretarz stanu w urzędzie obsługującym ministra właściwego do spraw informatyzacji.”;	Przepis określa, kto może zostać Pełnomocnikiem Rządu do Spraw Cyberbezpieczeństwa.
Art. 1 pkt 71	71) w art. 62: a) w ust. 1 w pkt 1 wyrazy „i CSIRT GOV” zastępuje się wyrazami „CSIRT GOV i CSIRT sektorowych”, b) w ust. 2 w pkt 3 wyrazy „zagrożeń cyberbezpieczeństwa” zastępuje się wyrazem „cyberzagrożeń”, c) po ust. 2 dodaje się ust. 3–8 w brzmieniu:	Przepis uzupełnia kompetencje Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa. Przepis nie nakłada obowiązków na przedsiębiorców.

	„3. Pełnomocnik może dokonywać zakupów produktów ICT, usług ICT lub procesów ICT z zakresu cyberbezpieczeństwa na rzecz podmiotów, o których mowa w art. 62a ust. 2 pkt 3, na podstawie umowy, przekazując prawa do zakupionych produktów ICT, usług ICT lub procesów ICT z zakresu cyberbezpieczeństwa. 4. Pełnomocnik może, w zakresie realizacji jego zadań, zlecać przeprowadzanie badań lub ekspertyz. 5. Pełnomocnik może, w drodze zarządzenia, powoływać zespoły doradcze. 6. Pełnomocnik może upoważnić do realizacji swoich zadań pracownika ministerstwa lub urzędu administracji rządowej go obsługującego, który: 1) pełni funkcję dyrektora departamentu, zastępcy dyrektora departamentu lub naczelnika wydziału; 2) spełnia wymagania określone w przepisach o ochronie informacji niejawnych w zakresie dostępu do informacji niejawnych o klauzuli „tajne”. 7. Organy administracji rządowej oraz jednostki organizacyjne podległe tym organom lub przez nie nadzorowane są obowiązane do udzielania pomocy Pełnomocnikowi przy realizacji jego zadań, w szczególności przez udostępnianie mu informacji i dokumentów. 8. Zadania Pełnomocnika są finansowane z części budżetowej, której dysponentem jest minister właściwy do spraw informatyzacji.”;	
Art. 1 pkt 72	72) po art. 62 dodaje się art. 62a w brzmieniu: „Art. 62a 1. Przy Pełnomocniku funkcjonuje PCOC, jako organ pomocniczy w sprawach koordynowania działań i realizowania polityki rządu w zakresie zapewnienia cyberbezpieczeństwa Rzeczypospolitej Polskiej. 2. W skład PCOC wchodzi: 1) Pełnomocnik; 2) sekretarz PCOC; 3) przedstawiciele: a) ministra – członka Rady Ministrów właściwego do spraw koordynowania działalności służb specjalnych, jeżeli został powołany, b) ministra właściwego do spraw informatyzacji, c) ministra właściwego do spraw wewnętrznych,	Przepis tworzy Połączone Centrum Operacyjne Cyberbezpieczeństwa (PCOC) będące organem pomocniczym w sprawach koordynowania działań i realizowania polityki rządu w zakresie zapewnienia cyberbezpieczeństwa. Przepis nie nakłada obowiązków na przedsiębiorców.

	d) ministra właściwego do spraw zagranicznych, e) Ministra Obrony Narodowej, f) Ministra Sprawiedliwości, g) Szefa Kancelarii Prezesa Rady Ministrów, h) organów właściwych do spraw cyberbezpieczeństwa, i) CSIRT GOV, j) CSIRT MON, k) CSIRT NASK, l) CSIRT sektorowych, m) Dowódcy Komponentu Wojsk Obrony Cyberprzestrzeni, n) dyrektora Rządowego Centrum Bezpieczeństwa, o) Komendanta Centralnego Biura Zwalczania Cyberprzestępczości, p) Komendanta Głównego Policji, q) Komendanta Służby Ochrony Państwa, r) Komendanta Głównego Straży Granicznej, s) Prokuratora Krajowego, t) Szefa Agencji Bezpieczeństwa Wewnętrznego, u) Szefa Agencji Wywiadu, v) Szefa Służby Kontrwywiadu Wojskowego, w) Szefa Służby Wywiadu Wojskowego. 3. Prezydent Rzeczypospolitej Polskiej może skierować do udziału w pracach PCOC swojego przedstawiciela. 4. Na posiedzenia PCOC mogą być zapraszani przedstawiciele podmiotów kluczowych, podmiotów ważnych lub innych podmiotów, jeżeli wymaga tego charakter spotkania. 5. Posiedzeniu PCOC przewodniczy Pełnomocnik. 6. Do zadań PCOC należy: 1) wymiana informacji na temat cyberzagrożeń, incydentów i podatności na poziomie krajowym; 2) wymiana informacji o wynikach szacowania ryzyka związanego z ujawnionym cyberzagroženiami oraz zaistniałymi incydentami; 3) wymiana informacji o przeprowadzanych badaniach, o których mowa w art. 33 ust. 1; 4) wymiana informacji dotyczących sytuacji kryzysowych w cyberprzestrzeni;	

	5) przygotowywanie bieżących informacji na temat sytuacji w cyberprzestrzeni dla Pełnomocnika; 6) wymiana informacji dotycząca procesów i współpracy międzynarodowej w zakresie bezpieczeństwa w cyberprzestrzeni 7. Sekretarz PCOC organizuje pracę PCOC i w tym zakresie może występować do CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT sektorowych oraz organów administracji rządowej o przedstawienie informacji niezbędnych w sprawach rozpatrywanych przez PCOC. 8. Sekretarza PCOC powołuje Pełnomocnik spośród osób spełniających wymagania określone w przepisach o ochronie informacji niejawnych w zakresie dostępu do informacji niejawnych o klauzuli „tajne”. Sekretarza PCOC odwołuje Pełnomocnik. 9. Sekretarz PCOC może powołać swojego zastępcę spośród osób spełniających wymagania określone w ust. 8. Zastępcę sekretarza PCOC odwołuje sekretarz PCOC. 10. W przypadku nieobecności sekretarza PCOC jego obowiązki wykonuje zastępca sekretarza PCOC. 11. Obsługę PCOC zapewnia ministerstwo lub inny urząd administracji rządowej obsługujący Pełnomocnika. 12. Pełnomocnik określi, w drodze zarządzenia, tryb pracy PCOC, mając na uwadze charakter zadań PCOC oraz konieczność zapewnienia jego sprawnej pracy. 13. Zarządzenie jest publikowane na stronie podmiotowej Biuletynu Informacji Publicznej Pełnomocnika.”;	
Art. 1 pkt 73	73) w art. 65: a) w ust. 1: – w pkt 1 wyrazy „zagrożeniom cyberbezpieczeństwa” zastępuje się wyrazem „cyberzagrożeniom”, – w pkt 2: – – wyrazy „sektorowe zespoły cyberbezpieczeństwa” zastępuje się wyrazami „CSIRT sektorowe”, – – wyrazy „zagrożeniom cyberbezpieczeństwa” zastępuje się wyrazem „cyberzagrożeniom”, – w pkt 3 wyrazy „i CSIRT NASK” zastępuje się wyrazami „CSIRT NASK i CSIRT sektorowych”,	Przepis uzupełnia zadania Kolegium do Spraw Cyberbezpieczeństwa oraz uspójnia przepisy w związku ze zmianami terminologicznymi wprowadzonymi w ustawie. Przepis nie nakłada obowiązków na przedsiębiorców.

	– w pkt 4 wyrazy „sektorowych zespołów cyberbezpieczeństwa” zastępuje się wyrazami „CSIRT sektorowych”, – pkt 8 otrzymuje brzmienie: „8) współdziałania zespołów CSIRT MON, CSIRT GOV, CSIRT NASK i CSIRT sektorowego w sektorze bankowym i infrastruktury rynków finansowych oraz właściwego organu w rozumieniu rozporządzenia 2022/2554, w zakresie działalności podmiotów finansowych będących podmiotami kluczowymi lub podmiotami ważnymi;”, – dodaje się pkt 9 w brzmieniu: „9) decyzji w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka.”, b) w ust. 2 wyrazy „Rady Ministrów” zastępuje się wyrazami „Prezesa Rady Ministrów”;	
Art. 1 pkt 75	75) w art. 66: a) w ust. 1 w pkt 4 w lit. g kropkę zastępuje się przecinkiem i dodaje się lit. h w brzmieniu: „h) organy właściwe do spraw cyberbezpieczeństwa.”, b) ust. 3 otrzymuje brzmienie: „3. Członkowie Kolegium, o których mowa w ust. 1 pkt 4 lit. a–e oraz lit. h, mogą być zastępowani przez upoważnionych przedstawicieli w randze sekretarza stanu, podsekretarza stanu, wiceprezesa urzędu lub zastępcy przewodniczącego.”, c) w ust. 4: – pkt 1 otrzymuje brzmienie: „1) dyrektor Rządowego Centrum Bezpieczeństwa albo jego zastępca;”, – w pkt 5 kropkę zastępuje się średnikiem i dodaje się pkt 6–9 w brzmieniu: „6) Dowódca Komponentu Wojsk Obrony Cyberprzestrzeni albo jego zastępca; 7) Prokurator Generalny albo jego zastępca; 8) Szef Agencji Wywiadu albo jego zastępca; 9) Szef Służby Wywiadu Wojskowego albo jego zastępca.”, d) w ust. 5 w pkt 2 kropkę zastępuje się średnikiem i dodaje się pkt 3–8 w brzmieniu:	Przepis uzupełnia skład Kolegium do Spraw Cyberbezpieczeństwa, uzupełnia zadania Przewodniczącego Kolegium do Spraw Cyberbezpieczeństwa oraz wprowadza stanowisko zastępcy sekretarza Kolegium. Przepis nie nakłada obowiązków na przedsiębiorców.

	„3) może pisemnie wnioskować o przeprowadzenie badania, o którym mowa w art. 33 ust. 1; 4) może zlecić CSIRT MON, CSIRT NASK lub CSIRT GOV, przeprowadzenie analizy dotyczącej wpływu konkretnych produktów ICT, usług ICT lub procesów ICT na bezpieczeństwo usług, o której mowa w art. 65a ust. 1; 5) może zlecić CSIRT MON, CSIRT NASK lub CSIRT GOV, przeprowadzenie analizy dotyczącej trybu i zakresu, w jakim dostawca sprawuje nadzór nad procesem wytwarzania i dostarczania produktów ICT, usług ICT lub procesów ICT, o której mowa w art. 65a ust. 2; 6) może wnioskować o wszczęcie postępowania w sprawie uznania dostawcy sprzętu i oprogramowania za dostawcę wysokiego ryzyka, o którym mowa w art. 67b ust. 1; 7) powołuje zespół opiniujący, o którym mowa w art. 67b ust. 13 pkt 1, oraz wskazuje przedstawicieli członków Kolegium wchodzących w jego skład; 8) rozstrzyga spór, o którym mowa w art. 67b ust. 13 pkt 2 zdanie drugie, wskazując właściwego członka zespołu opiniującego.”, e) po ust. 5 dodaje się ust. 5a w brzmieniu: „5a. Kolegium przyjmuje i rozpatruje sprawy na posiedzeniu albo w drodze korespondencyjnego uzgodnienia stanowisk (tryb obiegowy).”, f) w ust. 7 wyrazy „sektorowych zespołów cyberbezpieczeństwa” zastępuje się wyrazami „CSIRT sektorowych”, g) po ust. 7 dodaje się ust. 7a i 7b w brzmieniu: „7a. Sekretarz Kolegium może powołać swojego zastępcę spośród osób spełniających wymagania określone w ust. 6. Zastępcę sekretarza Kolegium odwołuje sekretarz Kolegium. 7b. W przypadku nieobecności sekretarza Kolegium jego obowiązki wykonuje zastępca sekretarza Kolegium, w tym zastępuje go na posiedzeniu Kolegium.”;	
Art. 1 pkt 76	76) po rozdziale 12 dodaje się rozdział 12a w brzmieniu: „Rozdział 12a Szczególne działania na rzecz zapewnienia cyberbezpieczeństwa na poziomie krajowym”	Wprowadzany jest nowy rozdział.

Art. 1 pkt 76 w zakresie art. 67a i art. 67b, art. 67d-67f oraz art. 67h-67l	76) „Art. 67a. 1. Pełnomocnik może wydać rekomendacje określające środki techniczne i organizacyjne stosowane w celu zwiększania poziomu bezpieczeństwa systemów informacyjnych podmiotów krajowego systemu cyberbezpieczeństwa. 2. Rekomendacje Pełnomocnika są publikowane na stronie podmiotowej Biuletynu Informacji Publicznej Pełnomocnika. 3. Pełnomocnik przed wydaniem rekomendacji może zasięgnąć opinii Kolegium. 4. W rekomendacjach Pełnomocnik może wskazać kategorie podmiotów, do których kierowane są rekomendacje. 5. Stosowanie rekomendacji jest dobrowolne. Art. 67b. 1. Minister właściwy do spraw informatyzacji, w celu ochrony bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego, może wszcząć, z urzędu albo na wniosek przewodniczącego Kolegium, postępowanie w sprawie uznania dostawcy sprzętu lub oprogramowania, które są wykorzystywane przez: 1) podmioty kluczowe lub podmioty ważne, z wyłączeniem podsektora komunikacji elektronicznej, 2) przedsiębiorców komunikacji elektronicznej, których roczne przychody z tytułu wykonywania działalności telekomunikacyjnej w poprzednim roku obrotowym były wyższe od kwoty 10 milionów złotych, 3) podmioty finansowe, z wyłączeniem podmiotów określonych w art. 16 rozporządzenia 2022/2554 – za dostawcę wysokiego ryzyka. 2. Do postępowania w sprawie uznania za dostawcę wysokiego ryzyka, jeżeli ustawa nie stanowi inaczej, stosuje się przepisy ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego, z wyłączeniem art. 28, art. 31, art. 51, art. 66a i art. 79 tej ustawy. 3. Stroną postępowania w sprawie uznania za dostawcę wysokiego ryzyka jest każdy, wobec kogo zostało wszczęte postępowanie w sprawie uznania za dostawcę wysokiego ryzyka. 4. Do postępowania w sprawie uznania za dostawcę wysokiego ryzyka może przystąpić, na wniosek, na prawach strony, przedsiębiorca telekomunikacyjny mający siedzibę na terytorium Rzeczypospolitej Polskiej wpisany do rejestru przedsiębiorców telekomunikacyjnych, który	Projektowane przepisy wprowadzają możliwość wydawania przez Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa rekomendacji określających środki techniczne i organizacyjne stosowane w celu zwiększania poziomu bezpieczeństwa systemów informacyjnych podmiotów krajowego systemu cyberbezpieczeństwa. Wprowadza się instytucję postępowania w sprawie uznania za dostawcę wysokiego ryzyka, co stanowi wdrożenie unijnego Toolboxa 5g. Wprowadza się także kwestie dotyczące monitorowania przez organy właściwe do spraw cyberbezpieczeństwa wykonania polecenia zabezpieczającego. Wprowadza się także możliwość przekazania niektórych zadań CSIRT poziomu krajowego Ministrowi Obrony Narodowej.

	w poprzednim roku obrotowym uzyskał przychód z tytułu prowadzenia działalności telekomunikacyjnej w wysokości co najmniej dwudziestotysięcznej krotności przeciętnego wynagrodzenia w gospodarce narodowej wskazanego w ostatnim komunikacie Prezesa Głównego Urzędu Statystycznego, o którym mowa w art. 20 pkt 1 lit. a ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych (Dz. U. z 2024 r. poz. 1631 i 1674 oraz z 2025 r. poz. 718, 769 i 1159). Przepisy art. 31 § 2 i 3 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego stosuje się odpowiednio. 5. Za poprzedni rok obrotowy uznaje się rok, przed którym postępowanie zostało wszczęte. Za ostatni komunikat Prezesa Głównego Urzędu Statystycznego uznaje się ostatni komunikat Prezesa Głównego Urzędu Statystycznego przed wszczęciem postępowania. 6. Minister właściwy do spraw informatyzacji zawiadamia o wszczęciu postępowania w sprawie uznania za dostawcę wysokiego ryzyka. Zawiadomienie udostępnia się także na stronie podmiotowej Biuletynu Informacji Publicznej ministra właściwego do spraw informatyzacji, niezwłocznie po doręczeniu tego zawiadomienia. 7. Minister właściwy do spraw informatyzacji zawiadamia Prokuratora Generalnego o wszczęciu postępowania w sprawie uznania za dostawcę wysokiego ryzyka. 8. Jeżeli dostawcą sprzętu lub oprogramowania jest strona niemająca siedziby na terytorium państwa członkowskiego Unii Europejskiej, Konfederacji Szwajcarskiej albo państwa członkowskiego Europejskiego Porozumienia o Wolnym Handlu (EFTA) – stronie umowy o Europejskim Obszarze Gospodarczym zawiadomienie, o którym mowa w ust. 6, publikuje się na stronie podmiotowej Biuletynu Informacji Publicznej ministra właściwego do spraw informatyzacji. Udostępnienie ma skutek doręczenia zawiadomienia stronie po upływie 14 dni od dnia jego dokonania. 9. W terminie 14 dni od dnia opublikowania na stronie podmiotowej Biuletynu Informacji Publicznej ministra właściwego do spraw informatyzacji zawiadomienia, o którym mowa w ust. 6 i 8, organizacja społeczna może przedstawić ministrowi właściwemu do spraw	

	informatyzacji stanowisko co do dostawcy sprzętu lub oprogramowania, wobec którego wszczęto postępowanie, oraz dostarczanych przez niego produktów ICT, usług ICT oraz procesów ICT. Minister właściwy do spraw informatyzacji, przed wydaniem decyzji, publikuje na swojej stronie podmiotowej Biuletynu Informacji Publicznej raport ze złożonych w terminie stanowisk, wskazując w szczególności główne uwagi zawarte w stanowiskach. 10. Przed wydaniem decyzji minister właściwy do spraw informatyzacji zasięga opinii Kolegium. Kolegium przekazuje opinię w terminie 3 miesięcy od dnia wystąpienia o opinię. Okresu od dnia wystąpienia o opinię do Kolegium do dnia jej otrzymania nie wlicza się do terminu załatwienia sprawy. Przepisu art. 106 § 5 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego nie stosuje się. 11. Opinia, o której mowa w ust. 10 zdanie pierwsze, zawiera analizę: 1) zagrożeń bezpieczeństwa narodowego o charakterze ekonomicznym, wywiadowczym i terrorystycznym oraz zagrożeń dla realizacji zobowiązań sojuszniczych i europejskich, jakie stanowi dostawca sprzętu i oprogramowania, z uwzględnieniem informacji o zagrożeniach uzyskanych od państw członkowskich Unii Europejskiej lub organów Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego; 2) prawdopodobieństwa z jakim dostawca sprzętu lub oprogramowania znajduje się pod kontrolą państwa spoza terytorium Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, z uwzględnieniem: a) przepisów prawa regulujących stosunki między dostawcą sprzętu lub oprogramowania, a tym państwem oraz praktyki stosowania prawa w tym zakresie, b) prawodawstwa oraz stosowania prawa w zakresie ochrony danych osobowych, w szczególności w przypadku, gdy nie ma porozumień w zakresie ochrony tych danych między Unią Europejską i tym państwem, c) struktury własnościowej dostawcy sprzętu lub oprogramowania, d) zdolności ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania; 3) powiązań dostawcy sprzętu lub oprogramowania z podmiotami określonymi w załączniku do rozporządzenia Rady (UE) 2019/796 z dnia	

	17 maja 2019 r. w sprawie środków ograniczających w celu zwalczania cyberataków zagrażających Unii lub jej państwom członkowskim (Dz. Urz. UE L 129I z 17.05.2019, str. 1, z późn. zm.); 4) liczby i rodzajów wykrytych podatności i incydentów dotyczących typów produktów ICT lub rodzajów usług ICT lub konkretnych procesów ICT dostarczanych przez dostawcę sprzętu lub oprogramowania oraz sposobu i czasu ich eliminowania; 5) trybu i zakresu, w jakim dostawca sprzętu lub oprogramowania sprawuje nadzór nad procesem wytwarzania i dostarczania sprzętu lub oprogramowania dla podmiotów, o których mowa w ust. 1, oraz ryzyka dla procesu wytwarzania i dostarczania sprzętu lub oprogramowania; 6) treści wydanych rekomendacji, o których mowa w art. 33 ust. 4, dotyczących sprzętu lub oprogramowania danego dostawcy. 12. Sporządzając opinię, o której mowa w ust. 10 zdanie pierwsze, Kolegium uwzględni: 1) certyfikaty wydane dla produktów ICT, usług ICT lub procesów ICT, wydane lub uznawane w państwach członkowskich Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, w szczególności certyfikaty wydane w ramach europejskich programów certyfikacji cyberbezpieczeństwa; 2) analizy, o których mowa w art. 65a ust. 1 i 2. 13. Procedura sporządzenia opinii, o której mowa w ust. 10 zdanie pierwsze, przebiega w następujący sposób: 1) przewodniczący Kolegium powołuje zespół w celu opracowania projektu opinii w sprawie uznania dostawcy za dostawcę wysokiego ryzyka, zwany dalej „zespołem opiniującym”, w skład którego wchodzi przedstawiciele członków Kolegium wskazani przez przewodniczącego Kolegium; 2) każdy członek zespołu opiniującego przygotowuje stanowisko, w zakresie swojej właściwości, które następnie przekazuje zespołowi opiniującemu. W przypadku wystąpienia negatywnego sporu co do	

	zakresu właściwości spór rozstrzyga przewodniczący Kolegium wskazując właściwego członka zespołu opiniującego; 3) jeżeli nie zostały wykonane analizy, o których mowa w art. 65a ust. 1 i 2, przewodniczący Kolegium zleca ich wykonanie; 4) zespół opiniujący przedstawia przewodniczącemu Kolegium projekt opinii; 5) ustalenie opinii następuje na posiedzeniu Kolegium; 6) ustaloną opinię przewodniczący Kolegium przekazuje ministrowi właściwemu do spraw informatyzacji. 14. W zespole opiniującym może wziąć udział również przedstawiciel Prezesa Urzędu Ochrony Konkurencji i Konsumentów. W posiedzeniu Kolegium, na którym następuje ustalenie opinii, może wziąć udział Prezes lub Wiceprezes Urzędu Ochrony Konkurencji i Konsumentów. 15. Minister właściwy do spraw informatyzacji, w drodze decyzji, uznaje dostawcę sprzętu lub oprogramowania oraz podmioty wchodzące w skład grupy kapitałowej, w rozumieniu art. 3 ust. 1 pkt 44 ustawy z dnia 29 września 1994 r. o rachunkowości, w ramach której funkcjonuje dostawca, za dostawcę wysokiego ryzyka, jeżeli dostawca ten stanowi zagrożenie dla podstawowego interesu bezpieczeństwa państwa. 16. Decyzja, o której mowa w ust. 15, zawiera w szczególności wskazanie typów produktów ICT, rodzajów usług ICT lub konkretnych procesów ICT pochodzących od dostawcy sprzętu lub oprogramowania uwzględnionych w postępowaniu w sprawie uznania za dostawcę wysokiego ryzyka. 17. Minister właściwy do spraw informatyzacji ogłasza decyzję, o której mowa w ust. 15, w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski” oraz publikuje na stronie podmiotowej Biuletynu Informacji Publicznej ministra właściwego do spraw informatyzacji, a także na stronie internetowej urzędu obsługującego tego ministra. 18. Decyzja, o której mowa w ust. 15, podlega natychmiastowemu wykonaniu. 19. Od decyzji, o której mowa w ust. 15, nie przysługuje wniosek o ponowne rozpatrzenie sprawy. Art. 67d. 1. Podmioty kluczowe lub podmioty ważne, są obowiązane przekazać informacje na wniosek uprawnionych organów, o których	

	mowa w ust. 2, o wycofywanych typach produktów ICT, rodzajach usług ICT i konkretnych procesach ICT w zakresie objętym decyzją, o której mowa w art. 67b ust. 15. 2. Uprawnionymi organami do uzyskania informacji, o których mowa w ust. 1, są organy właściwe do spraw cyberbezpieczeństwa. 3. Wniosek, o którym mowa w ust. 1, zawiera: 1) wskazanie podmiotu obowiązującego do przekazania informacji; 2) datę wydania decyzji, o której mowa w art. 67b ust. 15; 3) wskazanie zakresu żądanych informacji; 4) wskazanie terminu przekazania informacji adekwatnego do zakresu tego żądania, nie krótszego niż 7 dni; 5) uzasadnienie; 6) pouczenie o zagrożeniu karą, o której mowa w art. 73. 4. Minister właściwy do spraw informatyzacji może zwrócić się do organów właściwych do spraw cyberbezpieczeństwa, aby uzyskały informacje, o których mowa w ust. 1. 5. Na wniosek ministra właściwego do spraw informatyzacji organ właściwy do spraw cyberbezpieczeństwa przekazuje uzyskane informacje, o których mowa w ust. 1, temu ministrowi. Art. 67e. 1. Sąd administracyjny rozpatruje skargę na decyzję, o której mowa w art. 67b ust. 15, na posiedzeniu niejawnym w składzie trzech sędziów. 2. Odpis sentencji wyroku z uzasadnieniem doręcza się wyłącznie ministrowi właściwemu do spraw informatyzacji. Skarżącemu doręcza się odpis wyroku z tą częścią uzasadnienia, która nie zawiera informacji niejawnych w rozumieniu przepisów o ochronie informacji niejawnych. Art. 67f. Minister właściwy do spraw informatyzacji publikuje na stronie podmiotowej Biuletynu Informacji Publicznej urzędu go obsługującego listę produktów ICT, usług ICT i konkretnych procesów ICT objętych decyzjami, o których mowa w art. 67b ust. 15. Art. 67h. Podmioty, których dotyczy polecenie zabezpieczające, są obowiązane przekazać informacje na wniosek organów właściwych do spraw cyberbezpieczeństwa, o wykonywaniu polecenia zabezpieczającego. Przepisy art. 67c ust. 2–5 stosuje się.	

	Art. 67i. 1. Skargę na polecenie zabezpieczające wnosi się w terminie 2 miesięcy od dnia, w którym komunikat o wydaniu polecenia zabezpieczającego został ogłoszony w dzienniku urzędowym ministra właściwego do spraw informatyzacji. 2. Sąd administracyjny zarządza połączenie wszystkich oddzielnych spraw toczących się przed nim w celu ich łącznego rozpoznania i rozstrzygnięcia, jeżeli dotyczą tej samej decyzji. 3. Wniosek o przywrócenie terminu na złożenie skargi jest niedopuszczalny. Art. 67j. 1. Do Narodowego Banku Polskiego nie stosuje się przepisów art. 67b, art. 67f oraz art. 67g. 2. Minister właściwy do spraw informatyzacji przekazuje niezwłocznie Prezesowi Narodowego Banku Polskiego informacje o decyzjach wydanych na podstawie art. 67b ust. 15 oraz art. 67f ust. 1. Art. 67k. 1. Do podmiotów finansowych niebędących podmiotami kluczowymi lub podmiotami ważnymi stosuje się przepisy art. 67c, art. 67d, art. 67g oraz art. 67h. 2. Obowiązków, o których mowa w ust. 1, nie stosuje się wobec podmiotów finansowych niebędących podmiotami kluczowymi lub podmiotami ważnymi, do których stosuje się art. 16 ust. 1 rozporządzenia 2022/2554. 3. Nadzór nad wykonywaniem obowiązków, o których mowa w ust. 1, sprawuje organ właściwy do spraw cyberbezpieczeństwa dla sektora bankowości i infrastruktury rynków finansowych. 4. Do nadzoru i kontroli wykonywania obowiązków wymienionych w ust. 1, oraz do kar pieniężnych nakładanych za naruszenia tych obowiązków, odpowiednio stosuje się przepisy rozdziałów 11 i 14. Art. 67l. 1. Prezes Rady Ministrów, działając na podstawie rekomendacji Kolegium, w uzgodnieniu z Ministrem Obrony Narodowej, może czasowo powierzyć temu ministrowi realizację wybranych zadań, o których mowa w art. 26. 2. Powierzając realizację wybranych zadań, o których mowa w art. 26, określa się w szczególności: 1) zakres powierzonych zadań;	

	2) czas realizacji powierzonych zadań, nie dłuższy niż 1 rok, lub sposób ich odwołania; 3) w razie potrzeby – szczególne zasady współpracy z CSIRT MON, CSIRT NASK i CSIRT GOV; 4) zasady informowania Kolegium o stanie realizacji powierzonych zadań. 3. Realizacja zadań, o których mowa w ust. 1, jest dokonywana przez Ministra Obrony Narodowej z wykorzystaniem jednostek mu podległych lub przez niego nadzorowanych, z uwzględnieniem art. 12a ustawy z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (Dz. U. z 2025 r. poz. 504). 4. Prezesa Rady Ministrów wydaje komunikat o powierzeniu realizacji zadań, o których mowa w ust. 1, i niezwłocznie ogłasza go w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski”. Informacja o komunikacie jest udostępniana również na stronach internetowych CSIRT MON, CSIRT NASK, CSIRT GOV lub na stronie podmiotowej Biuletynu Informacji Publicznej Pełnomocnika.”;	
Art. 1 pkt 82 lit. a (w zakresie art. 73 ust. 1 pkt 18-20)	82) w art. 73: a) ust. 1 otrzymuje brzmienie: „1. Karze pieniężnej podlega podmiot kluczowy lub podmiot ważny, który (...): 18) nie wykonuje obowiązków, o których mowa w art. 67c ust. 1, 2, 4 i 5; 19) nie wdrożył w terminie określonym w poleceniu zabezpieczającym, o którym mowa w art. 67g ust. 9 pkt 3, określonego zachowania, o którym mowa w art. 67g ust. 10; 20) odstąpił od wykonywania zawartego w poleceniu zabezpieczającym, o którym mowa w art. 67g ust. 9, określonego zachowania, o którym mowa w art. 67g ust. 10, przed wygaśnięciem polecenia zabezpieczającego.”,	Wprowadza się kary za nie wdrożenie polecenia zabezpieczającego oraz nie wycofanie sprzętu pochodzącego od dostawcy wysokiego ryzyka.
Art. 1 pkt 88	88) w art. 93 uchyla się ust. 8 i 23;	Uchyla się przepisy dotyczące maksymalnego limitu wydatków dla części budżetowej Komisji Nadzoru Finansowego, ponieważ ta część już nie istnieje. Przepis nie nakłada obowiązków na przedsiębiorców.

Art. 1 pkt 90	90) dodaje się załącznik nr 3 i 4.	Załącznik nr 3 określa funkcje krytyczne. Jest on oparty na rozwiązaniach innych państw europejskich, zwłaszcza francuskiej liście funkcji krytycznych. Załącznik ten wskazuje funkcje, których narażenie szczególnie zagroziłoby systemowi czy sieci, w ramach której funkcjonują. Produkty, usługi lub procesy pochodzące od dostawcy wysokiego ryzyka muszą być wycofane w pierwszej kolejności co odzwierciedla krótszy termin na wykonanie tego obowiązku. Załącznik nr 4 obejmuje uproszczone wymagania dla samorządowych podmiotów publicznych, które są podmiotami ważnymi. Mają one charakter listy kontrolnej minimalnych wymogów, takich jak inwentaryzacja zasobów informatycznych, weryfikacja uprawnień personelu, stosowanie oprogramowania antywirusowego czy stosowanie zasad cyberhigieny. Zrezygnowano więc z podejścia opartego na ryzyku, ponieważ wymagałoby to najpierw posiadania odpowiedniego personelu przez mniejsze jednostki samorządowe, który potrafiłby przeprowadzić szacowanie ryzyka i na podstawie tego wprowadzić odpowiednie środki techniczne i organizacyjne. Mniejsze jednostki samorządowe nie posiadają takich zasobów osobowych, stąd obniżono wymagania z zakresu cyberbezpieczeństwa.
Art. 2	Art. 2. W ustawie z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2025 r. poz. 1153) wprowadza się następujące zmiany: 1) w art. 10a: a) po pkt 2 dodaje się pkt 2a w brzmieniu: „2a) spółkom, o których mowa w art. 9 ust. 1 ustawy z dnia 20 grudnia 1996 r. o gospodarce komunalnej (Dz. U. z 2021 r. poz. 679),” b) pkt 3 otrzymuje brzmienie: „3a) innym zaliczanym do sektora finansów publicznych gminnym osobom prawnym utworzonym na podstawie odrębnych ustaw w celu wykonywania zadań publicznych, z wyłączeniem przedsiębiorstw, instytutów badawczych i banków”;	Przepis umożliwia powierzenie wspólnej obsługi samorządowych jednostek organizacyjnych także gminnym spółkom prawa handlowego realizującym zadania z zakresu gospodarki komunalnej.

	2) w art. 10b ust. 1 otrzymuje brzmienie: „1. Wspólną obsługę mogą prowadzić urząd gminy, inna jednostka organizacyjna gminy, jednostka organizacyjna związku międzygminnego, jednostka organizacyjna związku powiatowo-gminnego albo spółka, o której mowa w art. 9 ust. 1 ustawy z dnia 20 grudnia 1996 r. o gospodarce komunalnej, w tym spółka prawa handlowego powołana w celu prowadzenia wspólnej obsługi, zwane dalej „jednostkami obsługującymi”.”.	
Art. 3	Art. 3. W ustawie z dnia 21 marca 1991 r. o obszarach morskich Rzeczypospolitej Polskiej i administracji morskiej (Dz. U. z 2024 r. poz. 1125 oraz z 2025 r. poz. 409) w art. 27d w ust. 2a wyrazy „o której mowa w załączniku nr 2 do ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2023 r. poz. 913 i 1703 oraz z 2024 r. poz. 834)” zastępuje się wyrazami „umożliwiającej dostęp do skalowalnego i elastycznego zbioru zasobów obliczeniowych do wspólnego wykorzystywania przez wielu użytkowników”.	Zmiany dotyczą wprowadzenia pojęcia usługi przetwarzania w chmurze, ponieważ obecnie występuje odwołanie do obecnego załącznika nr 2 ustawy o KSC – który jest zmieniany. Przepis nie nakłada obowiązków na przedsiębiorców.
Art. 4	Art. 4. W ustawie z dnia 24 sierpnia 1991 r. o Państwowej Straży Pożarnej (Dz. U. z 2025 r. poz. 1312) wprowadza się następujące zmiany: 1) w art. 93 w ust. 1 w pkt 7 kropkę zastępuje się średnikiem i dodaje się pkt 8 w brzmieniu: „8) świadczenie teleinformatyczne, o którym mowa w art. 5 ustawy z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1662 oraz z 2025 r. poz. 1017), zwane dalej „świadczeniem teleinformatycznym”.”; 2) po art. 97f dodaje się art. 97g w brzmieniu: „Art. 97g. 1. Strażakowi wykonującemu zadania z zakresu cyberbezpieczeństwa, o których mowa w art. 26, art. 42 ust. 1, art. 44 ust. 1, art. 62 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077 i 1222 oraz z 2025 r. poz. 1017, 1069 i), lub w zakresie zapewnienia cyberbezpieczeństwa w Państwowej Straży Pożarnej przyznaje się na okres ich wykonywania świadczenie teleinformatyczne. 2. Do ustalenia wysokości świadczenia teleinformatycznego stosuje się przepisy wydane na podstawie art. 8 ust. 1 ustawy z dnia 2 grudnia 2021	Przepis umożliwia przyznanie strażakowi świadczenia teleinformatycznego za realizację zadań z zakresu cyberbezpieczeństwa. Przepis nie nakłada obowiązków na przedsiębiorców.

	r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa. 3. Decyzję o przyznaniu świadczenia teleinformatycznego wydaje przełożony uprawniony do mianowania lub powołania nie później niż w terminie 30 dni po rozpoczęciu przez strażaka wykonywania zadań, o których mowa w ust. 1. 4. Przed wydaniem decyzji, o której mowa w ust. 3, strażak podlega opiniowaniu służbowemu na zasadach, o których mowa w art. 36a, jeżeli od dnia wydania ostatniej opinii o tym strażaku upłynęły co najmniej 3 miesiące. 5. Świadczenia teleinformatycznego nie przyznaje się w przypadkach, o których mowa w art. 97e ust. 6. Przepisy art. 97e ust. 7 i 8 stosuje się. 6. Świadczenia teleinformatycznego nie wypłaca się w przypadkach, o których mowa w art. 97e ust. 9. 7. Do wypłaty świadczenia teleinformatycznego stosuje się przepisy art. 97e ust. 9.”.	
Art. 5	Art. 5. W ustawie z dnia 20 sierpnia 1997 r. o Krajowym Rejestrze Sądowym (Dz. U. z 2025 r. poz. 869) wprowadza się następujące zmiany: 1) w art. 4d: a) w ust. 2 w pkt 3 kropkę zastępuje się średnikiem i dodaje się pkt 4 w brzmieniu: „4) w wykazach prowadzonych przez organy właściwe do spraw cyberbezpieczeństwa na podstawie art. 42 ust. 11 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077 i 1222 oraz z 2005 r. poz. 1017, 1069 i ...).”; b) w ust. 5 w pkt 4 dodaj się przecinek i pkt 5 w brzmieniu: „5) w art. 53 ust. 9 pkt 6 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa”; 2) w art. 21 dodaje się ust. 4 w brzmieniu: „4. Minister Sprawiedliwości, na podstawie wykazu, o którym mowa w art. 42 ust. 12 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, przekazuje sądowi rejestrowemu, za pośrednictwem systemu teleinformatycznego, po otrzymaniu żądania z tego systemu, informacje o osobach objętych zakazem pełnienia w	Przepis umożliwia wymianę między organami właściwym do spraw cyberbezpieczeństwa, a sądami powszechnymi informacji o osobach objętych zakazem pełnienia w podmiocie kluczowym funkcji zarządczych na podstawie decyzji organów właściwych do spraw cyberbezpieczeństwa. Przepis nie nakłada obowiązków na przedsiębiorców.

	podmiocie kluczowym funkcji zarządczych na podstawie decyzji organów właściwych do spraw cyberbezpieczeństwa.”.	
Art. 6	Art. 6. W ustawie z dnia 29 sierpnia 1997 r. – Ordynacja podatkowa (Dz. U. z 2025 r. poz. 111, z późn. zm.) po art. 299h dodaje się art. 299i w brzmieniu: „Art. 299i. § 1. Szef Krajowej Administracji Skarbowej udostępnia nieodpłatnie organom właściwym do spraw cyberbezpieczeństwa oraz Zespołowi Reagowania na Incydynty Bezpieczeństwa Komputerowego działającemu na poziomie krajowym, prowadzonemu przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy nieodpłatnie, w drodze teletransmisji, bez konieczności składania każdorazowo pisemnych wniosków o udostępnienie, dane w zakresie niezbędnym do dokonania przez te podmioty weryfikacji wielkości przedsiębiorstwa zgodnie z art. 5 ust. 1 i ust. 2 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077 i 1222 oraz z 2025 r. poz. 1017, 1069 i ...). § 2. Dane, o których mowa w § 1, obejmują roczne zatrudnienie, a także roczny obrót netto ze sprzedaży towarów, wyrobów i usług oraz z operacji finansowych. § 3. Sposób udostępniania danych, o których mowa w § 1, określają porozumienia zawarte pomiędzy Szefem Krajowej Administracji Skarbowej a podmiotami, o których mowa w § 1.”.	Przepis dotyczy umożliwienia organom podatkowym przekazywania informacji organom właściwym do spraw cyberbezpieczeństwa oraz Zespołowi Reagowania na Incydynty Bezpieczeństwa Komputerowego działającemu na poziomie krajowym, prowadzonemu przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy. Dane te są niezbędne do realizacji ustawowych zadań tych podmiotów, a w szczególności do oceny czy dany podmiot spełnia przesłanki bycia podmiotem kluczowym lub ważnym oraz co do jego znaczenia w danym sektorze gospodarki. Przepis nie nakłada obowiązków na przedsiębiorców.
Art. 7	Art. 7. W ustawie z dnia 5 czerwca 1998 r. o samorządzie województwa (Dz. U. z 2025 r. poz. 581) wprowadza się następujące zmiany: 1) w art. 8c: a) po pkt 2 dodaje się pkt 2a w brzmieniu: „2a) spółkom, o których mowa w art. 9 ust. 1 ustawy z dnia 20 grudnia 1996 r. o gospodarce komunalnej (Dz. U. z 2021 r. poz. 679),” b) pkt 3 otrzymuje brzmienie: „3) innym zaliczanym do sektora finansów publicznych wojewódzkim osobom prawnym utworzonym na podstawie odrębnych ustaw w celu wykonywania zadań publicznych, z wyłączeniem przedsiębiorstw, instytutów badawczych i banków”; 2) w art. 8d ust. 1 otrzymuje brzmienie:	Przepis umożliwia powierzenie wspólnej obsługi samorządowych jednostek organizacyjnych także wojewódzkim spółkom prawa handlowego realizującym zadania zakresu gospodarki komunalnej.

	„1. Wspólną obsługę mogą prowadzić urząd marszałkowski, inna wojewódzka samorządowa jednostka organizacyjna albo spółka, o której mowa w art. 9 ust. 1 ustawy z dnia 20 grudnia 1996 r. o gospodarce komunalnej, w tym spółka prawa handlowego powołana w celu prowadzenia wspólnej obsługi, zwane dalej „jednostkami obsługującymi.”.	
Art. 8	Art. 8. W ustawie z dnia 5 czerwca 1998 r. o samorządzie powiatowym (Dz. U. z 2024 r. poz. 107 i 1907) wprowadza się następujące zmiany: 1) w art. 6a: a) po pkt 2 dodaje się pkt 2a w brzmieniu: „2a) spółkom, o których mowa w art. 9 ust. 1 ustawy z dnia 20 grudnia 1996 r. o gospodarce komunalnej (Dz. U. z 2021 r. poz. 679),” b) pkt 3 otrzymuje brzmienie: „3) innym zaliczanym do sektora finansów publicznych powiatowym osobom prawnym utworzonym na podstawie odrębnych ustaw w celu wykonywania zadań publicznych, z wyłączeniem przedsiębiorstw, instytutów badawczych i banków”; 2) w art. 6b ust. 1 otrzymuje brzmienie: „1. Wspólną obsługę mogą prowadzić starostwo powiatowe, inna jednostka organizacyjna powiatu, jednostka organizacyjna związku powiatów, jednostka organizacyjna związku powiatowo-gminnego albo spółka, o której mowa w art. 9 ust. 1 ustawy o gospodarce komunalnej, w tym spółka prawa handlowego powołana w celu prowadzenia wspólnej obsługi, zwane dalej „jednostkami obsługującymi.”.	Przepis umożliwia powierzenie wspólnej obsługi samorządowych jednostek organizacyjnych także powiatowym spółkom prawa handlowego realizującym zadania zakresu gospodarki komunalnej.
Art. 9	Art. 9. W ustawie z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych (Dz. U. z 2025 r. poz. 350, z późn. zm.) w art. 50 dodaje się ust. 28 w brzmieniu: „28. Zakład udostępnia organom właściwym do spraw cyberbezpieczeństwa i Zespołowi Reagowania na Incydynty Bezpieczeństwa Komputerowego działającemu na poziomie krajowym, prowadzonemu przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy, drogą elektroniczną, dane obejmujące roczną liczbę ubezpieczonych, którzy zostali zgłoszeni przez płatnika, w zakresie niezbędnym do realizacji ich ustawowych zadań. Dane, o których mowa w zdaniu pierwszym, obejmują ubezpieczonych zgłoszonych przez	Przepis umożliwia organom właściwym do spraw cyberbezpieczeństwa uzyskiwanie informacji o rocznej liczbie pracowników lub rocznej liczbie ubezpieczonych – co pozwoli na ustalenie wielkości przedsiębiorcy, a co za tym idzie statusu podmiotu kluczowego lub podmiotu ważnego. Przepis nie nakłada obowiązków na przedsiębiorców.

	płatnika do Zakładu od dnia 1 stycznia do dnia 31 grudnia danego roku. Udostępnienie informacji następuje nieodpłatnie.”.	
Art. 10	Art. 10. W ustawie z dnia 24 maja 2000 r. o Krajowym Rejestrze Karnym (Dz. U. z 2024 r. poz. 276 oraz z 2025 r. poz. 1235) w art. 6 w ust. 1 po pkt 10a dodaje się pkt 10b w brzmieniu: „10b) podmiotom kluczowym lub podmiotom ważnym w rozumieniu art. 5 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077 i 1222 oraz z 2025 r. poz. 1017, 1069 i ...) w zakresie niezbędnym do weryfikacji niekaralności osoby realizującej zadania, o których mowa w art. 8 i 11 tej ustawy;”.	Zmiany wynikają z wprowadzenia obowiązku weryfikacji niekaralności osób realizujących zadania z zakresu cyberbezpieczeństwa.
Art. 11	Art. 11. W ustawie z dnia 21 grudnia 2000 r. o dozorze technicznym (Dz. U. z 2024 r. poz. 1194) w art. 37 w pkt 21 kropkę zastępuje się średnikiem i dodaje się pkt 22 w brzmieniu: „22) wykonywanie zadań określonych w przepisach ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077 i 1222 oraz z 2025 r. poz. 1017, 1069 i ...), w szczególności w zakresie zadań powierzonych przez organ właściwy do spraw cyberbezpieczeństwa w ramach zadań CSIRT sektorowego.”.	Zmiany mają umożliwić urzędowi dozoru technicznego sprawną realizacją zadań CSIRT sektorowego.
Art. 12	Art. 12. W ustawie z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (Dz. U. z 2025 r. poz. 504) po art. 12 dodaje się art. 12a w brzmieniu: „Art. 12a. W celu zabezpieczenia realizacji przewidzianych w art. 26 ust. 1a i ust. 3, art. 41 pkt 6 i pkt 9, art. 41a ust. 2, art. 44, art. 51, art. 52, art. 52f, ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077 i 1222 oraz z 2025 r. poz. 1017, 1069 i ...) zadań CSIRT MON oraz zadań Ministra Obrony Narodowej, Minister Obrony Narodowej, w drodze decyzji niepodlegającej ogłoszeniu, wydzieli z Dowództwa Komponentu Wojsk Obrony Cyberprzestrzeni oraz z jednostek podporządkowanych Dowódcy Komponentu Wojsk Obrony Cyberprzestrzeni zespoły specjalistów oraz zasoby materiałowe i sprzętowe, które będą podlegać Ministrowi Obrony Narodowej w przypadku mianowania Naczelnego Dowódcy Sił Zbrojnych i przejęcia przez niego dowodzenia Siłami Zbrojnymi.”.	Przepis wprowadza możliwość zabezpieczenia realizacji zadań Ministra Obrony Narodowej w wypadku mianowania Naczelnego Dowódcy Sił Zbrojnych poprzez wyodrębnienie zespołów specjalistów, zasobów materiałowych i sprzętowych, które będą podlegać MON. Przepis nie nakłada obowiązków na przedsiębiorców.

Art. 13	Art. 13. W ustawie z dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym (Dz. U. z 2025 r. poz. 640 i 1069) wprowadza się następujące zmiany: 1) w art. 18zg: a) w ust. 2 pkt 1 i 2 otrzymują brzmienie: „1) podmiotu finansowego będącego podmiotem kluczowym, 2) podmiotu finansowego będącego podmiotem ważnym – w rozumieniu art. 5 ust. 1 i ust. 2 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.”, b) w ust. 3 wyrazy „, o którym mowa w ust. 4 i 5” zastępuje się wyrazami „kluczowym lub podmiotem ważnym”, c) uchyla się ust. 4 i 5; 2) w art. 19 ust. 6 otrzymuje brzmienie: „6. Z przychodów, o których mowa w ust. 2, pokrywa się koszty funkcjonowania Urzędu Komisji i jego organów oraz koszty realizacji zadań Komisji wynikających z ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.”.	Przepis uzupełnia regulacje dotyczące przychodów Urzędu Komisji Nadzoru Finansowego o dotacje z budżetu państwa służące realizacji zadań organu właściwego do spraw cyberbezpieczeństwa oraz CSIRT sektorowego w sektorze bankowości i infrastruktury rynków finansowych.
Art. 14	Art. 14. W ustawie z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz. U. z 2025 r. poz. 302 i 779) w art. 19 ust. 16 otrzymuje brzmienie: „16. Podmiot prowadzący rejestr medyczny określony w przepisach wydanych na podstawie art. 20 ust. 1 opracowuje, wdraża, nadzoruje, utrzymuje oraz w uzasadnionych przypadkach modyfikuje system zarządzania bezpieczeństwem informacji, zgodnie z wymogami określonymi w art. 8 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 11077 i 1222 oraz z 2025 r. poz. 1017, 1069 i ...).”.	Przepis wskazuje, że podmiot prowadzący rejestr medyczny ma obowiązek posiadać system zarządzania bezpieczeństwem informacji zgodny z ustawą o KSC.
Art. 16	Art. 16. W ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781) art. 104 otrzymuje brzmienie: „Art. 104. 1. Środki z administracyjnej kary pieniężnej stanowią dochód budżetu państwa, z uwzględnieniem ust. 2. 2. Środki z administracyjnej kary pieniężnej nałożonej za naruszenie art. 5 ust. 1 lit. f, art. 28 ust. 3 lit. c oraz art. 32 ust. 1 i 2 rozporządzenia 2016/679 stanowią w 50% dochód budżetu państwa, a w 50% dochód Funduszu Cyberbezpieczeństwa, o którym mowa w art. 2 ustawy o	Zmiany wzmocnią Fundusz Cyberbezpieczeństwa zwiększając jego przychody. Dzięki nim możliwe będzie zwiększenie środków przeznaczanych na realizację zadań z zakresu cyberbezpieczeństwa w organach administracji rządowej.

	szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1662 oraz z 2025 r. poz. 1017).”.	
Art. 17	Art. 17. W ustawie z dnia 11 września 2019 r. – Prawo zamówień publicznych (Dz. U. z 2024 r. poz. 1320, z późn. zm.) w art. 226 w ust. 1: 1) pkt 17 otrzymuje brzmienie: „17) obejmuje ona produkt ICT, usługę ICT lub proces ICT wskazane w rekomendacji, o której mowa w art. 33 ust. 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077 i 1222 oraz z 2025 r. poz. 1017, 1069 i ...), stwierdzającej ich negatywny wpływ na bezpieczeństwo państwa;”; 2) w pkt 18 kropkę zastępuje się średnikiem i dodaje się pkt 19 w brzmieniu: „19) obejmuje ona produkt ICT, którego typ został określony w decyzji w sprawie uznania dostawcy za dostawcę wysokiego ryzyka, o której mowa w art. 67b ust. 15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, lub usługę ICT, lub proces ICT, określone w tej decyzji.”.	Zmiana reguluje sytuacje, w której zamawiający odrzuca ofertę złożoną w ramach postępowania o zamówienie publiczne. Kolejną przesłanką odrzucenia oferty będzie sytuacja, gdy oferta obejmuje produkt ICT, którego typ został określony w decyzji w sprawie uznania dostawcy za dostawcę wysokiego ryzyka, o której mowa w art. 66a ust. 13 ustawy o KSC oraz usługę ICT lub proces ICT, określone w tej decyzji.
Art. 18	Art. 18. W ustawie z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1662 oraz z 2025 r. poz. 1017) wprowadza się następujące zmiany: 1) w art. 2: a) ust. 4: – pkt 1 otrzymuje brzmienie: „1) wpływy z kar pieniężnych, o których mowa w art. 73–73c ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077 i 1222 oraz z 2025 r. poz. 1017, 1069 i ...);”; – po pkt 1a dodaje się pkt 1b w brzmieniu: „1b) wpływy z kar pieniężnych, o których mowa w art. 101 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781 oraz z 2025 r. poz. ...);”; b) w ust. 9 po wyrazie „Funduszu” dodaje się wyrazy „na wypłatę świadczenia teleinformatycznego”; 2) w art. 3 w ust. 1 wprowadzenie do wyliczenia otrzymuje brzmienie:	Zmiany dotyczą: 1) wskazania, że świadczenie teleinformatyczne przysługuje pracownikom zatrudnionym w zespołach CSIRT sektorowych. Przepis nie nakłada obowiązków na przedsiębiorców; Przepis wskazuje, że świadczenie teleinformatyczne będzie przysługiwać również osobom realizującym zadania w zakresie zapewnienia cyberbezpieczeństwa w Urzędzie Ochrony Danych Osobowych oraz w jednostkach Krajowej Administracji Skarbowej. Przychody z kar pieniężnych o których mowa w art. 101 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych staną się jednym z przychodów Funduszu Cyberbezpieczeństwa. Zmiany te pozwolą zwiększyć przychody Funduszu Cyberbezpieczeństwa co pozwoli na zwiększenie wsparcia

	„Warunkiem ubiegania się o wsparcie ze środków Funduszu na wypłatę świadczenia teleinformatycznego, jest złożenie przez podmiot, o którym mowa w art. 5, wniosku do ministra właściwego do spraw informatyzacji, zawierającego:”; 3) w art. 4 w ust. 1 po wyrazie „wniosek” dodaje się wyrazy „, o którym mowa w art. 3 ust. 1,”; 4) w art. 5: a) pkt 1 otrzymuje brzmienie: „1) w CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT sektorowych, organach właściwych do spraw cyberbezpieczeństwa lub w urzędzie obsługującym Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa, o których mowa odpowiednio w art. 26, art. 41, art. 44 lub art. 60 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;”; b) w pkt 2 w lit. n dodaje się przecinek i dodaje się lit. o–zg w brzmieniu: „o) Generalnej Dyrekcji Dróg Krajowych i Autostrad, p) Głównym Inspektoracie Transportu Drogowego, q) Instytucie Badawczym Dróg i Mostów w Warszawie, r) Instytucie Kolejnictwa w Warszawie, s) Instytucie Meteorologii i Gospodarki Wodnej – Państwowego Instytutu Badawczego, t) Instytucie Transportu Samochodowego w Warszawie, u) jednostkach organizacyjnych Krajowej Administracji Skarbowej, o których mowa w art. 36 ust. 1 pkt 3 i 5 ustawy z dnia 16 listopada 2016 r. o Krajowej Administracji Skarbowej (Dz. U. z 2025 r. poz. 1131), v) Państwowej Straży Pożarnej, w) Państwowym Gospodarstwie Wodnym Wody Polskie, x) sądach powszechnych, y)Transportowym Dozorze Technicznym, z) Urzędzie do spraw Cudzoziemców, za) Urzędzie Lotnictwa Cywilnego, zb) Urzędzie Morskim w Gdyni, zc) Urzędzie Morskim w Szczecinie, zd) Urzędzie Ochrony Danych Osobowych, ze) Urzędzie Żeglugi Śródlądowej w Bydgoszczy, zf) Urzędzie Żeglugi Śródlądowej w Szczecinie.	udzielanego organom administracji na zapewnienie cyberbezpieczeństwa ich systemów informacyjnych.

	zg) Urzędzie Żeglugi Śródlądowej we Wrocławiu.”; 5) po art. 26a dodaje się art. 26b w brzmieniu: „Art. 26b. Świadczenie teleinformatyczne żołnierzom zawodowym realizującym zadania z zakresu cyberbezpieczeństwa w urzędzie obsługującym Ministra Obrony Narodowej przyznaje i cofa Minister Obrony Narodowej.”; 6) w art. 27 w ust. 1 pkt 5–10 otrzymują brzmienie: „5) w 2026 r. – 351,922 mln zł; 6) w 2027 r. – 351,935 mln zł; 7) w 2028 r. – 351,964 mln zł; 8) w 2029 r. – 351,996 mln zł; 9) w 2030 r. – 352,030 mln zł; 10) w 2031 r. – 352,067 mln zł.”.	
Art. 19	Art. 19. W ustawie z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej (Dz. U. z 2024 r. poz. 1803) w art. 2 pkt 11 otrzymuje brzmienie: „11) podmiot publiczny – podmiot wskazany w sektorze podmiotów publicznych w załączniku nr 1 i 2 do ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;”.	Zmiana polega na zmianie definicji podmiotu publicznego.
Art. 20	Art. 20. W ustawie z dnia 12 lipca 2024 r. – Prawo komunikacji elektronicznej (Dz. U. z 2024 r. poz. 1221 oraz z 2025 r. poz. 637 i 820) w art. 40 w ust. 1 w pkt 2 w lit. b wyrazy „operatorów usług” zastępuje się wyrazem „podmiotów”.	Zmiana dotyczy dostosowania przepisów do nowej siatki pojęciowej zawartej w ustawie o KSC.
Art. 22	Art. 22. Operatorzy usług kluczowych, o których mowa w ustawie zmienianej w art. 1, stają się podmiotami kluczowymi, z dniem wejścia w życie niniejszej ustawy. 2. Do operatorów usług kluczowych, o których mowa w ust. 1, będących podmiotami podległymi lub nadzorowanymi przez Ministra Obrony Narodowej nie stosuje się art. 5 ust. 10 i 11 ustawy zmienianej w art. 1 w brzmieniu nadanym niniejszą ustawą.	Zmiana ta dostosuje przepisy do nowej siatki pojęciowej zawartej w ustawie o KSC.
Art. 23	Art. 23. Do obsługi incydentu, o której mowa w art. 11 pkt 1 ustawy zmienianej w art. 1, rozpoczętej i niezakończonej przed dniem wejścia w życie niniejszej ustawy, stosuje się przepisy dotychczasowe.	Przepis zagwarantuje ciągłość w zakresie obsługi incydentów.

Art. 24	Art. 24. 1. Do audytu, o którym mowa w art. 15 ust. 1 ustawy zmienianej w art. 1, przeprowadzanego i niezakończonego w dniu wejścia w życie niniejszej ustawy stosuje się przepisy dotychczasowe. 2. Do praktyki audytorów w zakresie audytu bezpieczeństwa systemów informacyjnych, o której mowa w art. 15 ust. 2 pkt 2 lit. b i c ustawy zmienianej w art. 1 w brzmieniu nadanym niniejszą ustawą zalicza się: 1) udokumentowane wykonanie w ciągu ostatnich 3 lat przed dniem rozpoczęcia audytu 3 audytów w zakresie bezpieczeństwa systemów informacyjnych lub ciągłości działania albo 2) wykonywanie audytów bezpieczeństwa systemów informacyjnych lub ciągłości działania w wymiarze czasu pracy nie mniejszym niż 1/2 etatu, związanych z przeprowadzaniem audytu wewnętrznego w zakresie bezpieczeństwa informacji, o którym mowa w przepisach wydanych na podstawie art. 18 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2024 r. poz. 1557 i 1717 oraz z 2025 r. poz. 1006,1019, 1158 i 1301) w brzmieniu przed dniem wejścia w życie niniejszej ustawy.	Przepis zagwarantuje ciągłość w zakresie audytów.
Art. 25	Art. 25. Do operatorów usług kluczowych, którzy wykonali audyt, o którym mowa w art. 15 ust. 1 ustawy zmienianej w art. 1, nie stosuje się art. 16 pkt 2 ustawy zmienianej w art. 1 w brzmieniu nadanym niniejszą ustawą.	Przepis ma pozwolić uniknąć nadmiernego obciążenia podmiotów, które wykonały swój obowiązek w zakresie audytu zgodnie z poprzednio obowiązującymi przepisami.
Art. 26	Art. 26. Do badania urządzenia informatycznego lub oprogramowania, o którym mowa w art. 33 ust. 1 ustawy zmienianej w art. 1, przeprowadzanego i niezakończonego przed dniem wejścia w życie niniejszej ustawy, stosuje się przepisy art. 33 ustawy zmienianej w art. 1 w brzmieniu nadanym niniejszą ustawą.	Przepisy przewidują rozszerzenie możliwości badania produktów przez zespoły CSIRT. Badaniu bezpieczeństwa nie mogą stać na drodze standardowe postanowienia licencji, które zakazują takich działań. Z tego względu w przepisach przejściowych dotyczących umów już obowiązujących konieczne było przesądzenie, że takie klauzule umowne utracą moc. Nie może być sytuacji, by umowa cywilnoprawna uniemożliwiała organom państwa skuteczne działania w zakresie bezpieczeństwa. W ramach zmian w funkcjonowaniu systemu S46 przewidziana jest rezygnacja z zawierania osobnych porozumień z przystępującymi obecnie podmiotami. Równocześnie w ramach tego systemu przyłączono już pewną liczbę podmiotów a ich prawa i obowiązki

		uregulowano w porozumieniach. W takim przypadku, dla zapewnienia efektywnej realizacji zadań, zasadnym jest utrzymanie tych porozumień w mocy.
Art. 27	Art. 27. 1. Rekomendacje Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa, o których mowa w art. 33 ust. 4 ustawy zmienianej w art. 1, wydane przed dniem wejścia w życie niniejszej ustawy zachowują moc. 2. Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa opublikuje dotychczas wydane rekomendacje na swojej stronie podmiotowej w Biuletynie Informacji Publicznej w terminie miesiąca od dnia wejścia w życie niniejszej ustawy. 3. Do rekomendacji Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa, o których mowa w art. 33 ust. 4 ustawy zmienianej w art. 1, wydanych przed dniem wejścia w życie niniejszej ustawy stosuje się przepisy dotychczasowe.	Przepis rozstrzyga status instytucji prawnej zmienionej przez przepisy ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw.
Art. 28	Art. 28. Do kontroli operatorów usług kluczowych i dostawców usług cyfrowych prowadzonych na podstawie art. 42 ust. 1 pkt 8 ustawy zmienianej w art. 1 w brzmieniu dotychczasowym wszczętych i niezakończonych przed dniem wejścia w życie niniejszej ustawy stosuje się przepisy dotychczasowe.	Przepis zagwarantuje ciągłość działań w obszarze kontroli podmiotów krajowego systemu cyberbezpieczeństwa.
Art. 29	Art. 29. Do postępowań administracyjnych w sprawie nałożenia kary pieniężnej, o której mowa w art. 73 ustawy zmienianej w art. 1, na operatora usługi kluczowej, dostawcę usługi cyfrowej albo kierownika operatora usługi kluczowej wszczętych i niezakończonych przed dniem wejścia w życie niniejszej ustawy stosuje się przepisy dotychczasowe.	Przepis zagwarantuje ciągłość w zakresie postępowań o nałożenie kar.
Art. 30	Art. 30. Do postępowań o udzielenie zamówienia publicznego wszczętych i niezakończonych przed dniem wejścia w życie niniejszej ustawy stosuje się przepis art. 226 ust. 1 pkt 17 ustawy zmienianej w art. 17 w brzmieniu nadanym niniejszą ustawą.	Przepis zagwarantuje ciągłość w zakresie prowadzonych postępowań o udzielenie zamówienia publicznego.
Art. 31	Art. 31. Sprawy związane z przeprowadzeniem postępowania konkursowego dotyczącego udzielenia pomocy <i>de minimis</i> wszczęte i niezakończone na podstawie art. 45a ustawy zmienianej w art. 1 w brzmieniu dotychczasowym są kontynuowane na podstawie przepisów dotychczasowych do czasu rozliczenia udzielonej pomocy <i>de minimis</i> .	Przepis gwarantuje ciągłość niezakończonych postępowań konkursowych dotyczących udzielenia pomocy <i>de minimis</i> .

Art. 32	Art. 32. Dotychczasowe przepisy wykonawcze wydane na podstawie: 1) art. 11 ust. 4 ustawy zmienianej w art. 1, zachowują moc do dnia wejścia w życie przepisów wykonawczych wydanych na podstawie art. 11 ust. 4 ustawy zmienianej w art. 1, 2) art. 66 ust. 9 ustawy zmienianej w art. 1, zachowują moc do dnia wejścia w życie przepisów wykonawczych wydanych na podstawie art. 66 ust. 9 ustawy zmienianej w art. 1 – jednak nie dłużej niż przez 12 miesięcy od dnia wejścia w życie niniejszej ustawy oraz mogą być zmieniane na podstawie tych przepisów.	Przepis przesądza utrzymanie w mocy dotychczasowych przepisów wykonawczych do czasu przyjęcia przepisów wykonawczych wydanych na podstawie zmienionej ustawy.
Art. 33	Art. 33. 1. Podmioty, które z dniem wejścia w życie niniejszej ustawy spełniają przesłanki uznania ich za podmiot kluczowy albo za podmiot ważny realizują obowiązki określone w rozdziale 3 ustawy zmienianej w art. 1, w brzmieniu nadanym niniejszą ustawą, w terminie 6 miesięcy od dnia wejścia w życie niniejszej ustawy. 2. Podmioty, które z dniem wejścia w życie niniejszej ustawy spełniają przesłanki uznania ich za podmiot kluczowy przeprowadzają pierwszy audyt, o którym mowa w art. 15 ust. 1 ustawy zmienianej w art. 1, w brzmieniu nadanym niniejszą ustawą, w terminie 24 miesięcy od dnia wejścia w życie niniejszej ustawy. 3. Podmioty, które z dniem wejścia w życie niniejszej ustawy spełniają przesłanki uznania ich za podmiot kluczowy albo za podmiot ważny, są obowiązane zarejestrować się w wykazie podmiotów kluczowych i podmiotów ważnych zgodnie z harmonogramem określonym w art. 34 ust. 3 pkt 1 niniejszej ustawy. 4. Podmioty kluczowe lub podmioty ważne, które przed dniem wejścia w życie ustawy były operatorami usług kluczowych zgłaszają incydenty poważne zgodnie z art. 11–art. 12b ustawy zmienianej w art. 1 w brzmieniu nadanym niniejszą ustawą w terminie 6 miesięcy od dnia wejścia w życie niniejszej ustawy. 5. Przedsiębiorcy telekomunikacyjni, którzy przed dniem wejścia w życie niniejszej ustawy realizowali obowiązki określone w dziale VIIa ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2024 r. poz. 34, 731 i 834), realizują te obowiązki na podstawie dotychczasowych przepisów do czasu rozpoczęcia realizacji obowiązków określonych w	Przepis wskazuje od kiedy podmioty kluczowe i ważne mają wykonywać obowiązki nałożone w ustawie i służy zapewnieniu im odpowiedniego okresu na dostosowanie do nowych przepisów.

	rozdziale 3 ustawy zmienianej w art. 1 w brzmieniu nadanym niniejszą ustawą. 6. Podmioty kluczowe lub podmioty ważne, które przed dniem wejścia w życie niniejszej ustawy były operatorami usług kluczowych do czasu wdrożenia systemu zarządzania bezpieczeństwem informacji zgodnego z art. 8 ustawy zmienianej w art. 1 w brzmieniu nadanym niniejszą ustawą, stosują system zarządzania bezpieczeństwem informacji zgodny z art. 8 ustawy zmienianej w art. 1 w brzmieniu dotychczasowym.	
Art. 34	Art. 34. 1. Minister właściwy do spraw informatyzacji utworzy wykaz podmiotów kluczowych i podmiotów ważnych, w terminie miesiąca od dnia wejścia w życie niniejszej ustawy². Minister właściwy do spraw informatyzacji wpisuje, z urzędu, do wykazu podmiotów kluczowych i podmiotów ważnych operatorów usług kluczowych wpisanych przed dniem wejścia w życie niniejszej ustawy do wykazu operatorów usług kluczowych. Przepis art. 7b ustawy zmienianej w art. 1 dodany niniejszą ustawą stosuje się odpowiedni³. Minister właściwy do spraw informatyzacji ogłasza w swoim dzienniku urzędowym, komunikat określający harmonogram¹ złożenia wniosków o wpis do wykazu podmiotów kluczowych i podmiotów ważnych przez podmioty kluczowe lub podmioty ważne, które w dniu wejścia w życie niniejszej ustawy spełniają przesłanki uznania ich za podmiot kluczowy albo podmiot ważny²) rozpoczęcia korzystania przez podmioty, o których mowa w pkt 1, z systemu teleinformatycznego, o którym mowa w art. 46 ust. 1 ustawy zmienianej w art. 1, w brzmieniu nadanym niniejszą ustawą. 4. W harmonogramie, o którym mowa w ust. 3, wskazuje się terminy dokonywania czynności przez poszczególne rodzaje podmiotów kluczowych lub podmiotów ważnych. 5. Komunikat, o którym mowa w ust. 3, może być zmieniany, jeżeli z powodów technicznych lub organizacyjnych niemożliwe jest dokonanie wpisów i rozpoczęcie korzystania z systemu teleinformatycznego, o którym mowa w art. 46 ust. 1, ustawy zmienianej w art. 1 przez podmioty kluczowe lub podmioty ważne w wyznaczonym harmonogramie.	Przepis określa od kiedy stosowany będzie system informacyjny w którym będzie prowadzony wykaz podmiotów kluczowych i ważnych.
Art. 35	Art. 35. Minister właściwy do spraw informatyzacji uruchomi funkcjonalności systemu teleinformatycznego, o których mowa w art. 46	Przepis wskazuje, że funkcjonalności systemu S46 w zakresie wspierania czynności nadzorczych oraz zgłaszania

	ust. 1 pkt 6 i 7 ustawy zmienianej w art. 1, w brzmieniu nadanym niniejszą ustawą, w terminie roku od dnia wejścia w życie niniejszej ustawy.	naruszeń ochrony danych osobowych minister uruchomi w terminie roku od dnia wejścia w życie ustawy.
Art. 36	Art. 36. Rejestr domen najwyższego poziomu (TLD) oraz podmiot świadczący usługi rejestracji nazw domen: 1) dostosowuje bazy danych dotyczących rejestracji nazw domen do wymagań określonych w art. 16b i art. 36c ustawy zmienianej w art. 1 dodany niniejszą ustawą, w terminie 6 miesięcy od dnia wejścia w życie niniejszej ustawy; 2) opracowuje i wdraża polityki i procedury, o których mowa w art. 16b i art. 16c ustawy zmienianej w art. 1 dodany niniejszą ustawą, w terminie 6 miesięcy od dnia wejścia w życie niniejszej ustawy.	Przepis reguluje okres dostosowawczy dla Rejestru domen najwyższego (TLD) oraz podmiotów świadczących usługi rejestracji nazw domen. Podmioty te mają 6 miesięcy od dnia wejścia w życie ustawy na dostosowanie się do nowych obowiązków dotyczących rejestracji nazw domen.
Art. 39	Art. 39. Postanowienia umów obowiązujących w dniu wejścia w życie niniejszej ustawy, uniemożliwiające przeprowadzenie badania, o którym mowa w art. 33 ust. 1b–1d ustawy zmienianej w art. 1 dodany niniejszą ustawą, są nieważne. 2. Porozumienia w sprawie korzystania z systemu teleinformatycznego, o którym mowa w art. 46 ust. 1 ustawy zmienianej w art. 1 w brzmieniu dotychczasowym, zawarte przed dniem wejścia w życie niniejszej ustawy, zachowują ważność do czasu ich wypowiedzenia. 3. Podmiot kluczowy i podmiot ważny będący stroną porozumienia w sprawie korzystania z systemu teleinformatycznego, o którym mowa w art. 46 ust. 1 ustawy zmienianej w art. 1 w brzmieniu dotychczasowym, może uwierzytelnić się w tym systemie za pomocą: 1) czynnika uwierzytelniania, o którym mowa w pkt 1 ppkt 2 lit. a załącznika do rozporządzenia wykonawczego Komisji (UE) nr 2015/1502 z dnia 8 września 2015 r. w sprawie ustanowienia minimalnych specyfikacji technicznych i procedur dotyczących poziomów bezpieczeństwa w zakresie środków identyfikacji elektronicznej na podstawie art. 8 ust. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (Dz. Urz. UE L 235 z 9.09.2015 r. str. 7), zwanego dalej „rozporządzeniem 2015/1502”, którym jest urządzenie wydane podmiotowi kluczowemu lub podmiotowi ważnemu przez ministra właściwego do spraw informatyzacji przed wejściem w życie niniejszej ustawy, oraz	Przepis reguluje ważność umów związanych z ustawą o KSC, które zostały zawarte przed wejściem w życie nowych przepisów.

	2) czynnika uwierzytelniania, o którym mowa w pkt 1 ppkt 2 lit. b załącznika do rozporządzenia 2015/1502, którym jest login oraz hasło.	
Art. 40	Art. 40. CSIRT MON, CSIRT NASK lub CSIRT GOV dostosują w terminie 3 miesięcy od dnia wejścia w życie niniejszej ustawy porozumienia, o których mowa w art. 26 ust. 10 ustawy zmienianej w art. 1 w brzmieniu dotychczasowym do przepisów art. 26 ustawy zmienianej w art. 1 w brzmieniu nadanym niniejszą ustawą.	W dotychczasowym stanie prawnym CSIRT MON, CSIRT NASK i CSIRT GOV mogły zawierać porozumienia przekazujące określone podmioty do właściwości CSIRT innego niż ten wskazany w ustawie o KSC. W związku ze zmianami w zakresie struktury podmiotowej krajowego systemu cyberbezpieczeństwa konieczne jest przesądzenie o sytuacji tych porozumień. Zawarte w ustawie rozwiązanie zapewniają podmiotom czas na dostosowanie tych porozumień do zmian w przepisach. Przepis nie nakłada obowiązków na przedsiębiorców.
Art. 41	Art. 41. 1. Organ właściwy do spraw cyberbezpieczeństwa ustanawia CSIRT sektorowy w terminie 18 miesięcy od dnia wejścia w życie niniejszej ustawy. 2. Organ właściwy do spraw cyberbezpieczeństwa ogłasza komunikat o osiągnięciu przez CSIRT sektorowy zdolności operacyjnej w swoim dzienniku urzędowym. 3. Informacja o osiągnięciu zdolności operacyjnej przez CSIRT sektorowy jest również publikowana na stronach internetowych: 1) ministerstwa albo innego urzędu administracji rządowej obsługującego Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa, 2) CSIRT MON, CSIRT NASK, CSIRT GOV – a także jest przekazywana za pomocą systemu teleinformatycznego, o którym mowa w art. 46 ust. 1 ustawy zmienianej w art. 1 w brzmieniu nadanym niniejszą ustawą.	Organy właściwe do spraw cyberbezpieczeństwa będą miały 18 miesięcy na utworzenie CSIRT sektorowych. Termin ten ma pozwolić na utworzenie nowych podmiotów, skompletowanie niezbędnej kadry oraz zapewnienie im zasobów do działań. Utworzenie CSIRT sektorowego podlega ogłoszeniu, w drodze komunikatu, w dzienniku urzędowym danego organu właściwego oraz na stronie internetowej m.in. Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa. Takie rozwiązanie pozwoli na precyzyjne określenie momentu od kiedy podmioty obowiązane będą miały realizować obowiązki do CSIRT sektorowych. Do tego czasu obowiązki te będą realizowane w stosunku do dotychczasowo właściwych CSIRT poziomu krajowego. Przepis nie nakłada obowiązków na przedsiębiorców.
Art. 42	Art. 42. 1. Do dnia wydania komunikatu, o którym mowa w art. 41 ust. 2 niniejszej ustawy, przez organ właściwy do spraw cyberbezpieczeństwa, o osiągnięciu przez właściwy CSIRT sektorowy zdolności operacyjnej, podmioty kluczowe lub podmioty ważne zgłaszają incydenty poważne zgodnie z art. 11–art. 12b ustawy zmienianej w art. 1 w brzmieniu nadanym niniejszą ustawą do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV.	Przepis służy zapewnieniu stosowania nowych przepisów do czasu osiągnięcia zdolności operacyjnej przez CSIRT sektorowe. W związku z tym, że ustawa przewiduje, że organy właściwe będą miały 18 miesięcy na powołanie CSIRT sektorowych konieczne jest uregulowanie do kogo podmioty kluczowe i ważne będą zgłaszać incydenty i przekazywać informacje do tego czasu.

	2. Podmiot kluczowy lub podmiot ważny zgłaszają incydenty poważne zgodnie z art. 11–art. 12b ustawy zmienianej w art. 1 w brzmieniu nadanym niniejszą ustawą do CSIRT sektorowego od dnia następującego po dniu opublikowania komunikatu o osiągnięciu przez właściwy CSIRT sektorowy zdolności operacyjnej. 3. Przepisów ust. 1 i 2 nie stosuje się w przypadku, gdy sektorowy zespół cyberbezpieczeństwa dla danego sektora został powołany przed 2025 r.	
Art. 43	Art. 43. W sprawozdaniu organu właściwego do spraw cyberbezpieczeństwa, o którym mowa w art. 44f ustawy zmienianej w art. 1 w brzmieniu nadanym niniejszą ustawą, które jest sporządzane za rok, w którym został utworzony CSIRT sektorowy, zawiera się informacje dotyczące utworzenia CSIRT sektorowego oraz jego funkcjonowania.	Przepis określa wygląd sprawozdania z działania CSIRT sektorowego w roku, w którym został on utworzony. W tym okresie podstawową kwestią będzie zapewnienie takiemu podmiotowi wszystkich narzędzi i zasobów niezbędnych do realizacji jego działań. Może on w tym okresie nie zrealizować swoich standardowych zadań. Z tego względu sprawozdanie to będzie zawierało kwestie związane z jego utworzeniem. Przepis nie nakłada obowiązków na przedsiębiorców.
Art. 44	Art. 44. Sektorowy zespół cyberbezpieczeństwa powołany na podstawie art. 44 ustawy zmienianej w art. 1 staje się CSIRT sektorowym, z dniem wejścia w życie niniejszej ustawy.	Powołane już sektorowe zespoły cyberbezpieczeństwa staną się z chwilą wejścia w życie ustawy CSIRT sektorowymi. Przepis ten pozwoli zapewnić pełną ciągłość ich działań. Przepis nie nakłada obowiązków na przedsiębiorców.

ZGŁOSZENIE ZAINTERESOWANIA PRACAMI NAD PROJEKTEM - ZGŁOSZENIE ZMIANY DANYCH*		
Projekt ustawy o zmianie niektórych ustaw o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) (tytuł projektu założeń projektu ustawy, projektu ustawy lub projektu rozporządzenia - zgodnie z jego treścią udostępnioną w Biuletynie Informacji Publicznej lub informacją zamieszczoną w wykazie prac legislacyjnych Rady Ministrów, Prezesa Rady Ministrów albo ministrów)		
A. OZNACZENIE PODMIOTU ZAINTERESOWANEGO PRACAMI NAD PROJEKTEM		
1. Nazwa/imię i nazwisko** KRZYSZTOF ROŻKO I WSPÓLNICY KANCELARIA PRAWNA SPÓŁKA KOMANDYTOWA		
2. Adres siedziby/adres miejsca zamieszkania** UL. WOJCIECHA GÓRSKIEGO 9, 00-033 WARSZAWA		
3. Adres do korespondencji i adres e-mail UL. WOJCIECHA GÓRSKIEGO 9, 00-033 WARSZAWA; BIURO@KRWLEGAL.PL		
B. WSKAZANIE OSÓB UPRAWNIONYCH DO REPREZENTOWANIA PODMIOTU WYMNIENIONEGO W CZĘŚCI A W PRACACH NAD PROJEKTEM		
Lp.	Imię i nazwisko	Adres
1	KRZYSZTOF ROŻKO	UL. WOJCIECHA GÓRSKIEGO 9, 00-033 WARSZAWA
2	TOMASZ KAMIŃSKI	UL. WOJCIECHA GÓRSKIEGO 9, 00-033 WARSZAWA
3	MARIUSZ BIAŁY	UL. WOJCIECHA GÓRSKIEGO 9, 00-033 WARSZAWA
4	NIKOLA JADWISZCZAK-NIEDBAŁKA	UL. WOJCIECHA GÓRSKIEGO 9, 00-033 WARSZAWA
5	BARTOSZ POSŁUSZNY	UL. WOJCIECHA GÓRSKIEGO 9, 00-033 WARSZAWA
C. OPIS POSTULOWANEGO ROZWIĄZANIA PRAWNEGO, ZE WSKAZANIEM INTERESU BĄDĄCEGO PRZEDMIOTEM OCHRONY		
1. POSTULOWANE ROZWIĄZANIA PRAWNE: POSTULOWANE ROZWIĄZANIA PRAWNE ZOSTAŁY ZAWARTE W ZAŁĄCZNIKU NR 2 DO ZGŁOSZENIA 2. INTERES BĄDĄCY PRZEDMIOTEM OCHRONY: ZAPEWNIENIE ODPOWIEDNIEGO OTOCZENIA REGULACYJNEGO DLA UCZESTNIKÓW OBROTU GOSPODARCZEGO		
D. ZAŁĄCZONE DOKUMENTY		
1	INFORMACJA ODPOWIADAJĄCA ODPISOWI AKTUALNEMU Z KRAJOWEGO REJESTRU PRZEDSIĘBIORCÓW (KRS 0000576857)	
2	SZCZEGÓŁOWY WYKAZ UWAG DO PROJEKTU USTAWY	
E. Niniejsze zgłoszenie dotyczy uzupełnienia braków formalnych/zmiany danych** zgłoszenia dokonanego dnia (podać datę z części F poprzedniego zgłoszenia)		
F. OSOBA SKŁADAJĄCA ZGŁOSZENIE		

Imię i nazwisko	Data	Podpis
KRZYSZTOF ROŻKO	Krzysztof Rożko 23 MAJA 2024 R.	
G. KLAUZULA ODPOWIEDZIALNOŚCI KARNEJ ZA SKŁADANIE FAŁSZYWYCH ZEZNAŃ Jestem świadomy odpowiedzialności karnej za złożenie fałszywego oświadczenia (podpis)		

* Jeżeli zgłoszenie nie jest składane w trybie art. 7 ust. 6 ustawy z dnia 7 lipca 2005 r. o działalności lobbingsowej w procesie stanowienia prawa - treść: "- Zgłoszenie zmiany danych" skreśla się.

** Niepotrzebne skreślić.

Pouczenie:

1. Jeżeli zgłoszenie ma na celu uwzględnienie zmian zaistniałych po dacie wniesienia urzędowego formularza zgłoszenia (art. 7 ust. 6 ustawy z dnia 7 lipca 2005 r. o działalności lobbingsowej w procesie stanowienia prawa.) lub uzupełnienie braków formalnych poprzedniego zgłoszenia (§ 3 rozporządzenia Rady Ministrów z dnia 22 sierpnia 2011 r. w sprawie zgłaszania zainteresowania pracami nad projektami aktów normatywnych oraz projektami założeń projektów ustaw (Dz. U. Nr 181, poz. 1080)), w nowym urzędowym formularzu zgłoszenia należy wypełnić wszystkie rubryki, powtarzając również dane, które zachowały swoją aktualność.
2. Część B formularza wypełnia się w przypadku zgłoszenia dotyczącego jednostki organizacyjnej oraz w sytuacji, gdy osoba fizyczna, która zgłasza zainteresowanie pracami nad projektem założeń projektu ustawy lub projektem aktu normatywnego, nie będzie uczestniczyła osobiście w tych pracach.
3. W części D formularza, stosownie do okoliczności, uwzględnia się dokumenty, o których mowa w art. 7 ust. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingsowej w procesie stanowienia prawa, a także pełnomocnictwa do wniesienia zgłoszenia lub do reprezentowania podmiotu w pracach nad projektem aktu normatywnego lub projektu założeń projektu ustawy.
4. Część E formularza wypełnia się w przypadku uzupełnienia braków formalnych lub zmiany danych dotyczących wniesionego zgłoszenia.

Warszawa, dnia 23 maja 2024 r.

**Szanowny Pan
Paweł Olszewski
Sekretarz Stanu**

Ministerstwo Cyfryzacji
ul. Królewska 27
00-060 Warszawa

Dotyczy: Projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

Szanowny Panie Ministrze,

w związku z zainicjowanym procesem uzgodnień, konsultacji publicznych i opiniowania projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) („Projekt”), działając w imieniu Krzysztof Rożko i Wspólnicy kancelaria Prawna Spółka komandytowa („Kancelaria”), niniejszym zgłaszam zainteresowani udziałem Kancelarii w toczących się pracach nad Projektem oraz przedstawiam propozycje zmian i komentarze odnośnie treści Projektu.

Z poważaniem,

Krzysztof Rożko

**Krzysztof Rożko
Radca prawny**

Wydruk informacji pobranej w trybie art. 4 ust. 4aa ustawy z dnia 20 sierpnia 1997 r. o Krajowym Rejestrze Sądowym, posiada moc dokumentu wydawanego przez Centralną Informację, nie wymaga podpisu i pieczęci.

CENTRALNA INFORMACJA KRAJOWEGO REJESTRU SĄDOWEGO

KRAJOWY REJESTR SĄDOWY

Stan na dzień 23.05.2024 godz. 13:05:44
Numer KRS: 0000576857

Informacja odpowiadająca odpisowi aktualnemu
Z REJESTRU PRZEDSIĘBIORCÓW

Data rejestracji w Krajowym Rejestrze Sądowym		22.09.2015		
Ostatni wpis	Numer wpisu	8	Data dokonania wpisu	19.04.2023
	Sygnatura akt	WA.XII NS-REJ.KRS/21969/23/540		
	Oznaczenie sądu	SĄD REJONOWY DLA M.ST. WARSZAWY W WARSZAWIE, XII WYDZIAŁ GOSPODARCZY KRAJOWEGO REJESTRU SĄDOWEGO		

Dział 1

Rubryka 1 - Dane podmiotu	
1.Oznaczenie formy prawnej	SPÓŁKA KOMANDYTOWA
2.Numer REGON/NIP	REGON: 362543036, NIP: 5252630217
3.Firma, pod którą spółka działa	KRZYSZTOF ROŻKO I WSPÓLNICY KANCELARIA PRAWNA SPÓŁKA KOMANDYTOWA
4.Dane o wcześniejszej rejestracji	-----
5.Czy przedsiębiorca prowadzi działalność gospodarczą z innymi podmiotami na podstawie umowy spółki cywilnej?	NIE
6.Czy podmiot posiada status organizacji pożytku publicznego?	NIE

Rubryka 2 - Siedziba i adres podmiotu	
1.Siedziba	kraj POLSKA, woj. MAZOWIECKIE, powiat WARSZAWA, gmina WARSZAWA, miejsc. WARSZAWA
2.Adres	ul. WOJCIECHA GÓRSKIEGO, nr 9, lok. ---, miejsc. WARSZAWA, kod 00-033, poczta WARSZAWA, kraj POLSKA
3.Adres poczty elektronicznej	-----
4.Adres strony internetowej	-----

Rubryka 3 - Oddziały	
Brak wpisów	

Rubryka 4 - Informacje o umowie		
1.Informacje o zawarciu lub zmianie umowy spółki	1	08.09.2015 R., NOTARIUSZ PIOTR SKOWORODKO, KANCELARIA NOTARIALNA W WARSZAWIE, PRZY ULICY WSPÓLNEJ 25; REP. A NR 6731/2015

Rubryka 5

1.Czas, na jaki została utworzona spółka	NIEOZNACZONY

Rubryka 6 - Sposób powstania spółki

Brak wpisów

Rubryka 7 - Dane wspólników

1	1.Nazwisko / Nazwa lub firma	ROŻKO
	2.Imiona	KRZYSZTOF
	3.Numer PESEL/REGON lub data urodzenia	██████████ -----
	4.Numer KRS	*****
	5.Czy wspólnik pozostaje w związku małżeńskim?	TAK
	6.Czy została zawarta małżeńska umowa majątkowa?	TAK
	7.Czy powstała rozdzielnosc majątkowa między małżonkami ?	TAK
	8.Czy wspólnik ma ograniczoną zdolność do czynności prawnych?	NIE
	9.Czy wspólnik jest komandytariuszem?	NIE
	10.Wysokość sumy komandytowej	*****
	11.Wartość wkładu umówionego	*****
	12.Czy jest w tym wkład niepieniężny?	*****
	Podrubryka 1 Wkład wniesiony	
	Brak wpisów	
2	Podrubryka 2 Wkład zwrócony	
	Brak wpisów	
	1.Nazwisko / Nazwa lub firma	MARIUSZ BAGIŃSKI I SPÓŁKA KOMANDYTOWO-AKCYJNA
	2.Imiona	*****
	3.Numer PESEL/REGON lub data urodzenia	361722096
	4.Numer KRS	0000561575
	5.Czy wspólnik pozostaje w związku małżeńskim?	*****
	6.Czy została zawarta małżeńska umowa majątkowa?	*****
	7.Czy powstała rozdzielnosc majątkowa między małżonkami ?	*****
	8.Czy wspólnik ma ograniczoną zdolność do czynności prawnych?	*****
	9.Czy wspólnik jest komandytariuszem?	TAK
	10.Wysokość sumy komandytowej	10.000 ZŁ

11.Wartość wkładu umówionego		6.000 Zł
12.Czy jest w tym wkład niepieniężny?		NIE
Podrubryka 1 Wkład wniesiony		
1	1.Wartość wkładu wniesionego	0.00 Zł
	2.Czy jest to wkład niepieniężny?	NIE
Podrubryka 2 Wkład zwrócony		
Brak wpisów		

Dział 2

Rubryka 1 - Uprawnieni do reprezentowania spółki		
1.Nazwa organu uprawnionego do reprezentowania podmiotu		WSPÓLNICY REPREZENTUJĄCY SPÓŁKĘ
2.Sposób reprezentacji podmiotu		WSPÓLNIK BĘDĄCY KOMPLEMENTARIUSZEM JEDNOOSOBOWO
Podrubryka 1 Dane wspólników reprezentujących spółkę		
1	1.Nazwisko / Nazwa lub Firma	ROŻKO
	2.Imiona	KRZYSZTOF
	3.Numer PESEL/REGON lub data urodzenia	██████████-----
	4.Numer KRS	*****

Rubryka 2 - Nie dotyczy	
Brak wpisów	

Rubryka 3 - Prokurenci	
Brak wpisów	

Dział 3

Rubryka 1 - Przedmiot działalności		
1.Przedmiot przeważającej działalności przedsiębiorcy	1	69, 10, Z, DZIAŁALNOŚĆ PRAWNICZA

Rubryka 2 - Wzmianki o złożonych dokumentach			
Rodzaj dokumentu	Nr kolejny w polu	Data złożenia	Za okres od do
1.Wzmianka o złożeniu rocznego sprawozdania finansowego	1	17.07.2017	OD 08.09.2015 DO 31.12.2015
	2	17.07.2017	OD 01.01.2016 DO 31.12.2016
	3	04.05.2020	OD 01.01.2018 DO 31.12.2018
	4	04.05.2020	OD 01.01.2019 DO 31.12.2019
3.Wzmianka o złożeniu	1	*****	OD 08.09.2015 DO 31.12.2015

uchwały lub postanowienia o zatwierdzeniu rocznego sprawozdania finansowego	2	*****	OD 01.01.2016 DO 31.12.2016

Rubryka 3 - Sprawozdania grupy kapitałowej

Brak wpisów

Rubryka 4 - Przedmiot działalności statutowej organizacji pożytku publicznego

Brak wpisów

Rubryka 5 - Informacja o dniu kończącym rok obrotowy

1.Dzień kończący pierwszy rok obrotowy, za który należy złożyć sprawozdanie finansowe	31.12.2015

Dział 4

Rubryka 1 - Zaległości

Brak wpisów

Rubryka 2 - Wierzytelności

Brak wpisów

Rubryka 3 - Informacje o oddaleniu wniosku o ogłoszenie upadłości na podstawie art. 13 ustawy z 28 lutego 2003 r. Prawo upadłościowe albo o zabezpieczeniu majątku dłużnika w postępowaniu w przedmiocie ogłoszenia upadłości albo w postępowaniu restrukturyzacyjnym albo po prawomocnym umorzeniu postępowania restrukturyzacyjnego

Brak wpisów

Rubryka 4 - Umorzenie prowadzonej przeciwko podmiotowi egzekucji z uwagi na fakt, że z egzekucji nie uzyska się sumy wyższej od kosztów egzekucyjnych

Brak wpisów

Dział 5

Rubryka 1 - Kurator

Brak wpisów

Dział 6

Rubryka 1 - Likwidacja

Brak wpisów

Rubryka 2 - Informacje o rozwiązaniu lub unieważnieniu podmiotu

Brak wpisów

Rubryka 3 - Informacje o połączeniu lub przekształceniu spółki

Brak wpisów

Rubryka 4 - Informacja o postępowaniu upadłościowym

Brak wpisów

Rubryka 5 - Informacja o postępowaniu układowym

Brak wpisów

Rubryka 6 - Informacje o postępowaniach restrukturyzacyjnych, o postępowaniu naprawczym lub o przymusowej restrukturyzacji

Brak wpisów

Rubryka 7 - Informacja o zawieszeniu działalności gospodarczej

Brak wpisów

data sporządzenia wydruku 23.05.2024

adres strony internetowej, na której są dostępne informacje z rejestru: prs.ms.gov.pl

Krzysztof Rożko



ZAŁĄCZNIK NR 2 – SZCZEGÓŁOWY WYKAZ UWAG DO PROJEKTU

Projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw

(Nr UC32 w wykazie prac legislacyjnych) („Ustawa”)

Zgłaszający uwagi: Krzysztof Rożko i Wspólnicy Kancelaria Prawna sp. k.

Szczegółowy wykaz uwag:

L.p.	Komentowany artykuł/paragraf	Treść uwagi
1)	Art. 1 pkt 2 lit. j)	Projekt ustawy o zmianie niektórych ustaw w związku z zapewnieniem operacyjnej odporności cyfrowej sektora finansowego (która na celu umożliwienie stosowania przepisów rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniającej rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (dalej odpowiednio „projekt ustawy wdrażającej DORA”, „Rozporządzenie 2022/2554”), przewiduje już dodanie w art. 2 pkt 11a)-c) w ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (dalej „uKSC”) o odmiennej jednakże treści. W związku z powyższym, postulujemy koordynację prac nad obydwoma aktami prawnymi i w rezultacie dostosowanie numeracji w art. 2 uKSC.
2)	Art. 1 pkt 2 m)	Zwracamy uwagę, że zarówno w art. 1 pkt 2 lit. m) projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (dalej „projekt nowelizacji uKSC”), jak również projekt ustawy wdrażającej DORA przewiduje dodanie do uKSC w art. 2 pkt.20 uKSC, zawierającego definicję znaczącego cyberzagrożenia.

Krzysztof Rożko



		Projekty przepisów, które przewidują wprowadzenie wskazanej definicji poprzez projekt ustawy wdrażającej DORA oraz poprzez nowelizację uKSC, w istocie dotyczą jednak różnych pojęć. W projekcie ustawy wdrażającej DORA, co zrozumiale, posłużono się odwołaniem do definicji znaczącego cyberzagrożenia zawartej w treści Rozporządzenia 2022/2554, natomiast w nowelizacji uKSC zdecydowano się na wprowadzenie autonomicznej definicji tego pojęcia bazującej jednak na definicji „poważnego cyberzagrożenia” zawartej w art. 6 pkt 11 dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 („Dyrektywa 2022/2555”). Pomimo, że brzmienie wskazanych wyżej definicji, tj. „znaczącego cyberzagrożenia” na gruncie Rozporządzenia 2022/2554 oraz „poważnego cyberzagrożenia” zdefiniowanego w Dyrektywie 2022/2555, może wydawać się zbliżone, to szczegółowa analiza ich treści prowadzi do wniosku, że zakres obydwu definicji jest różny. Wobec powyższego proponujemy rozróżnienie rzeczonych pojęć na gruncie przepisów krajowych, tj. UKSC, poprzez odrębne zdefiniowanie: 1) „Znaczącego cyberzagrożenia związanego z ICT” – przez odwołanie do art. 3 pkt 13 Rozporządzenia 2022/2554, 2) „Poważnego cyberzagrożenia” – poprzez zastąpienie pojęcia „znaczącego cyberzagrożenia”, którym posłużono się w art. 1 pkt 2) lit. m nowelizacji uKSC, pojęciem „poważnego cyberzagrożenia”.
3)	Art. 1 pkt 8)	Projekt nowelizacji uKSC, wymienia w art. 1 pkt 8) (wprowadzając zmianę do art. 5 ust. 6) uKSC CSIRT MON, CSIRT NASK lub CSIRT GOV jako właściwe do zwrócenia się w związku z obowiązkami podmiotu wynikającymi z ustawy. Projekt pomija możliwość zwrócenia się do podmiotu w związku z obowiązkami wynikającymi z ustawy przez CSIRT sektorowy. W art. 6 pkt 34) dyrektywa NIS 2 określa organ krajowy lub CSIRT jako mogące się zwrócić w związku z obowiązkami podmiotu przewidzianymi w niniejszej dyrektywie, co pozwala stwierdzić, że CSIRT sektorowe, również powinny być uprawnione do zwrócenia w związku z obowiązkami podmiotu wynikającymi z ustawy.
4)	Art. 1 pkt 13)	Zwracamy uwagę, że w projekcie nowelizacji uKSC, w art. 1 pkt 13 (w proj art. 8i uKSC), przewidziano wyłączenie od stosowania przepisów rozdziału 3. uKSC w zakresie w jakim podmioty kluczowe i ważne z sektora bankowości i infrastruktura rynków finansowych mają obowiązek stosować Rozporządzenie 2022/2554. Tymczasem w projekcie

		art. 16a uKSC proponowanym na podstawie projektu ustawy wdrażającej DORA, przewidziana jest analogiczna regulacja, w której jednak wprost wskazano konkretne przepisy uKSC, które nie znajdują zastosowania do podmiotów ważnych lub kluczowych w rozumieniu Dyrektywy NIS 2. Wobec powyższego postulujemy odpowiednie skoordynowanie treści projektowanych przepisów w celu uniknięcia nałożenia się zakresu regulacji. W przypadku pozostawienia metody regulacji, określonej w projekcie ustawy wdrażającej DORA, która zakłada wprost wymienienie przepisów, do których stosowania nie są zobowiązane podmioty, do których stosuje się przepisy rozporządzenia DORA, co jest metodą zapewniającą większą jasność odnośnie zakresu obowiązków spoczywających na takich podmiotach, należałoby zrewidować przepisy, z których stosowania są zwolnione podmioty kluczowe lub podmioty ważne, z sektora „Bankowość i infrastruktura rynków finansowych”. Przykładowo błędnym wydaje się wyłączenie ze stosowania przez takie podmioty art. 11a uKSC, którego wprowadzenie zostało zaproponowane na gruncie projektu ustawy wdrażającej DORA.
5)	Art. 1 pkt 22)	Zważywszy, że art. 10 pkt 4) projektu ustawy wdrażającej DORA przewiduje dodanie art. 16a do uKSC, zwracamy uwagę, by w art. 1 pkt 22 projektu nowelizacji uKSC, który przewiduje dodanie rozdziału 3a, zaczynającego się od art. 16a, uwzględnione zostały stosowne zmiany w numeracji przepisów.
6)	Art. 5 pkt 67 a) tiret piąte	Niniejszy przepis przewiduje dodanie w art. 65 ust. 1 nowego pkt 8). Zwracamy uwagę, że w projekcie ustawy wdrażającej DORA na podstawie art. 10 pkt 5, w art. 65 ust. 1 uKSC również proponuje się dodanie pkt 8), który jednak odnosi się do odmiennej materii. Wobec powyższego postulujemy odpowiednie skoordynowanie treści projektowanych przepisów.
7)	Art. 1 pkt 68 lit. a)	Projekt ustawy wdrażającej DORA przewiduje uwzględnienie w art. 66 ust. 4 pkt. 5 uKSC Przewodniczącego Komisji Nadzoru Finansowego, jako uczestnika posiedzeń Kolegium. W projekcie nowelizacji uKSC w art. 1 pkt 68 lit. a) również uwzględniony został Przewodniczący Komisji Nadzoru Finansowego jako uczestnik posiedzeń Kolegium. Wobec powyższego postulujemy odpowiednie skoordynowanie treści projektowanych przepisów.

8)	Art. 1 pkt 74 lit. d) i f)	Art. 1 pkt 74 lit. d) projektu nowelizacji uKSC wprowadza w art. 73 ust 3 uKSC wysokość kary minimalnej dla podmiotu kluczowego jako nie niższej niż 20 000 zł i odpowiednio w art. 1 pkt. 74 lit. f) karę minimalną dla podmiotu ważnego w wysokości nie niższej niż 15 000 zł, podczas, gdy dyrektywa NIS 2 nie określa kar minimalnych. Zważywszy na fakt, iż kary takiej wysokości nakładane mogłyby być na podmioty małe, o utrudnionym procesie adaptacji do zaostrzonych wymogów wprowadzonych w nowelizacji uKSC proponujemy zrezygnowanie z regulowania wysokości kary minimalnej.
9)	Art. 1 pkt 79 ppkt 1)	Zważywszy, że art. 10 pkt 7) projektu ustawy wdrażającej DORA również przewiduje dodanie art. 76a do uKSC, który jednakże reguluje odmienną materię, niż art. 76a, w brzmieniu proponowanym projektem nowelizacji uKSC, zwracamy uwagę by w art. 1 pkt 79 ppkt 1) projektu nowelizacji uKSC, uwzględnione zostały stosowne zmiany w numeracji przepisów.

ROZPORZĄDZENIE

RADY MINISTRÓW

z dnia r.

w sprawie progów uznania incydentu za poważny

Na podstawie art. 11 ust. 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077 i 1222 oraz z 2025 r. poz. 1017, 1069 i ...) zarządza się, co następuje:

§ 1. Określa się progi uznania incydentu za poważny według rodzaju zdarzenia w poszczególnych sektorach i podsektorach określonych w załączniku nr 1 i 2 do ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, stanowiące załącznik do rozporządzenia.

§ 2. Rozporządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia.¹⁾

PREZES RADY MINISTRÓW

¹⁾ Niniejsze rozporządzenie było poprzedzone rozporządzeniem Rady Ministrów z dnia 31 października 2018 r. w sprawie uznania incydentu za poważny (Dz. U. poz. 2180), które traci moc z dniem wejścia w życie niniejszego rozporządzenia zgodnie z art. 32 pkt 1 ustawy z dnia ... o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (Dz. U. poz. ...).

Załącznik do rozporządzenia Rady
Ministrów z dnia r.
(Dz. U. poz. ...)

Progi uznania incydentu za poważny według rodzaju zdarzenia w poszczególnych sektorach
i podsektorach

Sektor	Podsektor	Zdarzenie	Progi
Energia	Wydobywanie kopalin	Incydent dotyczący wydobycia kopalin	1) liczba użytkowników, których dotyczy zakłócenie świadczenia usługi: nie dotyczy; 2) czas oddziaływania incydentu na świadczoną usługę: incydent doprowadził do przerwania wydobycia na okres dłuższy niż 72 godziny; 3) zasięg geograficzny obszaru, którego dotyczy incydent: nie dotyczy; 4) inne czynniki charakterystyczne dla danego podsektora: incydent spowodował co najmniej jedną z poniżej wymienionych okoliczności:

			a) śmierć człowieka, b) ciężki uszczerbek na zdrowiu, c) inny niż ciężki uszczerbek na zdrowiu więcej niż jednej osoby, d) straty finansowe przekraczające 250 tys. zł.
	Energia elektryczna	Incydent dotyczący pokrycia zapotrzebowania o zasięgu lokalnym	1) liczba użytkowników, których dotyczy zakłócenie świadczenia usługi: nie dotyczy; 2) czas oddziaływania incydentu na świadczoną usługę: utrata na co najmniej 3 minuty zasilania odbiorców w wysokości powyżej 10% rzeczywistego zapotrzebowania systemu w okresie poprzedzającym incydent; 3) zasięg geograficzny obszaru, którego dotyczy incydent: nie dotyczy;

			4) inne czynniki charakterystyczne dla danego podsektora: nie dotyczy.
		Incydent dotyczący pokrycia zapotrzebowania o zasięgu krajowym	1) liczba użytkowników, których dotyczy zakłócenie świadczenia usługi: nie dotyczy; 2) czas oddziaływania incydentu na świadczoną usługę: utrata, na co najmniej 3 minuty, zasilania odbiorców w wysokości powyżej 10% rzeczywistego zapotrzebowania systemu w okresie poprzedzającym incydent; 3) zasięg geograficzny obszaru, którego dotyczy incydent: nie dotyczy; 4) inne czynniki charakterystyczne dla danego podsektora: nie dotyczy.
		Incydent dotyczący sieci przesyłowej	1) liczba użytkowników,

			których dotyczy zakłócenie świadczenia usługi: nie dotyczy; 2) czas oddziaływania incydentu na świadczoną usługę; 3) zasięg geograficzny obszaru, którego dotyczy incydent: nie dotyczy; 4) inne czynniki charakterystyczne dla danego podsektora: awaryjne, równoczesne wyłączenie co najmniej dwóch elementów sieci przesyłowej powodujące: a) istotne pogorszenie warunków pracy systemu lub b) ograniczające zdolności wymiany transgranicznej, lub c) ogłoszenie przez Operatora Systemu Przesyłowego stanu zagrożenia systemu przesyłowego lub

			stanu zaniku zasilania lub stanu odbudowy systemu zgodnie z klasyfikacją stanów systemu określoną w art. 18 rozporządzenia Komisji (UE) 2017/1485 z dnia 2 sierpnia 2017 r. ustanawiającego wytyczne dotyczące pracy systemu przesyłowego energii elektrycznej (Dz. Urz. UE L 220 z 25.08.2017, str. 1, z późn. zm. ²⁾).
		Incydent dotyczący modułów wytwarzania energii	1) liczba użytkowników, których dotyczy zakłócenie świadczenia usługi: nie dotyczy; 2) czas oddziaływania incydentu na świadczoną usługę: trwające powyżej 15 minut: a) równoczesne,

²⁾ Zmiany wymienionego rozporządzenia zostały ogłoszone w Dz. Urz. UE L 62 z 23.02.2021, str. 24.

			nieplanowane wyłączenie co najmniej dwóch modułów wytwarzania energii w jednej elektrowni o sumarycznej mocy powyżej 400 MW brutto lub b) równoczesne, nieplanowane ograniczenie mocy lub wyłączenie modułów wytwarzania energii w łącznej wielkości mocy powyżej 1500 MW brutto; 3) zasięg geograficzny obszaru, którego dotyczy incydent: nie dotyczy; 4) inne czynniki charakterystyczne dla danego podsektora: nie dotyczy.
		Incydent dotyczący urządzeń i narzędzi wykorzystywanych do monitorowania i sterowania pracą systemu	1) liczba użytkowników, których dotyczy zakłócenie świadczenia usługi: nie dotyczy; 2) czas oddziaływania

			incydentu na świadczoną usługę: utrata jednego z następujących urządzeń lub narzędzi wykorzystywanych w czasie rzeczywistym, przy jednoczesnym braku dostępności urządzeń i narzędzi podstawowych i rezerwowych: a) środków łączności dyspozytorskiej, przez okres co najmniej 1 godziny lub b) systemów zdalnego sterowania urządzeniami stacijnymi i źródłami wytwórczymi przez okres powyżej 15 minut, lub c) systemów monitorowania pracy systemu (w tym estymacji stanu systemu) przez okres powyżej 15 minut, lub d) narzędzi wykorzystywanych do

			oceny bezpieczeństwa pracy systemu przez okres powyżej 15 minut, lub e) systemów klasy „smart metering” w przypadku braku możliwości pozyskania danych z co najmniej 30% planowanych do odczytu układów pomiarowych, przez okres powyżej 48 godzin; 3) zasięg geograficzny obszaru, którego dotyczy incydent: nie dotyczy; 4) inne czynniki charakterystyczne dla danego podsektora: nie dotyczy.
	Ciepło	Incydent dotyczący wytwarzania ciepła	1) liczba użytkowników, których dotyczy zakłócenie świadczenia usługi: nie dotyczy; 2) czas oddziaływania incydentu na świadczoną usługę:

			incydent doprowadził do przerwania wytwarzania ciepła na okres dłuższy niż 24 godziny; 3) zasięg geograficzny obszaru, którego dotyczy incydent: nie dotyczy; 4) inne czynniki charakterystyczne dla danego podsektora: incydent spowodował co najmniej jedną z poniżej wymienionych okoliczności: a) śmierć człowieka, b) ciężki uszczerbek na zdrowiu, c) inny niż ciężki uszczerbek na zdrowiu więcej niż jednej osoby, d) straty finansowe przekraczające 250 tys. zł.
		Incydent dotyczący obrotu lub przesyłania lub dystrybucji ciepła	1) liczba użytkowników, których dotyczy zakłócenie świadczenia usługi:

			nie dotyczy; 2) czas oddziaływania incydentu na świadczoną usługę: incydent doprowadził do przerwania przesyłania lub dystrybucji ciepła na dłużej niż 24 godziny; 3) zasięg geograficzny obszaru, którego dotyczy incydent: nie dotyczy; 4) inne czynniki charakterystyczne dla danego podsektora: incydent spowodował co najmniej jedną z poniżej wymienionych okoliczności: a) śmierć człowieka, b) ciężki uszczerbek na zdrowiu, c) inny niż ciężki uszczerbek na zdrowiu więcej niż jednej osoby, d) straty finansowe przekraczające 250 tys. zł.
	Ropa i paliwa	Incydent dotyczący	1) liczba

		przesyłu ropy naftowej i paliw ciekłych	użytkowników, których dotyczy zakłócenie świadczenia usługi: nie dotyczy; 2) czas oddziaływania incydentu na świadczoną usługę: incydent skutkuje niemożliwością terminowego i w ilościach nominowanych dostarczania i przesyłu ropy naftowej, przez okres dłuższy niż 20 godzin; 3) zasięg geograficzny obszaru, którego dotyczy incydent: nie dotyczy; 4) inne czynniki charakterystyczne dla danego podsektora: niekontrolowany wyciek ropy naftowej lub innych substancji niebezpiecznych do atmosfery lub gruntu.
		Incydent dotyczący produkcji, wydobywania,	1) liczba użytkowników, których dotyczy

		wytwarzania paliw ciekłych, magazynowania ropy naftowej, przeładunku ropy naftowej, magazynowania paliw ciekłych, przeładunku paliw ciekłych, obrotu paliwami ciekłymi i obrotu paliwami ciekłymi z zagranicą, wytwarzania paliw syntetycznych	zakłócenie świadczenia usługi: nie dotyczy; 2) czas oddziaływania incydentu na świadczoną usługę: incydent skutkuje zakłóceniem w produkcji lub rafinacji lub w funkcjonowaniu urządzeń przetwarzających lub magazynowaniu i przesyłaniu ropy naftowej, dłuższym niż 20 godzin; 3) zasięg geograficzny obszaru, którego dotyczy incydent: nie dotyczy; 4) inne czynniki charakterystyczne dla danego podsektora: a) znacząca utrata integralności stacji lub b) utrata ochrony stacji przeciwko efektom eksplozji, lub c) utrata stacji utrzymania w przypadku instalacji

			mobilnych, lub d) niekontrolowany wyciek ropy naftowej lub innych substancji niebezpiecznych do atmosfery lub gruntu.
	Gaz	Incydent dotyczący wytwarzania paliw gazowych, przesyłania paliw gazowych, dystrybucji paliw gazowych, obrotu paliwami gazowymi lub obrotu gazem ziemnym z zagranicą, magazynowania paliw gazowych, skraplania lub regazyfikacji LNG lub sprowadzania i wyładunku LNG	1) liczba użytkowników, których dotyczy zakłócenie świadczenia usługi: nie dotyczy; 2) czas oddziaływania incydentu na świadczoną usługę: incydent skutkuje niemożliwością prawidłowego dostarczania i przesyłu gazu ziemnego w okresie co najmniej 24 godzin lub zakłóceniem w produkcji lub w funkcjonowaniu urządzeń przetwarzających lub magazynowaniu lub przesyłaniu gazu ziemnego, przez okres dłuższy niż 20 godzin; 3) zasięg geograficzny

			obszaru, którego dotyczy incydent: nie dotyczy; 4) inne czynniki charakterystyczne dla danego podsektora: a) nieplanowany wyciek gazu lub innych substancji niebezpiecznych, niezależnie od tego czy doszło do zapłonu, stanowiący bezpośrednie niebezpieczeństwo: – utraty życia lub spowodowania uszczerbku na zdrowiu lub – wyrządzenia szkody w wielkich rozmiarach, lub b) niekontrolowane obniżenie lub wzrost ciśnienia w sieci gazowej, lub c) zatrzymanie pracy tłoczni gazu lub stacji gazowej, lub d) niekontrolowane zamknięcie lub otwarcie armatury na

			obiektach sieci gazowej.
	Energetyka jądrowa	Incydent dotyczący wytwarzania energii jądrowej	1) liczba użytkowników, których dotyczy zakłócenie świadczenia usługi: nie dotyczy; 2) czas oddziaływania incydentu na świadczoną usługę: incydent skutkuje niemożliwością prawidłowego wytwarzania energii jądrowej; 3) zasięg geograficzny obszaru, którego dotyczy incydent: nie dotyczy; 4) inne czynniki charakterystyczne dla danego podsektora: a) nieplanowany wyciek substancji radioaktywnych do środowiska: – utraty życia lub spowodowania uszczerbku na zdrowiu lub – wyrządzenia szkody

			w wielkich rozmiarach, lub b) promieniotwórcze skażenie środowiska.
		Incydent dotyczący utrzymania rezerw strategicznych lub zapasów agencyjnych ropy naftowej, produktów naftowych i gazu ziemnego	1) liczba użytkowników, których dotyczy zakłócenie świadczenia usługi: nie dotyczy; 2) czas oddziaływania incydentu na świadczoną usługę: incydent skutkuje przerwaniem realizacji procesu udostępniania rezerw strategicznych lub uwalniania zapasów agencyjnych ropy naftowej, produktów naftowych i gazu ziemnego na czas dłuższy niż 4 godziny; 3) zasięg geograficzny obszaru, którego dotyczy incydent: nie dotyczy; 4) inne czynniki charakterystyczne dla danego podsektora: nie dotyczy.

		Incydent dotyczący postępowania z odpadami promieniotwórczymi	1) liczba użytkowników, których dotyczy zakłócenie świadczenia usługi: minimum 200 użytkowników, od których odbiera się odpady promieniotwórcze; 2) czas oddziaływania incydentu na świadczoną usługę: nie dotyczy; 3) zasięg geograficzny obszaru, którego dotyczy incydent: terytorium całego kraju; 4) inne czynniki charakterystyczne dla danego podsektora: incydent skutkuje bezpośrednim niebezpieczeństwem spowodowania uszczerbku na zdrowiu lub długotrwałym skażeniem środowiska.
	Wodór	Incydent dotyczący wytwarzania wodoru	1) liczba użytkowników,

		i przesyłania wodoru	których dotyczy zakłócenie świadczenia usługi: nie dotyczy; 2) czas oddziaływania incydentu na świadczoną usługę: a) incydent skutkuje zakłóceniem w produkcji wodoru lub w funkcjonowaniu urządzeń przetwarzających wodór, lub przeładunku wodoru, lub obrocie wodorem, lub obrocie wodorem z zagranicą, w okresie dłuższym niż 4 godziny lub b) incydent skutkuje przerwą w dostawie energii elektrycznej do systemu przesyłowego wodoru przez okres powyżej 8 godzin, lub c) incydent skutkuje przerwą w dostawie energii elektrycznej do systemu magazynowego wodoru przez okres

			powyżej 8 godzin; 3) zasięg geograficzny obszaru, którego dotyczy incydent: nie dotyczy; 4) inne czynniki charakterystyczne dla danego podsektora: nie dotyczy.
Transport	Transport lotniczy	Incydent dotyczący transportu lotniczego pasażerskiego	1) liczba użytkowników, których dotyczy zakłócenie świadczenia usługi: nie dotyczy; 2) czas oddziaływania incydentu na świadczoną usługę: nie dotyczy; 3) zasięg geograficzny obszaru, którego dotyczy incydent: nie dotyczy; 4) inne czynniki charakterystyczne dla danego podsektora: a) przerwanie realizacji usług przez przewoźnika lotniczego na czas dłuższy niż 2 godziny lub

			b) uszkodzenie statku powietrznego lub systemów informacyjnych kluczowych dla jego sterowania i funkcjonowania, lub c) incydent spowodował śmierć lub uszczerbek na zdrowiu ludzi.
		Incydent dotyczący transportu lotniczego towarów	1) liczba użytkowników, których dotyczy zakłócenie świadczenia usługi: nie dotyczy; 2) czas oddziaływania incydentu na świadczoną usługę: nie dotyczy; 3) zasięg geograficzny obszaru, którego dotyczy incydent: nie dotyczy; 4) inne czynniki charakterystyczne dla danego podsektora: a) przerwanie realizacji usług przez przewoźnika lotniczego na czas

			dłuższy niż 2 godziny lub b) uszkodzenie statku powietrznego lub systemów informacyjnych kluczowych dla jego sterowania i funkcjonowania, lub c) incydent spowodował śmierć lub uszczerbek na zdrowiu ludzi.
		Incydent dotyczący podmiotu o statusie zarejestrowanego agenta	1) liczba użytkowników, których dotyczy zakłócenie świadczenia usługi: nie dotyczy; 2) czas oddziaływania incydentu na świadczoną usługę: nie dotyczy; 3) zasięg geograficzny obszaru, którego dotyczy incydent: nie dotyczy; 4) inne czynniki charakterystyczne dla danego podsektora: a) przerwanie realizacji procesu

			kontroli bezpieczeństwa przez zarejestrowanego agenta na czas dłuższy niż 2 godziny lub b) zakłócenie wykonywania usług przekazu informacji o statusie ochrony nadany przesyłce na czas dłuższy niż 2 godziny.
		Incydent dotyczący dostępności obsługi naziemnej	1) liczba użytkowników, których dotyczy zakłócenie świadczenia usługi: nie dotyczy; 2) czas oddziaływania incydentu na świadczoną usługę: nie dotyczy; 3) zasięg geograficzny obszaru, którego dotyczy incydent: nie dotyczy; 4) inne czynniki charakterystyczne dla danego podsektora: incydent doprowadził do braku dostępności usługi wykonywanej

			przez agenta obsługi naziemnej na czas dłuższy niż 2 godziny lub doprowadził do braku dostępności usług wykonywanych przez inne podmioty w podsektorze.
		Incydent dotyczący zarządzającego lotniskiem	1) liczba użytkowników, których dotyczy zakłócenie świadczenia usługi: nie dotyczy; 2) czas oddziaływania incydentu na świadczoną usługę: nie dotyczy; 3) zasięg geograficzny obszaru, którego dotyczy incydent: nie dotyczy; 4) inne czynniki charakterystyczne dla danego podsektora: a) zakłócenie wykonywania operacji lotniczych na czas dłuższy niż 2 godziny lub b) incydent spowodował śmierć

			lub uszczerbek na zdrowiu ludzi lub c) incydent doprowadził do braku dostępności usług wykonywanych przez inne podmioty w podsektorze.
		Incydent dotyczący instytucji zapewniającej służby żeglugi powietrznej	1) liczba użytkowników, których dotyczy zakłócenie świadczenia usługi: nie dotyczy; 2) czas oddziaływania incydentu na świadczoną usługę: nie dotyczy; 3) zasięg geograficzny obszaru, którego dotyczy incydent: nie dotyczy; 4) inne czynniki charakterystyczne dla danego podsektora: incydent doprowadził do zakłócenia systemu zarządzania ruchem lotniczym i ograniczenia przepustowości przestrzeni

			powietrznej o co najmniej 30%.
	Transport kolejowy	Incydent dotyczący konstrukcji rozkładu jazdy pociągów	1) liczba użytkowników, których dotyczy zakłócenie świadczenia usługi: nie dotyczy; 2) czas oddziaływania incydentu na świadczoną usługę: nie dotyczy; 3) zasięg geograficzny obszaru, którego dotyczy incydent: nie dotyczy; 4) inne czynniki charakterystyczne dla danego podsektora: brak możliwości konstrukcji rozkładów jazdy pociągów wynikający z: a) awarii oprogramowania powyżej 12 godzin lub b) braku zasilania energetycznego powodującego niedostępność usługi powyżej 2 godzin, lub c) awarii sieci

			teleinformatycznych powyżej 12 godzin.
		Incydent dotyczący jazdy pociągów	1) liczba użytkowników, których dotyczy zakłócenie świadczenia usługi: nie dotyczy; 2) czas oddziaływania incydentu na świadczoną usługę: nie dotyczy; 3) zasięg geograficzny obszaru, którego dotyczy incydent: nie dotyczy; 4) inne czynniki charakterystyczne dla danego podsektora: brak możliwości uruchomienia pociągów i prowadzenia ruchu kolejowego spowodowany brakiem możliwości konstrukcji rozkładu jazdy powyżej 2 godzin.
		Incydent w transporcie kolejowym	1) liczba użytkowników, których dotyczy

		pasażerskim	zakłócenie świadczenia usługi: nie dotyczy; 2) czas oddziaływania incydentu na świadczoną usługę: nie dotyczy; 3) zasięg geograficzny obszaru, którego dotyczy incydent: nie dotyczy; 4) inne czynniki charakterystyczne dla danego podsektora: a) przerwanie realizacji usług przez przewoźnika na czas dłuższy niż 2 godziny lub b) uszkodzenie systemów informacyjnych kluczowych dla sterowania i funkcjonowania pojazdu szynowego.
		Incydent w transporcie kolejowym towarów	1) liczba użytkowników, których dotyczy zakłócenie świadczenia usługi: nie dotyczy;

			2) czas oddziaływania incydentu na świadczoną usługę: nie dotyczy; 3) zasięg geograficzny obszaru, którego dotyczy incydent: nie dotyczy; 4) inne czynniki charakterystyczne dla danego podsektora: a) przerwanie realizacji usług przez przewoźnika na czas dłuższy niż 6 godzin lub b) uszkodzenie systemów informacyjnych kluczowych dla sterowania i funkcjonowania pojazdu szynowego.
	Transport wodny	Incydent dotyczący armatorów w transporcie morskim pasażerów podczas żeglugi	1) liczba użytkowników, których dotyczy zakłócenie świadczenia usługi: nie dotyczy; 2) czas oddziaływania incydentu na świadczoną usługę:

			nie dotyczy; 3) zasięg geograficzny obszaru, którego dotyczy incydent: nie dotyczy; 4) inne czynniki charakterystyczne dla danego sektora lub podsektora: incydent spowodował uszkodzenie systemów informacyjnych kluczowych dla sterowania i funkcjonowania statku, powodujące zagrożenie dla zdrowia lub życia ludzkiego, środowiska naturalnego albo mienia.
		Incydent dotyczący armatorów w transporcie morskim pasażerów podczas cumowania	1) liczba użytkowników, których dotyczy zakłócenie świadczenia usługi: nie dotyczy; 2) czas oddziaływania incydentu na świadczoną usługę: incydent spowodował brak możliwości

			świadczenia usługi na czas dłuższy niż 48 godzin; 3) zasięg geograficzny obszaru, którego dotyczy incydent: nie dotyczy; 4) inne czynniki charakterystyczne dla danego sektora lub podsektora: nie dotyczy.
		Incydent dotyczący armatorów w transporcie morskim towarów podczas żeglugi	1) liczba użytkowników, których dotyczy zakłócenie świadczenia usługi: nie dotyczy; 2) czas oddziaływania incydentu na świadczoną usługę: nie dotyczy; 3) zasięg geograficzny obszaru, którego dotyczy incydent: nie dotyczy; 4) inne czynniki charakterystyczne dla danego sektora lub podsektora: incydent spowodował uszkodzenie systemów

			informacyjnych kluczowych dla sterowania i funkcjonowania statku, powodujące zagrożenie dla zdrowia lub życia ludzkiego, środowiska naturalnego albo mienia.
		Incydent dotyczący armatorów w transporcie morskim towarów podczas cumowania	1) liczba użytkowników, których dotyczy zakłócenie świadczenia usługi: nie dotyczy; 2) czas oddziaływania incydentu na świadczoną usługę: incydent spowodował brak możliwości świadczenia usługi w czasie dłuższym niż 48 godzin; 3) zasięg geograficzny obszaru, którego dotyczy incydent: nie dotyczy; 4) inne czynniki charakterystyczne dla danego sektora lub podsektora: nie

			dotyczy.
		Incydent dotyczący armatorów w transporcie wodnym śródlądowym pasażerskim	1) liczba użytkowników, których dotyczy zakłócenie świadczenia usługi: co najmniej 30% pasażerów transportu pasażerskiego żeglugi śródlądowej rocznie określonych na podstawie danych Głównego Urzędu Statystycznego z roku poprzedniego; 2) czas oddziaływania incydentu na świadczoną usługę: incydent spowodował brak dostępu do systemu teleinformatycznego na czas dłuższy niż 72 godziny; 3) zasięg geograficzny obszaru, którego dotyczy incydent: nie dotyczy; 4) inne czynniki charakterystyczne dla danego sektora lub podsektora: nie

			dotyczy.
		Incydent dotyczący armatorów w transporcie wodnym śródlądowym towarów	1) liczba użytkowników, których dotyczy zakłócenie świadczenia usługi: nie dotyczy; 2) czas oddziaływania incydentu na świadczoną usługę: incydent spowodował brak dostępu do systemu teleinformatycznego w czasie dłuższym niż 72 godziny; 3) zasięg geograficzny obszaru, którego dotyczy incydent: nie dotyczy; 4) inne czynniki charakterystyczne dla danego sektora lub podsektora: nie dotyczy.
		Incydent dotyczący funkcjonowania organów zarządzających portami	1) liczba użytkowników, których dotyczy zakłócenie świadczenia usługi: nie dotyczy; 2) czas oddziaływania

			incydentu na świadczoną usługę: incydent spowodował brak możliwości świadczenia usługi przez czas dłuższy niż 12 godzin; 3) zasięg geograficzny obszaru, którego dotyczy incydent: nie dotyczy; 4) inne czynniki charakterystyczne dla danego sektora lub podsektora: nie dotyczy.
		Incydent dotyczący bezpieczeństwa organów zarządzających portami	1) liczba użytkowników, których dotyczy zakłócenie świadczenia usługi: nie dotyczy; 2) czas oddziaływania incydentu na świadczoną usługę: nie dotyczy; 3) zasięg geograficzny obszaru, którego dotyczy incydent: nie dotyczy; 4) inne czynniki charakterystyczne dla

			danego sektora lub podsektora: incydent spowodował uszkodzenie systemów informacyjnych kluczowych dla funkcjonowania portu, powodujące niedostępność portu lub ograniczoną dostępność portu.
		Incydent dotyczący funkcjonowania organów zarządzających obiektami portowymi	1) liczba użytkowników, których dotyczy zakłócenie świadczenia usługi: nie dotyczy; 2) czas oddziaływania incydentu na świadczoną usługę: incydent spowodował brak możliwości świadczenia usługi przez czas dłuższy niż 12 godzin; 3) zasięg geograficzny obszaru, którego dotyczy incydent: nie dotyczy; 4) inne czynniki charakterystyczne dla danego sektora lub

			podsektora: nie dotyczy.
		Incydent dotyczący bezpieczeństwa organów zarządzających obiektami portowymi	1) liczba użytkowników, których dotyczy zakłócenie świadczenia usługi: nie dotyczy; 2) czas oddziaływania incydentu na świadczoną usługę: nie dotyczy; 3) zasięg geograficzny obszaru, którego dotyczy incydent: nie dotyczy; 4) inne czynniki charakterystyczne dla danego sektora lub podsektora: incydent spowodował uszkodzenie systemów informacyjnych kluczowych dla funkcjonowania obiektu portowego, powodujące zagrożenie dla zdrowia lub życia ludzkiego, środowiska naturalnego lub mienia albo dla

			funkcjonowania portu.
		Incydent dotyczący funkcjonowania podmiotów prowadzących na terenie portu działalność wspomagającą transport morski	1) liczba użytkowników, których dotyczy zakłócenie świadczenia usługi: nie dotyczy; 2) czas oddziaływania incydentu na świadczoną usługę: incydent spowodował brak możliwości świadczenia usługi przez czas dłuższy niż 12 godzin; 3) zasięg geograficzny obszaru, którego dotyczy incydent: nie dotyczy; 4) inne czynniki charakterystyczne dla danego sektora lub podsektora: nie dotyczy.
		Incydent dotyczący bezpieczeństwa podmiotów prowadzących na terenie portu działalność wspomagającą transport morski	1) liczba użytkowników, których dotyczy zakłócenie świadczenia usługi: nie dotyczy; 2) czas oddziaływania incydentu na

			świadczoną usługę: nie dotyczy; 3) zasięg geograficzny obszaru, którego dotyczy incydent: nie dotyczy; 4) inne czynniki charakterystyczne dla danego sektora lub podsektora: incydent spowodował uszkodzenie systemów informacyjnych kluczowych dla funkcjonowania obiektu portowego, powodujące utrudnienia dla funkcjonowania portu.
		Incydent dotyczący funkcjonowania VTS (Służba Kontroli Ruchu Statków)	1) liczba użytkowników, których dotyczy zakłócenie świadczenia usługi: nie dotyczy; 2) czas oddziaływania incydentu na świadczoną usługę: incydent spowodował brak możliwości świadczenia usługi przez czas dłuższy niż

			12 godzin; 3) zasięg geograficzny obszaru, którego dotyczy incydent: nie dotyczy; 4) inne czynniki charakterystyczne dla danego sektora lub podsektora: nie dotyczy.
		Incydent dotyczący bezpieczeństwa VTS (Służba Kontroli Ruchu Statków)	1) liczba użytkowników, których dotyczy zakłócenie świadczenia usługi: nie dotyczy; 2) czas oddziaływania incydentu na świadczoną usługę: nie dotyczy; 3) zasięg geograficzny obszaru, którego dotyczy incydent: nie dotyczy; 4) inne czynniki charakterystyczne dla danego sektora lub podsektora: incydent spowodował uszkodzenie systemów informacyjnych kluczowych dla

			funkcjonowania Służby VTS, powodujące zagrożenie dla zdrowia lub życia ludzkiego, środowiska naturalnego lub mienia albo dla funkcjonowania portu.
	Transport drogowy	Incydent dotyczący zarządzania drogami	1) liczba użytkowników, których dotyczy zakłócenie świadczenia usługi: nie dotyczy; 2) czas oddziaływania incydentu na świadczoną usługę: nie dotyczy; 3) zasięg geograficzny obszaru, którego dotyczy incydent: nie dotyczy; 4) inne czynniki charakterystyczne dla danego podsektora: incydent spowodował awarię sygnalizacji światłowej lub awarię innych urządzeń służących do informowania

			uczestników ruchu drogowego, w wyniku których doszło do wypadku, gdzie liczba zabitych lub rannych przekracza 11 osób.
		Incydent dotyczący inteligentnych systemów transportowych	1) liczba użytkowników, których dotyczy zakłócenie świadczenia usługi: nie dotyczy; 2) czas oddziaływania incydentu na świadczoną usługę: nie dotyczy; 3) zasięg geograficzny obszaru, którego dotyczy incydent: nie dotyczy; 4) inne czynniki charakterystyczne dla danego podsektora: a) incydent spowodował awarię sygnalizacji świetlnej lub awarię innych urządzeń służących do informowania uczestników ruchu drogowego, w wyniku których doszło do

			wypadku, gdzie liczba zabitych lub rannych przekracza 11 osób lub b) incydent spowodował brak wpływów z tytułu opłat za przejazd drogami krajowymi, oznaczający straty finansowe przekraczające 10 mln zł.
Bankowość i infrastruktura rynków finansowych		Incydent dotyczący funkcjonowania banków, instytucji kredytowych i infrastruktury rynków finansowych	1) liczba użytkowników, których dotyczy zakłócenie świadczenia usługi: nie dotyczy; 2) czas oddziaływania incydentu na świadczoną usługę: nie dotyczy; 3) zasięg geograficzny obszaru, którego dotyczy incydent: nie dotyczy; 4) inne czynniki charakterystyczne dla danego sektora lub podsektora: a) szacowana strata finansowa przekracza

			5 mln euro lub b) incydent będzie prowadził do naruszenia interesów osób trzecich, lub c) incydent doprowadził do uruchomienia planu awaryjnego umożliwiającego przywrócenie gotowości do pracy po wystąpieniu sytuacji nadzwyczajnej.
		Incydent dotyczący transakcji	1) liczba użytkowników, których dotyczy zakłócenie świadczenia usługi: nie dotyczy; 2) czas oddziaływania incydentu na świadczoną usługę: nie dotyczy; 3) zasięg geograficzny obszaru, którego dotyczy incydent: nie dotyczy; 4) inne czynniki charakterystyczne dla danego sektora lub podsektora: incydent

			obejmuje 25% płaćności (pod względem liczby transakcji) lub 5 mln euro realizowanych przez dany podmiot będący: a) instytucją kredytową, w rozumieniu art. 4 ust. 1 pkt 17 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe (Dz. U. z 2024 r. poz. 1646, z późn. zm.³⁾), b) bankiem krajowym, w rozumieniu art. 4 ust. 1 pkt 1 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe, c) oddziałem instytucji kredytowej w rozumieniu art. 4 ust. 1 pkt 18 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe, d) spółdzielczą kasą

³⁾ Zmiany tekstu jednolitego wymienianej ustawy zostały ogłoszone w Dz. U. z 2024 r. poz. 1685 i 1864 oraz z 2025 r. poz. 146, 222, 525, 769, 820, 1069, 1170, 1191 i 1216.

			oszczędnościowo-kredytową w rozumieniu ustawy z dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych (Dz. U. z 2025 r. poz. 379, 820, 1069, 1170 i 1191).
		Incydent dotyczący użytkowników usług płatniczych	1) liczba użytkowników, których dotyczy zakłócenie świadczenia usługi: nie dotyczy; 2) czas oddziaływania incydentu na świadczoną usługę: nie dotyczy; 3) zasięg geograficzny obszaru, którego dotyczy incydent: nie dotyczy; 4) inne czynniki charakterystyczne dla danego sektora lub podsektora: incydent obejmuje 50 000 użytkowników lub

			25% płatności realizowanych przez użytkowników danego podmiotu.
Ochrona zdrowia	Udzielanie świadczeń zdrowotnych i zdrowie publiczne	Incydent dotyczący systemu świadczenia świadczeń gwarantowanych	1) liczba użytkowników, których dotyczy zakłócenie świadczenia usługi: nie dotyczy; 2) czas oddziaływania incydentu na świadczoną usługę: incydent doprowadził do braku dostępności usługi powyżej 24 godzin; 3) zasięg geograficzny obszaru, którego dotyczy incydent: nie dotyczy; 4) inne czynniki charakterystyczne dla danego sektora lub podsektora: a) incydent doprowadził do braku poufności danych przetwarzanych w usłudze lub b) incydent doprowadził do braku

			integralności danych przetwarzanych w usłudze.
		Incydent dotyczący udzielania świadczenia opieki zdrowotnej	1) liczba użytkowników, których dotyczy zakłócenie świadczenia usługi: nie dotyczy; 2) czas oddziaływania incydentu na świadczoną usługę: incydent doprowadził do braku dostępności usługi powyżej 24 godzin; 3) zasięg geograficzny obszaru, którego dotyczy incydent: nie dotyczy; 4) inne czynniki charakterystyczne dla danego sektora lub podsektora: incydent spowodował co najmniej jedną z poniżej wymienionych okoliczności: a) śmierć człowieka, b) ciężki uszczerbek na zdrowiu,

			c) inny niż ciężki uszczerbek na zdrowiu więcej niż jednej osoby, d) brak poufności danych przetwarzanych w usłudze, e) brak integralności danych przetwarzanych w usłudze.
		Incydent dotyczący gromadzenia i udostępniania elektronicznej dokumentacji medycznej	1) liczba użytkowników, których dotyczy zakłócenie świadczenia usługi: nie dotyczy; 2) czas oddziaływania incydentu na świadczoną usługę: incydent doprowadził do braku dostępności usługi powyżej 1 godziny; 3) zasięg geograficzny obszaru, którego dotyczy incydent: nie dotyczy; 4) inne czynniki charakterystyczne dla danego sektora lub

			podsektora: a) incydent doprowadził do braku poufności danych przetwarzanych w usłudze lub b) incydent doprowadził do braku integralności danych przetwarzanych w usłudze.
		Incydent dotyczący zarządzania danymi epidemiologicznymi	1) liczba użytkowników, których dotyczy zakłócenie świadczenia usługi: nie dotyczy; 2) czas oddziaływania incydentu na świadczoną usługę: incydent doprowadził do braku dostępności usługi powyżej 2 godzin; 3) zasięg geograficzny obszaru, którego dotyczy incydent: nie dotyczy; 4) inne czynniki charakterystyczne dla danego sektora lub podsektora:

			a) incydent doprowadził do braku poufności danych przetwarzanych w usłudze lub b) incydent doprowadził do braku integralności danych przetwarzanych w usłudze.
		Incydent dotyczący dowodzenia jednostkami systemu Państwowego Ratownictwa Medycznego	1) liczba użytkowników, których dotyczy zakłócenie świadczenia usługi: nie dotyczy; 2) czas oddziaływania incydentu na świadczoną usługę: incydent doprowadził do braku dostępności usługi powyżej 1 godziny; 3) zasięg geograficzny obszaru, którego dotyczy incydent: nie dotyczy; 4) inne czynniki charakterystyczne dla danego sektora lub podsektora: incydent spowodował co

			najmniej jedną z poniżej wymienionych okoliczności: a) śmierć człowieka, b) ciężki uszczerbek na zdrowiu, c) inny niż ciężki uszczerbek na zdrowiu więcej niż jednej osoby, d) brak poufności danych przetwarzanych w usłudze, e) brak integralności danych przetwarzanych w usłudze.
	Produkcja i dystrybucja substancji czynnych, produktów leczniczych i wyrobów medycznych	Incydent dotyczący obrotu i dystrybucji produktów leczniczych	1) liczba użytkowników, których dotyczy zakłócenie świadczenia usługi: nie dotyczy; 2) czas oddziaływania incydentu na świadczoną usługę: incydent doprowadził do braku dostępności usługi powyżej 24 godzin;

			3) zasięg geograficzny obszaru, którego dotyczy incydent: nie dotyczy; 4) inne czynniki charakterystyczne dla danego sektora lub podsektora: incydent spowodował co najmniej jedną z poniżej wymienionych okoliczności: a) śmierć człowieka, b) ciężki uszczerbek na zdrowiu, c) inny niż ciężki uszczerbek na zdrowiu więcej niż jednej osoby, d) brak poufności danych przetwarzanych w usłudze, e) brak integralności danych przetwarzanych w usłudze.
Zaopatrzenie w wodę pitną i jej dystrybucja		Incydent dotyczący poboru wody	1) liczba użytkowników, których dotyczy zakłócenie

			świadczenia usługi: incydent doprowadził do braku dostępności usługi dla co najmniej 100 000 użytkowników przez czas dłuższy niż 8 godzin; 2) czas oddziaływania incydentu na świadczoną usługę: nie dotyczy; 3) zasięg geograficzny obszaru, którego dotyczy incydent: terenu 2 lub więcej gmin; 4) inne czynniki charakterystyczne dla danego sektora lub podsektora: nie dotyczy.
		Incydent dotyczący uzdatniania wody	1) liczba użytkowników, których dotyczy zakłócenie świadczenia usługi: incydent doprowadził do braku dostępności usługi dla co najmniej 100 000 użytkowników przez

			czas dłuższy niż 8 godzin; 2) czas oddziaływania incydentu na świadczoną usługę: nie dotyczy; 3) zasięg geograficzny obszaru, którego dotyczy incydent: terenu 2 lub więcej gmin; 4) inne czynniki charakterystyczne dla danego sektora lub podsektora: nie dotyczy.
		Incydent dotyczący dostarczania wody	1) liczba użytkowników, których dotyczy zakłócenie świadczenia usługi: incydent doprowadził do braku dostępności usługi dla co najmniej 100 000 użytkowników przez czas dłuższy niż 8 godzin; 2) czas oddziaływania incydentu na świadczoną usługę: nie dotyczy;

			3) zasięg geograficzny obszaru, którego dotyczy incydent: incydent dotyczy terenu 2 lub więcej gmin; 4) inne czynniki charakterystyczne dla danego sektora lub podsektora: nie dotyczy.
Zbiorowe odprowadzanie ścieków		Incydent dotyczący odprowadzania ścieków	1) liczba użytkowników, których dotyczy zakłócenie świadczenia usługi: incydent doprowadził do braku dostępności usługi dla co najmniej 100 000 równoważnej liczby mieszkańców (RLM) przez czas dłuższy niż 8 godzin; 2) czas oddziaływania incydentu na świadczoną usługę: nie dotyczy; 3) zasięg geograficzny obszaru, którego dotyczy incydent: nie dotyczy; 4) inne czynniki

			charakterystyczne dla danego sektora lub podsektora: nie dotyczy.
		Incydent dotyczący oczyszczania ścieków	1) liczba użytkowników, których dotyczy zakłócenie świadczenia usługi: incydent doprowadził do braku dostępności usługi dla co najmniej 100 000 RLM przez czas dłuższy niż 8 godzin; 2) czas oddziaływania incydentu na świadczoną usługę: nie dotyczy; 3) zasięg geograficzny obszaru, którego dotyczy incydent: nie dotyczy; 4) inne czynniki charakterystyczne dla danego sektora lub podsektora: nie dotyczy.
Infrastruktura cyfrowa	Infrastruktura cyfrowa z wyłączeniem komunikacji	Incydent dotyczący prowadzenia punktu wymiany ruchu internetowego (IXP)	1) liczba użytkowników, których dotyczy zakłócenie

	elektronicznej		świadczenia usługi: nie dotyczy; 2) czas oddziaływania incydentu na świadczoną usługę: nieplanowany brak dostępności usługi przez co najmniej 8 godzin; 3) zasięg geograficzny obszaru, którego dotyczy incydent: nie dotyczy; 4) inne czynniki charakterystyczne dla danego sektora lub podsektora: nie dotyczy.
		Incydent dotyczący świadczania usługi rejestracji nazw domen.	1) liczba użytkowników, których dotyczy zakłócenie świadczania usługi: nie dotyczy; 2) czas oddziaływania incydentu na świadczoną usługę: nieplanowany brak dostępności usługi przez co najmniej 8 godzin; 3) zasięg geograficzny

			obszaru, którego dotyczy incydent: nie dotyczy; 4) inne czynniki charakterystyczne dla danego sektora lub podsektora: nie dotyczy.
	Komunikacja elektroniczna	Incydent dotyczący komunikacji elektronicznej	1) liczba użytkowników, których dotyczy zakłócenie świadczenia usługi: incydent doprowadził do braku dostępności usługi dla co najmniej 10 000 użytkowników końcowych przez czas dłuższy niż 8 godzin; 2) czas oddziaływania incydentu na świadczoną usługę: nie dotyczy; 3) zasięg geograficzny obszaru, którego dotyczy incydent: incydent dotyczy obszaru co najmniej 2 powiatów; 4) inne czynniki charakterystyczne dla danego sektora lub

			podsektora: a) incydent uniemożliwia realizację zadań obowiązków na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego, b) incydent skutkuje niedostępnością numerów alarmowych i liczba użytkowników danego przedsiębiorcy telekomunikacyjnego pozbawionych możliwości wykonywania połączeń z numerami alarmowymi przekroczyła: – 10 000 przez co najmniej 15 minut lub – 100 000.
Przestrzeń kosmiczna		Incydent dotyczący funkcjonowania operatora infrastruktury naziemnej, który wspiera świadczenie	1) liczba użytkowników, których dotyczy zakłócenie świadczenia usługi: nie dotyczy;

		usług kosmicznych	2) czas oddziaływania incydentu na świadczoną usługę: incydent spowodował niedostępność usługi powyżej 8 godzin, 3) zasięg geograficzny obszaru, którego dotyczy incydent: nie dotyczy; 4) inne czynniki charakterystyczne dla danego sektora lub podsektora: nie dotyczy
Podmioty publiczne		Incydent dotyczący realizacji zadania publicznego	1) liczba użytkowników, których dotyczy zakłócenie świadczenia usługi: nie dotyczy; 2) czas oddziaływania incydentu na świadczoną usługę: incydent doprowadził do braku dostępności usługi powyżej 8 godzin; 3) zasięg geograficzny obszaru, którego dotyczy incydent: nie dotyczy;

			4) inne czynniki charakterystyczne dla danego sektora lub podsektora: incydent spowodował co najmniej jedną z poniżej wymienionych okoliczności: a) brak poufności danych przetwarzanych w usłudze, b) brak integralności danych przetwarzanych w usłudze.
Usługi pocztowe		Incydent dotyczący usług pocztowych	1) liczba użytkowników, których dotyczy zakłócenie świadczenia usługi: nie dotyczy; 2) czas oddziaływania incydentu na świadczoną usługę: incydent doprowadził do braku dostępności usługi powyżej 8 godzin; 3) zasięg geograficzny obszaru, którego

			dotyczy incydent: nie dotyczy; 4) inne czynniki charakterystyczne dla danego sektora lub podsektora: incydent uniemożliwia realizację zadań i obowiązków operatora pocztowego na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego.
Inwestycje energetyki jądrowej		Incydent dotyczący budowy obiektu energetyki jądrowej	1) liczba użytkowników, których dotyczy zakłócenie świadczenia usługi: nie dotyczy; 2) czas oddziaływania incydentu na świadczoną usługę: nie dotyczy; 3) zasięg geograficzny obszaru, którego dotyczy incydent: nie dotyczy; 4) inne czynniki charakterystyczne dla

			danego sektora lub podsektora: incydent spowodował co najmniej jedną z poniżej wymienionych okoliczności: a) brak poufności danych przetwarzanych w usłudze, b) brak integralności danych przetwarzanych w usłudze.
Gospodarowanie odpadami	Zbieranie odpadów	Incydent dotyczący zbierania odpadów	1) liczba użytkowników, których dotyczy zakłócenie świadczenia usługi: incydent doprowadził do braku dostępności usługi dla co najmniej 100 000 RLM przez czas dłuższy niż 8 godzin; 2) czas oddziaływania incydentu na świadczoną usługę: nie dotyczy; 3) zasięg geograficzny obszaru, którego

			dotyczy incydent: nie dotyczy; 4) inne czynniki charakterystyczne dla danego sektora lub podsektora: nie dotyczy.
	Transport odpadów	Incydent dotyczący transportu odpadów	1) liczba użytkowników, których dotyczy zakłócenie świadczenia usługi: incydent doprowadził do braku dostępności usługi dla co najmniej 100 000 RLM przez czas dłuższy niż 8 godzin; 2) czas oddziaływania incydentu na świadczoną usługę: nie dotyczy; 3) zasięg geograficzny obszaru, którego dotyczy incydent: nie dotyczy; 4) inne czynniki charakterystyczne dla danego sektora lub podsektora: nie dotyczy.
	Przetwarzanie	Incydent dotyczący	1) liczba

	odpadów, w tym sortowanie, wraz z nadzorem nad wymienionymi działaniami, a także późniejsze postępowanie z miejscami unieszkodliwiania odpadów	przetwarzania odpadów	użytkowników, których dotyczy zakłócenie świadczenia usługi: incydent doprowadził do braku dostępności usługi dla co najmniej 100 000 użytkowników przez czas dłuższy niż 8 godzin; 2) czas oddziaływania incydentu na świadczoną usługę: nie dotyczy; 3) zasięg geograficzny obszaru, którego dotyczy incydent: nie dotyczy; 4) inne czynniki charakterystyczne dla danego sektora lub podsektora: nie dotyczy.
	Działania wykonywane w charakterze sprzedawcy odpadów lub pośrednika w obrocie odpadami	Incydent dotyczący sprzedaży lub obrotu odpadami	1) liczba użytkowników, których dotyczy zakłócenie świadczenia usługi: nie dotyczy; 2) czas oddziaływania incydentu na

			świadczoną usługę: incydent skutkuje nieдоступnością systemów służących sprzedażą lub obrotem odpadami powyżej 8 godzin; 3) zasięg geograficzny obszaru, którego dotyczy incydent: nie dotyczy; 4) inne czynniki charakterystyczne dla danego sektora lub podsektora: nie dotyczy.
Produkcja, wytwarzanie i dystrybucja chemikaliów		Incydent dotyczący wytwarzania i dystrybucji chemikaliów	1) liczba użytkowników, których dotyczy zakłócenie świadczenia usługi: nie dotyczy; 2) czas oddziaływania incydentu na świadczoną usługę: a) incydent skutkuje zakłóceniem w produkcji chemikaliów, w okresie dłuższym niż 4 godziny, lub b) incydent skutkuje

			przerwą w dostawie chemikaliów przez okres powyżej 8 godzin, 3) zasięg geograficzny obszaru, którego dotyczy incydent: nie dotyczy; 4) inne czynniki charakterystyczne dla danego podsektora: nie dotyczy.
Produkcja, przetwarzanie i dystrybucja żywności		Incydent dotyczący przetwarzania i dystrybucji żywności	1) liczba użytkowników, których dotyczy zakłócenie świadczenia usługi: nie dotyczy; 2) czas oddziaływania incydentu na świadczoną usługę: a) incydent skutkuje zakłóceniem w przetwarzaniu żywności, w okresie dłuższym niż 4 godziny lub b) incydent skutkuje przerwą w dostawie żywności przez okres powyżej 8 godzin, lub 3) zasięg geograficzny

			obszaru, którego dotyczy incydent: nie dotyczy; 4) inne czynniki charakterystyczne dla danego podsektora: nie dotyczy.
Produkcja	Produkcja wyrobów medycznych i wyrobów medycznych do diagnostyki in vitro	Incydent dotyczący wytwarzania wyrobów medycznych i wyrobów medycznych do diagnostyki in vitro	1) liczba użytkowników, których dotyczy zakłócenie świadczenia usługi: nie dotyczy; 2) czas oddziaływania incydentu na świadczoną usługę: a) incydent skutkuje zakłóceniem w wytwarzania wyrobów medycznych i wyrobów medycznych do diagnostyki in vitro dłuższym niż 4 godziny lub b) incydent skutkuje przerwą w dostawie wytwarzania wyrobów medycznych i wyrobów medycznych do diagnostyki in vitro

			przez okres powyżej 8 godzin, 3) zasięg geograficzny obszaru, którego dotyczy incydent: nie dotyczy; 4) inne czynniki charakterystyczne dla danego podsektora: nie dotyczy.
	Produkcja komputerów, wyrobów elektronicznych i optycznych	Incydent dotyczący produkcji komputerów, wyrobów elektronicznych i optycznych	1) liczba użytkowników, których dotyczy zakłócenie świadczenia usługi: nie dotyczy; 2) czas oddziaływania incydentu na świadczoną usługę: incydent skutkuje niedostępnością produkcji dłuższą niż 8 godzin, 3) zasięg geograficzny obszaru, którego dotyczy incydent: nie dotyczy; 4) inne czynniki charakterystyczne dla danego podsektora: nie dotyczy.
	Produkcja urządzeń	Incydent dotyczący	1) liczba

	elektrycznych	produkcji urządzeń elektrycznych	użytkowników, których dotyczy zakłócenie świadczenia usługi: nie dotyczy; 2) czas oddziaływania incydentu na świadczoną usługę: incydent skutkuje nieдоступnością produkcji dłuższą niż 8 godzin, 3) zasięg geograficzny obszaru, którego dotyczy incydent: nie dotyczy; 4) inne czynniki charakterystyczne dla danego podsektora: nie dotyczy.
	Produkcja maszyn i urządzeń, gdzie indziej niesklasyfikowana	Incydent dotyczący produkcji maszyn i urządzeń, gdzie indziej niesklasyfikowana	1) liczba użytkowników, których dotyczy zakłócenie świadczenia usługi: nie dotyczy; 2) czas oddziaływania incydentu na świadczoną usługę: incydent skutkuje nieдоступnością produkcji dłuższą niż

			8 godzin, 3) zasięg geograficzny obszaru, którego dotyczy incydent: nie dotyczy; 4) inne czynniki charakterystyczne dla danego podsektora: nie dotyczy.
	Produkcja pojazdów samochodowych, przyczep i naczep	Incydent dotyczący produkcji pojazdów samochodowych, przyczep i naczep	1) liczba użytkowników, których dotyczy zakłócenie świadczenia usługi: nie dotyczy; 2) czas oddziaływania incydentu na świadczoną usługę: incydent skutkuje niedostępnością produkcji dłuższą niż 8 godzin, 3) zasięg geograficzny obszaru, którego dotyczy incydent: nie dotyczy; 4) inne czynniki charakterystyczne dla danego podsektora: nie dotyczy.
	Produkcja pozostałego sprzętu	Incydent dotyczący produkcji pozostałego	1) liczba użytkowników,

	transportowego	sprzętu transportowego	których dotyczy zakłócenie świadczenia usługi: nie dotyczy; 2) czas oddziaływania incydentu na świadczoną usługę: incydent skutkuje niedostępnością produkcji dłuższą niż 8 godzin, 3) zasięg geograficzny obszaru, którego dotyczy incydent: nie dotyczy; 4) inne czynniki charakterystyczne dla danego podsektora: nie dotyczy.
Badania naukowe		Incydent dotyczący organizacji badań naukowych	1) liczba użytkowników, których dotyczy zakłócenie świadczenia usługi: nie dotyczy; 2) czas oddziaływania incydentu na świadczoną usługę: incydent skutkuje niedostępnością systemów służących badaniom naukowym

			dłuższą niż 8 godzin, 3) zasięg geograficzny obszaru, którego dotyczy incydent: nie dotyczy; 4) inne czynniki charakterystyczne dla danego podsektora: nie dotyczy.

UZASADNIENIE

Projektowane rozporządzenie stanowi wykonanie upoważnienia ustawowego zawartego w art. 11 ust. 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077 i 1222 oraz z 2025 r. poz. 1017, 1069 i ...), zwanej dalej „ustawą”, i określa progi uznania incydentu za poważny według rodzaju zdarzenia w poszczególnych sektorach i podsektorach określonych w załączniku nr 1 i 2 do ustawy. Wydając projektowane rozporządzenie Rada Ministrów uwzględnia:

- 1) liczbę użytkowników, których dotyczy zakłócenie świadczenia usługi;
 - 2) czas oddziaływania incydentu na świadczoną usługę;
 - 3) zasięg geograficzny obszaru, którego dotyczy incydent;
 - 4) inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują
- kierując się potrzebą zapewnienia ochrony przed zagrożeniem życia lub zdrowia ludzi, znacznymi stratami majątkowymi oraz obniżeniem jakości świadczonej usługi.

Projektowane rozporządzenie będzie wykorzystywane przez podmioty kluczowe i podmioty ważne w procesie zgłaszania i obsługi incydentu. Podmioty kluczowe i podmioty ważne identyfikując incydent i rejestrując go, będą dokonywały klasyfikacji incydentu na podstawie progów uznawania incydentu za poważny. Progi, w zależności od rodzaju zdarzenia, określają liczbę użytkowników, których dotyczy zakłócenie świadczenia usługi, czas oddziaływania incydentu na świadczoną usługę, zasięg geograficzny obszaru, którego dotyczy incydent lub inne czynniki charakterystyczne dla danego sektora lub podsektora.

Przygotowując projektowane rozporządzenie uwzględniono fakt, że dla niektórych podmiotów kluczowych i podmiotów ważnych progi incydentu zostały ustalone w rozporządzeniu wykonawczym Komisji (UE) 2024/2690 z dnia 17 października 2024 r. ustanawiającym zasady stosowania dyrektywy (UE) 2022/2555 w odniesieniu do wymogów technicznych i metodycznych dotyczących środków zarządzania ryzykiem w cyberbezpieczeństwie oraz doprecyzowujące przypadki, w których incydent uznaje się za poważny w odniesieniu do dostawców usług DNS, rejestrów nazw TLD, dostawców usług chmurowych, dostawców usług ośrodka przetwarzania danych, dostawców sieci dostarczania treści, dostawców usług zarządzanych, dostawców usług zarządzanych w zakresie bezpieczeństwa, dostawców internetowych platform handlowych, wyszukiwarek internetowych i platform usług sieci społecznościowych oraz dostawców usług zaufania. Dlatego nie wskazano progów incydentów dla następujących rodzajów podmiotów:

Sektor	Rodzaj podmiotu
Infrastruktura cyfrowa	Dostawca usług DNS, z wyłączeniem operatorów głównych serwerów nazw.
	Rejestr nazw domen najwyższego poziomu (TLD).
	Dostawca chmury obliczeniowej.
	Dostawca usług centrum przetwarzania danych.
	Dostawca sieci dostarczania treści.
	Dostawca usług zaufania.
Zarządzanie usługami ICT	Dostawca usług zarządzanych.
	Dostawca usług zarządzanych w zakresie cyberbezpieczeństwa.
Dostawcy usług cyfrowych	Dostawca internetowej platformy handlowej.
	Dostawca wyszukiwarki internetowej.
	Dostawca platformy sieci usług społecznościowych.

W zakresie sektora „Infrastruktury cyfrowej” ustalono progi dla pozostałych podmiotów z tego sektora, którym Komisja Europejska nie ustaliła progów incydentów w rozporządzeniu wykonawczym, to jest dla dostawcy punktu wymiany ruchu internetowego, podmiotu świadczącego usługę rejestracji nazw domen oraz przedsiębiorcy komunikacji elektronicznej.

Projektowane rozporządzenie wejdzie w życie po upływie 14 dni od dnia ogłoszenia.

Projekt rozporządzenia jest zgodny z prawem Unii Europejskiej.

Projekt rozporządzenia nie podlega przedstawieniu właściwym organom i instytucjom Unii Europejskiej, w tym Europejskiemu Bankowi Centralnemu, w celu uzyskania opinii, dokonania powiadomienia, konsultacji albo uzgodnienia.

Projektowana regulacja nie zawiera przepisów technicznych w rozumieniu rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. poz. 2039 oraz z 2004 r. poz. 597) i nie podlega notyfikacji Komisji Europejskiej.

Projektowana regulacja nie będzie wymagała notyfikacji Komisji Europejskiej w trybie ustawy z dnia 30 kwietnia 2004 r. o postępowaniu w sprawach dotyczących pomocy publicznej (Dz. U. z 2025 r. poz. 468).

Wejście w życie rozporządzenia nie będzie miało wpływu na działalność mikroprzedsiębiorców, małych przedsiębiorców.

Wejście w życie projektowanego rozporządzenia będzie miało wpływ na działalność średnich przedsiębiorców, którzy są podmiotami kluczowymi lub podmiotami ważnymi. Niezależnie od wielkości podmiotu rozporządzenie będzie miało wpływ na podmioty świadczące usługi rejestracji nazw domen oraz na przedsiębiorców komunikacji elektronicznej. Wynika to z przepisów ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, które nakładają na te podmioty obowiązek zgłoszenia incydentu poważnego niezależnie od wielkości podmiotu. Okazjonalnie może się zdarzyć że rozporządzenie będzie miało wpływ na mikroprzedsiębiorców i małych przedsiębiorców z innych sektorów. Będzie się tak działo, jeżeli będzie to dotyczyć podmiotów krytycznych (w rozumieniu – dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylającej dyrektywę Rady 2008/114/WE (Dz. Urz. UE L 333 z 27.12.2022, str. 164) (dyrektywy CER)) oraz podmiotów, które zostały uznane jako podmiot kluczowy albo podmiot ważny w drodze decyzji administracyjnej. Są to jednak sytuacje wyjątkowe.

Obowiązek zgłoszenia incydentu poważnego może się wydawać obciążeniem, jednakże trzeba pamiętać, że wiąże się z tym pomoc właściwego CSIRT sektorowego podczas etapu reagowania na ten incydent. Ponadto są to zdarzenia, które uniemożliwiają świadczenie usług przez dany podmiot kluczowy lub podmiot ważny – zgłoszenie incydentu poważnego i pomoc zespołu CSIRT przyspieszy.

Stosownie do postanowień art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingsowej w procesie stanowienia prawa (Dz. U. z 2025 r. poz. 677), projekt zostanie udostępniony na stronie Rządowego Centrum Legislacji w serwisie „Rządowy Proces Legislacyjny” oraz w Biuletynie Informacji Publicznej na stronie podmiotowej urzędu obsługującego ministra właściwego do spraw informatyzacji. Ponadto, zgodnie z § 52 ust. 1 uchwały nr 190 Rady Ministrów z dnia 29 października 2013 r. – Regulamin pracy Rady Ministrów (M.P. z 2024 r. poz. 806 oraz z 2025 r. poz. 408).

Nazwa projektu Rozporządzenie Rady Ministrów w sprawie progów uznania incydentu za poważny Ministerstwo wiodące i ministerstwa współpracujące Ministerstwo Cyfryzacji Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu Paweł Olszewski, Sekretarz Stanu w Ministerstwie Cyfryzacji Kontakt do opiekuna merytorycznego projektu Łukasz Wojewoda, dyrektor Departamentu Cyberbezpieczeństwa w Ministerstwie Cyfryzacji, Marcin Wysocki, zastępca dyrektora Departamentu Cyberbezpieczeństwa w Ministerstwie Cyfryzacji, e-mail: sekretariat.dc@cyfra.gov.pl tel. + 48 22 245 59 22	Data sporządzenia 06.10.2025 Źródło: art. 11 ust. 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077 i 1222 oraz z 2025 r. poz. 1017, 1069 i ...) Nr w wykazie prac legislacyjnych i programowych Rady Ministrów Kliknij lub naciśnij tutaj, aby wprowadzić tekst.

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

W związku z nowelizacją ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa zaistniała konieczność dostosowania rozwiązań wynikających ustawy w rozporządzeniu Rady Ministrów z dnia 31 października 2018 r. w sprawie progów uznania incydentu za poważny (Dz. U. poz. 2180). Dotyczy to uznania za poważny incydent występującego w podmiocie kluczowym lub w podmiocie ważnym. Taki incydent podlega obligatoryjnemu zgłoszeniu do zespołu CSIRT sektorowego. Brak zgłoszenia spowoduje konieczność nałożenia administracyjnej kary pieniężnej.

Jedynym sposobem rozwiązania tego problemu jest wydanie projektowanego rozporządzenia.

2. Rekomendowane rozwiązanie, w tym planowane narzędzia interwencji, i oczekiwany efekt

Projektowane rozporządzenie będzie wykorzystywane przez podmioty kluczowe i podmioty ważne w procesie zgłaszania i obsługi incydentu. Podmioty kluczowe i podmioty ważne identyfikując incydent i rejestrując go, będą dokonywały klasyfikacji incydentu na podstawie progów uznawania incydentu za poważny. Progi, w zależności od rodzaju zdarzenia, określają liczbę użytkowników, których dotyczy zakłócenie świadczenia usługi, czas oddziaływania incydentu na świadczoną usługę, zasięg geograficzny obszaru, którego dotyczy incydent lub inne czynniki charakterystyczne dla danego sektora lub podsektora.

Projektowane rozporządzenie określa rodzaj zdarzenia i progi powodujące uznanie incydentu za poważny.

3. Jak problem został rozwiązany w innych krajach, w szczególności krajach członkowskich OECD/UE?

Z uwagi na szczegółowość regulacji odstępiono od analizy prawno-porównawczej projektu rozporządzenia na tle innych państw.

4. Podmioty, na które oddziałuje projekt

Grupa	Wielkość	Źródło danych	Oddziaływanie
podmioty kluczowe i podmioty ważne z podsektora produkcji wyrobów medycznych i wyrobów medycznych do diagnostyki in vitro	44	REGON PKD sekcja C dział 32 podklasa 3250z	Dzięki określeniu kryteriów uznania incydentu za incydent poważny podmioty z tego sektora będą wiedziały kiedy należy zgłosić incydent do zespołu CSIRT sektorowego.
podmioty kluczowe i podmioty ważne z sektora podmiotów publicznych	27905	REGON	Dzięki określeniu kryteriów uznania incydentu za incydent poważny podmioty z tego sektora będą wiedziały

			kiedy należy zgłosić incydent do zespołu CSIRT sektorowego.
podmioty ważne z sektora badań naukowych	169	REGON PKD sekcja M dział 72 podklasa: 7219Z Badania naukowe i prace rozwojowe w dziedzinie pozostałych nauk przyrodniczych i technicznych 7220Z Badania naukowe i prace rozwojowe w dziedzinie nauk społecznych i humanistycznych	Dzięki określeniu kryteriów uznania incydentu za incydent poważny podmioty z tego sektora będą wiedziały kiedy należy zgłosić incydent do zespołu CSIRT sektorowego.
podmioty kluczowe i podmioty ważne z sektora bankowości i infrastruktury rynków finansowych	547	szacunki KNF	Dzięki określeniu kryteriów uznania incydentu za incydent poważny podmioty z tego sektora będą wiedziały kiedy należy zgłosić incydent do zespołu CSIRT sektorowego.
podmioty kluczowe i podmioty ważne z sektora energii	365	szacunki Ministerstwa Klimatu i Środowiska	Dzięki określeniu kryteriów uznania incydentu za incydent poważny podmioty z tego sektora będą wiedziały kiedy należy zgłosić incydent do zespołu CSIRT sektorowego.
podmioty ważne z sektora gospodarowania odpadami	276	REGON PKD: sekcja E dział 38 podklasa 3811Z Zbieranie odpadów innych niż niebezpieczne sekcja E dział 38 podklasa 3812Z Zbieranie odpadów niebezpiecznych sekcja E dział 38 podklasa 3821Z Obróbka i usuwanie odpadów innych niż niebezpieczne sekcja E dział 38 podklasa 3822Z Przetwarzanie i unieszkodliwianie odpadów niebezpiecznych	Dzięki określeniu kryteriów uznania incydentu za incydent poważny podmioty z tego sektora będą wiedziały kiedy należy zgłosić incydent do zespołu CSIRT sektorowego.

		sekcja E dział 38 podklasa 3831Z Demontaż wyrobów zużytych sekcja E dział 38 podklasa 3832Z Odzysk surowców z materiałów segregowanych sekcja E dział 38 podklasa 3900Z Działalność związana z rekultywacją i pozostała działalność usługowa związana z gospodarką odpadami	
podmioty kluczowe i podmioty ważne z podsektora komunikacji elektronicznej	3784 w zakresie podmiotów świadczących usługę komunikacji interpersonalnej niewykorzystującej numerów (OTT-1) brak danych	Rejestr przedsiębiorców telekomunikacyjnych	Dzięki określeniu kryteriów uznania incydentu za incydent poważny podmioty z tego sektora będą wiedziały kiedy należy zgłosić incydent do zespołu CSIRT sektorowego.
podmioty ważne z sektora poczty	280	Rejestr operatorów pocztowych	Dzięki określeniu kryteriów uznania incydentu za incydent poważny podmioty z tego sektora będą wiedziały kiedy należy zgłosić incydent do zespołu CSIRT sektorowego.
podmioty kluczowe i podmioty ważne z sektora produkcja, przetwarzanie i dystrybucja żywności	1204	REGON PKD: sekcja C dział 10 Produkcja artykułów spożywczych sekcja H dział 46 podklasa 4631Z Sprzedaż hurtowa owoców i warzyw sekcja H dział 46 podklasa 4632Z Sprzedaż hurtowa mięsa i wyrobów z mięsa sekcja H dział 46 podklasa 4633Z Sprzedaż hurtowa mleka, wyrobów mleczarskich, jaj, olejów i tłuszczów jadalnych	Dzięki określeniu kryteriów uznania incydentu za incydent poważny podmioty z tego sektora będą wiedziały kiedy należy zgłosić incydent do zespołu CSIRT sektorowego.

		sekcja H dział 46 podklasa 4634A Sprzedaż hurtowa napojów alkoholowych sekcja H dział 46 podklasa 4634B Sprzedaż hurtowa napojów bezalkoholowych	
podmioty kluczowe i podmioty ważne z sektora produkcja, wytwarzanie i dystrybucja chemikaliów	214	REGON PKD sekcja C dział 20 Produkcja chemikaliów i wyrobów chemicznych	Dzięki określeniu kryteriów uznania incydentu za incydent poważny podmioty z tego sektora będą wiedziały kiedy należy zgłosić incydent do zespołu CSIRT sektorowego.
podmioty kluczowe i podmioty ważne z sektora produkcji, z wyłączeniem wyrobów medycznych	1120	REGON PKD sekcja C dział 26 Produkcja komputerów, wyrobów elektronicznych i optycznych PKD sekcja C dział 27 Produkcja urządzeń elektrycznych PKD sekcja C dział 28 Produkcja maszyn i urządzeń, gdzie indziej niesklasyfikowana PKD sekcja C dział 29 Produkcja pojazdów samochodowych, przyczep i naczep, z wyłączeniem motocykli PKD sekcja C dział 30 Produkcja pozostałego sprzętu transportowego	Dzięki określeniu kryteriów uznania incydentu za incydent poważny podmioty z tego sektora będą wiedziały kiedy należy zgłosić incydent do zespołu CSIRT sektorowego.
podmioty kluczowe i podmioty ważne z sektora ścieków	102	REGON PKD sekcja E dział 37 podklasa 3700z Odprowadzanie i oczyszczanie ścieków	Dzięki określeniu kryteriów uznania incydentu za incydent poważny podmioty z tego sektora będą wiedziały kiedy należy zgłosić incydent do zespołu CSIRT sektorowego.
podmioty kluczowe i podmioty ważne z sektora transportu	co najmniej 450	szacunki Ministerstwa Infrastruktury	Dzięki określeniu kryteriów uznania incydentu za incydent poważny podmioty z tego sektora będą wiedziały kiedy należy zgłosić incydent do zespołu CSIRT sektorowego.

podmioty kluczowe i podmioty ważne z sektora transportu wodnego	11	REGON	Dzięki określeniu kryteriów uznania incydentu za incydent poważny podmioty z tego sektora będą wiedziały kiedy należy zgłosić incydent do zespołu CSIRT sektorowego.
podmioty kluczowe i podmioty ważne z sektora wody pitnej	268	REGON PKD Sekcja E dział 36 podklasa 3600Z Pobór, uzdatnianie i dostarczanie wody	Dzięki określeniu kryteriów uznania incydentu za incydent poważny podmioty z tego sektora będą wiedziały kiedy należy zgłosić incydent do zespołu CSIRT sektorowego.
podmioty kluczowe i podmioty ważne z sektora zdrowia	1248	REGON PKD Dział 21 Produkcja podstawowych substancji farmaceutycznych oraz leków i pozostałych wyrobów farmaceutycznych PKD Dział 86 Opieka zdrowotna PKD sekcja M dział 72 podklasa 7211Z Badania naukowe i prace rozwojowe w dziedzinie biotechnologii rozporządzenie Ministra Zdrowia z dnia 19 czerwca 2012 r. w sprawie wykazu laboratoriów referencyjnych	Dzięki określeniu kryteriów uznania incydentu za incydent poważny podmioty z tego sektora będą wiedziały kiedy należy zgłosić incydent do zespołu CSIRT sektorowego.
CSIRT MON, CSIRT NASK, CSIRT GOV	3	informacje ogólnodostępne	Prawidłowe określenie kryteriów uznania incydentu za incydent poważny umożliwi zgłoszenie incydentów w istotny sposób wpływających na społeczeństwo i gospodarkę do zespołów CSIRT. Te zespoły następnie będą w stanie zaradzić problemowi.
CSIRT sektorowe	co najmniej 10 (obejmujące wszystkie sektory z ustawy o krajowym systemie cyberbezpieczeństwa)	informacje ogólnodostępne	

5. Informacje na temat zakresu, czasu trwania i podsumowanie wyników konsultacji

Stosownie do postanowień art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingsowej w procesie stanowienia prawa (Dz. U. z 2025 r. poz. 677), projekt rozporządzenia zostanie udostępniony w Biuletynie Informacji Publicznej na stronie podmiotowej urzędu obsługującego ministra właściwego do spraw informatyzacji. Ponadto zgodnie z § 52 ust. 1 uchwały nr 190 Rady Ministrów z dnia 29 października 2013 r. – Regulamin pracy Rady Ministrów (M.P. z 2024 r. poz. 806 oraz z 2025 r. poz. 408), projekt rozporządzenia zostanie udostępniony

Projekt rozporządzenia zostanie przekazany do konsultacji publicznych i opiniowania, w tym zostanie skonsultowany z organizacjami zrzeszającymi podmioty krajowego systemu cyberbezpieczeństwa. Wyniki przeprowadzonych konsultacji publicznych i opiniowania zostaną omówione w raporcie z konsultacji.

[illegible]

Źródła finansowania	Projekt rozporządzenia nie ma wpływu na wydatki sektora finansów publicznych.

Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	

Czas w latach od wejścia w życie zmian		Skutki						
		0	1	2	3	5	10	<i>Łącznie (0-10)</i>
W ujęciu pieniężnym (w mln zł, ceny stałe z r.)	duże przedsiębiorstwa							
	sektor mikro-, małych i średnich przedsiębiorstw							
	rodzina, obywatele oraz gospodarstwa domowe							

W ujęciu niepieniężny m	duże przedsiębiorstwa	Duże przedsiębiorstwa, które są podmiotami kluczowymi lub podmiotami ważnymi uzyskują informacje, kiedy mają obowiązek zgłosić incydent do CSIRT sektorowego.
	sektor mikro-, małych i średnich przedsiębiorstw	Średnie przedsiębiorstwa, które są podmiotami kluczowymi lub podmiotami ważnymi, a także w wyjątkowych przypadkach mikro i małe przedsiębiorstwa uzyskują informacje, kiedy mają obowiązek zgłosić incydent do CSIRT sektorowego.
	rodzina, obywatele oraz gospodarstwa domowe	Incydenty poważne wpływają na świadczenie usług dla obywateli. Prawidłowe określenie kryteriów tego rodzaju zdarzeń pozwoli na ich identyfikację oraz szybką reakcję ze strony zespołów CSIRT.
Niemierzalne		

Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	

8. Zmiana obciążeń regulacyjnych (w tym obowiązków informacyjnych) wynikających z projektu

☐ nie dotyczy

Wprowadzane są obciążenia poza bezwzględnie wymaganymi przez UE (szczegóły w odwróconej tabeli zgodności).	☐ tak ☒ nie ☐ nie dotyczy
☐ zmniejszenie liczby dokumentów ☐ zmniejszenie liczby procedur ☐ skrócenie czasu na załatwienie sprawy ☐ inne: Kliknij lub naciśnij tutaj, aby wprowadzić tekst.	☐ zwiększenie liczby dokumentów ☒ zwiększenie liczby procedur ☐ wydłużenie czasu na załatwienie sprawy ☐ inne: Kliknij lub naciśnij tutaj, aby wprowadzić tekst.
Wprowadzane obciążenia są przystosowane do ich elektronizacji.	☒ tak ☐ nie ☐ nie dotyczy

Komentarz:

Dla dotychczasowych podmiotów krajowego systemu cyberbezpieczeństwa pozostawiono dobrze im znane progi incydentu poważnego. Progi będą nowością dla tych podmiotów kluczowych lub podmiotów ważnych, które do tej pory nie kwalifikowały się jako operatorzy usług kluczowych. Obowiązek zgłoszenia incydentu poważnego wynika jednak z ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

9. Wpływ na rynek pracy

Projektowane rozporządzenie nie ma wpływu na rynek pracy.

10. Wpływ na pozostałe obszary

☐ środowisko naturalne ☐ sytuacja i rozwój regionalny ☐ sądy powszechne, administracyjne lub wojskowe	☐ demografia ☐ mienie państwowe ☐ inne: Kliknij lub naciśnij tutaj, aby wprowadzić tekst.	☒ informatyzacja ☐ zdrowie
Omówienie wpływu	Projektowane rozporządzenie określa progi incydentów poważnych, które wymagają obligatoryjnego zgłoszenia do jednego z CSIRT sektorowych zgodnie z ustawą o	

	krajowym systemie cyberbezpieczeństwa. Prawidłowe określenie tych progów umożliwi adekwatną reakcję na incydenty, które rzeczywiście mają duży wpływ na społeczeństwo i gospodarkę.
11. Planowane wykonanie przepisów aktu prawnego	
Projektowane rozporządzenie wejdzie w życie po upływie 14 dni od dnia ogłoszenia.	
12. W jaki sposób i kiedy nastąpi ewaluacja efektów projektu oraz jakie mierniki zostaną zastosowane?	
Po roku obowiązywania rozporządzenia zostanie przeprowadzona analiza adekwatności zastosowanych w rozporządzeniu kryteriów uznania incydentu za incydent poważny.	
13. Załączniki (istotne dokumenty źródłowe, badania, analizy itp.)	
Brak	

ROZPORZĄDZENIE

RADY MINISTRÓW

z dnia r.

**w sprawie oceny bezpieczeństwa systemów informacyjnych wykorzystywanych przez
podmioty krajowego systemu cyberbezpieczeństwa¹⁾**

Na podstawie art. 36d ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077 i 1222 oraz z 2025 r. poz. 1017, 1069 i ...) zarządza się, co następuje:

§ 1. Rozporządzenie określa:

- 1) tryb przeprowadzania oceny bezpieczeństwa, o której mowa w art. 36a ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, zwanej dalej „ustawą”;
- 2) szczegółowe informacje przekazywane do CSIRT niezbędne do przeprowadzenia oceny bezpieczeństwa;
- 3) rodzaje przeprowadzanych testów bezpieczeństwa w ramach oceny bezpieczeństwa, o których mowa w art. 36a ust. 2 ustawy;
- 4) sposób niszczenia materiałów zawierających informacje, o których mowa w art. 36b ust. 10 ustawy;
- 5) tryb działania komisji, o której mowa w art. 36b ust. 11 zdanie pierwsze ustawy;
- 6) wzór protokołu zniszczenia materiałów zawierających informacje, o których mowa w art. 36b ust. 10 ustawy.

§ 2. Użyty w rozporządzeniu skrót „CSIRT” oznacza CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT sektorowy przeprowadzający ocenę bezpieczeństwa, o której mowa w art. 36a ustawy.

¹⁾ Niniejsze rozporządzenie w zakresie swojej regulacji wdraża dyrektywę Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniającą rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającą dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz. Urz. UE L 333 z 27.12.2022, str. 80).

§ 3. W ramach oceny bezpieczeństwa, o której mowa w art. 36a ustawy, przeprowadza się następujące czynności:

- 1) pasywne zbieranie informacji – zbieranie w sieci internet informacji związanych z funkcjonowaniem systemu informacyjnego poddawanego ocenie bezpieczeństwa, zwanego dalej „systemem”, wpływających na jego bezpieczeństwo;
- 2) półpasywne zbieranie informacji – zbieranie w systemie informacji związanych z funkcjonowaniem tego systemu, wpływających na jego bezpieczeństwo, na zasadach właściwych dla użytkownika tego systemu, z wyłączeniem uprawnień wymagających uwierzytelnienia w tym systemie; czynności te mogą być uzupełnione zbieraniem informacji wynikających z analizy architektury systemu;
- 3) aktywne zbieranie informacji – zbieranie w systemie informacji związanych z funkcjonowaniem tego systemu, wpływających na jego bezpieczeństwo, w sposób przekraczający uprawnienia użytkownika systemu, w tym wymagających uwierzytelnienia w systemie, w szczególności polegających na enumeracji usług, portów, wykrywaniu urządzeń pośredniczących, wykrywaniu systemów wykrywania i zapobiegania włamaniom oraz zapór ogniowych;
- 4) identyfikacja podatności architektury systemu i usług sieciowych – podejmowanie czynności mających na celu identyfikację podatności, dokonywanych na podstawie informacji uzyskanych w ramach czynności, o których mowa w pkt 1–3, oraz informacji na temat architektury systemu udostępnionych przez podmiot kluczowy zarządzający systemem.

§ 4. 1. Przed przeprowadzeniem oceny bezpieczeństwa CSIRT zwraca się do podmiotu krajowego systemu cyberbezpieczeństwa z żądaniem przekazania informacji dotyczących systemu, które mogą obejmować:

- 1) architekturę systemu, w tym informacje o produktach ICT, usługach ICT i procesach ICT wchodzących w skład infrastruktury systemu;
- 2) adresację sieciową infrastruktury systemu;
- 3) informację o posiadaniu aktualnej kopii bezpieczeństwa systemu i zasad jej aktualizacji;
- 4) określenie wymaganego czasu przywrócenia systemu z kopii bezpieczeństwa systemu;
- 5) informację o posiadaniu środowiska testowego i jego zakresu;
- 6) zabezpieczenia systemu;
- 7) procedury bezpieczeństwa systemu.

2. Podmiot kluczowy przekazuje informacje, o których mowa w ust. 1, w terminie 14 dni od dnia otrzymania żądania informacji.

§ 5. CSIRT przeprowadza w ramach oceny bezpieczeństwa, o której mowa w art. 36a ust. 2 ustawy, następujące rodzaje testów bezpieczeństwa:

- 1) w zależności od wykorzystywanej infrastruktury do przeprowadzenia oceny bezpieczeństwa:
 - a) testy zewnętrzne z sieci internet,
 - b) testy wewnętrzne w sieci lokalnej podmiotu zarządzającego systemem;
- 2) w zależności od środowiska, w którym przeprowadzana jest ocena bezpieczeństwa:
 - a) testy na środowisku testowym,
 - b) testy na środowisku produkcyjnym systemu informacyjnego;
- 3) w zależności od wiedzy na temat badanego systemu posiadanej przez CSIRT:
 - a) testy podczas, których CSIRT nie dysponuje żadną wiedzą o systemie podlegającym ocenie bezpieczeństwa,
 - b) testy podczas, których CSIRT dysponuje wiedzą o systemie podlegającym ocenie bezpieczeństwa.

§ 6. 1. W terminie 30 dni od dnia otrzymania informacji, o których mowa w § 4 ust. 1, CSIRT przekazuje podmiotowi krajowego systemu cyberbezpieczeństwa projekt porozumienia w sprawie przeprowadzenia oceny bezpieczeństwa obejmujący:

- 1) datę rozpoczęcia i zakończenia oceny bezpieczeństwa oraz jej harmonogram;
- 2) zakres przeprowadzanych testów bezpieczeństwa, w tym czynności, o których mowa w § 3;
- 3) rodzaj przeprowadzanych testów bezpieczeństwa;
- 4) sposób udostępniania pomieszczeń lub urządzeń wchodzących w skład infrastruktury tego systemu.

2. Podmiot kluczowy może wnieść zastrzeżenia do projektu porozumienia, o którym mowa w ust. 1, w terminie 14 dni od dnia doręczenia projektu porozumienia do tego podmiotu. CSIRT odnosi się do zastrzeżeń do w terminie 14 dni od dnia ich doręczenia.

3. Po uzgodnieniu projektu porozumienia, o którym mowa w ust. 1, CSIRT i podmiot krajowego systemu cyberbezpieczeństwa zawierają porozumienie, o którym mowa w ust. 1.

4. CSIRT przeprowadzający ocenę bezpieczeństwa zapoznaje się z wyjaśnieniami udzielonymi przez przedstawiciela podmiotu kluczowego.

5. Z przeprowadzonej oceny bezpieczeństwa CSIRT sporządza raport, o którym mowa w art. 36b ust. 13 ustawy.

§ 7. 1. Zniszczenia materiałów zawierających informacje, o których mowa w art. 36b ust. 10 ustawy, dokonuje się przez:

- 1) trwałe usunięcie zapisów informacji utrwalonych na informatycznych nośnikach danych lub ich kopiach, na których informacje zostały utrwalone, w sposób uniemożliwiający odtworzenie treści tych zapisów;
- 2) fizyczne zniszczenie materiałów i dokumentów sporządzonych na ich podstawie, za pomocą urządzeń niszczących w sposób uniemożliwiający ich ponowne odczytanie.

2. Trwałe usunięcie zapisów informacji utrwalonych na informatycznych nośnikach danych lub ich kopiach, o którym mowa w ust. 1 pkt 1, jest wykonywane przez co najmniej siedmiokrotne nadpisanie całej przestrzeni tych nośników lub ich kopii dowolnym jawnym ciągiem bajtów.

3. W przypadku gdy trwałe usunięcie zapisów informacji utrwalonych na informatycznych nośnikach danych lub ich kopiach, o którym mowa w ust. 1 pkt 1, nie jest możliwe, nośniki te lub ich kopie uszkadza się w sposób uniemożliwiający ich odczytanie albo dokonuje się ich fizycznego zniszczenia.

§ 8. 1. Komisja, o której mowa w art. 36b ust. 11 zdanie pierwsze ustawy, zbiera się na posiedzeniu w terminie 14 dni od dnia jej powołania.

2. Komisja, o której mowa w art. 36b ust. 11 zdanie pierwsze ustawy, obraduje na posiedzeniach, na których sprawdza kompletność materiałów zawierających informacje, o których mowa w art. 36b ust. 10 ustawy, przekazanych do zniszczenia.

3. Komisja, o której mowa w art. 36b ust. 11 zdanie pierwsze ustawy, podejmuje rozstrzygnięcia w drodze uchwały.

4. Z posiedzeń komisji, o której mowa w art. 36b ust. 11 zdanie pierwsze ustawy, sporządza się protokół, który podpisują członkowie komisji, w jednym egzemplarzu, który pozostaje w CSIRT przeprowadzającej ocenę bezpieczeństwa.

5. Po stwierdzeniu kompletności materiałów zawierających informacje, o których mowa w art. 36b ust. 10 ustawy, przekazanych do zniszczenia komisja dokonuje ich zniszczenia.

6. Ze zniszczenia materiałów zawierających informacje, o których mowa w art. 36b ust. 10 ustawy, komisja, o której mowa w art. 36b ust. 11 zdanie pierwsze ustawy, sporządza

protokół w jednym egzemplarzu, który pozostaje w komórce organizacyjnej dokonującej zniszczenia, którego wzór określa załącznik do rozporządzenia.

7. Protokół ze zniszczenia materiałów zawierających informacje, o których mowa w art. 36b ust. 10 ustawy, zatwierdza kierownik podmiotu prowadzącego CSIRT przeprowadzającej ocenę bezpieczeństwa.

§ 9. Rozporządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

PREZES RADY MINISTRÓW

Załącznik do rozporządzenia Rady
Ministrów z dnia r.
(Dz. U. poz. ...)

WZÓR

.....
Pieczęć

.....
(klauzula tajności po wypełnieniu)

.....
Znak sprawy

.....
miejsowość i data

Egzemplarz pojedynczy

PROTOKÓŁ ZNISZCZENIA MATERIAŁÓW ZAWIERAJĄCYCH INFORMACJE UZYSKANE W WYNIKU PRZEPROWADZENIA OCENY BEZPIECZEŃSTWA

Komisja powołana na podstawie zarządzenia nr z dnia w składzie:

1.
2.
3.

w dniu dokonała usunięcia zapisów informacji uzyskanych / zniszczenia materiałów zawierających informacje uzyskane / zniszczenia dokumentów sporządzonych na podstawie informacji utrwalonych na nośnikach uzyskanych* w wyniku przeprowadzenia oceny bezpieczeństwa prowadzonej przez w okresie od do

Wykaz zniszczonych informacji / materiałów / dokumentów:

.....
.....
.....

Numer strony/liczba stron

.....
(klauzula tajności po wypełnieniu)
.....

*) Niepotrzebne skreślić.

(klauzula tajności po wypełnieniu)

.....

.....

.....

.....

.....

.....

Podpisy członków komisji:

1.
2.
3.

KIEROWNIK PODMIOTU
PROWADZĄCEGO CSIRT

Wykonano w egz. pojedynczym:

Wykonał:

numer strony/liczba stron

.....

(klauzula tajności po wypełnieniu)

UZASADNIENIE

Projekt rozporządzenia stanowi wykonanie upoważnienia ustawowego zawartego z art. 36d ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077 i 1222 oraz z 2025 r. poz. 1017, 1069 i ...), zwanej dalej „ustawą”, zgodnie z którym Rada Ministrów może określić, w drodze rozporządzenia

- 1) tryb przeprowadzania oceny bezpieczeństwa, o której mowa w art. 36a ustawy;
- 2) szczegółowe informacje przekazywane do CSIRT niezbędne do przeprowadzenia oceny bezpieczeństwa;
- 3) rodzaje przeprowadzanych testów bezpieczeństwa w ramach oceny bezpieczeństwa, o których mowa w art. 36a ust. 2 ustawy;
- 4) sposób niszczenia materiałów zawierających informacje, o których mowa w art. 36b ust. 10 ustawy;
- 5) tryb działania komisji, o której mowa w art. 36b ust. 11 zdanie pierwsze ustawy;
- 6) wzór protokołu zniszczenia materiałów zawierających informacje, o których mowa w art. 36b ust. 10 ustawy.

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz. Urz. UE L 333 z 27.12.2022, str. 80) w art. 32 ust. 2 lit. d przewiduje środek nadzorczy w postaci skanów bezpieczeństwa wobec podmiotów kluczowych. Projekt ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa w rozdziale poświęconym ocenie bezpieczeństwa wdraża ww. przepis art. 32. W celu wykonania przepisów tego rozdziału niektóre sprawy zostały przekazane do uregulowania w rozporządzeniu. Z tego powodu można uznać, że niniejszy projekt rozporządzenia również wdraża dyrektywę NIS 2.

Projektowane rozporządzenie wypełnia upoważnienie ustawowe. Określa ono czynności podejmowane w ramach oceny bezpieczeństwa, rodzaje testów, które mogą być przeprowadzone w ramach tej oceny.

Wskazano także tryb oceny – najpierw CSIRT uzyskuje informacje o systemie poddawanych ocenie, następnie uzgadniany jest projekt porozumienia w sprawie tej oceny (porozumienie to określa m. in. harmonogram oceny i rodzaje testów przeprowadzonych w ramach oceny), potem jest przeprowadzana ocena, a następnie przekazywany jest raport z oceny.

Określono także tryb działania komisji niszczącej materiały uzyskane w trakcie oceny bezpieczeństwa, a także sposób zniszczenia tych materiałów i wzór protokołu z tej czynności. W załączniku do rozporządzenia określono wzór formularza protokołu zniszczenia materiałów zawierających informacje uzyskane w wyniku przeprowadzenia oceny bezpieczeństwa.

W projekcie rozporządzenia wskazano, że niszczenie materiałów odbywa się w sposób komisyjny i protokolarny. Zniszczenie materiałów zarządza kierownik podmiotu prowadzącego zespół CSIRT, niezwłocznie po zakończeniu oceny bezpieczeństwa. Jednocześnie w projekcie określono sposoby niszczenia materiałów, mając na względzie rodzaj materiału podlegającego zniszczeniu. W związku z powyższym, wskazano, iż zniszczenia materiałów dokonuje się przez:

- 1) trwałe i nieodwracalne usunięcie zapisów informacji utrwalonych na informatycznych nośnikach danych lub ich kopiach, na których informacje zostały utrwalone, w sposób uniemożliwiający odtworzenie treści tych zapisów;
- 2) fizyczne zniszczenie materiałów i dokumentów sporządzonych na ich podstawie, za pomocą urządzeń niszczących w sposób uniemożliwiający ich ponowne odczytanie.

Dodatkowo w projekcie rozporządzenia przewidziano rozwiązanie w sytuacji, gdy usunięcie z nośników utrwalonych na nich zapisów nie jest możliwe. W takim przypadku nośniki należy uszkodzić w sposób uniemożliwiający ich odczytanie albo fizycznie zniszczyć.

Wytyczne do wydania rozporządzenia zrealizowano w następujący sposób:

- *konieczność zapewnienia sprawnego przeprowadzenia oceny bezpieczeństwa* – poprzez określenie prostej procedury przeprowadzania oceny bezpieczeństwa,
- *bezpieczeństwo systemów informacyjnych podlegających ocenie* – poprzez dokładne wskazanie jakie czynności podejmuje się w ramach testów bezpieczeństwa oraz jakie informacje są zbierane przez CSIRT przeprowadzający ocenę,
- *rodzaj materiałów podlegających zniszczeniu* – wskazano sposób niszczenia materiałów uniemożliwiający ich odtworzenie,
- *i konieczność zapewnienia efektywności i przejrzystości prowadzonych działań komisji* – wskazano krótką procedurę działania komisji, ograniczając czynności do niezbędnego minimum.

Projektowane rozporządzenie wejdzie w życie po upływie 14 dni od dnia ogłoszenia.

Projektowane rozporządzenie jest zgodne z prawem Unii Europejskiej.

Projekt rozporządzenia nie zawiera przepisów technicznych w rozumieniu przepisów rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. poz. 2039 oraz z 2004 r. poz. 597) i w związku z tym nie podlega procedurze notyfikacji.

Projekt rozporządzenia nie będzie przedstawiany instytucjom i organom Unii Europejskiej, w tym Europejskiemu Bankowi Centralnemu, celem uzyskania opinii, dokonania konsultacji albo uzgodnienia.

Stosownie do postanowień art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingsowej w procesie stanowienia prawa (Dz. U. z 2025 r. poz. 677), projekt rozporządzenia zostanie udostępniony w Biuletynie Informacji Publicznej na stronie podmiotowej urzędu obsługującego ministra właściwego do spraw informatyzacji. Ponadto, zgodnie z § 52 ust. 1 uchwały nr 190 Rady Ministrów z dnia 29 października 2013 r. – Regulamin pracy Rady Ministrów (M.P. z 2024 r. poz. 806 oraz z 2025 r. poz. 408), projekt rozporządzenia zostanie udostępniony w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji, w serwisie Rządowy Proces Legislacyjny.

Nazwa projektu Rozporządzenie Rady Ministrów w sprawie oceny bezpieczeństwa systemów informacyjnych wykorzystywanych przez podmioty krajowego systemu cyberbezpieczeństwa Ministerstwo wiodące i ministerstwa współpracujące Ministerstwo Cyfryzacji Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu Paweł Olszewski, Sekretarz Stanu w Ministerstwie Cyfryzacji Kontakt do opiekuna merytorycznego projektu Łukasz Wojewoda, dyrektor Departamentu Cyberbezpieczeństwa w Ministerstwie Cyfryzacji, Marcin Wysocki, zastępca dyrektora Departamentu Cyberbezpieczeństwa w Ministerstwie Cyfryzacji, e-mail: sekretariat.dc@cyfra.gov.pl tel. + 48 22 245 59 22	Data sporządzenia 06.10.2025 Źródło: upoważnienie ustawowe art. 36d ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077 i 1222 oraz z 2025 r. poz. 1017, 1069 i ...) Nr w wykazie prac legislacyjnych i programowych Rady Ministrów Kliknij lub naciśnij tutaj, aby wprowadzić tekst.

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

Znowelizowana ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa przekazała do uregulowania w rozporządzeniu tryb przeprowadzania oceny bezpieczeństwa systemu informacyjnego podmiotu kluczowego przez zespoły CSIRT. Ponadto w projektowanym rozporządzeniu należy uregulować szczegółowe informacje przekazywane do CSIRT niezbędne do przeprowadzenia oceny bezpieczeństwa, rodzaje przeprowadzanych testów bezpieczeństwa w ramach oceny bezpieczeństwa, sposób niszczenia materiałów zawierających informacje uzyskanych w ramach tejże oceny, tryb działania komisji niszczącej materiały, a także wzór protokołu zniszczenia materiałów zawierających informacje.

2. Rekomendowane rozwiązanie, w tym planowane narzędzia interwencji, i oczekiwany efekt

Projektowane rozporządzenie wypełnia upoważnienie ustawowe. Określa ono czynności podejmowane w ramach oceny bezpieczeństwa, rodzaje testów, które mogą być przeprowadzone w ramach tej oceny. Wskazano także tryb oceny – najpierw CSIRT uzyskuje informacje o systemie poddawany ocenie, następnie uzgadniany jest projekt porozumienia w sprawie tej oceny (porozumienie to określa m. in. harmonogram oceny i rodzaje testów przeprowadzonych w ramach oceny), potem jest przeprowadzana ocena, a następnie przekazywany jest raport z oceny. Określono także tryb działania komisji niszczącej materiały uzyskane w trakcie oceny bezpieczeństwa, a także sposób zniszczenia tych materiałów i wzór protokołu z tej czynności. Jedynym sposobem rozwiązania problemu jest wydanie projektowanego rozporządzenia.

3. Jak problem został rozwiązany w innych krajach, w szczególności krajach członkowskich OECD/UE?

Z uwagi na szczegółowość regulacji odstąpiono od analizy prawno-porównawczej projektu na tle innych państw.

4. Podmioty, na które oddziałuje projekt

Grupa	Wielkość	Źródło danych	Oddziaływanie
CSIRT MON, CSIRT NASK, CSIRT GOV	3	informacje ogólnodostępne	Pozytywne. Określa jasny sposób postępowania
CSIRT sektorowy	co najmniej 10 (obejmujące wszystkie sektory z ustawy z dnia 5 lipca 2018 r. o krajowym systemie	OSR do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)	podczas oceny bezpieczeństwa systemu informacyjnego podmiotu kluczowego.

	cyberbezpieczeństwa)		
Podmiot kluczowy, którego system informacyjny podlega ocenie	W zależności od okoliczności, obecnie trudno przewidzieć ile będzie takich podmiotów.		

5. Informacje na temat zakresu, czasu trwania i podsumowanie wyników konsultacji

Stosownie do postanowień art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2025 r. poz. 677), projekt rozporządzenia zostanie udostępniony w Biuletynie Informacji Publicznej urzędu obsługującego ministra właściwego do spraw informatyzacji. Ponadto zgodnie z § 52 ust. 1 uchwały nr 190 Rady Ministrów z dnia 29 października 2013 r. – Regulamin pracy Rady Ministrów (M.P. z 2024 r. poz. 806 oraz z 2025 r. poz. 408), projekt rozporządzenia zostanie udostępniony w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji, w serwisie Rządowy Proces Legislacyjny. Projekt rozporządzenia zostanie przekazany do konsultacji publicznych i opiniowania, w tym zostanie skonsultowany z organizacjami zrzeszającymi podmioty krajowego systemu cyberbezpieczeństwa. Wyniki przeprowadzonych konsultacji publicznych i opiniowania zostaną omówione w raporcie z konsultacji.

6. Wpływ na sektor finansów publicznych

(ceny stałe z r.)	Skutki w okresie 10 lat od wejścia w życie zmian [mln zł]											
	0	1	2	3	4	5	6	7	8	9	10	Łącznie (0-10)
Dochody ogółem	0	0	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
pozostałe jednostki (oddzielnie)	0	0	0	0	0	0	0	0	0	0	0	0
Wydatki ogółem	0	0	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
pozostałe jednostki (oddzielnie)	0	0	0	0	0	0	0	0	0	0	0	0
Saldo ogółem	0	0	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
pozostałe jednostki (oddzielnie)	0	0	0	0	0	0	0	0	0	0	0	0

Źródła finansowania	Projektowane rozporządzenie nie spowoduje skutków finansowych dla sektora finansów publicznych.
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	

7. Wpływ na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców oraz na rodzinę, obywateli i gospodarstwa domowe

		Skutki						
Czas w latach od wejścia w życie zmian		0	1	2	3	5	10	Łącznie (0-10)
W ujęciu pieniężnym (w mln zł, ceny stałe z r.)	duże przedsiębiorstwa							
	sektor mikro-, małych i średnich przedsiębiorstw							
	rodzina, obywatele oraz gospodarstwa domowe							
W ujęciu niepieniężnym	duże przedsiębiorstwa	Projekt rozporządzenia nie określa zasad podejmowania, wykonywania lub zakończenia działalności gospodarczej, w związku z czym odstąpiono od analiz i oceny przewidywanych skutków społeczno-gospodarczych, wskazanych w art. 66 ust. 1 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców (Dz. U. z 2024 r. poz. 236, z późn. zm.).						
	sektor mikro-, małych i średnich przedsiębiorstw	Projekt rozporządzenia nie określa zasad podejmowania, wykonywania lub zakończenia działalności gospodarczej, w związku z czym odstąpiono od analiz i oceny przewidywanych skutków społeczno-gospodarczych, wskazanych w art. 66 ust. 1 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców.						
	rodzina, obywatele oraz gospodarstwa domowe	Projekt rozporządzenia nie uwzględnia regulacji, które będą miałyby wpływ na funkcjonowanie rodzin, obywateli i gospodarstw domowych.						
Niemierzalne								
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń								
8. Zmiana obciążeń regulacyjnych (w tym obowiązków informacyjnych) wynikających z projektu								
☐ nie dotyczy								
Wprowadzane są obciążenia poza bezwzględnie wymaganymi przez UE (szczegóły w odwróconej tabeli zgodności).				☐ tak ☐ nie ☒ nie dotyczy				
☐ zmniejszenie liczby dokumentów ☐ zmniejszenie liczby procedur ☐ skrócenie czasu na załatwienie sprawy ☐ inne: Kliknij lub naciśnij tutaj, aby wprowadzić tekst.				☒ zwiększenie liczby dokumentów ☒ zwiększenie liczby procedur ☐ wydłużenie czasu na załatwienie sprawy ☐ inne: Kliknij lub naciśnij tutaj, aby wprowadzić tekst.				
Wprowadzane obciążenia są przystosowane do ich elektronizacji.				☒ tak ☐ nie ☐ nie dotyczy				

Komentarz: Projekt rozporządzenia przewiduje zawieranie porozumień między CSIRT przeprowadzającym ocenę bezpieczeństwa a podmiotem kluczowym poddającym swój system informacyjny tej ocenie. Będzie również sporządzony raport z przeprowadzonej oceny bezpieczeństwa oraz protokół zniszczenia materiałów uzyskanych w drodze oceny bezpieczeństwa.			
9. Wpływ na rynek pracy			
Projekt rozporządzenia zawiera regulacje, które zwiększą zapotrzebowanie w zespołach CSIRT MON, CSIRT NASK i CSIRT GOV oraz CSIRT sektorowych na specjalistów posiadających wiedzę specjalistyczną w zakresie przeprowadzania testów bezpieczeństwa.			
10. Wpływ na pozostałe obszary			
☐ środowisko naturalne ☐ sytuacja i rozwój regionalny ☐ sądy powszechne, administracyjne lub wojskowe		☐ demografia ☐ mienie państwowe ☐ inne: Kliknij lub naciśnij tutaj, aby wprowadzić tekst.	
		☒ informatyzacja ☐ zdrowie	
Omówienie wpływu	Projekt rozporządzenia zawiera regulacje, które mają pozytywny wpływ na cyberbezpieczeństwo, gdyż gwarantują podmiotom poddającym się ocenie bezpieczeństwa, że ich wrażliwe informacje nie będą wykorzystane przeciwko nim.		
11. Planowane wykonanie przepisów aktu prawnego			
Projektowane rozporządzenie wejdzie w życie po upływie 14 dni od dnia jego ogłoszenia.			
12. W jaki sposób i kiedy nastąpi ewaluacja efektów projektu oraz jakie mierniki zostaną zastosowane?			
Ewaluacja będzie przeprowadzana po 2 latach od wejścia w życie rozporządzenia przez Ministerstwo Cyfryzacji.			
13. Załączniki (istotne dokumenty źródłowe, badania, analizy itp.)			
Brak			

ROZPORZĄDZENIE

RADY MINISTRÓW

z dnia r.

w sprawie zakresu działania oraz trybu pracy Kolegium do Spraw Cyberbezpieczeństwa

Na podstawie art. 66 ust. 9 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077 i 1222 oraz z 2025 r. poz. 1017, 1069 i) zarządza się, co następuje:

§ 1. 1. Kolegium do Spraw Cyberbezpieczeństwa, zwane dalej „Kolegium”, rozpatruje sprawy na posiedzeniach, w terminach określonych w planie pracy Kolegium.

2. Przewodniczący Kolegium może, z własnej inicjatywy lub na wniosek członka Kolegium albo osoby, o której mowa w art. 66 ust. 1 pkt 2 i 3 oraz ust. 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, zwanej dalej „ustawą”, zwołać posiedzenie Kolegium w innym terminie niż określony w planie pracy Kolegium.

3. Przewodniczący Kolegium albo działający z jego upoważnienia sekretarz Kolegium może, z inicjatywy własnej albo na wniosek członka Kolegium, zarządzić rozpatrzenie sprawy w drodze korespondencyjnego uzgodnienia stanowisk (tryb obiegowy).

§ 2. 1. Zawiadomienie o terminie posiedzenia Kolegium wraz z porządkiem obrad sekretarz Kolegium doręcza uczestnikom posiedzenia nie później niż na pięć dni przed wyznaczonym terminem posiedzenia.

2. W przypadku zwołania posiedzenia, o którym mowa w § 1 ust. 2, zawiadomienie o terminie posiedzenia Kolegium wraz z porządkiem obrad sekretarz Kolegium doręcza uczestnikom posiedzenia niezwłocznie po podjęciu przez przewodniczącego Kolegium decyzji o zwołaniu posiedzenia.

3. Przewodniczący Kolegium w trakcie posiedzenia może, z własnej inicjatywy lub na wniosek członka Kolegium albo osoby, o której mowa w art. 66 ust. 1 pkt 2 i 3 oraz ust. 4 ustawy, wprowadzić do porządku obrad sprawy nieprzewidziane w tym porządku.

§ 3. 1. Przewodniczący Kolegium może, z własnej inicjatywy lub na wniosek członka Kolegium albo osoby, o której mowa w art. 66 ust. 1 pkt 2 i 3 oraz ust. 4 ustawy, podjąć decyzję o niejawnym charakterze określonej części lub całości posiedzenia Kolegium.

2. Przewodniczący Kolegium przed posiedzeniem Kolegium określa, które z osób wymienionych w art. 66 ust. 5 pkt 2 ustawy uczestniczą w całości lub określonej części posiedzenia.

3. Doręczenie uczestnikom posiedzenia informacji w zakresie, o którym mowa w ust. 2, następuje nie później niż na dwa dni przed wyznaczonym terminem posiedzenia Kolegium. W wyjątkowych sytuacjach informacja może zostać wysłana w dniu poprzedzającym posiedzenie.

§ 4. 1. Kolegium wyraża swoje stanowisko w formie rekomendacji lub opinii.

2. Ustalenia stanowiska Kolegium dokonuje się w drodze głosowania. Przewodniczący Kolegium zarządza głosowanie wśród członków Kolegium oraz osób, o których mowa w art. 66 ust. 1 pkt 2 i ust. 4 ustawy, obecnych na posiedzeniu Kolegium. O treści stanowiska decyduje większość głosów. W przypadku równej liczby głosów rozstrzyga głos przewodniczącego Kolegium.

3. Członkowie Kolegium oraz osoby, o których mowa w art. 66 ust. 1 pkt 2 i ust. 4 ustawy, mogą zgłosić do protokołu zdanie odrębne w stosunku do przyjętego stanowiska.

§ 5. 1. Z posiedzenia Kolegium sporządza się protokół oraz pełny zapis jego przebiegu.

2. Protokół zawiera w szczególności:

- 1) porządek obrad;
- 2) listę obecności osób uczestniczących w posiedzeniu;
- 3) wnioski formalne osób uczestniczących w posiedzeniu;
- 4) przyjęte przez Kolegium stanowisko w formie rekomendacji lub opinii;
- 5) wykaz dokumentów stanowiących przedmiot obrad wraz z informacją o sposobie zapoznania się z nimi.

3. Protokół podpisuje przewodniczący Kolegium i sekretarz Kolegium.

4. Protokół z posiedzenia Kolegium jest udostępniany niezwłocznie przez sekretarza Kolegium:

- 1) osobom, o których mowa w art. 66 ust. 1 pkt 1, 2 i 4 oraz ust. 4 ustawy;
- 2) osobom, o których mowa w art. 66 ust. 5 pkt 2 ustawy, w części, w jakiej uczestniczyli w posiedzeniu Kolegium.

5. W terminie siedmiu dni od dnia podpisania protokołu osoby uczestniczące w posiedzeniu mogą wnieść sprostowanie do zamieszczonych w protokole sformułowań własnych wypowiedzi i wniosków formalnych. Sprostowanie podpisane przez osobę, która je wniosła, umieszcza się w aneksie do protokołu.

§ 6. 1. W uzasadnionych przypadkach przewodniczący Kolegium może powołać, w ramach Kolegium, zespół o charakterze doraźnym, którego zadaniem będzie szczegółowe rozpatrzenie danej sprawy.

2. Przewodniczący Kolegium określa skład zespołu, o którym mowa w ust. 1, oraz zakres jego zadań.

§ 7. Do obowiązków sekretarza Kolegium, w zakresie wskazanym w art. 66 ust. 7 ustawy, należy:

- 1) przygotowanie projektów planów pracy Kolegium;
- 2) koordynacja przygotowania oraz dostarczenia materiałów i projektów dokumentów przeznaczonych do rozpatrzenia przez Kolegium;
- 3) informowanie członków Kolegium oraz innych uczestników posiedzenia Kolegium o terminie posiedzenia oraz o jego porządku obrad;
- 4) sporządzanie protokołów z posiedzeń Kolegium i przedstawianie ich do podpisu przewodniczącemu Kolegium;
- 5) udostępnianie protokołów z posiedzeń Kolegium;
- 6) prowadzenie rejestru rekomendacji i opinii Kolegium;
- 7) gromadzenie i przechowywanie dokumentacji Kolegium;
- 8) zapewnienie właściwego przygotowania i sprawnej obsługi posiedzeń Kolegium;
- 9) sporządzanie projektu rocznego sprawozdania z działalności Kolegium i przedstawianie go przewodniczącemu Kolegium;
- 10) monitorowanie wykonywania zadań wynikających z rekomendacji i opinii Kolegium oraz decyzji przewodniczącego Kolegium;
- 11) wykonywanie innych zadań zleconych przez Kolegium i przewodniczącego Kolegium.

§ 8. Rozporządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia.¹⁾

PREZES RADY MINISTRÓW

¹⁾ Niniejsze rozporządzenie było poprzedzone rozporządzeniem Rady Ministrów z dnia 2 października 2018 r. w sprawie zakresu działania oraz trybu pracy Kolegium do Spraw Cyberbezpieczeństwa (Dz. U. z 2025 r. poz. 1328), które traci moc z dniem wejścia w życie niniejszego rozporządzenia zgodnie z art. 32 pkt 2 ustawy z dnia ... o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (Dz. U. poz. ...).

UZASADNIENIE

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077 i 1222 oraz z 2025 r. poz. 1017, 1069 i ...), zwana dalej „ustawą”, ustanowiła przy Radzie Ministrów Kolegium do Spraw Cyberbezpieczeństwa, zwane dalej „Kolegium”, będące organem o charakterze opiniodawczo-doradczym. Kolegium, jak stanowi art. 64 ustawy, jest organem właściwym w sprawach:

- 1) cyberbezpieczeństwa oraz
- 2) działalności w tym zakresie zespołów CSIRT MON, CSIRT NASK, CSIRT GOV, sektorowych zespołów cyberbezpieczeństwa i organów właściwych do spraw cyberbezpieczeństwa.

Zgodnie z brzmieniem art. 66 ust. 8 ustawy obsługę Kolegium zapewnia ministerstwo lub inny urząd administracji rządowej, który obsługuje Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa. Ustawodawca w art. 66 ust. 9 ustawy upoważnił Radę Ministrów do wydania rozporządzenia określającego szczegółowy zakres działania oraz tryb pracy Kolegium. W związku z tym zostało wydane rozporządzenie Rady Ministrów z dnia 2 października 2018 r. w sprawie zakresu działania oraz trybu pracy Kolegium do Spraw Cyberbezpieczeństwa (Dz. U. z 2025 r. poz. 1328).

Ustawa z dnia ... o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw wprowadziła zmiany w przepisach materialnych dotyczących funkcjonowania Kolegium do Spraw Cyberbezpieczeństwa, zwane dalej „Kolegium”. Wprowadzono możliwość pracy Kolegium w trybie obiegowym.

Z uwagi na wyżej wymienione zmiany w ustawie doszło do pośredniej zmiany upoważnienia ustawowego. Z tego powodu należy wydać nowe rozporządzenie określające szczegółowy zakres działania oraz tryb pracy Kolegium, które będzie odpowiadało aktualnemu brzmieniu przepisów materialnych.

Proponuje się, aby rozporządzenie weszło w życie po upływie 14 dni od dnia ogłoszenia.

Projekt rozporządzenia nie ma wpływu na działalność mikroprzedsiębiorców oraz małych i średnich przedsiębiorców.

Projekt rozporządzenia nie będzie miał wpływu na sytuację ekonomiczną i społeczną rodziny, osób niepełnosprawnych oraz osób starszych.

Projekt rozporządzenia jest zgodny z prawem Unii Europejskiej.

Projekt rozporządzenia nie wymaga przedstawiania organom i instytucjom Unii

Europejskiej, w tym Europejskiemu Bankowi Centralnemu, w celu uzyskania opinii, dokonania powiadomienia, konsultacji albo uzgodnienia.

Projekt rozporządzenia nie zawiera przepisów technicznych w rozumieniu przepisów rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. poz. 2039 oraz z 2004 r. poz. 597) i w związku z tym nie podlega procedurze notyfikacji.

Stosownie do postanowień art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingsowej w procesie stanowienia prawa (Dz. U. z 2025 r. poz. 677), projekt rozporządzenia zostanie udostępniony w Biuletynie Informacji Publicznej na stronie podmiotowej urzędu obsługującego ministra właściwego do spraw informatyzacji. Ponadto, zgodnie z § 52 ust. 1 uchwały nr 190 Rady Ministrów z dnia 29 października 2013 r. – Regulamin pracy Rady Ministrów (M.P. z 2024 r. poz. 806 oraz z 2025 r. poz. 408), projekt rozporządzenia zostanie udostępniony w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji, w serwisie Rządowy Proces Legislacyjny.

Nazwa projektu Rozporządzenie Rady Ministrów w sprawie zakresu działania oraz trybu pracy Kolegium do Spraw Cyberbezpieczeństwa Ministerstwo wiodące i ministerstwa współpracujące Ministerstwo Cyfryzacji Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu Paweł Olszewski, Sekretarz Stanu w Ministerstwie Cyfryzacji Kontakt do opiekuna merytorycznego projektu Łukasz Wojewoda, dyrektor Departamentu Cyberbezpieczeństwa w Ministerstwie Cyfryzacji, Marcin Wysocki, zastępca dyrektora Departamentu Cyberbezpieczeństwa w Ministerstwie Cyfryzacji, e-mail:sekretariat.dc@cyfra.gov.pl tel. + 48 22 245 59 22	Data sporządzenia 06.10.2025 Źródło: art. 66 ust. 9 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077 i 1222 oraz z 2025 r. poz. 1017, 1069 i ...) Nr w wykazie prac legislacyjnych i programowych Rady Ministrów Kliknij lub naciśnij tutaj, aby wprowadzić tekst.

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

Ustawa z dnia ... o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw wprowadziła zmiany w przepisach materialnych dotyczących funkcjonowania Kolegium do Spraw Cyberbezpieczeństwa, zwane dalej „Kolegium”. Wprowadzono możliwość pracy Kolegium w trybie obiegowym. Ponadto powstała funkcja zastępcy sekretarza Kolegium.

Zgodnie z art. 66 ust. 9 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa szczegółowy zakres działania oraz tryb pracy Kolegium określa rozporządzenie Rady Ministrów. Na podstawie tego przepisu wydano rozporządzenie Rady Ministrów z dnia 2 października 2018 r. w sprawie zakresu działania oraz trybu pracy Kolegium do Spraw Cyberbezpieczeństwa (Dz. U. z 2025 r. poz. 1328).

Z uwagi na wyżej wymienione zmiany w ustawie doszło do pośredniej zmiany upoważnienia ustawowego. Z tego powodu należy wydać nowe rozporządzenie określające szczegółowy zakres działania oraz tryb pracy Kolegium, które będzie odpowiadało aktualnemu brzmieniu przepisów materialnych zawartych w ustawie.

2. Rekomendowane rozwiązanie, w tym planowane narzędzia interwencji, i oczekiwany efekt

Rozporządzenie reguluje tryb zwoływania posiedzeń Kolegium do Spraw Cyberbezpieczeństwa, elementy protokołu sporządzonego z posiedzenia Kolegium i obowiązki Sekretarza Kolegium do Spraw Cyberbezpieczeństwa. W tym zakresie projekt powtarza regulacje poprzedniego rozporządzenia. Natomiast nowością jest rozpatrywanie spraw przez Kolegium w trybie obiegowym, co pozwoli na podejmowanie stanowisk Kolegium w sprawach, w których nie jest konieczne zwoływanie posiedzenia Kolegium.

3. Jak problem został rozwiązany w innych krajach, w szczególności krajach członkowskich OECD/UE?

Z uwagi na wewnętrzny charakter proponowanych przepisów nie przeprowadzono analizy prawnoporównawczej.

4. Podmioty, na które oddziałuje projekt

Grupa	Wielkość	Źródło danych	Oddziaływanie
Kolegium do Spraw Cyberbezpieczeństwa	1	informacja ogólnodostępna	Pozytywne. Umożliwienie pracy Kolegium w trybie obiegowym.
Sekretarz Kolegium do Spraw Cyberbezpieczeństwa	1	informacja ogólnodostępna	Pozytywne. Uregulowanie sytuacji, w której sekretarz Kolegium nie jest obecny na posiedzeniu.

Zastępca sekretarza Kolegium	1	informacja ogólnodostępna	Będzie mógł podpisać protokół z posiedzenia Kolegium w czasie nieobecności sekretarza Kolegium.

5. Informacje na temat zakresu, czasu trwania i podsumowanie wyników konsultacji

Stosownie do postanowień art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2025 r. poz. 677), projekt rozporządzenia zostanie udostępniony w Biuletynie Informacji Publicznej urzędu obsługującego ministra właściwego do spraw informatyzacji . Ponadto zgodnie z § 52 ust. 1 uchwały nr 190 Rady Ministrów z dnia 29 października 2013 r. – Regulamin pracy Rady Ministrów (M.P. z 2024 r. poz. 806 oraz z 2025 r. poz. 408), projekt rozporządzenia zostanie udostępniony w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji, w serwisie Rządowy Proces Legislacyjny. Projekt rozporządzenia zostanie przekazany do konsultacji publicznych i opiniowania.

Wyniki przeprowadzonych konsultacji publicznych i opiniowania zostaną omówione w raporcie z konsultacji.

6. Wpływ na sektor finansów publicznych

(ceny stałe z r.)	Skutki w okresie 10 lat od wejścia w życie zmian [mln zł]											
	0	1	2	3	4	5	6	7	8	9	10	Łącznie (0-10)
Dochody ogółem	0	0	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
pozostałe jednostki (oddzielnie)	0	0	0	0	0	0	0	0	0	0	0	0
Wydatki ogółem	0	0	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
pozostałe jednostki (oddzielnie)	0	0	0	0	0	0	0	0	0	0	0	0
Saldo ogółem	0	0	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
pozostałe jednostki (oddzielnie)	0	0	0	0	0	0	0	0	0	0	0	0

Źródła finansowania	Przyjęte rozwiązania nie spowodują dodatkowych skutków finansowych dla sektora finansów publicznych, w tym budżetu państwa i budżetów jednostek samorządu terytorialnego.
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	

7. Wpływ na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców oraz na rodzinę, obywateli i gospodarstwa domowe

Skutki								
Czas w latach od wejścia w życie zmian		0	1	2	3	5	10	Łącznie (0-10)
	duże przedsiębiorstwa							

W ujęciu pieniężnym (w mln zł, ceny stałe z r.)	sektor mikro-, małych i średnich przedsiębiorstw							
	rodzina, obywatele oraz gospodarstwa domowe							
W ujęciu niepieniężnym	duże przedsiębiorstwa	Projekt rozporządzenia nie określa zasad podejmowania, wykonywania lub zakończenia działalności gospodarczej, w związku z czym odstąpiono od analiz i oceny przewidywanych skutków społeczno-gospodarczych, wskazanych w art. 66 ust. 1 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców (Dz. U. z 2024 r. poz. 236, z późn. zm.).						
	sektor mikro-, małych i średnich przedsiębiorstw	Projekt rozporządzenia nie określa zasad podejmowania, wykonywania lub zakończenia działalności gospodarczej, w związku z czym odstąpiono od analiz i oceny przewidywanych skutków społeczno-gospodarczych, wskazanych w art. 66 ust. 1 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców.						
	rodzina, obywatele oraz gospodarstwa domowe	Projekt rozporządzenia nie uwzględnia regulacji, które będą miały wpływ na sytuację ekonomiczną i społeczną rodziny, obywateli, gospodarstw domowych, osób niepełnosprawnych oraz osób starszych.						
Niemierzalne								
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń								
8. Zmiana obciążeń regulacyjnych (w tym obowiązków informacyjnych) wynikających z projektu								
☐ nie dotyczy								
Wprowadzane są obciążenia poza bezwzględnie wymaganymi przez UE (szczegóły w odwróconej tabeli zgodności).				☐ tak ☐ nie ☒ nie dotyczy				
☐ zmniejszenie liczby dokumentów ☐ zmniejszenie liczby procedur ☐ skrócenie czasu na załatwienie sprawy ☐ inne: Kliknij lub naciśnij tutaj, aby wprowadzić tekst.				☐ zwiększenie liczby dokumentów ☒ zwiększenie liczby procedur ☐ wydłużenie czasu na załatwienie sprawy ☐ inne: Kliknij lub naciśnij tutaj, aby wprowadzić tekst.				
Wprowadzane obciążenia są przystosowane do ich elektronizacji.				☒ tak ☐ nie ☐ nie dotyczy				
Komentarz: Projekt rozporządzenia ma na celu usprawnienie prac Kolegium, w tym przez wprowadzenie możliwości pracy Kolegium w trybie obiegowym, co zapewni sprawność jego działania.								
9. Wpływ na rynek pracy								
Proponowane zmiany nie wywierają wpływu na funkcjonowanie rynku pracy.								
10. Wpływ na pozostałe obszary								

☐ środowisko naturalne ☐ sytuacja i rozwój regionalny ☐ sądy powszechne, administracyjne lub wojskowe	☐ demografia ☐ mienie państwowe ☐ inne: Kliknij lub naciśnij tutaj, aby wprowadzić tekst.	☐ informatyzacja ☐ zdrowie
Omówienie wpływu	Brak wpływu.	
11. Planowane wykonanie przepisów aktu prawnego		
Rozporządzenie wejdzie w życie po upływie 14 dni od dnia ogłoszenia.		
12. W jaki sposób i kiedy nastąpi ewaluacja efektów projektu oraz jakie mierniki zostaną zastosowane?		
Z uwagi na głównie porządkowy charakter rozporządzenia nie przewiduje się ewaluacji efektów projektu. Cel zostanie osiągnięty wraz z wejściem w życie tej regulacji.		
13. Załączniki (istotne dokumenty źródłowe, badania, analizy itp.)		