Prezes
Rady Ministrów

Donald Tusk

Warszawa, dnia /elektroniczny znacznik czasu/

RM-0610-6-26
UC47

Pan Włodzimierz CZARZASTY
Marszałek Sejmu

Szanowny Panie Marszałku,

na podstawie art. 118 ust. 1 Konstytucji Rzeczypospolitej Polskiej przedstawiam Sejmowi projekt ustawy o zmianie ustawy o zarządzaniu kryzysowym oraz niektórych innych ustaw.
Projekt ma na celu wykonanie prawa Unii Europejskiej.
Do prezentowania stanowiska Rządu w tej sprawie w toku prac parlamentarnych został upoważniony Prezes Rady Ministrów.

Z poważaniem
Donald Tusk
/podpisano kwalifikowanym podpisem elektronicznym/

Do wiadomości:
wnioskodawca

tel. +48 (22) 694 75 00
dkpl@kprm.gov.pl
gov.pl/premier

Al. Ujazdowskie 1/3; 00-583
Warszawa

Projekt

U S T A W A

z dnia

o zmianie ustawy o zarządzaniu kryzysowym oraz niektórych innych ustaw[1), 2)]

Art. 1. W ustawie z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2023 r. poz. 122, z późn. zm.[3)]) wprowadza się następujące zmiany:

1) do tytułu ustawy dodaje się odnośnik nr 1 w brzmieniu:

„1) Niniejsza ustawa w zakresie swojej regulacji wdraża dyrektywę 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 333 z 27.12.2022, str. 164).”;

2) po tytule ustawy wprowadza się oznaczenie i tytuł rozdziału w brzmieniu:

„Rozdział 1

Przepisy ogólne”;

3) art. 1 otrzymuje brzmienie:

„Art. 1. 1. Ustawa określa:

---

1) Niniejsza ustawa w zakresie swojej regulacji wdraża dyrektywę 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 333 z 27.12.2022 r. str. 164).

2) Niniejszą ustawą zmienia się ustawy: ustawę z dnia 21 marca 1985 r. o drogach publicznych, ustawę z dnia 6 kwietnia 1990 r. o Policji, ustawę z dnia 12 października 1990 r. o Straży Granicznej, ustawę z dnia 24 sierpnia 1991 r. o ochronie przeciwpożarowej, ustawę z dnia 24 sierpnia 1991 r. o Państwowej Straży Pożarnej, ustawę z dnia 22 sierpnia 1997 r. o ochronie osób i mienia, ustawę z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych, ustawę z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, ustawę z dnia 28 marca 2003 r. o transporcie kolejowym, ustawę z dnia 11 marca 2004 r. o ochronie zdrowia zwierząt oraz zwalczaniu chorób zakaźnych zwierząt, ustawę z dnia 4 września 2008 r. o ochronie żeglugi i portów morskich, ustawę z dnia 18 marca 2010 r. o szczególnych uprawnieniach ministra właściwego do spraw aktywów państwowych oraz ich wykonywaniu w niektórych spółkach kapitałowych lub grupach kapitałowych prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych, ustawę z dnia 14 grudnia 2012 r. o odpadach, ustawę z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej, ustawę z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych, ustawę z dnia 20 lipca 2017 r. – Prawo wodne, ustawę z dnia 8 grudnia 2017 r. o Służbie Ochrony Państwa, ustawę z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, ustawę z dnia 17 grudnia 2020 r. o rezerwach strategicznych, ustawę z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa, ustawę z dnia 12 lipca 2024 r. – Prawo komunikacji elektronicznej oraz ustawę z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej.

3) Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2024 r. poz. 834, 1222, 1473, 1572 i 1907 oraz z 2025 r. poz. 1795.

1) organy właściwe w sprawach zarządzania kryzysowego oraz ich zadania i zasady działania;
2) organy właściwe w sprawach identyfikacji i ochrony infrastruktury krytycznej;
3) zadania i obowiązki operatorów infrastruktury krytycznej;
4) usługi kluczowe oraz zadania i obowiązki podmiotów krytycznych;
5) organy właściwe do spraw podmiotów krytycznych oraz zadania i obowiązki tych organów;
6) zasady sprawowania nadzoru nad podmiotami krytycznymi oraz ich kontroli;
7) zasady finansowania zadań, o których mowa w pkt 1–6.

2. Ustawy w zakresie, o którym mowa w:

1) ust. 1 pkt 3 i 4, nie stosuje się do organów oraz jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych;
2) ust. 1 pkt 4 nie stosuje się do podmiotów, które w zakresie swojej działalności prowadzą postępowania przygotowawcze, o których mowa w art. 297 ustawy z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (Dz. U. z 2025 r. poz. 46, z późn. zm.[4)]).”;

4) w art. 3:
   a) pkt 1 otrzymuje brzmienie:
      „1) sytuacji kryzysowej – należy przez to rozumieć sytuację wpływającą negatywnie na poziom bezpieczeństwa ludzi, mienia w znacznych rozmiarach, środowiska lub dziedzictwa kulturowego, wywołującą znaczne ograniczenia w działaniu właściwych organów administracji publicznej ze względu na nieadekwatność posiadanych sił i środków lub zakłócenia obsługi tych organów;”,
   b) po pkt 1 dodaje się pkt 1a–1g w brzmieniu:
      „1a) podmiocie krytycznym – należy przez to rozumieć operatora infrastruktury krytycznej wpisanego do wykazu podmiotów krytycznych, realizującego co najmniej jedną usługę kluczową, prowadzącego działalność w sektorze lub podsektorze wymienionym w załączniku do ustawy oraz posiadającego infrastrukturę krytyczną na terytorium Rzeczypospolitej Polskiej lub na obszarach morskich Rzeczypospolitej Polskiej, o których mowa w ustawie z

---

[4)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2025 r. poz. 304, 1178, 1420 i 1872 oraz z 2026 r. poz. 187.

dnia 21 marca 1991 r. o obszarach morskich Rzeczypospolitej Polskiej i administracji morskiej (Dz. U. z 2024 r. poz. 1125, z 2025 r. poz. 409, 1535 i 1668 oraz z 2026 r. poz. 252);

1b) podmiocie krytycznym o szczególnym znaczeniu europejskim – należy przez to rozumieć podmiot krytyczny świadczący co najmniej jedną usługę kluczową lub świadczący te same lub podobne usługi kluczowe, na rzecz co najmniej sześciu państw członkowskich Unii Europejskiej lub w co najmniej sześciu państwach członkowskich Unii Europejskiej, uznany za taki podmiot przez Komisję Europejską;

1c) podmiocie publicznym – należy przez to rozumieć podmiot wskazany w załączniku do ustawy w sektorze administracji publicznej;

1d) odporności podmiotu krytycznego – należy przez to rozumieć zdolność do zapobiegania incydentowi, ochrony przed incydentem realizowanej w drodze zaplanowanych działań, z wykorzystaniem posiadanych zasobów, reagowania w przypadku wystąpienia incydentu i jego absorbowania oraz adaptacji i usuwania skutków incydentu, w tym odtwarzania infrastruktury krytycznej niezbędnej do świadczenia usługi kluczowej;

1e) usłudze kluczowej – należy przez to rozumieć usługę, która ma decydujące znaczenie dla utrzymania niezbędnych funkcji społecznych, niezbędnej działalności gospodarczej, zdrowia i bezpieczeństwa publicznego lub środowiska, wskazaną w przepisach wydanych na podstawie art. 6zp ust. 3;

1f) incydencie – należy przez to rozumieć każde zdarzenie mające lub mogące mieć niekorzystny wpływ na świadczenie usługi kluczowej;

1g) incydencie istotnym – należy przez to rozumieć incydent, który powoduje lub może spowodować istotne obniżenie jakości lub przerwanie ciągłości świadczenia usługi kluczowej, spełniający progi uznania incydentu za istotny wskazane w przepisach wydanych na podstawie art. 6zv ust. 4;”,

c) pkt 2 otrzymuje brzmienie:

„2) infrastrukturze krytycznej – należy przez to rozumieć obiekt, urządzenie, instalację, sieć, system oraz usługę lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje, sieci, systemy oraz usługi niezbędne do:

a) realizacji ważnych interesów państwa, w tym zapewnienia funkcjonowania organów administracji publicznej,

b) zapewnienia funkcjonowania przedsiębiorstw,

c) zaspokajania oraz utrzymania potrzeb obywateli, w tym potrzeb o charakterze lokalnym,

d) zapewnienia świadczenia usług kluczowych;”,

d) uchyla się pkt 2a,

e) po pkt 2a dodaje się pkt 2b w brzmieniu:

„2b) potencjalnej infrastrukturze krytycznej – należy przez to rozumieć obiekt, urządzenie, instalację, sieć, system oraz usługę lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje, sieci, systemy oraz usługi będące w fazie projektowania lub budowy, które po ich zakończeniu mogą być niezbędne do:

a) realizacji ważnych interesów państwa, w tym zapewnienia funkcjonowania organów administracji publicznej,

b) zapewnienia funkcjonowania przedsiębiorstw,

c) zaspokajania oraz utrzymywania potrzeb obywateli, w tym potrzeb o charakterze lokalnym,

d) zapewnienia świadczenia usług kluczowych;”,

f) pkt 3 otrzymuje brzmienie:

„3) ochronie infrastruktury krytycznej – należy przez to rozumieć wszelkie działania zmierzające do zapewnienia funkcjonalności, ciągłości działania oraz integralności infrastruktury krytycznej;”,

g) po pkt 3 dodaje się pkt 3a w brzmieniu:

„3a) operatorze infrastruktury krytycznej – należy przez to rozumieć właściciela lub posiadacza obiektu, urządzenia, instalacji, sieci, systemu oraz usługi lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji, sieci, systemów oraz usług wpisanych do wykazu infrastruktury krytycznej;”,

h) pkt 8 otrzymuje brzmienie:

„8) siatce bezpieczeństwa – należy przez to rozumieć zestawienie potencjalnych zagrożeń ze wskazaniem podmiotu wiodącego oraz podmiotów współpracujących w realizacji działań, o których mowa w art. 2;”,

i) uchyla się pkt 9 i 10,

j) w pkt 11 kropkę zastępuje się średnikiem i dodaje się pkt 12–31 w brzmieniu:

„12) ryzyku – należy przez to rozumieć prawdopodobieństwo wystąpienia zagrożenia wraz z jego skutkami;

13) ocenie ryzyka – należy przez to rozumieć proces identyfikacji zagrożenia, podatności na zagrożenie, prawdopodobieństwa wystąpienia zagrożenia oraz skutków wystąpienia zagrożenia, który określa wartość ryzyka;

14) zarządzaniu ryzykiem – należy przez to rozumieć działania polegające na:
   a) ocenie ryzyka,
   b) planowaniu działań postępowania z ryzykiem,
   c) wdrażaniu działań postępowania z ryzykiem,
   d) osiąganiu gotowości do reagowania w przypadku wystąpienia sytuacji kryzysowej,
   e) okresowej ocenie osiągniętych efektów;

15) module zadaniowym – należy przez to rozumieć zestawienie przedsięwzięć i zadań przewidzianych do realizacji w sytuacji kryzysowej przez podmioty wskazane w siatce bezpieczeństwa, z wykorzystaniem własnych sił i środków, a także możliwego, zaplanowanego i uzgodnionego wsparcia ze strony innych podmiotów wskazanych w siatce bezpieczeństwa;

16) planach zarządzania kryzysowego – należy przez to rozumieć plany zarządzania ryzykiem oraz plany reagowania kryzysowego;

17) planach zarządzania ryzykiem – należy przez to rozumieć Krajowy Plan Zarządzania Ryzykiem, plany zarządzania ryzykiem ministrów kierujących działami administracji rządowej i kierowników urzędów centralnych oraz wojewódzkie, powiatowe i gminne plany zarządzania ryzykiem;

18) planach reagowania kryzysowego – należy przez to rozumieć Krajowy Plan Reagowania Kryzysowego, plany reagowania kryzysowego ministrów kierujących działami administracji rządowej i kierowników urzędów centralnych oraz wojewódzkie, powiatowe i gminne plany reagowania kryzysowego;

19) decyzji 1313/2013/UE – należy przez to rozumieć decyzję Parlamentu Europejskiego i Rady nr 1313/2013/EU z dnia 17 grudnia 2013 r. w sprawie

Unijnego Mechanizmu Ochrony Ludności (Dz. Urz. UE L 347 z 20.12.2013, str. 924, z późn. zm.[5)]);

20) dyrektywie 2022/2557 – należy przez to rozumieć dyrektywę 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 333 z 27.12.2022 r. str. 164);

21) Grupie do spraw Odporności Podmiotów Krytycznych – należy przez to rozumieć grupę, o której mowa w art. 19 dyrektywy 2022/2557;

22) misji doradczej – należy przez to rozumieć misję doradczą, o której mowa w art. 18 ust. 1 dyrektywy 2022/2557;

23) zagrożeniu hybrydowym – należy przez to rozumieć kombinację wrogich działań realizowanych przy zastosowaniu środków politycznych, gospodarczych, dyplomatycznych, informacyjnych, militarnych lub innych, które nie stanowią agresji militarnej w ujęciu prawa międzynarodowego;

24) zagrożeniu antagonistycznym – należy przez to rozumieć rodzaj zagrożenia hybrydowego, ukierunkowanego przeciwko usługom kluczowym i infrastrukturze krytycznej niezbędnej do świadczenia tych usług, realizowanego w sposób celowy i świadomy, bez względu na motywację postępowania;

25) normie – należy przez to rozumieć normę, o której mowa w art. 2 pkt 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1025/2012 z dnia 25 października 2012 r. w sprawie normalizacji europejskiej, zmieniającego dyrektywy Rady 89/686/EWG i 93/15/EWG oraz dyrektywy Parlamentu Europejskiego i Rady 94/9/WE, 94/25/WE, 95/16/WE, 97/23/WE, 98/34/WE, 2004/22/WE, 2007/23/WE, 2009/23/WE i 2009/105/WE oraz uchylającego decyzję Rady 87/95/EWG i decyzję Parlamentu Europejskiego i Rady nr 1673/2006/WE (Dz. Urz. UE L 316 z 14.11.2012, str. 12, z późn. zm.[6)]);

26) specyfikacji technicznej – należy przez to rozumieć specyfikację techniczną, o której mowa w art. 2 pkt 4 rozporządzenia Parlamentu Europejskiego i Rady

---

[5)] Zmiany wymienionej decyzji zostały ogłoszone w Dz. Urz. UE L 250 z 04.10.2018, str. 1, Dz. Urz. UE L 77I z 20.03.2019, str. 1, Dz. Urz. UE L 185 z 26.05.2021, str. 1 oraz Dz. Urz. UE L 2023/2671 z 28.11.2023.

[6)] Zmiany wymienionego rozporządzenia zostały ogłoszone w Dz. Urz. UE L 323 z 19.12.2022, str. 1 oraz Dz. Urz. UE L 135 z 23.5.2023, str. 1.

(UE) nr 1025/2012 z dnia 25 października 2012 r. w sprawie normalizacji europejskiej, zmieniającego dyrektywy Rady 89/686/EWG i 93/15/EWG oraz dyrektywy Parlamentu Europejskiego i Rady 94/9/WE, 94/25/WE, 95/16/WE, 97/23/WE, 98/34/WE, 2004/22/WE, 2007/23/WE, 2009/23/WE i 2009/105/WE oraz uchylającego decyzję Rady 87/95/EWG i decyzję Parlamentu Europejskiego i Rady nr 1673/2006/WE;

27) jednostce certyfikującej – należy przez to rozumieć jednostkę oceniającą zgodność akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2025 r. poz. 568) lub upoważnioną do certyfikacji zgodnie z przepisami ustawy z dnia 12 września 2002 r. o normalizacji (Dz. U. z 2015 r. poz. 1483);

28) certyfikacie – należy przez to rozumieć dokument wydany przez jednostkę certyfikującą potwierdzający, że wyrób, instalacja, system, proces, usługa lub osoba spełniają odpowiednie wymagania;

29) certyfikacji – należy przez to rozumieć działania jednostki certyfikującej, wykazujące, że wyrób, instalacja, system, proces, usługa lub osoba spełniają odpowiednie wymagania;

30) zdolności do ochrony informacji niejawnych – należy przez to rozumieć spełnienie wymagań określonych w ustawie z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2025 r. poz. 1209);

31) realizacji zadań z zakresu obrony cywilnej oraz ochrony ludności – należy przez to rozumieć realizację zadań, o których mowa w ustawie z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej (Dz. U. poz. 1907, z 2025 r. poz. 1705 oraz …).”;

5) w art. 4 w ust. 1 po pkt 1 dodaje się pkt 1a w brzmieniu:

„1a) prowadzenie oceny ryzyka;”,

6) uchyla się art. 5–6d,

7) po art. 6d dodaje się rozdziały 2–15 oraz oznaczenie i tytuł rozdziału 16 w brzmieniu:

„Rozdział 2

Dokumenty strategiczne

Art. 6e. 1. W celu dokonania oceny ryzyka zidentyfikowanych zagrożeń opracowuje się Krajową Ocenę Ryzyka, zwaną dalej „KOR”. Rada Ministrów przyjmuje KOR w drodze uchwały.

2. KOR zawiera:

1) zidentyfikowane istotne zagrożenia:
   a) stanowiące katastrofę naturalną lub awarię techniczną w rozumieniu przepisów ustawy z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej (Dz. U. z 2025 r. poz. 112),
   b) hybrydowe,
   c) cyberbezpieczeństwa,
   d) o charakterze terrorystycznym,
   e) mogące spowodować niedostępność usług kluczowych,
   f) inne mogące spowodować znaczące negatywne skutki dla ludności, gospodarki lub dóbr kultury;
2) zagrożenia niezidentyfikowane jednoznacznie, które mogą wystąpić w przyszłości;
3) ocenę ryzyka wystąpienia zidentyfikowanych istotnych zagrożeń.

3. Przy opracowaniu oceny ryzyka uwzględnia się w szczególności:

1) zagrożenia, o których mowa w ust. 2 pkt 1;
2) powiązania między zagrożeniami wynikające z oddziaływań transgranicznych, zależności międzysektorowych i zmian klimatu;
3) ogólną ocenę ryzyka przeprowadzoną na podstawie art. 6 ust. 1 decyzji nr 1313/2013/UE;
4) dane o stratach i szkodach spowodowanych przez zagrożenia wskazane w ust. 2 pkt 1, gromadzone przez podmioty, o których mowa w art. 6g ust. 2;
5) inne istotne oceny ryzyka przeprowadzone zgodnie z wymogami właściwych sektorowych aktów Unii Europejskiej.

4. Ocena ryzyka w odniesieniu do podmiotów krytycznych uwzględnia dodatkowo:

1) wykaz usług kluczowych, o którym mowa w przepisach wydanych na podstawie art. 6zp ust. 3;
2) zidentyfikowane zagrożenia antagonistyczne;

3) ryzyka określane jako potencjalne straty lub potencjalne zakłócenia spowodowane incydentami, wyrażane jako wypadkowe skali tych strat lub zakłóceń oraz prawdopodobieństwa wystąpienia takich incydentów;
4) istotne ryzyka wynikające ze stopnia wzajemnej zależności między sektorami określonymi w załączniku do ustawy;
5) zależność ciągłości działania usług kluczowych od funkcjonowania podmiotów znajdujących się w innych państwach członkowskich i państwach trzecich;
6) wpływ znaczącego zakłócenia w jednym sektorze na inne sektory, w tym wszelkie istotne czynniki ryzyka dla obywateli i rynku wewnętrznego;
7) wpływ, jaki znaczące zakłócenie w jednym sektorze może mieć wpływ na inne sektory, w tym wszelkie istotne czynniki ryzyka dla obywateli i rynku wewnętrznego;
8) informacje dotyczące incydentów zgłaszanych przez podmioty krytyczne świadczące usługi kluczowe.

5. Projekt KOR opracowuje dyrektor Rządowego Centrum Bezpieczeństwa, zwanego dalej „Centrum”.

6. Na potrzeby opracowania projektu KOR dyrektor Centrum wydaje wytyczne do jego opracowania obejmujące elementy, o których mowa w ust. 2, oraz uwzględniające elementy, o których mowa w ust. 3 i 4.

7. Dyrektor Centrum przekazuje wytyczne do opracowania projektu KOR:
1) ministrom kierującym działami administracji rządowej;
2) Szefowi Agencji Bezpieczeństwa Wewnętrznego, Szefowi Agencji Wywiadu oraz Szefowi Centralnego Biura Antykorupcyjnego;
3) wojewodom;
4) Pełnomocnikowi Rządu do spraw Cyberbezpieczeństwa;
5) innym niż wymienione w pkt 1–4 podmiotom, jeżeli jest to konieczne.

8. W zakresie swojej właściwości organy i podmioty, o których mowa w ust. 7, uwzględniając wytyczne przekazane przez dyrektora Centrum, opracowują propozycje do ujęcia w projekcie KOR.

9. Propozycje do ujęcia w projekcie KOR, wraz z danymi stanowiącymi podstawę do ich przygotowania, z wyłączeniem informacji niejawnych, organy i podmioty, o których mowa w ust. 7, przekazują dyrektorowi Centrum we wskazanym przez niego terminie.

10. Dyrektor Centrum może wystąpić do organów i podmiotów, o których mowa w ust. 7, o przekazanie dodatkowych propozycji do ujęcia w projekcie KOR, jeżeli uzna, że ich umieszczenie w KOR jest niezbędne. Dyrektor Centrum uzasadnia wystąpienie przekazania dodatkowych propozycji.

11. Propozycje do ujęcia w projekcie KOR przekazane przez ministra kierującego działem administracji rządowej uwzględniają wkład do propozycji do ujęcia w projekcie KOR kierownika urzędu centralnego podległego temu ministrowi lub przez niego nadzorowanego.

12. Kierownik urzędu centralnego podległy ministrowi kierującemu działem administracji rządowej lub przez niego nadzorowany opracowuje i przekazuje wkład do propozycji do ujęcia w projekcie KOR ministra kierującego działem administracji rządowej.

13. Dyrektor Centrum przedkłada Radzie Ministrów projekt KOR nie rzadziej niż raz na trzy lata.

14. KOR uwzględnia się w:

1) planach zarządzania kryzysowego;
2) procesach identyfikacji podmiotów krytycznych;
3) opracowywaniu ocen ryzyka podmiotów krytycznych oraz wdrażaniu przez podmioty krytyczne środków w zakresie zwiększenia ich odporności;
4) innych dokumentach opracowywanych przez organy administracji publicznej w zakresie zarządzania kryzysowego.

15. Dyrektor Centrum, na podstawie KOR, opracowuje i udostępnia Komisji Europejskiej streszczenie istotnych elementów oceny ryzyka, o której mowa w art. 6 ust. 1 lit. a decyzji 1313/2013/UE.

16. Dyrektor Centrum, na podstawie KOR, opracowuje i udostępnia Komisji Europejskiej informacje dotyczące rodzajów ryzyka oraz wyników oceny ryzyka w odniesieniu do sektorów i podsektorów, o których mowa w załączniku do ustawy, w terminie trzech miesięcy od przyjęcia KOR.

Art. 6f. 1. W celu zwiększenia odporności podmiotów krytycznych opracowuje się Krajową Strategię Odporności Podmiotów Krytycznych, zwaną dalej „KSOPK”. Rada Ministrów przyjmuje KSOPK w drodze uchwały.

2. KSOPK:

1) określa cele strategiczne i priorytety w zakresie zapewnienia niezakłóconego świadczenia usług kluczowych przez podmioty krytyczne oraz niezakłóconego funkcjonowania infrastruktury krytycznej, z uwzględnieniem powiązań między zagrożeniami wynikającymi z oddziaływań transgranicznych oraz zależności międzysektorowych;
2) określa zakresy działań oraz formy działań służące osiąganiu celów strategicznych i priorytetów przez:
   a) organy właściwe w sprawach podmiotów krytycznych,
   b) ministrów kierujących działami administracji rządowej, którzy identyfikują infrastrukturę krytyczną,
   c) Komisję Nadzoru Finansowego identyfikującą, w zakresie swojej właściwości infrastrukturę krytyczną,
   d) wojewodów, którzy identyfikują infrastrukturę krytyczną,
   e) podmioty niewymienione w lit. a–d, zaangażowane we wdrażanie i realizację KSOPK;
3) zawiera opisy:
   a) procesów identyfikujących podmioty krytyczne,
   b) środków niezbędnych do zwiększenia ogólnej odporności podmiotów krytycznych, w tym opis oceny ryzyka, o której mowa w KOR,
   c) procesów wspierania podmiotów krytycznych przez podmioty, o których mowa w pkt 2 lit. a–d,
   d) środków mających na celu ułatwienie wypełniania obowiązków wynikających z rozdziału III dyrektywy 2022/2557 przez małe i średnie przedsiębiorstwa, w rozumieniu załącznika do zalecenia Komisji 2003/361/WE z dnia 6 maja 2003 r. dotyczącego definicji mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw, które zostały zidentyfikowane jako podmioty krytyczne (Dz. Urz. UE L 124 z 20.05.2003, str. 36);
4) określa zakres koordynacji działań organów do spraw podmiotów krytycznych i organów właściwych do spraw cyberbezpieczeństwa, o których mowa w ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2026 r. poz. 20, 252 i …).

3. Na potrzeby opracowania projektu KSOPK dyrektor Centrum wydaje wytyczne do jego opracowania obejmujące elementy, o których mowa w ust. 2.

4. Dyrektor Centrum przekazuje wytyczne do opracowania projektu KSOPK:

1) ministrom kierującym działami administracji rządowej;
2) Szefowi Agencji Bezpieczeństwa Wewnętrznego, Szefowi Agencji Wywiadu oraz Szefowi Centralnego Biura Antykorupcyjnego;
3) Komisji Nadzoru Finansowego;
4) wojewodom;
5) innym niż wymienione w pkt 1–4 podmiotom, jeżeli jest to konieczne.

5. W zakresie swojej właściwości organy i podmioty, o których mowa w ust. 4, uwzględniając wytyczne przekazane przez dyrektora Centrum, opracowują propozycje do ujęcia w projekcie KSOPK.

6. Propozycje do ujęcia w projekcie KSOPK, wraz z danymi stanowiącymi podstawę do ich przygotowania, z wyłączeniem informacji niejawnych, organy i podmioty, o których mowa w ust. 4, przekazują dyrektorowi Centrum we wskazanym przez niego terminie.

7. Dyrektor Centrum może wystąpić do organów i podmiotów, o których mowa w ust. 4, o przekazanie dodatkowych propozycji do ujęcia w projekcie KSOPK, jeżeli uzna, że ich umieszczenie w KSOPK jest niezbędne. Dyrektor Centrum uzasadnia wystąpienie o przekazanie dodatkowych propozycji.

8. Propozycje do ujęcia w projekcie KSOPK przekazane przez ministra kierującego działem administracji rządowej uwzględniają wkład do propozycji do ujęcia w projekcie KSOPK kierownika urzędu centralnego podległego temu ministrowi lub przez niego nadzorowanego.

9. Kierownik urzędu centralnego podległy ministrowi kierującemu działem administracji rządowej lub przez niego nadzorowany opracowuje i przekazuje wkład do propozycji do ujęcia w projekcie KSOPK ministra kierującego działem administracji rządowej.

10. Dyrektor Centrum może udostępnić opracowany projekt KSOPK na stronie podmiotowej Biuletynu Informacji Publicznej Centrum.

11. Dyrektor Centrum kieruje projekt KSOPK do 30-dniowych konsultacji publicznych, z przeprowadzenia których sporządza raport, wskazując główne tezy zawarte w stanowiskach zgłoszonych do projektu KSOPK oraz odniesienie się do nich.

12. Dyrektor Centrum udostępnia raport, o którym mowa w ust. 11, na stronie podmiotowej Biuletynu Informacji Publicznej Centrum.

13. Dyrektor Centrum przedkłada Radzie Ministrów projekt KSOPK raz na trzy lata.

14. Dyrektor Centrum udostępnia Komisji Europejskiej KSOPK nie później niż w terminie trzech miesięcy od dnia jej przyjęcia przez Radę Ministrów.

15. Przepisy ust. 3–12 i 14 stosuje się do aktualizacji KSOPK.

16. Dyrektor Centrum monitoruje wdrażanie postanowień KSOPK oraz w terminie do dnia 31 marca każdego roku przedkłada Radzie Ministrów sprawozdanie z jej wdrażania za poprzedni rok.

Rozdział 3

Plany zarządzania kryzysowego

Art. 6g. 1. Plany zarządzania ryzykiem zawierają:

1) cele strategiczne;
2) opis zasad współdziałania między podmiotami wskazanymi w siatce bezpieczeństwa;
3) uporządkowaną listę działań na rzecz ograniczenia ryzyka katastrof naturalnych lub awarii technicznych w zakresie organizacyjnym, technicznym i finansowym, 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.

2. Plany zarządzania ryzykiem opracowują:

1) dyrektor Centrum – Krajowy Plan Zarządzania Ryzykiem, zwany dalej „KPZR”;
2) minister kierujący działem administracji rządowej – plan zarządzania ryzykiem ministra kierującego działem administracji rządowej;
3) Szef Agencji Bezpieczeństwa Wewnętrznego, Szef Agencji Wywiadu oraz Szef Centralnego Biura Antykorupcyjnego – plan zarządzania ryzykiem odpowiednio Szefa Agencji Bezpieczeństwa Wewnętrznego, Szefa Agencji Wywiadu oraz Szefa Centralnego Biura Antykorupcyjnego;
4) kierownik urzędu centralnego wskazany przez ministra kierującego działem administracji rządowej, któremu podlega lub jest przez tego ministra nadzorowany – plan zarządzania ryzykiem kierownika urzędu centralnego;

5) wojewoda – wojewódzki plan zarządzania ryzykiem;

6) starosta – powiatowy plan zarządzania ryzykiem;

7) wójt (burmistrz, prezydent miasta) – gminny plan zarządzania ryzykiem.

3. Plany zarządzania ryzykiem, o których mowa w ust. 2, opracowuje się z uwzględnieniem zagrożeń wskazanych w Krajowej Ocenie Ryzyka.

4. Plany zarządzania ryzykiem, o których mowa w ust. 2 pkt 2–5, opracowuje się z zachowaniem spójności z KPZR.

5. W planach, o których mowa w ust. 2 pkt 6 i 7, uwzględnia się postanowienia KPZR.

Art. 6h. 1. Na potrzeby opracowania projektu KPZR dyrektor Centrum wydaje wytyczne do jego opracowania, obejmujące elementy, o których mowa w art. 6g ust. 1.

2. Dyrektor Centrum przekazuje wytyczne do opracowania projektu KPZR:

1) ministrom kierującym działami administracji rządowej;

2) Szefowi Agencji Bezpieczeństwa Wewnętrznego, Szefowi Agencji Wywiadu oraz Szefowi Centralnego Biura Antykorupcyjnego;

3) wojewodom;

4) innym niż wymienione w pkt 1–3 podmiotom, jeżeli jest to konieczne.

3. W zakresie swojej właściwości organy i podmioty, o których mowa w ust. 2, uwzględniając wytyczne przekazane przez dyrektora Centrum, opracowują propozycje do ujęcia w projekcie KPZR.

4. Propozycje do ujęcia w projekcie KPZR wraz z danymi stanowiącymi podstawę do ich przygotowania, z wyłączeniem informacji niejawnych, organy i podmioty, o których mowa w ust. 2, przekazują dyrektorowi Centrum we wskazanym przez niego terminie.

5. Dyrektor Centrum może wystąpić do organów i podmiotów, o których mowa w ust. 2, o przekazanie dodatkowych propozycji do ujęcia w projekcie KPZR, jeżeli uzna, że ich umieszczenie w KPZR jest niezbędne.

6. Propozycje do ujęcia w projekcie KPZR przekazane przez ministra kierującego działem administracji rządowej uwzględniają wkład do propozycji do ujęcia w projekcie KPZR kierownika urzędu centralnego podległego temu ministrowi lub przez niego nadzorowanego.

7. Kierownik urzędu centralnego podległy ministrowi kierującemu działem administracji rządowej lub przez niego nadzorowany opracowuje i przekazuje wkład do

propozycji do ujęcia w projekcie KPZR ministra kierującego działem administracji rządowej.

8. Dyrektor Centrum przedkłada Radzie Ministrów projekt KPZR nie rzadziej niż raz na trzy lata. Rada Ministrów przyjmuje KPZR w drodze uchwały.

9. Na podstawie KPZR dyrektor Centrum opracowuje i udostępnia Komisji Europejskiej streszczenie istotnych elementów krajowej oceny zdolności zarządzania ryzykiem, o której mowa w art. 6 ust. 1 lit. b decyzji 1313/2013/UE.

Art. 6i. 1. Plan zarządzania ryzykiem ministra kierującego działem administracji rządowej obejmuje własny plan zarządzania ryzykiem oraz plany zarządzania ryzykiem kierowników urzędów centralnych podległych temu ministrowi lub przez niego nadzorowanych.

2. Minister kierujący działem administracji, w zakresie swojej właściwości, wskazuje kierownika urzędu centralnego podległego lub nadzorowanego, który jest obowiązany do opracowania własnego planu zarządzania ryzykiem.

3. Plan zarządzania ryzykiem Ministra Obrony Narodowej uwzględnia plany zarządzania ryzykiem Szefa Służby Kontrwywiadu Wojskowego oraz Szefa Służby Wywiadu Wojskowego.

4. Minister kierujący działem administracji rządowej, Szef Agencji Bezpieczeństwa Wewnętrznego, Szef Agencji Wywiadu, Szef Centralnego Biura Antykorupcyjnego:

1) uzgadnia projekt planu zarządzania ryzykiem z dyrektorem Centrum pod względem spójności z KPZR;
2) zatwierdza uzgodniony plan zarządzania ryzykiem;
3) przekazuje kopię zatwierdzonego planu zarządzania ryzykiem dyrektorowi Centrum.

5. Kierownik urzędu centralnego, o którym mowa w ust. 2:

1) uzgadnia projekt planu zarządzania ryzykiem z ministrem kierującym działem administracji rządowej, któremu podlega lub przez którego jest nadzorowany;
2) uzgadnia projekt planu zarządzania ryzykiem z dyrektorem Centrum pod względem spójności z KPZR;
3) zatwierdza uzgodniony plan zarządzania ryzykiem;
4) przekazuje kopię zatwierdzonego planu zarządzania ryzykiem właściwemu ministrowi oraz dyrektorowi Centrum.

6. Wojewoda:

1) przekazuje projekt wojewódzkiego planu zarządzania ryzykiem do zatwierdzenia ministrowi właściwemu do spraw administracji publicznej;
2) przekazuje zatwierdzony wojewódzki plan zarządzania ryzykiem do wiadomości dyrektorowi Centrum.

7. Starosta przekazuje projekt powiatowego planu zarządzania ryzykiem do zatwierdzenia właściwemu wojewodzie.

8. Wójt (burmistrz, prezydent miasta) przekazuje projekt gminnego planu zarządzania ryzykiem do zatwierdzenia właściwemu staroście.

Art. 6j. 1. Plany reagowania kryzysowego opracowują:

1) dyrektor Centrum – Krajowy Plan Reagowania Kryzysowego, zwany dalej „KPRK”;
2) minister kierujący działem administracji rządowej – plan reagowania kryzysowego ministra kierującego działem administracji rządowej;
3) Szef Agencji Bezpieczeństwa Wewnętrznego, Szef Agencji Wywiadu oraz Szef Centralnego Biura Antykorupcyjnego – plan reagowania kryzysowego odpowiednio Szefa Agencji Bezpieczeństwa Wewnętrznego, Szefa Agencji Wywiadu oraz Szefa Centralnego Biura Antykorupcyjnego;
4) kierownik urzędu centralnego wskazany przez ministra kierującego działem administracji rządowej, któremu podlega lub jest przez tego ministra nadzorowany – plan reagowania kryzysowego kierownika urzędu centralnego;
5) wojewoda – wojewódzki plan reagowania kryzysowego;
6) starosta – powiatowy plan reagowania kryzysowego;
7) wójt (burmistrz, prezydent miasta) – gminny plan reagowania kryzysowego.

2. Plany reagowania kryzysowego, o których mowa w ust. 1, opracowuje się w odniesieniu do zagrożeń wskazanych w KOR oraz z uwzględnieniem odpowiedniego planu zarządzania ryzykiem.

3. Plany reagowania kryzysowego, o których mowa w ust. 1 pkt 2–5, opracowuje się z zachowaniem spójności z KPRK.

Art. 6k. 1. KPRK zawiera:

1) określenie zadań i obowiązków uczestników zarządzania kryzysowego w formie siatki bezpieczeństwa w zakresie reagowania w przypadku wystąpienia sytuacji kryzysowej oraz usuwania jej skutków;

2) zasady współdziałania między uczestnikami, o których mowa w pkt 1, w tym wymiany informacji w relacjach krajowych i międzynarodowych;
3) zestawienie sił i środków planowanych do wykorzystania w sytuacjach kryzysowych lub w zakresie realizacji zadań związanych z ochroną ludności oraz obroną cywilną;
4) zestawienie modułów zadaniowych pogrupowanych w katalogi;
5) załączniki określające:
   a) opis organizacji systemu monitorowania zagrożeń, ostrzegania i alarmowania,
   b) opis organizacji łączności,
   c) opis informowania ludności o zagrożeniach i sposobach postępowania na wypadek zagrożeń,
   d) procedury oceniania i dokumentowania strat i szkód,
   e) procedury uruchamiania rezerw strategicznych,
   f) procedury realizacji zadań związanych z ochroną ludności oraz obroną cywilną,
   g) procedury reagowania kryzysowego – standardowe procedury operacyjne,
   h) priorytety w zakresie ochrony oraz odtwarzania infrastruktury krytycznej.

2. Dyrektor Centrum we współpracy z podmiotami, o których mowa w art. 6j ust. 1 pkt 2–5, opracowuje projekt KPRK.

3. Dyrektor Centrum przedkłada projekt KPRK Radzie Ministrów nie rzadziej niż raz na trzy lata. Rada Ministrów przyjmuje KPRK w drodze uchwały.

Art. 6l. 1. Plan reagowania kryzysowego ministra kierującego działem administracji rządowej, Szefa Agencji Bezpieczeństwa Wewnętrznego, Szefa Agencji Wywiadu, Szefa Centralnego Biura Antykorupcyjnego oraz kierownika urzędu centralnego podległego ministrowi kierującemu działem administracji rządowej lub przez niego nadzorowanego zawiera:

1) określenie zadań i obowiązków uczestników zarządzania kryzysowego w formie siatki bezpieczeństwa w zakresie reagowania w przypadku wystąpienia sytuacji kryzysowej oraz usuwania jej skutków;
2) określenie zadań w zakresie monitorowania zagrożeń;
3) zestawienie przedsięwzięć realizowanych w ramach przypisanych katalogów i modułów zadaniowych wraz z ich opisem;
4) określenie organizacji realizacji zadań z zakresu ochrony infrastruktury krytycznej lub zapewnienia ciągłości świadczenia usług kluczowych.

2. Plan reagowania kryzysowego ministra kierującego działem administracji rządowej obejmuje własny plan reagowania kryzysowego oraz plany reagowania kryzysowego kierowników urzędów centralnych podległych temu ministrowi lub przez niego nadzorowanych.

3. Minister kierujący działem administracji, w zakresie swojej właściwości, wskazuje kierownika urzędu centralnego podległego lub nadzorowanego, który jest obowiązany do opracowania własnego planu reagowania kryzysowego.

4. Plan reagowania kryzysowego Ministra Obrony Narodowej uwzględnia plany reagowania kryzysowego Szefa Służby Kontrwywiadu Wojskowego oraz Szefa Służby Wywiadu Wojskowego.

5. Minister kierujący działem administracji rządowej, Szef Agencji Bezpieczeństwa Wewnętrznego, Szef Agencji Wywiadu, Szef Centralnego Biura Antykorupcyjnego:

1) uzgadnia projekt planu reagowania kryzysowego z dyrektorem Centrum pod względem spójności z KPRK;
2) zatwierdza uzgodniony plan reagowania kryzysowego;
3) przekazuje kopię zatwierdzonego planu reagowania kryzysowego dyrektorowi Centrum.

6. Kierownik urzędu centralnego, o którym mowa w ust. 3:

1) uzgadnia projekt planu reagowania kryzysowego z ministrem kierującym działem administracji rządowej, któremu podlega lub przez którego jest nadzorowany;
2) uzgadnia projekt planu reagowania kryzysowego z dyrektorem Centrum pod względem spójności z KPRK;
3) zatwierdza uzgodniony plan reagowania kryzysowego;
4) przekazuje kopię zatwierdzonego planu reagowania kryzysowego właściwemu ministrowi oraz dyrektorowi Centrum.

Art. 6m. 1. Wojewódzki plan reagowania kryzysowego zawiera:

1) elementy, o których mowa w art. 6k ust. 1 pkt 1–3 i 5 oraz art. 6l ust. 1 pkt 2 i 3;
2) zestawienie przedsięwzięć minimalizujących skutki zakłócenia funkcjonowania infrastruktury krytycznej dla ludności na terenie województwa wraz z ich opisem.

2. Wojewoda:

1) przekazuje projekt wojewódzkiego planu reagowania kryzysowego do zatwierdzenia ministrowi właściwemu do spraw administracji publicznej;

2) przekazuje zatwierdzony wojewódzki plan reagowania kryzysowego do wiadomości dyrektorowi Centrum.

Art. 6n. 1. Powiatowy plan reagowania kryzysowego oraz gminny plan reagowania kryzysowego zawierają:

1) elementy, o których mowa w art. 6k ust. 1 pkt 1–3 i 5 oraz art. 6l ust. 1 pkt 2 i 3;
2) zestawienie przedsięwzięć minimalizujących skutki zakłócenia funkcjonowania infrastruktury krytycznej dla ludności na terenie właściwej jednostki samorządu terytorialnego, wraz z ich opisem.

2. Starosta przekazuje projekt powiatowego planu reagowania kryzysowego do zatwierdzenia właściwemu wojewodzie.

3. Wójt (burmistrz, prezydent miasta) przekazuje projekt gminnego planu reagowania kryzysowego do zatwierdzenia właściwemu staroście.

Art. 6o. 1. Plany zarządzania kryzysowego podlegają systematycznej aktualizacji w cyklu planowania nie dłuższym niż trzy lata.

2. Plany zarządzania kryzysowego uzgadnia się z właściwymi podmiotami, w zakresie ich dotyczącym, planowanymi do wykorzystania przy realizacji przedsięwzięć określonych w planie.

3. Przy opracowywaniu planów zarządzania kryzysowego uwzględnia się:

1) zawarte umowy i porozumienia,
2) plany opracowane na podstawie odrębnych przepisów, w tym wynikające z aktów Unii Europejskiej

– niezbędne do realizacji przedsięwzięć określonych w planach zarządzania kryzysowego.

4. Minister kierujący działem administracji rządowej może wydać, w drodze zarządzenia, wytyczne do opracowania planów zarządzania kryzysowego kierowników urzędów centralnych podległych temu ministrowi lub przez niego nadzorowanych, kierując się zachowaniem spójności z planami zarządzania kryzysowego opracowanymi przez ministra.

Rozdział 4

Infrastruktura krytyczna

Art. 6p. Zadania dotyczące infrastruktury krytycznej obejmują:

1) identyfikację oraz wyznaczanie infrastruktury krytycznej;

2) gromadzenie i przetwarzanie informacji dotyczących zagrożeń infrastruktury krytycznej;
3) opracowywanie i wdrażanie procedur na wypadek wystąpienia zagrożeń infrastruktury krytycznej;
4) odtwarzanie infrastruktury krytycznej;
5) współpracę między organami administracji publicznej a operatorami infrastruktury krytycznej w zakresie ochrony infrastruktury krytycznej.

Art. 6q. 1. Organami właściwymi w sprawie identyfikacji infrastruktury krytycznej oraz współpracy z operatorami infrastruktury krytycznej, w zakresie swoich właściwości, są:

1) ministrowie kierujący działami administracji rządowej;
2) wojewodowie;
3) Komisja Nadzoru Finansowego.

2. Organy, o których mowa w ust. 1, w zakresie identyfikacji infrastruktury krytycznej współpracują z dyrektorem Centrum.

3. Minister kierujący działem administracji rządowej, wojewoda, Komisja Nadzoru Finansowego, w zakresie swojej właściwości, oraz dyrektor Centrum, zapewniają bieżącą współpracę z operatorem infrastruktury krytycznej, w szczególności przez:

1) prowadzenie bieżącej wymiany informacji na temat zagrożeń;
2) prowadzenie działań informacyjnych dotyczących dobrych praktyk, działań edukacyjnych na rzecz poszerzania wiedzy w zakresie bezpieczeństwa oraz zapewnienia funkcjonowania infrastruktury krytycznej, w tym organizowanie, konferencji, seminariów lub forów wymiany wiedzy;
3) udzielanie wsparcia merytorycznego operatorom infrastruktury krytycznej:
   a) w zakresie wdrażania dobrych praktyk oraz niezbędnych rozwiązań dotyczących ochrony infrastruktury krytycznej,
   b) w celu zapewnienia właściwego funkcjonowania infrastruktury krytycznej, jej ochrony lub odbudowy,
   c) w sytuacji kryzysowej lub w przypadku możliwości wystąpienia sytuacji kryzysowej.

Rozdział 5

Identyfikowanie infrastruktury krytycznej

Art. 6r. 1. Dyrektor Centrum w celu zapewnienia:

1) identyfikacji obiektu, urządzenia, instalacji, sieci, systemu oraz usługi lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji, sieci, systemów oraz usług jako infrastruktury krytycznej,
2) realizacji zadań w zakresie ochrony infrastruktury krytycznej

– prowadzi wykaz infrastruktury krytycznej.

2. Wykaz infrastruktury krytycznej zawiera:

1) nazwę i lokalizację infrastruktury krytycznej, w tym wskazanie infrastruktury krytycznej niezbędnej do świadczenia usług kluczowych;
2) dane operatora infrastruktury krytycznej, w tym siedzibę i adres oraz numer identyfikacji podatkowej (NIP), jeżeli został nadany;
3) wskazanie organu identyfikującego infrastrukturę krytyczną.

3. Wykaz infrastruktury krytycznej prowadzony jest w postaci elektronicznej. Do wykazu stosuje się przepisy ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych.

4. Obiekt, urządzenie, instalacja, sieć, system oraz usługa lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje, sieci, systemy oraz usługi zostają wpisane do wykazu infrastruktury krytycznej w przypadku gdy spełniają kryteria, o których mowa w przepisach wydanych na podstawie ust. 5.

5. Rada Ministrów określi, w drodze uchwały, kryteria pozwalające identyfikować obiekt, urządzenie, instalację, sieć, system oraz usługę lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje, sieci, systemy oraz usługi jako infrastrukturę krytyczną, w tym:

1) kryteria sektorowe – progi, w tym progi liczbowe, charakteryzujące zdolność obiektu, urządzenia, instalacji, sieci, systemu oraz usługi lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji, sieci, systemów oraz usług do zapewnienia, funkcjonowania organów administracji publicznej, zapewnienia funkcjonowania przedsiębiorstw, zaspokajania potrzeb obywateli oraz zapewnienia świadczenia usług kluczowych,

2) kryteria przekrojowe – progi odnoszące się do znaczenia obiektu, urządzenia, instalacji, sieci, systemu oraz usługi lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji, sieci, systemów oraz usług obejmujące:
   a) kryteria ofiar w ludziach – oceniane w odniesieniu do ewentualnej liczby ofiar śmiertelnych lub liczby rannych,
   b) kryteria ewakuacji – oceniane w odniesieniu do liczby osób ewakuowanych lub czasu ewakuacji,
   c) kryteria skutków ekonomicznych – oceniane w odniesieniu do znaczenia strat ekonomicznych lub pogorszenia świadczenia jakości usług kluczowych,
   d) kryteria skutków społecznych – oceniane w odniesieniu do wpływu na zaufanie opinii publicznej lub zakłócenia codziennego życia obywateli, w tym utraty usług kluczowych,
   e) kryteria wpływu międzynarodowego – oceniane w odniesieniu do pogorszenia wizerunku kraju na arenie międzynarodowej lub możliwości realizacji zobowiązań międzynarodowych,
   f) kryteria unikatowości – oceniane w odniesieniu do braku możliwości zastąpienia lub odtworzenia w akceptowalnym czasie

– uwzględniając sektory lub podsektory, o których mowa w załączniku do ustawy, znaczenie obiektu, urządzenia, instalacji, sieci, systemu oraz usługi lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji, sieci, systemów oraz usług dla realizacji interesów państwa, funkcjonowania przedsiębiorców, zaspokajania potrzeb obywateli, w tym potrzeb o charakterze lokalnym oraz zapewnienia świadczenia usług kluczowych.

6. Do uchwały stosuje się przepisy ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych.

Art. 6s. 1. Dyrektor Centrum dokonuje wpisu do wykazu infrastruktury krytycznej na podstawie wniosku złożonego przez:

1) ministra kierującego działem administracji rządowej;
2) właściwego miejscowo wojewodę;
3) Komisję Nadzoru Finansowego.

2. Dyrektor Centrum opracowuje wyciągi z wykazu infrastruktury krytycznej znajdującej się na terenie poszczególnych województw i przekazuje je właściwym wojewodom.

Art. 6t. 1. Minister kierujący działem administracji rządowej we współpracy z dyrektorem Centrum identyfikuje obiekt, urządzenie, instalację, sieć, system oraz usługę lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje, sieci, systemy oraz usługi mogące stanowić infrastrukturę krytyczną.

2. W przypadku identyfikacji prowadzonej przez ministra kierującego działem administracji rządowej, obiekt, urządzenie, instalację, sieć, system oraz usługę lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje, sieci, systemy oraz usługi zostają wpisane do wykazu infrastruktury krytycznej, jeżeli spełniają łącznie kryterium sektorowe, o którym mowa w art. 6r ust. 5 pkt 1, oraz co najmniej jedno z kryteriów przekrojowych, o których mowa w art. 6r ust. 5 pkt 2.

3. Minister kierujący działem administracji rządowej może wystąpić do właściciela lub posiadacza obiektu, urządzenia, instalacji, sieci, systemu oraz usługi lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji, sieci, systemów oraz usług o udzielenie informacji, które umożliwią ocenę, czy spełniają one warunki do uznania ich za infrastrukturę krytyczną, przekazując dokumenty niezbędne do udzielenia informacji.

4. Minister kierujący działem administracji rządowej w wystąpieniu, o którym mowa w ust. 3, wskazuje termin udzielenia informacji. Wyznaczony termin nie może być krótszy niż 14 dni, licząc od dnia otrzymania wystąpienia przez podmiot.

5. Minister kierujący działem administracji rządowej składa do dyrektora Centrum wniosek o wpis obiektu, urządzenia, instalacji, sieci, systemu oraz usługi lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji, sieci, systemów oraz usługi do wykazu infrastruktury krytycznej. Wniosek zawiera informacje obejmujące:

1) nazwę i lokalizację obiektu, urządzenia, instalacji, sieci, systemu oraz usługi lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji, sieci, systemów oraz usług;
2) dane właściciela lub posiadacza obiektu, urządzenia, instalacji, sieci, systemu oraz usługi lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji, sieci, systemów oraz usług w tym siedzibę i adres oraz numer identyfikacji podatkowej (NIP), jeżeli został nadany.

6. Wniosek sporządza się i składa na piśmie utrwalonym w postaci elektronicznej, opatrzonym kwalifikowanym podpisem elektronicznym, podpisem osobistym, podpisem zaufanym albo kwalifikowaną pieczęcią elektroniczną.

Art. 6u. 1. Wojewoda we współpracy z dyrektorem Centrum identyfikuje obiekt, urządzenie, instalację lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje oraz sieć, system lub usługę mogące stanowić infrastrukturę krytyczną na terenie województwa.

2. W przypadku identyfikacji prowadzonej przez wojewodę, obiekt, urządzenie, instalację, sieć, system oraz usługę lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje, sieci, systemy oraz usługi mogą zostać wpisane do wykazu infrastruktury krytycznej, jeżeli spełniają co najmniej jedno z kryteriów przekrojowych, o których mowa w art. 6r ust. 5 pkt 2. Przepisy art. 6t ust. 3–6 stosuje się odpowiednio.

Art. 6v. 1. Komisja Nadzoru Finansowego, w zakresie swojej właściwości, we współpracy z dyrektorem Centrum, identyfikuje obiekt, urządzenie, instalację, sieć, system oraz usługę lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje, sieci, systemy oraz usługi mogące stanowić infrastrukturę krytyczną.

2. W przypadku identyfikacji prowadzonej przez Komisję Nadzoru Finansowego, obiekt, urządzenie, instalacja, sieć, system oraz usługa lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje, sieci, systemy oraz usługi mogą zostać wpisane do wykazu infrastruktury krytycznej, jeżeli spełniają łącznie kryterium sektorowe, o którym mowa w art. 6r ust. 5 pkt 1, oraz co najmniej jedno z kryteriów, o których mowa w art. 6r ust. 5 pkt 2. Przepis art. 6t ust. 3–6 stosuje się odpowiednio.

Art. 6w. 1. Dyrektor Centrum informuje właściciela lub posiadacza obiektu, urządzenia, instalacji, sieci, systemu oraz usługi lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji, sieci, systemów oraz usług o dokonaniu wpisu do wykazu infrastruktury krytycznej oraz obowiązkach z tym związanych w terminie 30 dni od wpisu do wykazu.

2. Informacje o realizacji czynności, o których mowa w ust. 1, dyrektor Centrum przekazuje organowi wnioskującemu o wpis do wykazu.

Art. 6x. Organy, o których mowa w art. 6s ust. 1, oraz dyrektor Centrum, prowadzą bieżącą wymianę informacji dotyczących realizacji czynności w zakresie identyfikacji obiektów, urządzeń, instalacji, sieci, systemów oraz usług lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji, sieci, systemów oraz usług, które mogą zostać wpisane do wykazu infrastruktury krytycznej.

Rozdział 6

Identyfikowanie potencjalnej infrastruktury krytycznej

Art. 6y. 1. Dyrektor Centrum w celu zapewnienia:

1) identyfikacji obiektu, urządzenia, instalacji, sieci, systemu oraz usługi lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji, sieci, systemów oraz usług, będących na etapie projektowania lub budowy jako potencjalnej infrastruktury krytycznej,
2) realizacji zadań w zakresie ochrony potencjalnej infrastruktury krytycznej

– prowadzi wykaz potencjalnej infrastruktury krytycznej.

2.Wykaz potencjalnej infrastruktury krytycznej zawiera:

1) nazwę i lokalizację potencjalnej infrastruktury krytycznej;
2) dane podmiotu będącego inwestorem, w rozumieniu ustawy z dnia 7 lipca 1994 r. – Prawo budowlane (Dz. U. z 2025 r. poz. 418, 1080, 1535, 1673 i 1847), prowadzącego prace projektowe lub budowlane dotyczące potencjalnej infrastruktury krytycznej, w tym siedzibę i adres oraz numer identyfikacji podatkowej (NIP), jeżeli został nadany;
3) wskazanie organu identyfikującego potencjalną infrastrukturę krytyczną.

3. Wykaz potencjalnej infrastruktury krytycznej prowadzony jest w postaci elektronicznej. Do wykazu stosuje się przepisy ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych.

4. Obiekt, urządzenie, instalacja, sieć, system oraz usługa lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje, sieci, systemy oraz usługi, które są na etapie projektowania lub budowy, mogą zostać wpisane do wykazu potencjalnej infrastruktury krytycznej, w przypadku gdy z założeń wynika, że spełnią kryteria, o których mowa w przepisach wydanych na podstawie aktu wykonawczego wydanego na podstawie art. 6r ust. 5.

Art. 6z. Dyrektor Centrum dokonuje wpisu do wykazu potencjalnej infrastruktury krytycznej na podstawie wniosku złożonego przez:

1) ministra kierującego działem administracji rządowej;
2) właściwego miejscowo wojewodę;
3) Komisję Nadzoru Finansowego.

Art. 6za. 1. Minister kierujący działem administracji rządowej, we współpracy z dyrektorem Centrum oraz inwestorem identyfikuje potencjalną infrastrukturę krytyczną. Przepisy art. 6t ust. 2–6 stosuje się odpowiednio.

2. Wojewoda, we współpracy z dyrektorem Centrum oraz inwestorem, identyfikuje potencjalną infrastrukturę krytyczną. Przepisy art. 6u ust. 2 oraz art. 6t ust. 3–6 stosuje się odpowiednio.

3. Komisja Nadzoru Finansowego, we współpracy z dyrektorem Centrum oraz inwestorem, identyfikuje potencjalną infrastrukturę krytyczną. Przepisy art. 6v ust. 2 oraz art. 6t ust. 3–6 stosuje się odpowiednio.

Art. 6zb. 1. Dyrektor Centrum informuje inwestora o dokonaniu wpisu do wykazu potencjalnej infrastruktury krytycznej oraz obowiązkach z tym związanych w terminie 30 dni od wpisu do wykazu.

2. Informacje o realizacji czynności, o których mowa w ust. 1, dyrektor Centrum przekazuje organowi wnioskującemu o wpis do wykazu.

Art. 6zc. 1. Organy, o których mowa w art. 6z, w zakresie swojej właściwości, we współpracy z dyrektorem Centrum, przedstawiają inwestorowi informacje oraz dokumenty pozwalające na uwzględnienie wymogów dotyczących infrastruktury krytycznej w dokumentacji projektowej lub podczas realizacji inwestycji oraz zapewniają bieżącą współpracę w zakresie, o którym mowa w art. 6p.

2. Do obowiązków inwestora w zakresie ochrony potencjalnej infrastruktury krytycznej nie stosuje się rozdziału 7 ustawy, z wyjątkiem przepisu art. 6ze ust. 1 pkt 1 i pkt 2 lit. a, pkt 3 lit. a oraz pkt 4, art. 6zf ust. 2 pkt 1 i pkt 2 lit. a oraz pkt 4 lit. a.

Art. 6zd. Podmioty, o których mowa w art. 6z oraz dyrektor Centrum, prowadzą bieżącą wymianę informacji dotyczących realizacji czynności w zakresie identyfikacji obiektów, urządzeń, instalacji, sieci, systemów oraz usług lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji, sieci, systemów oraz usług będących w fazie projektowania lub budowy, które mogą zostać wpisane do wykazu potencjalnej infrastruktury krytycznej.

Rozdział 7

Obowiązki operatora infrastruktury krytycznej

Art. 6ze. 1. Operator infrastruktury krytycznej zapewnia jej ochronę, w szczególności przez:

1) prowadzenie systematycznej analizy zagrożeń dla infrastruktury krytycznej;
2) wdrażanie adekwatnych do wyników przeprowadzonej analizy zagrożeń rozwiązań w zakresie:
   a) bezpieczeństwa fizycznego, w tym ochrony fizycznej oraz zabezpieczeń technicznych uwzględniających kontrolę dostępu,
   b) bezpieczeństwa technicznego,
   c) bezpieczeństwa osobowego dotyczącego pracowników i dostawców zewnętrznych,
   d) cyberbezpieczeństwa,
   e) bezpieczeństwa prawnego,
   f) ciągłości działania i odtwarzania, w tym utrzymywania własnych systemów rezerwowych zapewniających bezpieczeństwo i podtrzymujących funkcjonowanie infrastruktury krytycznej do czasu jej pełnego odtworzenia;
3) bieżącą współpracę z organami zarządzania kryzysowego, służbami, stażami i inspekcjami oraz dyrektorem Centrum przez przekazywanie i odbieranie informacji o:
   a) zagrożeniach zakłócających lub mogących zakłócić funkcjonowanie infrastruktury krytycznej,
   b) spodziewanych przerwach lub zakłóceniach w funkcjonowaniu infrastruktury krytycznej;
4) sporządzanie i przekazywanie informacji w zakresie zapewnienia ochrony infrastruktury krytycznej, na żądanie:
   a) odpowiednio:
      – ministra, o którym mowa w art. 6t ust. 1,
      – właściwego miejscowo wojewody,
      – Komisji Nadzoru Finansowego,
   b) dyrektora Centrum,
   c) Szefa Agencji Bezpieczeństwa Wewnętrznego oraz Szefa Agencji Wywiadu;
5) zapewnienie zdolności do ochrony informacji niejawnych w zakresie realizacji przedsięwzięć związanych z ochroną infrastruktury krytycznej.

2. Operator infrastruktury krytycznej przeprowadza po raz pierwszy analizę zagrożeń, o której mowa w ust. 1 pkt 1, w terminie 6 miesięcy od dnia otrzymania informacji o dokonaniu wpisu do wykazu infrastruktury krytycznej.

3. Operator infrastruktury krytycznej wdraża rozwiązania, o których mowa w ust. 1 pkt 2, w terminie 6 miesięcy od dnia przeprowadzenia po raz pierwszy analizy zagrożeń, a następnie stosowanie do potrzeb, w zależności od wyników przeprowadzonej analizy zagrożeń.

4. Rada Ministrów określi, w drodze rozporządzenia, minimalne wymagania w zakresie bezpieczeństwa fizycznego, technicznego, osobowego, cyberbezpieczeństwa, prawnego oraz ciągłości działania, niezbędne do wdrażania rozwiązań, o których mowa w ust. 1 pkt 2, mając na uwadze:

1) rekomendacje o charakterze specjalistycznym w zakresie ochrony infrastruktury krytycznej, niezbędne do wdrażania rozwiązań w zakresie bezpieczeństwa infrastruktury krytycznej;
2) lokalizację i charakterystykę infrastruktury krytycznej;
3) potrzebę podejmowania działań zapewniających bezpieczeństwo infrastruktury krytycznej.

5. Operator infrastruktury krytycznej, przy opracowywaniu i zawieraniu umów zapewniających wdrażanie rozwiązań, o których mowa w ust. 1 pkt 2, żąda od usługodawców:

1) certyfikatów, uwzględniając dokumenty równoważne, zgodnie z zasadami wzajemnego uznawania w Unii Europejskiej, lub w przypadku ich braku – innych dokumentów właściwych dla poszczególnych rozwiązań, potwierdzających posiadanie odpowiednich kompetencji i uprawnień niezbędnych do ich realizacji;
2) potwierdzenia zdolności do ochrony informacji niejawnych oraz stosowania przepisów o ochronie informacji niejawnych, jeżeli opracowanie, przygotowanie i wykonanie umowy wiążą się dostępem do informacji niejawnych.

6. Minister kierujący działem administracji rządowej, właściwy terytorialnie wojewoda lub Komisja Nadzoru Finansowego, po zasięgnięciu opinii właściwych sektorowych rad do spraw kompetencji, o których mowa w art. 4c ust. 1 pkt 2 ustawy z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości (Dz. U. z 2025 r. poz. 98), może opracować i udostępnić na stronie podmiotowej Biuletynu Informacji Publicznej zestawienie certyfikatów lub innych dokumentów właściwych dla realizacji rozwiązań wskazanych w ust. 1 pkt 2.

7. Minister kierujący działem administracji rządowej, właściwy terytorialnie wojewoda lub Komisja Nadzoru Finansowego, w zakresie swojej właściwości, we

współpracy z dyrektorem Centrum ustalają klauzule tajności oraz szczegółowe wymagania dotyczące ochrony informacji niejawnych związanych z realizacją przez operatora infrastruktury krytycznej przedsięwzięć związanych z ochroną tej infrastruktury.

Art. 6zf. 1. Operator infrastruktury krytycznej opracowuje, stosuje i na bieżąco aktualizuje dokumentację ochrony infrastruktury krytycznej.

2. Dokumentacja ochrony infrastruktury krytycznej zawiera:

1) charakterystykę infrastruktury krytycznej oraz analizę zagrożeń, o której mowa w art. 6ze ust. 1 pkt 1;
2) opis zastosowanych, adekwatnie do przeprowadzonej analizy zagrożeń, rozwiązań w zakresie:
   a) bezpieczeństwa fizycznego, w tym opis organizacji i wykonywania ochrony fizycznej infrastruktury krytycznej, zawierający dane specjalistycznej uzbrojonej formacji ochronnej chroniącej infrastrukturę krytyczną, 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 oraz …) – jeżeli występuje,
   b) bezpieczeństwa technicznego,
   c) bezpieczeństwa osobowego,
   d) cyberbezpieczeństwa,
   e) bezpieczeństwa prawnego,
   f) ciągłości działania i odtwarzania;
3) opis:
   a) zasobów umożliwiających podtrzymanie funkcjonowania infrastruktury krytycznej do czasu jej pełnego odtworzenia,
   b) współpracy z organami zarządzania kryzysowego, służbami, stażami i inspekcjami oraz dyrektorem Centrum, dotyczący wymiany informacji o zdarzeniu zakłócającym lub mogącym zakłócić funkcjonowanie infrastruktury krytycznej oraz sposobu postępowania w przypadku takiego zdarzenia;
4) procedury:
   a) działania w sytuacji zagrożenia lub zakłócenia funkcjonowania infrastruktury krytycznej,
   b) zapewnienia ciągłości funkcjonowania infrastruktury krytycznej,

c) odtwarzania infrastruktury krytycznej;

5) inne elementy niż wskazane w pkt 1–4, biorąc pod uwagę charakterystykę infrastruktury krytycznej.

3. Procedury, o których mowa w ust. 2 pkt 4 lit. a, uzgadnia się z właściwymi organami zarządzania kryzysowego, służbami, strażami i inspekcjami, w zakresie ich dotyczącym, planowanymi do wykorzystania w realizacji przedsięwzięć określonych w dokumentacji.

4. Do dokumentacji ochrony infrastruktury krytycznej stosuje się przepisy ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych.

5. Operator infrastruktury krytycznej w terminie 15 miesięcy od uzyskania informacji o dokonaniu wpisu do wykazu infrastruktury krytycznej przedkłada oświadczenie o opracowaniu dokumentacji ochrony infrastruktury krytycznej, odpowiednio:

1) ministrowi, o którym mowa w art. 6t ust. 1;
2) właściwemu miejscowo wojewodzie;
3) Komisji Nadzoru Finansowego;
4) dyrektorowi Centrum.

6. Operator infrastruktury krytycznej może dołączyć do oświadczenia o opracowaniu dokumentacji ochrony infrastruktury krytycznej informację o braku możliwości wdrożenia określonych rozwiązań, wskazując przyczynę tego braku, wraz z uzasadnieniem. Operator infrastruktury krytycznej uzgadnia odpowiednio z ministrem, wojewodą lub Komisją Nadzoru Finansowego działania mające na celu wdrożenie brakujących rozwiązań.

7. Operator infrastruktury krytycznej przekazuje dokumentację ochrony infrastruktury krytycznej na żądanie organów, o których mowa w ust. 4 pkt 1–3 oraz dyrektora Centrum.

8. Operator infrastruktury krytycznej, będący jednocześnie podmiotem kluczowym w rozumieniu ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, w dokumentacji ochrony infrastruktury krytycznej uwzględnia dokumentację dotyczącą bezpieczeństwa systemu informacyjnego, o której mowa w art. 10 tej ustawy.

Art. 6zg. 1. Operator infrastruktury krytycznej sporządza, w terminie do dnia 31 marca każdego roku, raport o stanie ochrony infrastruktury krytycznej za rok ubiegły.

2. Raport o stanie ochrony infrastruktury krytycznej zawiera w szczególności informacje dotyczące jej ochrony w zakresie zapewnienia:

1) bezpieczeństwa fizycznego;
2) bezpieczeństwa technicznego;
3) bezpieczeństwa osobowego;
4) cyberbezpieczeństwa;
5) bezpieczeństwa prawnego;
6) ciągłości działania i odtwarzania.

3. Raport o stanie ochrony infrastruktury krytycznej sporządza się z uwzględnieniem:

1) analizy zagrożeń dla infrastruktury krytycznej, o której mowa w art. 6ze ust. 1 pkt 1;
2) wdrożonych rozwiązań, o których mowa w art. 6ze ust. 1 pkt 2;
3) zagrożeń, które zakłóciły lub mogły zakłócić funkcjonowanie infrastruktury krytycznej, a nie były uwzględnione w analizie, o której mowa w art. 6ze ust. 1 pkt 1;
4) wyników przeprowadzonych kontroli i audytów odnoszących się do wdrożonych rozwiązań, o których mowa w art. 6ze ust. 1 pkt 2;
5) opisu działań podjętych przez operatora infrastruktury krytycznej w przypadkach wystąpienia zagrożeń.

4. Operator infrastruktury krytycznej przekazuje, w terminie do dnia 31 marca każdego roku, raport o stanie ochrony infrastruktury krytycznej odpowiednio:

1) ministrowi, o którym mowa w art. 6t ust. 1;
2) właściwemu miejscowo wojewodzie;
3) Komisji Nadzoru Finansowego.

5. Operator infrastruktury krytycznej przekazuje raport o stanie ochrony infrastruktury krytycznej na żądanie dyrektora Centrum, Szefa Agencji Bezpieczeństwa Wewnętrznego lub Szefa Agencji Wywiadu.

6. Do raportu o stanie ochrony infrastruktury krytycznej stosuje się przepisy ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych.

Art. 6zh. 1. W przypadku pracownika zatrudnionego na stanowisku umożliwiającym dostęp do informacji o bezpieczeństwie obiektu infrastruktury krytycznej i osoby ubiegającej się o zatrudnienie na tym stanowisku, operator infrastruktury krytycznej żąda od pracownika i tej osoby przedłożenia informacji

dotyczących karalności, w tym informacji, czy ich dane osobowe są zgromadzone w Krajowym Rejestrze Karnym.

2. Operator infrastruktury krytycznej żąda od pracownika danych biometrycznych w postaci odcisków linii papilarnych palców, głosu, obrazu rogówki, sieci żył palców lub biometrii twarzy, które są odpowiednie do wdrożonych środków kontroli dostępu niezbędnych dla ochrony szczególnie ważnych informacji o bezpieczeństwie infrastruktury krytycznej lub dostępu do stref, obiektów lub pomieszczeń wymagających szczególnej kontroli.

3. Operator infrastruktury krytycznej przetwarza informacje i dane, o których mowa w ust. 1 i 2, przez okres uzasadniony celem przetwarzania.

Art. 6zi. 1. W celu realizacji zadań, o których mowa w art. 6ze ust. 1, art. 6zf ust. 1 oraz art. 6zg ust. 1, operator infrastruktury krytycznej wyznacza koordynatora ochrony infrastruktury krytycznej oraz zastępcę koordynatora ochrony infrastruktury krytycznej.

2. Operator infrastruktury krytycznej wyznacza koordynatora ochrony infrastruktury krytycznej oraz zastępcę koordynatora ochrony infrastruktury krytycznej w terminie 30 dni od dnia otrzymania informacji o ujęciu w wykazie infrastruktury krytycznej.

3. Zastępca koordynatora infrastruktury krytycznej zastępuje koordynatora w czasie jego nieobecności lub czasowej niemożności wykonywania przez niego obowiązków.

4. Koordynatorem ochrony infrastruktury krytycznej może być osoba, która:

1) jest pracownikiem operatora infrastruktury krytycznej albo żołnierzem lub funkcjonariuszem pełniącym służbę w jednostce organizacyjnej będącej operatorem infrastruktury krytycznej;
2) korzysta z pełni praw publicznych;
3) posiada wiedzę, umiejętności i doświadczenie w zakresie zarządzania bezpieczeństwem, z uwzględnieniem przedmiotu działalności operatora infrastruktury krytycznej;
4) nie była skazana prawomocnym wyrokiem za umyślne przestępstwo lub umyślne przestępstwo skarbowe;
5) spełnia wymagania bezpieczeństwa osobowego w zakresie dostępu do informacji niejawnych o klauzuli ustalonej w trybie określonym w art. 6ze ust. 7.

5. Koordynator ochrony infrastruktury krytycznej podlega bezpośrednio organowi zarządzającemu operatora infrastruktury krytycznej.

6. O wyznaczeniu koordynatora operator infrastruktury krytycznej informuje odpowiednio:

1) ministra, o którym mowa w art. 6t ust. 1;
2) właściwego miejscowo wojewodę;
3) Komisję Nadzoru Finansowego;
4) dyrektora Centrum.

7. Operator infrastruktury krytycznej zapewnia koordynatorowi ochrony infrastruktury krytycznej organizacyjne i techniczne warunki realizacji zadań, w tym dostęp do niezbędnych dokumentów i informacji.

8. Przepisy ust. 4–7 stosuje się do zastępcy koordynatora ochrony infrastruktury krytycznej.

Art. 6zj. 1. Operator infrastruktury krytycznej informuje Prezesa Urzędu Komunikacji Elektronicznej oraz kierownika jednostki organizacyjnej podległej Ministrowi Obrony Narodowej właściwej w sprawach zarządzania częstotliwościami o możliwości zastosowania urządzeń uniemożliwiających telekomunikację na określonym obszarze. Informacja, o której mowa w zdaniu pierwszym, zawiera:

1) nazwę i rodzaj planowanych do zastosowania urządzeń uniemożliwiających telekomunikację na określonym obszarze;
2) parametry techniczne urządzeń uniemożliwiających telekomunikację na określonym obszarze, w tym zakresy częstotliwości pracy, moc promieniowaną w poszczególnych zakresach częstotliwości, rodzaje oraz charakterystyki anten wraz z wysokością ich zawieszenia oraz współrzędnymi miejsca ich zainstalowania, a także sektory planowanego oddziaływania urządzeń.

2. W celu zapewnienia ochrony infrastruktury krytycznej operator infrastruktury krytycznej w przypadkach, o których mowa:

1) w art. 156ze ust. 1 ustawy z dnia 3 lipca 2002 r. – Prawo lotnicze (Dz. U. z 2025 r. poz. 1431 i 1668 oraz z 2026 r. poz. 176) lub
2) w art. 28a ust. 1 ustawy z dnia 4 września 2008 r. o ochronie żeglugi i portów morskich (Dz. U. z 2024 r. poz. 597 oraz ……), lub
3) w art. 11 pkt 17 ustawy z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej (Dz. U. z 2026 r. poz. 244 i …)

– może podjąć decyzję o dopuszczalności zastosowania urządzeń, o których mowa w ust. 1, przez czas niezbędny do wykonywania czynności przez pracowników ochrony

specjalistycznych uzbrojonych formacji ochronnych, z uwzględnieniem konieczności minimalizacji skutków braku możliwości korzystania z usług telekomunikacyjnych.

3. O zastosowaniu urządzeń, o których mowa w ust. 1, operator infrastruktury krytycznej niezwłocznie informuje Prezesa Urzędu Komunikacji Elektronicznej oraz kierownika jednostki organizacyjnej podległej Ministrowi Obrony Narodowej właściwej w sprawach zarządzania częstotliwościami.

4. Jeżeli jest to niezbędne dla zapewnienia obronności i bezpieczeństwa państwa, Minister Obrony Narodowej może nakazać operatorowi infrastruktury krytycznej zaprzestanie stosowania urządzeń uniemożliwiających telekomunikację, o których mowa w ust. 1, lub zmianę sposobu ich wykorzystywania, o czym informuje dyrektora Centrum oraz właściwego komendanta wojewódzkiego Policji.

5. Minister Obrony Narodowej może powierzyć realizację zadania, o którym mowa w ust. 4, kierownikowi komórki organizacyjnej lub jednostki organizacyjnej podległej Ministrowi Obrony Narodowej lub przez niego nadzorowanej właściwej w sprawach zarządzania częstotliwościami.

Rozdział 8

Organy do spraw podmiotów krytycznych

Art. 6zk. 1. Organami do spraw podmiotów krytycznych są:

1) dla sektora energii:
   a) minister właściwy do spraw energii w podsektorach:
      – energii elektrycznej,
      – ciepła,
   b) minister właściwy do spraw gospodarki surowcami energetycznymi w podsektorach:
      – wydobywania kopalin,
      – ropy i paliw,
      – gazu,
      – energetyki jądrowej,
      – wodoru;
2) dla sektora transportu:
   a) minister właściwy do spraw transportu w podsektorach:
      – transport lotniczy,

– transport kolejowy,
– transport publiczny,
– transport drogowy,

b) minister właściwy do spraw gospodarki morskiej oraz minister właściwy do spraw żeglugi śródlądowej w podsektorze transportu wodnego;

3) dla sektora bankowości i infrastruktury rynków finansowych – Komisja Nadzoru Finansowego;

4) dla sektora ochrony zdrowia – minister właściwy do spraw zdrowia;

5) dla sektora zaopatrzenia w wodę pitną i jej dystrybucji oraz sektora zbiorowego odprowadzania ścieków – minister właściwy do spraw gospodarki wodnej;

6) dla sektora infrastruktury cyfrowej:
   a) minister właściwy do spraw informatyzacji – w podsektorze infrastruktury cyfrowej z wyłączeniem komunikacji elektronicznej,
   b) Prezes Urzędu Komunikacji Elektronicznej – w podsektorze komunikacji elektronicznej;

7) dla sektora administracji publicznej:
   a) minister właściwy do spraw administracji publicznej – w podsektorze podmiotów publicznych,
   b) minister właściwy do spraw finansów publicznych – w podsektorze finansów publicznych;

8) dla sektora przestrzeni kosmicznej – minister właściwy do spraw gospodarki;

9) dla sektora produkcji, przetwarzania i dystrybucji żywności – minister właściwy do spraw rolnictwa;

10) dla sektora zarządzania usługami ICT – minister właściwy do spraw informatyzacji;

11) dla sektora produkcji, wytwarzania i dystrybucji chemikaliów – minister właściwy do spraw gospodarki;

12) dla sektora usług pocztowych – Prezes Urzędu Komunikacji Elektronicznej;

13) dla sektora gospodarowania odpadami – minister właściwy do spraw klimatu.

2. Dla podmiotu publicznego, który jest wymieniony w innym sektorze niż sektor administracji publicznej, organem do spraw podmiotów krytycznych jest organ właściwy dla danego sektora.

Art. 6zl. Organ do spraw podmiotów krytycznych:

1) prowadzi bieżącą analizę operatorów infrastruktury krytycznej pod kątem uznania ich za podmiot krytyczny w danym sektorze lub podsektorze;
2) prowadzi bieżącą analizę podmiotów krytycznych w danym sektorze lub podsektorze pod kątem niespełniania warunków kwalifikujących dany podmiot jako podmiot krytyczny;
3) składa wnioski o dokonanie wpisu do wykazu podmiotów krytycznych oraz wykreślenia z tego wykazu;
4) prowadzi bieżącą wymianę informacji z podmiotami krytycznymi oraz ułatwia dobrowolną wymianę informacji między podmiotami krytycznymi w danym sektorze lub podsektorze;
5) współpracuje z podmiotami krytycznymi w danym sektorze lub podsektorze w zakresie obsługi incydentów;
6) monitoruje stosowanie przepisów ustawy przez podmioty krytyczne;
7) prowadzi kontrole podmiotów krytycznych;
8) prowadzi działania informacyjne dotyczące dobrych praktyk, działań edukacyjnych i kampanii na rzecz poszerzania wiedzy i budowania odporności podmiotów krytycznych;
9) uczestniczy w planowaniu i organizowaniu ćwiczeń podmiotów krytycznych oraz w razie potrzeby bierze w nich udział;
10) współpracuje z innymi organami do spraw podmiotów krytycznych oraz organami właściwymi do spraw cyberbezpieczeństwa, o których mowa w ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;
11) współpracuje, za pośrednictwem Pojedynczego Punktu Kontaktowego, z odpowiednimi organami państw członkowskich;
12) nakłada kary pieniężne na podmiot krytyczny.

Rozdział 9

Pojedynczy Punkt Kontaktowy

Art. 6zm. 1. Dyrektor Centrum prowadzi Pojedynczy Punkt Kontaktowy, do którego zadań należy:

1) odbieranie zgłoszeń incydentów istotnych z pojedynczych punktów kontaktowych w innych państwach członkowskich Unii Europejskiej;

2) przekazywanie zgłoszeń incydentów istotnych dotyczących innych państw członkowskich Unii Europejskiej do pojedynczych punktów kontaktowych tych państw;
3) opracowywanie i przekazywanie raz na dwa lata Komisji Europejskiej oraz Grupie do spraw Odporności Podmiotów Krytycznych sprawozdań dotyczących incydentów istotnych zgłaszanych przez podmioty krytyczne mających wpływ na ciągłość świadczonych przez nich usług kluczowych na terytorium Rzeczypospolitej Polskiej oraz ciągłość świadczonych usług kluczowych w państwach członkowskich Unii Europejskiej;
4) zapewnienie reprezentacji Rzeczypospolitej Polskiej w Grupie do spraw Odporności Podmiotów Krytycznych;
5) zapewnienie współpracy z Komisją Europejską w obszarze zapewnienia bezpieczeństwa świadczenia usług kluczowych;
6) koordynacja współpracy między organami do spraw podmiotów krytycznych i organami administracji publicznej w Rzeczypospolitej Polskiej z odpowiednimi organami w państwach członkowskich Unii Europejskiej;
7) zapewnienie wymiany informacji na potrzeby Grupy Współpracy, o której mowa w dyrektywie (UE) 2022/2555, oraz organów właściwych do spraw cyberbezpieczeństwa;
8) współpraca z pojedynczym punktem kontaktowym, o którym mowa w ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

2. Pojedynczy Punkt Kontaktowy przekazuje Grupie do spraw Odporności Podmiotów Krytycznych:

1) informacje na temat infrastruktury krytycznej zlokalizowanej na terytorium Rzeczypospolitej Polskiej służącej realizacji usług kluczowych w innych państwach członkowskich;
2) dobre praktyki związane ze zgłaszaniem i obsługą incydentów istotnych;
3) propozycje do programu prac Grupy do spraw Odporności Podmiotów Krytycznych;
4) dobre praktyki krajowe dotyczące podnoszenia świadomości, szkoleń, badań i rozwoju w obszarze zapewnienia ciągłości świadczenia usług kluczowych;
5) dobre praktyki w odniesieniu do identyfikowania podmiotów krytycznych, w tym w odniesieniu do występujących w dwóch lub większej liczbie państw członkowskich Unii Europejskiej zależności dotyczących ryzyka i incydentów.

3. Dane przekazywane Grupie do spraw Odporności Podmiotów Krytycznych nie obejmują informacji, które dotyczą bezpieczeństwa narodowego oraz porządku publicznego.

4. Pojedynczy Punkt Kontaktowy przekazuje organom do spraw podmiotów krytycznych oraz innym organom administracji publicznej zgodnie z ich właściwością informacje pochodzące z Grupy do spraw Odporności Podmiotów Krytycznych dotyczące:

1) analiz i ocen krajowych strategii państw członkowskich Unii Europejskiej w zakresie odporności podmiotów krytycznych, a także dobrych praktyk w obszarze zapewnienia świadczenia usług kluczowych;
2) wytycznych o charakterze strategicznym w obszarze zapewnienia świadczenia usług kluczowych;
3) dobrych praktyk w zakresie wymiany informacji związanych ze zgłaszaniem w Unii Europejskiej incydentów istotnych przez podmioty krytyczne;
4) dobrych praktyk w krajach członkowskich Unii Europejskiej dotyczących innowacji badań i rozwoju w zakresie budowania odporności podmiotów krytycznych;
5) dobrych praktyk w zakresie identyfikowania podmiotów krytycznych przez państwa członkowskie Unii Europejskiej, w tym w odniesieniu do transgranicznych i międzysektorowych zależności, dotyczących ryzyka i incydentów.

5. Pojedynczy Punkt Kontaktowy przekazuje Komisji Europejskiej:

1) niezwłocznie informacje o:
   a) wyznaczonych organach do spraw podmiotów krytycznych, Pojedynczym Punkcie Kontaktowym, ich zadaniach oraz późniejszych zmianach w tym zakresie,
   b) przepisach dotyczących kar pieniężnych;
2) raz na dwa lata informacje umożliwiające ocenę wdrażania dyrektywy 2022/2557, obejmujące w szczególności:
   a) środki umożliwiające identyfikację podmiotów krytycznych,
   b) wykaz usług kluczowych,
   c) liczbę zidentyfikowanych podmiotów krytycznych w każdym sektorze lub podsektorze, o którym mowa w załączniku do ustawy, oraz wskazanie ich znaczenia w odniesieniu do tego sektora lub podsektora,

d) progi istotności skutku zakłócającego dla świadczonej usługi kluczowej brane pod uwagę przy kwalifikowaniu podmiotów jako podmiotów krytycznych, przedstawiane wprost lub w formie zagregowanej;

3) informacje o środkach mających na celu zwiększenie odporności podmiotów krytycznych.

Art. 6zn. 1. Na potrzeby realizacji zadań, o których mowa w art. 6zl, organy do spraw podmiotów krytycznych, za pośrednictwem Pojedynczego Punktu Kontaktowego, prowadzą konsultacje z właściwymi organami państw członkowskich, w przypadku gdy podmioty krytyczne:

1) korzystają z infrastruktury krytycznej, która jest fizycznie połączona na terytorium co najmniej dwóch państw członkowskich;

2) są częścią struktur przedsiębiorstw połączonych lub powiązanych z podmiotami krytycznymi w innych państwach członkowskich;

3) zostały zidentyfikowane jako podmioty krytyczne w jednym państwie członkowskim i świadczą usługi kluczowe na rzecz innych państw członkowskich lub w innych państwach członkowskich.

2. W konsultacjach, o których mowa w ust. 1, organy do spraw podmiotów krytycznych wypracowują, w zależności od potrzeb, rozwiązania w zakresie zwiększania odporności lub redukcji obciążeń administracyjnych podmiotów krytycznych.

Rozdział 10

Identyfikowanie podmiotów krytycznych

Art. 6zo. 1. Dyrektor Centrum w celu zapewnienia:

1) identyfikacji podmiotów krytycznych,

2) prowadzenia czynności nadzorczych nad podmiotami krytycznymi

– prowadzi wykaz podmiotów krytycznych.

2. Wykaz podmiotów krytycznych zawiera:

1) nazwę (firmę) podmiotu krytycznego;

2) siedzibę i adres oraz adres do doręczeń elektronicznych;

3) numer identyfikacji podatkowej (NIP), jeżeli został nadany;

4) nazwę usługi kluczowej, zgodną z wykazem usług kluczowych;

5) wskazanie sektora, podsektora i kategorii podmiotu;

6) datę rozpoczęcia świadczenia usługi kluczowej;

7) informację, w których państwach członkowskich Unii Europejskiej podmiot został uznany za podmiot świadczący usługę kluczową;
8) datę zakończenia świadczenia usługi kluczowej;
9) datę wykreślenia z wykazu podmiotów krytycznych.

3. Wykaz podmiotów krytycznych prowadzony jest w systemie teleinformatycznym, o którym mowa w art. 46 ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

4. 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 z 2025 r. poz. 1844) oraz ustawy z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystaniu informacji sektora publicznego (Dz. U. z 2023 r. poz. 1524).

5. Dane, o których mowa w ust. 2, w zakresie niezbędnym do realizacji ich ustawowych zadań, organ właściwy do spraw podmiotów krytycznych udostępnia, na wniosek, następującym podmiotom:
1) Agencji Bezpieczeństwa Wewnętrznego;
2) Agencji Wywiadu;
3) Centralnemu Biuru Antykorupcyjnemu;
4) organom Krajowej Administracji Skarbowej;
5) Policji;
6) Pełnomocnikowi Rządu do Spraw Cyberbezpieczeństwa;
7) Prezesowi Urzędu Ochrony Danych Osobowych;
8) Prokuratorii Generalnej Rzeczypospolitej Polskiej;
9) prokuraturze;
10) sądom;
11) Służbie Kontrwywiadu Wojskowego;
12) Służbie Ochrony Państwa;
13) Służbie Wywiadu Wojskowego;
14) Straży Granicznej;
15) Żandarmerii Wojskowej;
16) wojewodom;
17) podmiotowi, w ramach którego funkcjonuje Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT) poziomu krajowego;

18) organom właściwym do spraw cyberbezpieczeństwa, o których mowa w art. 41 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

Art. 6zp. 1. Operator infrastruktury krytycznej zostaje wpisany do wykazu podmiotów krytycznych, w przypadku gdy:

1) świadczy co najmniej jedną usługę kluczową;
2) incydent miałby istotny skutek zakłócający dla świadczenia usługi kluczowej.

2. Istotność skutku zakłócającego incydentu dla świadczenia usługi kluczowej, o którym mowa w ust. 1 pkt 2, jest określana na podstawie progów istotności skutku zakłócającego określonych w przepisach wydanych na podstawie ust. 3.

3. Rada Ministrów określi, w drodze rozporządzenia, wykaz usług kluczowych w podziale na sektory, podsektory i kategorie podmiotów wymienionych w załączniku do ustawy oraz progi istotności skutku zakłócającego dla świadczenia usług kluczowych, wymienionych w wykazie usług kluczowych, w zależności od:

1) liczby użytkowników zależnych od usługi kluczowej świadczonej przez dany podmiot;
2) stopnia, w jakim inne sektory lub podsektory, o których mowa w załączniku do ustawy, są zależne od usługi świadczonej przez ten podmiot;
3) wpływu, jaki incydent – jeżeli chodzi o jego skalę i czas trwania – mógłby mieć na działalność gospodarczą i społeczną, środowisko, bezpieczeństwo publiczne lub na zdrowie ludności;
4) udziału podmiotu krytycznego w rynku w odniesieniu do świadczonej usługi kluczowej;
5) obszaru geograficznego, którego mógłby dotyczyć incydent, biorąc pod uwagę wpływ transgraniczny oraz stopień odizolowania geograficznego;
6) znaczenia podmiotu w utrzymywaniu wystarczającego poziomu świadczenia usługi kluczowej przy uwzględnieniu dostępności alternatywnych sposobów jej świadczenia;
7) innych czynników charakterystycznych dla danego sektora lub podsektora, jeżeli występują.

Wydając rozporządzenie, należy określić co najmniej jeden próg istotności skutku zakłócającego dla świadczenia danej usługi kluczowej, uwzględniając znaczenie danej usługi dla utrzymania niezbędnych funkcji społecznych, niezbędnej działalności

gospodarczej, zdrowia i bezpieczeństwa publicznego lub środowiska naturalnego oraz obniżenia jakości świadczonej usługi kluczowej.

Art. 6zq. 1. W celu podjęcia decyzji o dokonaniu wpisu do wykazu podmiotów krytycznych organ do spraw podmiotów krytycznych występuje do operatora infrastruktury krytycznej o udzielenie informacji, które umożliwią wstępną ocenę, czy spełnia warunki do uznania za podmiot krytyczny, w szczególności w zakresie spełniania warunków, o których mowa w art. 6zp ust. 1, oraz wskazania infrastruktury krytycznej niezbędnej do świadczenia usługi kluczowej.

2. Organ do spraw podmiotów krytycznych w wystąpieniu, o którym mowa w ust. 1:

1) przekazuje operatorowi infrastruktury krytycznej dokumenty w zakresie niezbędnym do udzielenia informacji;
2) wskazuje termin udzielenia informacji, nie krótszy niż 14 dni, licząc od dnia otrzymania wystąpienia przez operatora infrastruktury krytycznej.

3. Operator infrastruktury krytycznej przekazuje organowi do spraw podmiotów krytycznych informacje żądane w wystąpieniu, wskazując jednocześnie infrastrukturę krytyczną niezbędną do świadczenia usługi kluczowej, w tym:

1) infrastrukturę krytyczną innego operatora;
2) obiekt, urządzenie, instalację, sieć, system oraz usługę lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje, sieci, systemy oraz usługi, którego właściciel lub posiadacz nie jest operatorem infrastruktury krytycznej.

Art. 6zr. 1. Organ do spraw podmiotów krytycznych składa wniosek o wpis do wykazu podmiotów krytycznych zawierający dane, o których mowa w art. 6zo ust. 2 pkt 1–7.

2. Wpis operatora infrastruktury krytycznej do wykazu podmiotów krytycznych dokonuje się automatycznie z chwilą złożenia wniosku w systemie teleinformatycznym, o którym mowa w art. 46 ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

3. Organ do spraw podmiotów krytycznych niezwłocznie, nie później jednak niż w ciągu miesiąca, informuje operatora infrastruktury krytycznej o dokonaniu wpisu do wykazu podmiotów krytycznych oraz obowiązkach z tym związanych.

4. Informację, o której mowa w ust. 3, organ do spraw podmiotów krytycznych niezwłocznie przekazuje:

1) dyrektorowi Centrum;

2) odpowiedniemu organowi właściwemu do spraw cyberbezpieczeństwa.

5. Dyrektor Centrum może weryfikować dane zawarte we wpisie do wykazu podmiotów krytycznych ze stanem faktycznym.

6. Dyrektor Centrum poprawia, z urzędu, oczywiste omyłki i błędy pisarskie zawarte we wpisie do wykazu podmiotów krytycznych.

Art. 6zs. 1. Podmiot krytyczny w przypadku zakończenia świadczenia usługi kluczowej niezwłocznie informuje właściwy organ do spraw podmiotów krytycznych o tym fakcie.

2. W przypadku zakończenia świadczenia usługi kluczowej przez podmiot krytyczny, organ do spraw podmiotów krytycznych składa wniosek o wykreślenie podmiotu krytycznego z wykazu podmiotów krytycznych, zawierający dane, o których mowa w art. 6zo ust. 2 pkt 1–8.

3. Wykreślenie podmiotu krytycznego z wykazu dokonuje się automatycznie z chwilą złożenia wniosku w systemie teleinformatycznym, o którym mowa w art. 46 ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

4. Organ do spraw podmiotów krytycznych niezwłocznie, nie później jednak niż w ciągu miesiąca, informuje podmiot krytyczny o wykreśleniu z wykazu podmiotów krytycznych i dacie wykreślenia.

5. Informację, o której mowa w ust. 4, organ do spraw podmiotów krytycznych przekazuje niezwłocznie:

1) dyrektorowi Centrum;

2) odpowiedniemu organowi właściwemu do spraw cyberbezpieczeństwa.

6. Dyrektor Centrum może weryfikować dane zawarte we wniosku o wykreślenie podmiotu krytycznego z wykazu podmiotów krytycznych ze stanem faktycznym.

7. Dyrektor Centrum poprawia, z urzędu, oczywiste omyłki i błędy pisarskie zawarte we wniosku o wykreślenie podmiotu krytycznego z wykazu.

Rozdział 11

Obowiązki podmiotów krytycznych

Art. 6zt. 1. Podmiot krytyczny wdraża zintegrowany system zarządzania bezpieczeństwem świadczenia usługi kluczowej obejmujący:

1) przeprowadzenie nie rzadziej niż raz na 2 lata oceny ryzyka z uwzględnieniem:

a) zagrożeń i związanych z tym ryzyk wymienionych w KOR oraz innych zagrożeń charakterystycznych dla świadczonej usługi kluczowej, w tym zagrożeń antagonistycznych,

b) stopnia zależności innych sektorów lub podsektorów określonych w załączniku do ustawy od usługi kluczowej świadczonej przez podmiot krytyczny oraz stopnia zależności tego podmiotu krytycznego od usług kluczowych świadczonych przez inne podmioty w innych sektorach, w tym w stosownych przypadkach w sąsiadujących państwach członkowskich Unii Europejskiej i w państwach trzecich,

c) identyfikacji alternatywnych łańcuchów dostaw w celu przywrócenia świadczenia usługi kluczowej,

d) ocen ryzyka prowadzonych na podstawie odrębnych przepisów;

2) wdrożenie odpowiednich i proporcjonalnych do wyników oceny ryzyka rozwiązań organizacyjno-technicznych, w szczególności:

a) polityk zarządzania ryzykiem,

b) bezpieczeństwa fizycznego, w tym ochrony fizycznej budynków i terenów należących do podmiotu krytycznego oraz zabezpieczeń technicznych, uwzględniających kontrolę dostępu,

c) ochrony infrastruktury krytycznej niezbędnej do świadczenia usługi kluczowej, zgodnie z wymogami ochrony infrastruktury krytycznej, o których mowa w przepisach rozdziału 7 ustawy,

d) bezpieczeństwa osobowego dotyczącego pracowników i dostawców zewnętrznych,

e) cyberbezpieczeństwa, zgodnie z wymogami dotyczącymi podmiotów kluczowych, o których mowa w przepisach ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa,

f) bezpieczeństwa prawnego świadczenia usługi kluczowej,

g) ciągłości działania i odtwarzania, w tym utrzymywania własnych systemów rezerwowych zapewniających bezpieczeństwo i podtrzymujących funkcjonowanie świadczenia usługi kluczowej do czasu jej pełnego odtworzenia,

h) zdolności do ochrony informacji niejawnych w niezbędnym zakresie do zapewnienia świadczenia usługi kluczowej,

i) szkoleń i ćwiczeń personelu w celu jego przygotowania na różnego rodzaju zagrożenia i incydenty,

j) realizacji okresowych audytów i certyfikacji;

3) bieżącą współpracę z właściwymi organami zarządzania kryzysowego oraz służbami, strażami i inspekcjami dotyczącą wymiany informacji o zagrożeniach i incydentach zakłócających lub mogących zakłócić funkcjonowanie usługi kluczowej oraz sposobu postępowania w przypadku takiego zdarzenia;

4) gromadzenie informacji o zagrożeniach i incydentach zakłócających lub mogących zakłócić świadczenie usługi kluczowej;

5) zarządzanie incydentami;

6) stosowanie środków zapobiegających i ograniczających wpływ incydentów na świadczenie usługi kluczowej.

2. Rozwiązania organizacyjno-techniczne, o których mowa w ust. 1 pkt 2, uwzględniają wymagania określone w normach oraz wytycznych do ich stosowania, wskazanych w przepisach wydanych na podstawie ust. 5.

3. Podmiot krytyczny przeprowadza po raz pierwszy ocenę ryzyka, o której mowa w ust. 1 pkt 1, w terminie 9 miesięcy od otrzymania informacji o ujęciu w wykazie podmiotów krytycznych.

4. Podmiot krytyczny wdraża rozwiązania organizacyjno-techniczne, o których mowa w ust. 1 pkt 2, w terminie 3 miesięcy od dnia przeprowadzenia po raz pierwszy oceny ryzyka, a następnie stosownie do potrzeb, w zależności od wyników przeprowadzonej oceny ryzyka.

5. Rada Ministrów określi, w drodze rozporządzenia, wykaz norm oraz wytycznych do ich stosowania, które podmiot krytyczny uwzględnia przy wdrażaniu rozwiązań organizacyjno-technicznych, w zakresie:

1) zarządzania bezpieczeństwem informacji;

2) zarządzania ciągłością działania usługi kluczowej;

3) zapewnienia bezpieczeństwa fizycznego, w tym ochrony fizycznej infrastruktury służącej do świadczenia usługi kluczowej oraz zabezpieczeń technicznych, uwzględniających kontrolę dostępu

– mając na względzie zapewnienie właściwego poziomu bezpieczeństwa świadczenia usług kluczowych.

6. Organ do spraw podmiotów krytycznych może opracować, odrębnie dla nadzorowanego sektora lub podsektora, i udostępnić 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, które podmiot krytyczny uwzględnia przy wdrażaniu rozwiązań organizacyjno-technicznych wskazanych w ust. 1 pkt 2.

7. W celu wdrożenia rozwiązań organizacyjno-technicznych, o których mowa w ust. 1 pkt 2, podmiot krytyczny uwzględnia specyfikacje techniczne określone w aktach wykonawczych Komisji Europejskiej, wydanych na podstawie art. 13 ust. 6 dyrektywy 2022/2557.

8. Podmiot krytyczny, przy opracowywaniu i zawieraniu umów zapewniających wdrożenie rozwiązań, o których mowa w ust. 1 pkt 2, żąda od usługodawców:

1) certyfikatów, uwzględniając dokumenty równoważne, zgodnie z zasadami wzajemnego uznawania w Unii Europejskiej lub w przypadku ich braku innych dokumentów właściwych dla poszczególnych rozwiązań, potwierdzających posiadanie odpowiednich kompetencji i uprawnień niezbędnych do ich realizacji;
2) potwierdzenia zdolności do ochrony informacji niejawnych oraz stosowania przepisów o ochronie informacji niejawnych, jeżeli opracowanie, przygotowanie i wykonanie umowy wiążą się dostępem do informacji niejawnych.

9. Organ do spraw podmiotów krytycznych, po zasięgnięciu opinii właściwych sektorowych rad do spraw kompetencji, o których mowa w art. 4c ust. 1 pkt 2 ustawy z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości, może opracować i udostępnić na stronie podmiotowej Biuletynu Informacji Publicznej zestawienie certyfikatów lub innych dokumentów właściwych dla realizacji rozwiązań wskazanych w ust. 1 pkt 2.

10. Organ do spraw podmiotów krytycznych we współpracy z dyrektorem Centrum ustala klauzulę tajności oraz szczegółowe wymagania dotyczące ochrony informacji niejawnych związanych z realizacją przez podmiot krytyczny przedsięwzięć związanych z zapewnieniem bezpieczeństwa świadczenia usługi kluczowej.

11. W przypadku gdy podmiot krytyczny prowadzi ocenę ryzyka oraz opracowuje dokumentację dotyczącą oceny ryzyka na podstawie odrębnych przepisów, odpowiadającą przepisom rozdziału 11 ustawy, uznaje się wymóg prowadzenia oceny ryzyka za spełniony w całości lub w części.

Art. 6zu. 1. Podmiot krytyczny opracowuje, stosuje i aktualizuje dokumentację zintegrowanego systemu zarządzania bezpieczeństwem świadczenia usługi kluczowej.

2. Dokumentację zintegrowanego systemu zarządzania bezpieczeństwem świadczenia usługi kluczowej stanowią:

1) dokumentacja systemu zarządzania bezpieczeństwem informacji;
2) dokumentacja systemu zarządzania ciągłością działania usługi kluczowej;
3) dokumentacja ochrony fizycznej oraz zabezpieczeń technicznych, o których mowa w art. 6zt ust. 1 pkt 2 lit. b oraz bezpieczeństwa osobowego, o którym mowa w art. 6zt ust. 1 pkt 2 lit. d;
4) dokumentacja ochrony infrastruktury krytycznej, o której mowa w art. 6zf ust. 1;
5) dokumentacja cyberbezpieczeństwa, opracowywana zgodnie z wymogami dla podmiotów kluczowych, o których mowa w przepisach ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;
6) inna dokumentacja niż wskazana w pkt 1–5, biorąc pod uwagę rodzaj świadczonej usługi kluczowej.

3. Dokumentacja może być prowadzona w postaci papierowej lub w postaci elektronicznej.

4. Podmiot krytyczny po raz pierwszy sporządza dokumentację w terminie 15 miesięcy od otrzymania informacji o ujęciu w wykazie podmiotów krytycznych, a następnie stosownie do potrzeb dokonuje jej aktualizacji.

5. Podmiot krytyczny jest obowiązany do ustanowienia nadzoru nad dokumentacją 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.

6. Podmiot krytyczny przechowuje dokumentację przez co najmniej 2 lata, licząc od 1 stycznia roku następującego po roku jej wycofania z użytkowania lub zakończenia świadczenia usługi. 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).

Art. 6zv. 1. Podmiot krytyczny jest obowiązany do zarządzania incydentem, w tym:

1) zapewnienia obsługi incydentu;

2) zapewnienia dostępu do informacji o zarejestrowanym incydencie organowi do spraw podmiotów krytycznych oraz dyrektorowi Centrum;
3) klasyfikowania incydentu jako istotnego, na podstawie progów uznawania incydentu za istotny, określonych w przepisach wykonawczych wydanych na podstawie ust. 4;
4) zgłaszania incydentu istotnego niezwłocznie, nie później niż w terminie 24 godzin od momentu jego wystąpienia lub wykrycia:
   a) właściwemu organowi do spraw podmiotów krytycznych oraz dyrektorowi Centrum,
   b) Szefowi Agencji Bezpieczeństwa Wewnętrznego,
   c) podmiotowi, w ramach którego funkcjonuje Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT) poziomu krajowego;
5) współdziałania podczas obsługi incydentu istotnego z właściwym organem do spraw podmiotów krytycznych lub dyrektorem Centrum;
6) informowania właściwego organu do spraw podmiotów krytycznych oraz dyrektora Centrum o usunięciu incydentu istotnego;
7) w szczególnie uzasadnionych przypadkach przekazywania sprawozdania z czynności, o których mowa w pkt 1–6, organowi do spraw podmiotów krytycznych oraz dyrektorowi Centrum w terminie nie dłuższym miesiąc, licząc od dnia wystąpienia incydentu istotnego.

2. Zgłoszenie, o którym mowa w ust. 1 pkt 4, dokonuje się za pomocą systemu, o którym mowa w art. 46 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

3. W przypadku braku możliwości dokonania zgłoszenia w systemie, o którym mowa w art. 46 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, zgłoszenie przekazywane jest na piśmie utrwalonym w postaci elektronicznej, opatrzonym kwalifikowanym podpisem elektronicznym, podpisem osobistym, podpisem zaufanym albo kwalifikowaną pieczęcią elektroniczną.

4. Rada Ministrów określi, w drodze rozporządzenia, progi uznania incydentu za incydent istotny według zdarzenia w poszczególnych sektorach i podsektorach określonych w załączniku do ustawy, w zależności od:
1) liczby użytkowników dotkniętych zakłóceniem,
2) czasu trwania zakłócenia usługi kluczowej,

3) obszaru geograficznego, którego dotyczy zakłócenie z uwzględnieniem jego odizolowania geograficznego,
4) innych czynników charakterystycznych dla danego sektora lub podsektora, jeżeli występują.

Wydając rozporządzenie, należy określić co najmniej jeden próg uznania incydentu za incydent istotny dla każdego zdarzenia, kierując się potrzebą zapewnienia ochrony przed zagrożeniami życia lub zdrowia ludzi, znacznymi stratami majątkowymi oraz zagrożeniem obniżenia jakości świadczonej usługi kluczowej.

Art. 6zw. 1. Zgłoszenie, o którym mowa w art. 6zv ust. 1 pkt 4, zawiera:

1) dane podmiotu zgłaszającego, w tym firmę przedsiębiorcy, numer we właściwym rejestrze, siedzibę i adres;
2) imię i nazwisko, numer telefonu oraz adres poczty elektronicznej osoby dokonującej zgłoszenia;
3) imię i nazwisko, numer telefonu oraz adres poczty elektronicznej osoby uprawnionej do składania wyjaśnień dotyczących zgłaszanych informacji;
4) opis wpływu incydentu istotnego na świadczenie usługi kluczowej, w tym:
   a) usługi kluczowej zgłaszającego, na którą incydent miał wpływ,
   b) liczbę użytkowników usługi kluczowej, na których incydent miał wpływ,
   c) moment wystąpienia i wykrycia incydentu istotnego oraz czas jego trwania,
   d) obszar geograficzny, którego dotyczy incydent istotny,
   e) wpływ incydentu istotnego na świadczenie usług kluczowych przez inne podmioty krytyczne,
   f) przyczynę zaistnienia incydentu istotnego i sposób jego przebiegu oraz skutki jego oddziaływania na świadczoną usługę kluczową;
5) informacje umożliwiające właściwemu organowi do spraw podmiotów krytycznych oraz dyrektorowi Centrum określenie, czy incydent istotny dotyczy innych państw członkowskich Unii Europejskiej;
6) informacje o podjętych działaniach zapobiegawczych;
7) informacje o podjętych działaniach naprawczych;
8) inne istotne informacje.

2. Podmiot krytyczny przekazuje informacje znane mu w chwili dokonywania zgłoszenia, które uzupełnia w trakcie obsługi incydentu istotnego.

3. Organ do spraw podmiotów krytycznych oraz dyrektor Centrum mogą zwrócić się do podmiotu krytycznego o uzupełnienie zgłoszenia o informacje w zakresie niezbędnym do realizacji zadań, o których mowa w ustawie.

4. Organ do spraw podmiotów krytycznych, za pośrednictwem Pojedynczego Punktu Kontaktowego, informuje Komisję Europejską o incydencie istotnym, który ma lub może mieć wpływ na ciągłość świadczenia usługi kluczowej na rzecz co najmniej sześciu państw członkowskich Unii Europejskiej lub w co najmniej sześciu państwach członkowskich Unii Europejskiej.

5. Organ do spraw podmiotów krytycznych informuje opinię publiczną o incydencie istotnym, jeżeli uzna, że leży to w interesie publicznym.

Art. 6zx.1. Podmiot krytyczny może przekazywać właściwym organom do spraw podmiotów krytycznych oraz dyrektorowi Centrum informacje dotyczące:

1) incydentów innych niż istotne;
2) zagrożeń dla niezakłóconego świadczenia usługi kluczowej.

2. Informacje, o których mowa w ust. 1, są przekazywane na piśmie utrwalonym w postaci elektronicznej, opatrzonym kwalifikowanym podpisem elektronicznym, podpisem osobistym, podpisem zaufanym albo kwalifikowaną pieczęcią elektroniczną, a w przypadku braku możliwości przekazania w postaci elektronicznej, przy użyciu innych dostępnych środków komunikacji.

Art. 6zy. Podmiot krytyczny informuje użytkowników świadczonej usługi kluczowej o zagrożeniach dla niezakłóconego świadczenia tej usługi i stosowaniu skutecznych sposobów zabezpieczania się przed tymi zagrożeniami, w szczególności przez udostępnianie informacji na ten temat na swojej stronie internetowej.

Art. 6zz. 1. Podmiot krytyczny przeprowadza co najmniej raz na 3 lata, na własny koszt, audyt zintegrowanego systemu zarządzania bezpieczeństwem świadczenia usługi kluczowej, zwanego dalej „audytem”, w zakresie:

1) zarządzania bezpieczeństwem informacji;
2) zarządzania ciągłością działania usługi kluczowej;
3) zapewnienia bezpieczeństwa fizycznego, w tym ochrony fizycznej budynków i terenów należących do podmiotu krytycznego oraz zabezpieczeń technicznych, uwzględniających kontrolę dostępu.

2. Podmiot krytyczny przedstawia w postaci elektronicznej kopię raportu z przeprowadzonego audytu organowi do spraw podmiotów krytycznych, w terminie trzech dni roboczych od dnia jego otrzymania przez podmiot krytyczny.

3. W przypadku wystąpienia incydentu istotnego, organ do spraw podmiotów krytycznych może nakazać podmiotowi krytycznemu, w drodze decyzji, przeprowadzenie zewnętrznego audytu, wraz z określeniem terminu przekazania kopii raportu z przeprowadzonego audytu i wskazaniem kategorii podmiotów do przeprowadzenia audytu. Organ do spraw podmiotów krytycznych może również określić zakres audytu. Decyzja nakazująca przeprowadzenie zewnętrznego audytu podlega natychmiastowemu wykonaniu.

Art. 6zza. 1. Audyt może być prowadzony przez:

1) jednostkę certyfikującą właściwą w zakresie, o którym mowa w art. 6zz ust. 1;
2) co najmniej dwóch audytorów, w tym jednego z ukończonym szkoleniem audytora wiodącego, posiadających certyfikaty określone w przepisach wykonawczych wydanych na podstawie ust. 10

– spełniających wymagania bezpieczeństwa osobowego i przemysłowego w zakresie dostępu do informacji niejawnych o klauzuli „poufne”.

2. Wymogu posiadania dostępu do informacji niejawnych o klauzuli „poufne” nie stosuje się do audytorów, o których mowa w art. 6zza ust. 1 pkt 2, w przypadku gdy są oni pracownikami podmiotu krytycznego.

3. Jednostka certyfikująca lub audytorzy są obowiązani do zachowania w tajemnicy informacji uzyskanych w związku z przeprowadzanym audytem, z zachowaniem przepisów o ochronie informacji niejawnych i innych informacji prawnie chronionych.

4. Audyt nie może być przeprowadzony przez osobę realizującą w podmiocie audytowanym zadania, o których mowa w art. 6zt ust. 1, w art. 6zu ust. 1 oraz w art. 6zv ust. 1, lub która realizowała te zadania w podmiocie audytowanym nie później niż w terminie 1 roku przed rozpoczęciem audytu.

5. Na podstawie zebranych dokumentów i dowodów jednostka certyfikująca lub audytorzy sporządzają raport z przeprowadzonego audytu i przekazuje je podmiotowi krytycznemu wraz z dokumentacją z przeprowadzonego audytu.

6. Obowiązek przeprowadzenia audytu uznaje się za spełniony w przypadku posiadania przez podmiot krytyczny certyfikatów w zakresie, o którym mowa w art. 6zz ust. 1.

7. Podmiot krytyczny przedstawia kopię raportu z przeprowadzonego audytu lub certyfikatu, o którym mowa w ust. 6, właściwemu organowi do spraw podmiotów krytycznych w terminie 7 dni roboczych od dnia jego otrzymania lub dyrektorowi Centrum na jego uzasadniony wniosek.

8. Kopię raportu z przeprowadzonego audytu lub certyfikatu, o którym mowa w ust. 6, przekazuje się za pomocą systemu, o którym mowa w art. 46 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

9. W przypadku braku możliwości przekazania kopii audytu lub certyfikatu, o którym mowa w ust. 7, za pomocą systemu, o którym mowa w art. 46 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, przekazanie następuje na piśmie utrwalonym w postaci elektronicznej, opatrzonym kwalifikowanym podpisem elektronicznym, podpisem osobistym, podpisem zaufanym albo kwalifikowaną pieczęcią elektroniczną.

10. Rada Ministrów określi, w drodze rozporządzenia, wymogi dla osób lub podmiotów przeprowadzających audyt, w tym zakres wymaganej wiedzy specjalistycznej oraz wymagane doświadczenie w dziedzinie objętej audytem, mając na względzie zapewnienie skutecznego i rzetelnego przeprowadzania audytu w zakresach określonych w ust. 1 pkt 1–3.

Art. 6zzb. 1. Podmiot krytyczny zapewnia udział struktur organizacyjnych lub pracowników niezbędnych do zapewnienia niezakłóconego świadczenia usługi kluczowej w szkoleniach lub ćwiczeniach:

1) obronnych;
2) obrony cywilnej;
3) ochrony ludności;
4) z zakresu przeciwdziałania zagrożeniom o charakterze terrorystycznym;
5) zarządzania kryzysowego.

2. Szkolenia, o których mowa w ust. 1, polegają na nabywaniu lub aktualizacji wiedzy i umiejętności niezbędnych do realizacji przedsięwzięć w zakresie, o którym mowa w ust. 1.

3. Ćwiczenia, o których mowa w ust. 1, polegają na nabywaniu przez ćwiczących umiejętności praktycznej realizacji zadań w zakresie, o którym mowa w ust. 1.

4. Podmiot krytyczny we współpracy z właściwym organem do spraw podmiotów krytycznych lub dyrektorem Centrum planuje i organizuje udział w szkoleniach i ćwiczeniach, o których mowa w ust. 1.

Art. 6zzc. 1. Podmiot krytyczny, w celu zapewnienia ochrony ciągłości świadczenia usługi kluczowej, może prowadzić sprawdzenie przeszłości w odniesieniu do:

1) pracownika podmiotu krytycznego lub kandydata na pracownika:
   a) pełniącego newralgiczną rolę bezpośrednio w strukturze organizacyjnej podmiotu krytycznego lub działając na jego rzecz, w tym:
      – reprezentującego podmiot krytyczny samodzielnie lub łącznie z innymi osobami na podstawie statutu, umowy lub innego aktu założycielskiego,
      – pełniącego funkcje kierownicze lub koordynacyjne,
   b) posiadającego bezpośredni lub zdalny dostęp do budynków i terenów podmiotu krytycznego, obiegu informacji lub systemów kontroli, w szczególności związanych z bezpieczeństwem podmiotu krytycznego,
   c) realizującego audyt, o którym mowa w art. 6zz ust. 1;
2) osoby świadczącej usługę na rzecz podmiotu krytycznego, niebędącej pracownikiem podmiotu krytycznego, posiadającej bezpośredni lub zdalny dostęp do budynków i terenów podmiotu krytycznego, obiegu informacji lub systemów kontroli, w szczególności związanych z bezpieczeństwem podmiotu krytycznego.

2. Sprawdzenie przeszłości osób, o których mowa w ust. 1, obejmuje:

1) potwierdzenie tożsamości;
2) ocenę informacji pozyskanych z rejestrów karnych pod kątem przestępstw, które mogą mieć znaczenie dla zajmowanego stanowiska, ubiegania się o to stanowisko lub świadczenia usług na rzecz podmiotu krytycznego.

3. Podmiot krytyczny, w odniesieniu do osoby, o której mowa w ust. 1 pkt 1, w celu:

1) potwierdzenia tożsamości:
   a) żąda przedłożenia ważnego dowodu osobistego lub ważnego dokumentu paszportowego tej osoby oraz podania nazwiska rodowego i poprzednio noszonego nazwiska, jeżeli było zmieniane, oraz nazwisk, imion, dat i miejsc urodzenia rodziców,
   b) wnioskuje do organu dowolnej gminy o udostępnienie danych jednostkowych zawartych w rejestrze PESEL oraz o udostępnienie danych w trybie jednostkowym z Rejestru Dowodów Osobistych;

2) dokonania oceny informacji pozyskanych z rejestrów karnych:
   a) pozyskuje informację z Krajowego Rejestru Karnego w zakresie skazań za przestępstwa umyślne ścigane z oskarżenia publicznego oraz umyślne przestępstwa skarbowe,
   b) występuje do Biura Informacyjnego Krajowego Rejestru Karnego z wnioskiem o wystąpienie do organów centralnych państw członkowskich Unii Europejskiej państwa obywatelstwa osoby podlegającej sprawdzeniu przeszłości z zapytaniem o udzielenie informacji o osobie, w przypadku gdy osoba podlegająca sprawdzeniu ma obywatelstwo państwa członkowskiego innego niż Rzeczpospolita Polska.

4. Podmiot krytyczny, w odniesieniu do osoby, o której mowa w ust. 1 pkt 2, ma prawo żądać:

1) przedłożenia przez tę osobę ważnego dowodu osobistego lub ważnego dokumentu paszportowego tej osoby oraz podania nazwiska rodowego i poprzednio noszonego nazwiska, jeżeli było zmieniane, oraz nazwisk, imion, dat i miejsc urodzenia rodziców;
2) przedłożenia przez tę osobę informacji z Krajowego Rejestru Karnego w zakresie skazań za przestępstwa umyślne ścigane z oskarżenia publicznego oraz umyślne przestępstwa skarbowe.

5. Podmiot krytyczny uwzględnia negatywny wynik sprawdzenia przeszłości w zakresie powierzania zadań osobom, o których mowa w ust. 1, w szczególności w przypadku skazania prawomocnym wyrokiem na karę pozbawienia wolności za przestępstwo umyślne ścigane z oskarżenia publicznego, także popełnione za granicą, lub umyślne przestępstwo skarbowe, jeżeli czyn, za który nastąpiło skazanie wywołuje uzasadnione wątpliwości w zakresie powierzenia realizacji tych zadań.

6. Sprawdzenie przeszłości przeprowadza się co najmniej raz na trzy lata.

7. Podmiot krytyczny przetwarza dane osobowe w zakresie realizacji czynności, o których mowa w ust. 1, w zakresie i w celu niezbędnym do ich realizacji.

8. Sprawdzenia przeszłości nie prowadzi się w odniesieniu do osoby wskazanej w ust. 1 pkt 1, która samodzielnie przedłożyła wymagane dokumenty albo posiada co najmniej poświadczenie bezpieczeństwa o klauzuli „poufne”.

Art. 6zzd. 1. W celu realizacji zadań, o których mowa w art. 6zt ust. 1, w art. 6zu ust. 1, w art. 6zv ust. 1, w art. 6zzb ust. 1 oraz w art. 6zzc ust. 1, podmiot krytyczny

wyznacza pełnomocnika bezpieczeństwa usługi kluczowej oraz zastępcę pełnomocnika bezpieczeństwa usługi kluczowej.

2. Podmiot krytyczny wyznacza pełnomocnika bezpieczeństwa usługi kluczowej oraz zastępcę pełnomocnika bezpieczeństwa usługi kluczowej w terminie 30 dni od dnia otrzymania informacji o ujęciu w wykazie podmiotów krytycznych.

3. Zastępca pełnomocnika bezpieczeństwa usługi kluczowej zastępuje pełnomocnika w czasie jego nieobecności lub czasowej niemożności wykonywania przez niego obowiązków.

4. Pełnomocnikiem bezpieczeństwa usługi kluczowej może być osoba, która:

1) jest pracownikiem podmiotu krytycznego albo żołnierzem lub funkcjonariuszem pełniącym służbę w jednostce organizacyjnej będącej podmiotem krytycznym;
2) korzysta z pełni praw publicznych;
3) posiada wiedzę, umiejętności i doświadczenie w zakresie zarządzania bezpieczeństwem, z uwzględnieniem przedmiotu działalności podmiotu świadczące usługę kluczową;
4) nie była skazana prawomocnym wyrokiem za umyślne przestępstwo lub umyślne przestępstwo skarbowe;
5) spełnia wymagania bezpieczeństwa osobowego w zakresie dostępu do informacji niejawnych o klauzuli „poufne”.

5. Pełnomocnik bezpieczeństwa usługi kluczowej podlega bezpośrednio organowi zarządzającemu podmiotu krytycznego.

6. O wyznaczeniu pełnomocnika bezpieczeństwa usługi kluczowej podmiot krytyczny informuje niezwłocznie właściwy organ do spraw podmiotów krytycznych oraz dyrektora Centrum, przekazując dane tej osoby obejmujące imię i nazwisko, numer telefonu oraz adres poczty elektronicznej.

7. Podmiot krytyczny zapewnia pełnomocnikowi bezpieczeństwa usługi kluczowej organizacyjne i techniczne warunki realizacji zadań, w tym dostęp do niezbędnych dokumentów i informacji.

8. Przepisy, o których mowa w ust. 4–7, stosuje się do zastępcy pełnomocnika bezpieczeństwa usługi kluczowej.

Art. 6zze. Podmioty krytyczne sektora bankowości i infrastruktury rynków finansowych przeprowadzają po raz pierwszy ocenę ryzyka, o której mowa w art. 6zt ust.

1 pkt 1, w terminie 10 miesięcy od otrzymania informacji o ujęciu w wykazie podmiotów krytycznych.

Rozdział 12

Podmiot krytyczny o szczególnym znaczeniu europejskim i misje doradcze

Art. 6zzf. 1. Podmiot krytyczny informuje właściwy organ do spraw podmiotów krytycznych oraz Pojedynczy Punkt Kontaktowy o fakcie świadczenia co najmniej jednej usługi kluczowej spośród usług kluczowych wskazanych w przepisach rozporządzenia delegowanego wydanego na podstawie art. 5 ust. 1 dyrektywy 2022/2557, lub świadczenia tych samych lub podobnych usług kluczowych, na rzecz co najmniej sześciu państw członkowskich Unii Europejskiej lub w co najmniej sześciu państwach członkowskich Unii Europejskiej.

2. W przypadku, o którym mowa w ust. 1, właściwy organ do spraw podmiotów krytycznych, za pośrednictwem Pojedynczego Punktu Kontaktowego informuje Komisję Europejską o potencjalnym podmiocie krytycznym o szczególnym znaczeniu europejskim, przekazując dane, o których mowa w art. 6zo ust. 2 pkt 1–7.

Art. 6zzg. 1. Organ do spraw podmiotów krytycznych, za pośrednictwem Pojedynczego Punktu Kontaktowego, inicjuje i prowadzi konsultacje z Komisją Europejską oraz właściwymi organami państw członkowskich Unii Europejskiej w celu ustalenia, czy podmiot krytyczny świadczący usługę kluczową na terytorium Rzeczypospolitej Polskiej, świadczy ją na rzecz co najmniej sześciu państw członkowskich Unii Europejskiej lub w co najmniej sześciu państwach członkowskich Unii Europejskiej.

2. W przypadku uznania przez Komisję Europejską podmiotu krytycznego, o którym mowa w art. 6zzf ust. 1, za podmiot krytyczny o szczególnym znaczeniu europejskim, organ do spraw podmiotów krytycznych informuje niezwłocznie podmiot krytyczny o tym fakcie oraz obowiązkach, o których mowa w przepisach rozdziału 11 ustawy.

Art. 6zzh. 1. Organ do spraw podmiotów krytycznych, za pośrednictwem Pojedynczego Punktu Kontaktowego, zapewnia współpracę z Komisją Europejską oraz właściwymi organami państwa członkowskiego, na rzecz którego lub w którym jest świadczona usługa kluczowa lub w przypadku gdy podmiot krytyczny o szczególnym znaczeniu europejskim zidentyfikowany przez państwo członkowskie świadczy usługę

kluczową na rzecz Rzeczypospolitej Polskiej lub na jej terytorium, w tym prowadzi wymianę informacji w zakresie:

1) oceny ryzyka podmiotu krytycznego o szczególnym znaczeniu europejskim;
2) wdrażania odpowiednich i proporcjonalnych do wyników oceny ryzyka rozwiązań organizacyjno-technicznych służących zapewnieniu odporności tego podmiotu;
3) działań z zakresu nadzoru oraz egzekwowania przepisów ustawy przez właściwy organ do spraw podmiotów krytycznych.

2. Właściwy organ do spraw podmiotów krytycznych, za pośrednictwem Pojedynczego Punktu Kontaktowego, współpracuje z Komisją Europejską w zakresie organizowania i zapewnienia obsługi misji doradczej, w tym:

1) przedkłada wniosek o zorganizowanie misji doradczej;
2) konsultuje program misji doradczej, w tym proponuje kandydatów do uczestnictwa w misji doradczej;
3) koordynuje realizację czynności związanych z dostępem przedstawicieli misji doradczej do informacji oraz budynków, terenów i infrastruktury krytycznej podmiotu krytycznego o szczególnym znaczeniu europejskim;
4) przeprowadza analizę sprawozdania z ustaleń misji doradczej.

3. Właściwy organ do spraw podmiotów krytycznych za pośrednictwem Pojedynczego Punktu Kontaktowego:

1) po dokonaniu analizy sprawozdania z ustaleń misji doradczej, przedkłada Komisji Europejskiej informację o stopniu wdrożenia rozwiązań organizacyjno-technicznych służących zapewnieniu odporności podmiotu krytycznego o szczególnym znaczeniu europejskim lub przedkłada rekomendacje w zakresie zwiększenia odporności tego podmiotu, w celu wydania przez Komisję Europejską opinii dotyczącej wywiązywania się z nałożonych obowiązków przez ten podmiot lub wskazującej środki, które można wprowadzić, aby zwiększyć odporność tego podmiotu;
2) przekazuje opinię, o której mowa w pkt 1, podmiotowi krytycznemu o szczególnym znaczeniu europejskim oraz zapewnia wsparcie w przypadku konieczności wdrożenia dodatkowych środków zwiększających odporność;
3) informuje Komisję Europejską oraz właściwe organy państwa członkowskiego, na rzecz którego lub w którym jest świadczona usługa kluczowa, o środkach

zwiększających odporność, wprowadzonych z uwzględnieniem opinii, o której mowa w pkt 1, albo informację o braku konieczności wprowadzania tych środków.

4. Przepisy ust. 2 i 3 stosuje się odpowiednio do misji doradczej organizowanej dla podmiotu krytycznego niebędącego podmiotem krytycznym o szczególnym znaczeniu europejskim za zgodą tego podmiotu, na wniosek organu do spraw podmiotów krytycznych, który zidentyfikował podmiot krytyczny.

5. Przepis ust. 2 stosuje się odpowiednio do wniosku o organizację misji doradczej, w przypadku gdy podmiot krytyczny o szczególnym znaczeniu europejskim zidentyfikowany przez państwo członkowskie świadczy usługę kluczową na rzecz Rzeczypospolitej Polskiej lub na jej terytorium.

Rozdział 13

Nadzór i kontrola podmiotów krytycznych

Art. 6zzi. 1. Nadzór w zakresie stosowania przepisów ustawy sprawują organy do spraw podmiotów krytycznych w zakresie:

1) spełniania przez podmioty krytyczne wymogów bezpieczeństwa dotyczących świadczenia usług kluczowych;
2) wykonywania przez podmioty krytyczne obowiązków wynikających z ustawy dotyczących przeciwdziałania zagrożeniom dla świadczonych usług kluczowych i zgłaszania incydentów istotnych.

2. W ramach nadzoru, o którym mowa w ust. 1, organ do spraw podmiotów krytycznych:

1) prowadzi kontrole podmiotów krytycznych, w siedzibie podmiotu, miejscu wykonywania działalności gospodarczej lub zdalnie;
2) zleca audyt zintegrowanego systemu zarządzania bezpieczeństwem świadczenia usługi kluczowej na koszt podmiotu krytycznego, w przypadku, o którym mowa w art. 6zz ust. 3;
3) nakłada kary pieniężne na podmioty krytyczne.

3. Organ do spraw podmiotów krytycznych może żądać od podmiotu krytycznego informacji w zakresie wdrożenia rozwiązań zawartych w dokumentacji cyberbezpieczeństwa, o której mowa w art. 6zu ust. 3 pkt 5, obejmujących:

1) wpływ wdrożonych rozwiązań na bezpieczeństwo świadczenia usługi kluczowej;

2) dowody potwierdzające wdrożone rozwiązania, w tym wyniki audytów przeprowadzonych przez podmiot krytyczny.

4. Organ do spraw podmiotów krytycznych wskazuje cel i uzasadnienie żądania, o którym mowa w ust. 3.

Art. 6zzj. Do kontroli realizowanej wobec podmiotów:

1) będących przedsiębiorcami stosuje się przepisy rozdziału 5 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców (Dz. U. z 2025 r. poz. 1480, 1795 i 1826);
2) niebędących przedsiębiorcami stosuje się przepisy ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (Dz. U. z 2026 r. poz. 158) określające zasady i tryb przeprowadzania kontroli.

Art. 6zzk. Osoba prowadząca czynności kontrolne wobec podmiotów będących przedsiębiorcami ma prawo do:

1) swobodnego wstępu i poruszania się po terenie podmiotu kontrolowanego;
2) wglądu do dokumentów dotyczących działalności podmiotu kontrolowanego, pobierania za pokwitowaniem oraz zabezpieczania dokumentów związanych z zakresem kontroli, z zachowaniem przepisów o tajemnicy prawnie chronionej;
3) sporządzania, a w razie potrzeby żądania sporządzenia, niezbędnych do kontroli kopii, odpisów lub wyciągów z dokumentów oraz zestawień lub obliczeń;
4) przetwarzania danych osobowych w zakresie niezbędnym do realizacji celu kontroli;
5) żądania złożenia ustnych lub pisemnych wyjaśnień w sprawach dotyczących zakresu kontroli;
6) przeprowadzania oględzin urządzeń, nośników oraz systemów informacyjnych.

Art. 6zzl. 1. Kontrolowane podmioty zapewniają osobie prowadzącej czynności kontrolne warunki niezbędne do sprawnego przeprowadzenia kontroli, w szczególności przez zapewnienie niezwłocznego przedstawienia żądanych dokumentów, terminowego udzielania ustnych i pisemnych wyjaśnień w sprawach objętych kontrolą, udostępniania niezbędnych urządzeń technicznych, a także sporządzania we własnym zakresie kopii lub wydruków dokumentów oraz informacji zgromadzonych na nośnikach, w urządzeniach lub w systemach informacyjnych.

2. Podmiot kontrolowany dokonuje potwierdzenia za zgodność z oryginałem sporządzonych kopii lub wydruków, o których mowa w ust. 1. W przypadku odmowy potwierdzenia za zgodność z oryginałem potwierdza je osoba prowadząca czynności kontrolne, o czym czyni wzmiankę w protokole kontroli.

Art. 6zzm. 1. Osoba prowadząca czynności kontrolne wobec podmiotów krytycznych ustala stan faktyczny na podstawie dowodów zebranych w toku kontroli, w szczególności dokumentów, przedmiotów, oględzin oraz ustnych lub pisemnych wyjaśnień i oświadczeń.

2. Osoba prowadząca czynności kontrolne wobec podmiotów krytycznych będących przedsiębiorcami przedstawia przebieg przeprowadzonej kontroli w protokole kontroli.

3. Protokół kontroli zawiera:

1) wskazanie nazwy oraz adresu podmiotu kontrolowanego;
2) imię i nazwisko osoby reprezentującej podmiot kontrolowany lub nazwę organu reprezentującego ten podmiot;
3) imię i nazwisko oraz stanowisko służbowe osoby prowadzącej czynności kontrolne;
4) datę rozpoczęcia i zakończenia czynności kontrolnych;
5) określenie przedmiotu, zakresu oraz okresu kontroli;
6) opis stanu faktycznego ustalonego w toku kontroli;
7) ocenę kontrolowanej działalności, w tym zakres, przyczyny i skutki stwierdzonych nieprawidłowości;
8) wyszczególnienie załączników.

4. Protokół kontroli podpisują osoba prowadząca czynności kontrolne oraz osoba reprezentująca podmiot kontrolowany.

5. W przypadku zastrzeżeń dotyczących ustaleń zawartych w protokole kontroli podmiot krytyczny ma prawo odmówić podpisania protokołu kontroli oraz złożyć umotywowane pisemne zastrzeżenia do tego protokołu w terminie 7 dni od dnia przedstawienia mu protokołu do podpisu.

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

7. W razie złożenia zastrzeżeń do protokołu kontroli kierownik komórki organizacyjnej prowadzącej czynności kontrolne dokonuje ich analizy.

8. Kierownik komórki organizacyjnej prowadzącej czynności kontrolne:

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.

9. W razie potrzeby, osoba prowadząca czynności kontrolne podejmuje dodatkowe czynności kontrolne, a w przypadku stwierdzenia przez kierownika komórki organizacyjnej prowadzącej czynności kontrolne zasadności zastrzeżeń do protokołu kontroli zmienia lub uzupełnia odpowiednią część protokołu kontroli w formie aneksu do protokołu.

10. Kierownik komórki organizacyjnej prowadzącej czynności kontrolne, po rozpatrzeniu zastrzeżeń do protokołu kontroli, sporządza stanowisko wobec tych zastrzeżeń.

11. W przypadku nieuwzględnienia zastrzeżeń do protokołu kontroli w całości albo w części kierownik komórki organizacyjnej prowadzącej czynności kontrolne informuje kontrolowany podmiot krytyczny na piśmie.

12. 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.

Art. 6zzn. 1. Jeżeli na podstawie informacji zgromadzonych w protokole kontroli organ do spraw podmiotów krytycznych uzna, że mogło dojść do naruszenia przepisów ustawy przez podmiot kontrolowany, przekazuje zalecenia pokontrolne dotyczące usunięcia nieprawidłowości, wskazując jednocześnie termin ich usunięcia. Przy określaniu terminu usunięcia nieprawidłowości, organ do spraw podmiotów krytycznych bierze pod uwagę zakres i rodzaj stwierdzonych naruszeń.

2. Od zaleceń pokontrolnych nie przysługują środki odwoławcze.

3. Podmiot kontrolowany, w wyznaczonym terminie, informuje organ do spraw podmiotów krytycznych o sposobie wykonania zaleceń.

Rozdział 14

Przepisy o karach pieniężnych dla podmiotów krytycznych

Art. 6zzo. 1. Karze pieniężnej podlega podmiot krytyczny, który:

1) nie przeprowadza systematycznej oceny ryzyka, o której mowa w art. 6zt ust. 1 pkt 1;
2) nie wdraża rozwiązań organizacyjno-technicznych, o których mowa w art. 6zt ust. 1 pkt 2;
3) nie prowadzi dokumentacji, o której mowa w art. 6zu ust. 1;

4) nie wykonuje obowiązku, o którym mowa w art. 6zv ust. 1 pkt 1, w zakresie obsługi incydentu istotnego;
5) nie wykonuje obowiązku, o którym mowa w art. 6zv ust. 1 pkt 4;
6) nie przeprowadza audytu, o którym mowa w art. 6zz ust. 1;
7) nie wyznacza pełnomocnika bezpieczeństwa usługi kluczowej lub zastępcy pełnomocnika bezpieczeństwa usługi kluczowej, o których mowa w art. 6zzd ust. 1;
8) uniemożliwia lub utrudnia wykonywanie kontroli, o której mowa w art. 6zzi ust. 2 pkt 1;
9) nie wykonał w wyznaczonym terminie zaleceń pokontrolnych, o których mowa w art. 6zzn ust. 1;
10) nie wdrożył rozwiązań dotyczących ochrony infrastruktury krytycznej, o których mowa w art. 6ze ust. 1 pkt 2, w odniesieniu do infrastruktury krytycznej niezbędnej do świadczenia usługi kluczowej;
11) nie opracował dokumentacji ochrony infrastruktury krytycznej, o której mowa w art. 6zf ust. 1, w odniesieniu do infrastruktury krytycznej niezbędnej do świadczenia usługi kluczowej.

2. Wysokość kary pieniężnej, o której mowa w:

1) ust. 1 pkt 1, wynosi do 100 000 zł;
2) ust. 1 pkt 2, wynosi do 150 000 zł;
3) ust. 1 pkt 3, wynosi do 50 000 zł;
4) ust. 1 pkt 4, wynosi do 20 000 zł za każdy stwierdzony przypadek zaniechania obsługi incydentu istotnego;
5) ust. 1 pkt 5, wynosi do 25 000 zł za każdy stwierdzony przypadek niezgłoszenia incydentu istotnego;
6) ust. 1 pkt 6, wynosi do 200 000 zł;
7) ust. 1 pkt 7, wynosi do 15 000 zł;
8) ust. 1 pkt 8, wynosi do 50 000 zł;
9) ust. 1 pkt 9, wynosi do 200 000 zł;
10) ust. 1 pkt 10, wynosi do 150 000 zł;
11) ust. 1 pkt 11, wynosi do 50 000 zł.

3. Kara, o której mowa w:

1) ust. 1 pkt 4, 5 i 7, nie może być niższa niż 2000 zł;
2) ust. 1 pkt 3, 8 i 11, nie może być niższa niż 5000 zł;

3) ust. 1 pkt 1, 2, 6, 9 i 10, nie może być niższa niż 15 000 zł.

Art. 6zzp. 1. Karę pieniężną, o której mowa w art. 6zzo, nakłada w drodze decyzji, organ do spraw podmiotów krytycznych.

2. Organ do spraw podmiotów krytycznych może decyzji, o której mowa w ust. 1, nadać rygor natychmiastowej wykonalności w całości albo w części, jeżeli wymaga tego ochrona bezpieczeństwa lub porządku publicznego oraz zagrożenie wywołania poważnych utrudnień w świadczeniu usług.

3. Wpływy z tytułu kar pieniężnych, o których mowa w art. 6zzo, stanowią:

1) w 70% dochód budżetu państwa;

2) w 30% 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, z 2025 r. poz. 1017 oraz z 2026 r. poz. 252 i …).

Art. 6zzq. 1. W przypadku naruszenia przepisów ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa przez podmiot krytyczny będący jednocześnie podmiotem kluczowym w rozumieniu przepisów tej ustawy, karę pieniężną na ten podmiot nakłada organ właściwy do spraw cyberbezpieczeństwa.

2. Do ustalenia wysokości kary pieniężnej w przypadku, o którym mowa w ust. 1, stosuje się przepisy ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

3. Organ właściwy do spraw cyberbezpieczeństwa niezwłocznie informuje organ do spraw podmiotów krytycznych, sprawujący nadzór nad podmiotem, o którym mowa w ust. 1, o:

1) wszczęciu wobec tego podmiotu postępowania w sprawie nałożenia kary pieniężnej;

2) naruszeniu dokonanym przez podmiot wraz z kwalifikacją prawną;

3) wysokości nałożonej na ten podmiot kary lub odstąpieniu od jej nałożenia.

4. Organ do spraw podmiotów krytycznych nie wszczyna postępowania w sprawie nałożenia kary pieniężnej w przypadku, o którym mowa w ust. 1, jeżeli postępowanie w przedmiocie tego naruszenia prowadzi organ właściwy do spraw cyberbezpieczeństwa.

Art. 6zzr. 1. Organ do spraw podmiotów krytycznych, podejmując decyzję o nałożeniu kary pieniężnej i ustalając jej wysokość, bierze pod uwagę:

1) wagę naruszenie i znaczenie naruszonych przepisów ustawy;

2) czas trwania naruszenia;

3) wcześniejsze naruszenia ze strony danego podmiotu krytycznego;
4) spowodowane szkody majątkowe i niemajątkowe, w tym wpływ na użytkowników usługi oraz na inne usługi kluczowe;
5) środki zastosowane przez podmiot w celu ograniczenia szkód, o których mowa w pkt 4;
6) umyślny lub nieumyślny charakter czynu ze strony sprawcy naruszenia;
7) stopień współpracy podmiotu krytycznego z organem do spraw podmiotów krytycznych.

2. Podejmując decyzję, organ uwzględnia również wysokość przychodu uzyskanego z działalności gospodarczej w roku obrotowym poprzedzającym wymierzenie kary pieniężnej lub możliwości finansowe podmiotu krytycznego będącego podmiotem publicznym.

3. W związku z toczącym się postępowaniem w sprawie nałożenia kary pieniężnej, organ do spraw podmiotów krytycznych może żądać od podmiotu krytycznego przekazania we wskazanym terminie, nie dłuższym niż 14 dni od dnia otrzymania żądania, informacji niezbędnych do określenia wymiaru kary pieniężnej.

4. W przypadku nieprzekazania informacji, o których mowa w ust. 2, lub przekazania informacji uniemożliwiających ustalenie podstawy wymiaru kary pieniężnej, organ do spraw podmiotów krytycznych ustala podstawę wymiaru kary pieniężnej w sposób szacunkowy, uwzględniając wielkość podmiotu krytycznego, specyfikę działalności tego podmiotu oraz 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 odrębny rachunek bankowy wskazany przez organ właściwy do spraw podmiotów krytycznych w decyzji o wymierzeniu kary pieniężnej.

6. Kara pieniężna nieuiszczona w terminie wraz z odsetkami podlega ściągnięciu w trybie określonym w przepisach o postępowaniu egzekucyjnym w administracji.

7. Organ właściwy do spraw podmiotów krytycznych może odstąpić od nałożenia kary pieniężnej, jeżeli waga naruszenia i znaczenie naruszonych przepisów jest znikome, a podmiot krytyczny zaprzestał naruszania prawa lub naprawił wyrządzoną szkodę.

Art. 6zzs. W zakresie nieuregulowanym w niniejszym rozdziale stosuje się odpowiednio przepisy działu IVa ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (Dz. U. z 2025 r. poz. 1691).

Rozdział 15

Przepisy szczególne dotyczące niektórych podmiotów krytycznych

Art. 6zzt. Do podmiotów krytycznych z sektora bankowości i infrastruktury rynków finansowych nie stosuje się przepisów rozdziałów 11–14, z wyjątkiem art. 6zt ust. 1 pkt 1, art. 6zt ust. 1 pkt 2 lit. b–d, f, h oraz i, art. 6zt pkt 3, art. 6zt ust. 2–11, art. 6zu ust. 1 i ust. 2 pkt 3, 4 i 6, art. 6zu ust. 3–6, art. 6zx, art. 6zy, art. 6zzb i art. 6zzd.

Art. 6zzu. Do podmiotów krytycznych z sektora infrastruktury cyfrowej nie stosuje się przepisów rozdziałów 11–14.

Rozdział 16

Organy właściwe w sprawach zarządzania kryzysowego i ich zadania”;

8) w art. 7a w ust. 3 pkt 2 otrzymuje brzmienie:

„2) zapewnienia właściwego funkcjonowania, ochrony, wzmocnienia oraz odbudowy infrastruktury krytycznej lub zapewnienia niezakłóconego świadczenia usługi kluczowej;”;

9) w art. 10 w ust. 1 skreśla się wyrazy „zwane dalej „Centrum”,”;

10) w art. 11:

a) w pkt 1 lit. b otrzymuje brzmienie:

„b) opracowywanie i aktualizowanie Krajowego Planu Zarządzania Ryzykiem oraz Krajowego Planu Reagowania Kryzysowego,”,

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

„1b. Centrum realizuje zadania, o których mowa w art. 22 ustawy z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej.”;

11) po art. 11a dodaje się art. 11b w brzmieniu:

„Art. 11b. W celu realizacji zadań planowania cywilnego wynikających z członkostwa Rzeczypospolitej Polskiej w Organizacji Traktatu Północnoatlantyckiego, Centrum:

1) koordynuje:

a) udział przedstawicieli Rzeczypospolitej Polskiej w pracach Komitetu do spraw Odporności Organizacji Traktatu Północnoatlantyckiego oraz zapewnia wsparcie merytoryczne prowadzonych prac,

b) opracowywanie stanowisk Rzeczypospolitej Polskiej na potrzeby procesów planowania cywilnego Organizacji Traktatu Północnoatlantyckiego;

2) zapewnienia funkcjonowanie punktu kontaktowego do przekazywania zadań oraz uruchamiania procedur wynikających z członkostwa Rzeczypospolitej Polskiej w Organizacji Traktatu Północnoatlantyckiego.”;

12) w art. 12:

a) ust. 1 otrzymuje brzmienie:

„1. Ministrowie kierujący działami administracji rządowej oraz kierownicy urzędów centralnych realizują, w zakresie swojej właściwości, zadania dotyczące zarządzania kryzysowego, w tym:

1) opracowują plany zarządzania kryzysowego;
2) organizują, prowadzą i koordynują szkolenia i ćwiczenia z zakresu zarządzania kryzysowego oraz biorą udział w ćwiczeniach krajowych i międzynarodowych;
3) współpracują z operatorami infrastruktury krytycznej lub podmiotami krytycznymi w zakresie realizacji zadań ochrony infrastruktury krytycznej oraz zapewnienia niezakłóconego świadczenia usług kluczowych;
4) zapewniają funkcjonowanie stałego dyżuru w ramach podwyższania gotowości obronnej państwa.”,

b) uchyla się ust. 2 i 2a,

c) ust. 2c otrzymuje brzmienie:

„2c. Do zadań zespołów, o których mowa w ust. 2b, należy:

1) dokonywanie okresowej oceny ryzyka na potrzeby Krajowej Oceny Ryzyka;
2) dokonywanie okresowej oceny gotowości do reagowania w przypadku wystąpienia sytuacji kryzysowej w zakresie organizacyjnym, technicznym i finansowym;
3) opiniowanie projektów planów zarządzania kryzysowego;
4) wypracowywanie wniosków i propozycji dotyczących zapobiegania i przeciwdziałania zagrożeniom.”;

13) w art. 14 ust. 3 otrzymuje brzmienie:

„3. Minister właściwy do spraw administracji publicznej w uzgodnieniu z ministrem właściwym do spraw wewnętrznych oraz po zasięgnięciu opinii dyrektora Centrum wydaje, w drodze zarządzenia, wojewodom wytyczne do wojewódzkich planów zarządzania kryzysowego. Wytyczne do wojewódzkich planów zarządzania kryzysowego mogą zostać wydane w każdym czasie, niezależnie od cyklu planowania.”;

14) w art. 25 w ust. 3 pkt 13 otrzymuje brzmienie:

„13) wspieranie w wykonywaniu zadań związanych z naprawą i odbudową infrastruktury technicznej;”;

15) uchyla się art. 25a–25d;

16) po art. 25d dodaje się oznaczenie i tytuł rozdziału 17 w brzmieniu:

„Rozdział 17

Finansowanie zadań zarządzania kryzysowego”;

17) w art. 26 dodaje się ust. 4a i 4b w brzmieniu:

„4a. Środki finansowe z rezerwy celowej, o której mowa w ust. 4, mogą być przeznaczone na realizację przedsięwzięć związanych z zarządzaniem ryzykiem, reagowaniem w przypadku wystąpienia sytuacji kryzysowej oraz usuwaniem jej skutków i odtwarzaniem zasobów, z uwzględnieniem planowanych działań z zakresu ochrony ludności i obrony cywilnej.

4b. Środki z rezerwy celowej, o której mowa w ust. 4, mogą być przeznaczane na pomoc finansową udzielaną innym jednostkom samorządu terytorialnego na realizację przez te jednostki przedsięwzięć, o których mowa w ust. 4a.”;

18) po art. 31 dodaje się oznaczenie i tytuł rozdziału 18 w brzmieniu:

„Rozdział 18

Przepisy dostosowujące, przejściowe i końcowe”;

19) do ustawy dodaje się załącznik w brzmieniu określonym w załączniku do niniejszej ustawy.

Art. 2. W ustawie z dnia 21 marca 1985 r. o drogach publicznych (Dz. U. z 2025 r. poz. 889) dodaje się art. 20i w brzmieniu:

„Art. 20i. 1. W sytuacji kryzysowej, jeżeli wymagają tego potrzeby obronności lub istotny interes bezpieczeństwa państwa, właściwy miejscowo wojewoda może, w drodze rozporządzenia porządkowego, po zasięgnięciu opinii zarządcy drogi, wprowadzić czasowe ograniczenia w korzystaniu z dróg publicznych, w tym czasowo wyłączyć je z ruchu.

2. Czasowe ograniczenia w korzystaniu z dróg publicznych, w tym ich czasowe wyłączenie z ruchu, wprowadza się w sposób, który umożliwia przemieszczanie się w określonych kierunkach za pomocą innych dróg niepodlegających ograniczeniom w korzystaniu i niewyłączonych z ruchu.

3. Rozporządzenie porządkowe w zakresie, o którym mowa w ust. 1, określa:

1) odcinki dróg publicznych wyznaczone za pomocą współrzędnych geograficznych lub oznakowania umieszczonego na słupkach hektometrowych i kilometrowych, na których wprowadzono czasowe ograniczenia w korzystaniu lub czasowe wyłączenie z ruchu;
2) rodzaj ograniczenia w korzystaniu z dróg publicznych;
3) okres, na który wprowadzono ograniczenia w korzystaniu z dróg publicznych lub czasowe wyłączenie z ruchu;
4) obowiązki zarządcy drogi, zarządzającego ruchem oraz innych organów i podmiotów w zakresie, o którym mowa w ust. 1.

4. Rozporządzenie porządkowe, o którym mowa w ust. 1, może być ogłoszone w drodze obwieszczenia lub za pomocą środków komunikacji elektronicznej, lub w inny sposób zwyczajowo przyjęty na danym terenie.”.

Art. 3. W ustawie z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2025 r. poz. 636, 718 i 1366 oraz z 2026 r. poz. 187) wprowadza się następujące zmiany:

1) w art. 16 ust. 1 otrzymuje brzmienie:

„1. W przypadkach, o których mowa w art. 11 ustawy z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej (Dz. U. z 2026 r. poz. 244 i …), policjanci mogą użyć środków przymusu bezpośredniego, o których mowa w art. 12 ust. 1 pkt 1−13 i 17−23 tej ustawy, lub wykorzystać te środki.”;

2) w art. 18c ust. 1 otrzymuje brzmienie:

„1. Komendant Główny Policji, Komendant CBŚP, Komendant CBZC lub komendant wojewódzki Policji:

1) w celu realizacji zadań, o których mowa w art. 1 ust. 2 pkt 1, 2, 3a, 4a, lub
2) w przypadkach, o których mowa:
   a) w art. 156ze ust. 1 ustawy z dnia 3 lipca 2002 r. – Prawo lotnicze (Dz. U. z 2025 r. poz. 1431 i 1668 oraz z 2026 r. poz. 176), lub
   b) w art. 28a ust. 1 ustawy z dnia 4 września 2008 r. o ochronie żeglugi i portów morskich (Dz. U. z 2024 r. poz. 597 oraz …), lub
   c) w art. 11 pkt 17 ustawy z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej, lub
3) po wprowadzeniu trzeciego lub czwartego stopnia alarmowego, o których mowa odpowiednio w art. 16 ust. 5 lub ust. 6 ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych

– może podjąć decyzję o dopuszczalności zastosowania przez Policję urządzeń uniemożliwiających telekomunikację na określonym obszarze, przez czas niezbędny do wyeliminowania zagrożenia lub jego skutków, z uwzględnieniem konieczności minimalizacji skutków braku możliwości korzystania z usług telekomunikacyjnych.”;

3) w art. 36k po ust. 3 dodaje się ust. 3a w brzmieniu:

„3a. W przypadku policjantów oddelegowanych do wykonywania zadań służbowych w urzędzie obsługującym ministra właściwego do spraw wewnętrznych albo w jednostce podległej lub nadzorowanej przez ministra właściwego do spraw wewnętrznych należności, o których mowa w ust. 3, wypłaca jednostka organizacyjna Policji, w której policjant pełnił służbę bezpośrednio przed oddelegowaniem w uzgodnieniu z kierownikiem urzędu albo jednostki, do której policjant został oddelegowany.”.

Art. 4. W ustawie z dnia 12 października 1990 r. o Straży Granicznej (Dz. U. z 2025 r. poz. 914 i 1366) wprowadza się następujące zmiany:

1) w art. 1 po ust. 3b dodaje się ust. 3c w brzmieniu:

„3c. Straż Graniczna zapewnia koordynację działań podejmowanych przez organy i podmioty realizujące zadania w ramach Centrum Bezpieczeństwa Morskiego, o którym mowa w art. 25a ustawy z dnia 4 września 2008 r. o ochronie żeglugi i portów morskich (Dz. U. z 2024 r. poz. 597 oraz …).”;

2) w art. 10e ust. 1 otrzymuje brzmienie:

„1. Komendant Główny Straży Granicznej, Komendant BSWSG lub komendant oddziału Straży Granicznej:

1) w celu realizacji zadań, o których mowa w art. 1 ust. 2 pkt 1, 2, 4–5d i 10, lub

2) w przypadkach, o których mowa:

a) w art. 156ze ust. 1 ustawy z dnia 3 lipca 2002 r. – Prawo lotnicze (Dz. U. z 2025 r. poz. 1431 i 1668 oraz z 2026 r. poz. 176), lub

b) w art. 28a ust. 1 ustawy z dnia 4 września 2008 r. o ochronie żeglugi i portów morskich, lub

c) w art. 11 pkt 17 ustawy z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej (Dz. U. z 2026 r. poz. 244 i …), lub

3) po wprowadzeniu trzeciego lub czwartego stopnia alarmowego, o których mowa odpowiednio w art. 16 ust. 5 lub ust. 6 ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych

– może podjąć decyzję o dopuszczalności zastosowania urządzeń uniemożliwiających telekomunikację na określonym obszarze, przez czas niezbędny do wykonywania czynności przez Straż Graniczną, z uwzględnieniem konieczności minimalizacji skutków braku możliwości korzystania z usług telekomunikacyjnych.”;

3) w art. 23 ust. 1 otrzymuje brzmienie:

„1. W przypadkach, o których mowa w art. 11 ustawy z 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej, funkcjonariusze mogą użyć środków przymusu bezpośredniego, o których mowa w art. 12 ust. 1 pkt 1−13 i 16−23 tej ustawy, lub wykorzystać te środki.”;

4) w art. 41i dodaje się ust. 3 w brzmieniu:

„3. W przypadku funkcjonariuszy oddelegowanych do wykonywania zadań służbowych w urzędzie obsługującym ministra właściwego do spraw wewnętrznych albo w jednostce podległej lub nadzorowanej przez ministra właściwego do spraw wewnętrznych należności, o których mowa w ust. 1, wypłaca jednostka organizacyjna, w której funkcjonariusz pełnił służbę przed oddelegowaniem w uzgodnieniu z kierownikiem urzędu albo jednostki, do której funkcjonariusz został oddelegowany.”.

Art. 5. W ustawie z dnia 24 sierpnia 1991 r. o ochronie przeciwpożarowej (Dz. U. z 2025 r. poz. 188) w art. 14fa ust. 3 otrzymuje brzmienie:

„3. Plany ratownicze w zakresie zdarzeń z dużą liczbą poszkodowanych oraz działań ratowniczych i działań pomocowych podczas katastrof, klęsk żywiołowych i zdarzeń nadzwyczajnych są skorelowane z planami reagowania kryzysowego, o których mowa w art. 6j ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, oraz z planami postępowania awaryjnego, o których mowa w art. 84 ust. 1 ustawy z dnia 29 listopada 2000 r. – Prawo atomowe (Dz. U. z 2026 r. poz. 1).”.

Art. 6. W ustawie z dnia 24 sierpnia 1991 r. o Państwowej Straży Pożarnej (Dz. U. z 2025 r. poz. 1312 i 1366 oraz z 2026 r. poz. 252) w art. 37r dodaje się ust. 3 w brzmieniu:

„3. W przypadku strażaków oddelegowanych do wykonywania zadań służbowych w urzędzie obsługującym ministra właściwego do spraw wewnętrznych albo w jednostce podległej lub nadzorowanej przez ministra właściwego do spraw wewnętrznych, należności, o których mowa w ust. 1, wypłaca jednostka organizacyjna Państwowej Straży Pożarnej, w której strażak pełnił służbę przed oddelegowaniem w uzgodnieniu z kierownikiem urzędu albo jednostki, do której strażak został oddelegowany.”.

Art. 7. W ustawie z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz. U. z 2025 r. poz. 532) wprowadza się następujące zmiany:

1) w art. 5:

a) w ust. 2:

– w pkt 1 w lit. c wyrazy „ustawy z dnia 29 października 2010 r. o rezerwach strategicznych (Dz. U. z 2020 r. poz. 2051)” zastępuje się wyrazami „ustawy z dnia 17 grudnia 2020 r. o rezerwach strategicznych (Dz. U. z 2024 r. poz. 1598 i 1907 oraz z 2026 r. poz. 203 i …)”,

– w pkt 3 lit. a otrzymuje brzmienie:

„a) zakłady, obiekty i urządzenia mające istotne znaczenie dla funkcjonowania powiatów lub miast na prawach powiatu, których zniszczenie lub uszkodzenie może stanowić zagrożenie dla życia i zdrowia ludzi oraz środowiska, w szczególności elektrownie i ciepłownie, ujęcia wody, wodociągi i oczyszczalnie ścieków,”,

– pkt 5 otrzymuje brzmienie:

„5) obiekt, urządzenie, instalację lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje ujęte w wykazie, o którym mowa w art. 6r ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2023 r. poz. 122, z późn. zm.[7)]).”,

b) ust. 3 otrzymuje brzmienie:

„3. Szczegółowe wykazy obszarów, obiektów i urządzeń, o których mowa w ust. 2, sporządzają i bieżąco aktualizują: Prezes Narodowego Banku Polskiego, Krajowa Rada Radiofonii i Telewizji, ministrowie, kierownicy urzędów centralnych i wojewodowie w stosunku do podległych, podporządkowanych lub nadzorowanych jednostek organizacyjnych, oraz Komisja Nadzoru Finansowego w stosunku do podmiotów podlegających nadzorowi Komisji Nadzoru Finansowego w rozumieniu ustawy z dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym (Dz. U. z 2025 r. poz. 640 i 1069 oraz z 2026 r. poz. 252). Umieszczenie w wykazie określonego obszaru, obiektu lub urządzenia następuje w drodze decyzji administracyjnej.”,

c) po ust. 3 dodaje się ust. 3a w brzmieniu:

[7)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2024 r. poz. 834, 1222, 1473, 1572 i 1907, z 2025 r. poz. 1795 oraz …

„3a. Do wykazów, o których mowa w ust. 3 , stosuje się przepisy ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2025 r. poz. 1209).”,

d) ust. 4 otrzymuje brzmienie:

„4. Podmioty, o których mowa w ust. 3, przekazują wykazy oraz ich aktualizacje właściwym terytorialnie wojewodom w terminie 14 dni odpowiednio od ich sporządzenia lub aktualizacji.”,

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

„4a. Starostowie i prezydenci miast na prawach powiatu informują wojewodę o zakładach, obiektach i urządzeniach, o których mowa w ust. 2 pkt 3 lit. a, znajdujących się na terenie powiatu.”,

f) ust. 5 otrzymuje brzmienie:

„5. Wojewodowie prowadzą ewidencję obszarów, obiektów i urządzeń podlegających obowiązkowej ochronie, znajdujących się na terenie województwa. Do ewidencji stosuje się przepisy ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych.”,

g) po ust. 5 dodaje się ust. 5a w brzmieniu:

„5a. Ewidencja, o której mowa w ust. 5, zawiera dane dotyczące w szczególności:

1) numeru wpisu;
2) nazwy obszaru, obiektu lub urządzenia;
3) adresu obszaru, obiektu lub urządzenia;
4) nazwy stanowiska kierownika jednostki, która zarządza obszarem, obiektem lub urządzeniem;
5) organu, o którym mowa w ust. 3, właściwego w stosunku do obszaru, obiektu lub urządzenia.”,

h) ust. 6 otrzymuje brzmienie:

„6. Wojewoda, w drodze decyzji administracyjnej, może umieścić w ewidencji, o której mowa w ust. 5, znajdujące się na terenie województwa obszary, obiekty i urządzenia inne niż wpisane do wykazów, o których mowa w ust. 3, lub do wykazu infrastruktury krytycznej, o którym mowa w art. 6r ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, w tym zakłady, obiekty i urządzenia, o których mowa w ust. 2 pkt 3 lit. a.”,

i) dodaje się ust. 7 i 8 w brzmieniu:

„7. Wojewoda, po otrzymaniu wykazów lub ich aktualizacji od podmiotów, o których mowa w ust. 3, niezwłocznie aktualizuje ewidencję, o której mowa w ust. 5.

8. Wojewoda, niezwłocznie po umieszczeniu obszaru, obiektu lub urządzenia w ewidencji, o której mowa w ust. 5, informuje o tym kierownika jednostki, który bezpośrednio zarządza obszarami, obiektami i urządzeniami umieszczonymi w ewidencji oraz odpowiednio podmioty, o których mowa w ust. 3, a także właściwego terytorialnie komendanta wojewódzkiego Policji oraz właściwego terytorialnie dyrektora delegatury Agencji Bezpieczeństwa Wewnętrznego.”;

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

„Art. 5a. Środki ochrony fizycznej oraz zabezpieczenia techniczne wykraczające poza granice obiektu lub urządzenia podlegającego obowiązkowej ochronie mogą być stosowane od strony wody w odniesieniu do:

1) obiektów, o których mowa w art. 5 ust. 1, będących jednocześnie obiektami portowymi w rozumieniu ustawy z 4 września 2008 r. o ochronie żeglugi i portów morskich (Dz. U. z 2024 r. poz. 597 oraz …);

2) sztucznych wysp, konstrukcji i urządzeń w obszarach morskich Rzeczypospolitej Polskiej, o których mowa w art. 23 ust. 1 ustawy z dnia 21 marca 1991 r. o obszarach morskich Rzeczypospolitej Polskiej i administracji morskiej (Dz. U. z 2024 r. poz. 1125, z 2025 r. poz. 409, 1535 i 1668 oraz z 2026 r. poz. 252);

3) kabli i rurociągów układanych i utrzymywanych w obszarach morskich Rzeczypospolitej Polskiej, o których mowa w art. 26 ust. 1 oraz art. 27 ust. 1 ustawy z dnia 21 marca 1991 r. o obszarach morskich Rzeczypospolitej Polskiej i administracji morskiej.”;

3) w art. 26 w ust. 1 w pkt 5 dodaje się lit. c w brzmieniu:

„c) w art. 36 ust. 1a–1c;”;

4) w art. 36:

a) w ust. 1 pkt 4 otrzymuje brzmienie:

„4) użycia lub wykorzystania środków przymusu bezpośredniego, o których mowa w art. 12 ust. 1 pkt 1 lit. a, b i d, pkt 2 lit. a, pkt 5, 7, 9, 11, pkt 12 lit. a, pkt 13 i 21–23 ustawy z 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej (Dz. U. z 2026 r. poz. 244 i …):

a) w granicach chronionych obiektów i obszarów − w przypadkach, o których mowa w art. 11 pkt 2, 5, 8, 10, 13,15–17 tej ustawy,

b) poza granicami obiektów i obszarów chronionych – w przypadku, o którym mowa w art. 11 pkt 9 tej ustawy;”,

b) ust. 1a otrzymuje brzmienie:

„1a. Środki przymusu bezpośredniego, o których mowa w art. 12 ust. 1 pkt 5 lub 11 ustawy z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej, mogą być wykorzystane wyłącznie zgodnie z art. 156ze ustawy z dnia 3 lipca 2002 r. – Prawo lotnicze (Dz. U. z 2025 r. poz. 1431 i 1668 oraz z 2026 r. poz. 176), art. 28a ustawy z dnia 4 września 2008 r. o ochronie żeglugi i portów morskich lub art. 11 pkt 17 ustawy z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej.”,

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

„1b. Pracownik ochrony przy wykonywaniu zadań ochrony obiektów, o których mowa w art. 5a pkt 1, w celu zabezpieczenia infrastruktury portowej przed uszkodzeniem, może patrolować ten obiekt od strony wody jednostką pływającą.

1c. Wykonując czynności, o których mowa w ust. 1b, pracownik ochrony ma prawo do wezwania osób przebywających w basenie portowym, a nieposiadających do tego uprawnień, do jego opuszczenia, a także do podjęcia interwencji wobec tych osób, w tym ujęcia ich oraz użycia środków przymusu bezpośredniego określonych w art. 12 ust. 1 pkt 1 lit. a, b i d, pkt 2 lit. a, pkt 11, 13 i 21–23 ustawy z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej w przypadkach, o których mowa w art. 11 pkt 2, 5, 8, 10, 13 i 15–17 tej ustawy.”;

5) w art. 47 w ust. 2 wprowadzenie do wyliczenia otrzymuje brzmienie:
„Współpracę, o której mowa w ust. 1, specjalistyczne uzbrojone formacje ochronne podejmują odpowiednio z właściwymi terytorialnie:”;

6) po art. 50b dodaje się art. 50c w brzmieniu:

„Art. 50c. 1. Kto nie będąc do tego uprawnionym, przebywa na obszarze lub obiekcie podlegającym obowiązkowej ochronie oraz takiego obszaru lub obiektu wbrew żądaniu osoby uprawnionej nie opuszcza, podlega grzywnie, karze ograniczenia wolności albo karze pozbawienia wolności do lat 2.

2. Kto nie będąc do tego uprawnionym, przebywając na obszarze lub obiekcie podlegającym obowiązkowej ochronie, utrudnia lub uniemożliwia korzystanie z tych

obszarów, obiektów lub znajdujących się na ich terenie urządzeń lub instalacji, podlega grzywnie, karze ograniczenia wolności albo karze pozbawienia wolności do lat 5.”.

Art. 8. W ustawie z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych (Dz. U. z 2026 r. poz. 159) wprowadza się następujące zmiany:

1) w art. 42 ust. 1 i 2 otrzymują brzmienie:

„Art. 42. 1. W przypadkach, o których mowa w art. 11 pkt 1−6 i 8−16 ustawy z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej, żołnierze Żandarmerii Wojskowej mogą użyć środków przymusu bezpośredniego, o których mowa w art. 12 ust. 1 pkt 1−9, pkt 11, pkt 12 lit. a, c i d, pkt 13–14 i 17−23 tej ustawy, lub wykorzystać te środki.

2.W przypadkach, o których mowa w art. 45 pkt 1 lit. a–c i e, pkt 2, 3 i pkt 4 lit. a i b oraz w art. 47 pkt 1–3 i 5–8 ustawy z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej, żołnierze Żandarmerii Wojskowej mogą użyć broni palnej lub ją wykorzystać.”;

2) w art. 51 ust. 2 i 3 otrzymują brzmienie:

„2. W przypadkach, o których mowa w art. 11 pkt 1–6 i 8–14 ustawy z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej, żołnierze wojskowych organów porządkowych wchodzących w skład służby garnizonowej i służby wewnętrznej jednostki wojskowej w związku z wykonywaniem czynności służbowych mogą użyć środków przymusu bezpośredniego, o których mowa w art. 12 ust. 1 pkt 1–5, 7–9, 11, pkt 12 lit. a, c i d, pkt 13, 17, 19–23 tej ustawy, lub wykorzystać te środki.

3. W przypadkach, o których mowa w art. 45 pkt 1 lit. a–c i e, pkt 2, 3 i pkt 4 lit. a i b oraz w art. 47 pkt 1–3 i 5–8 ustawy z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej, żołnierze wojskowych organów porządkowych wchodzących w skład służby garnizonowej i służby wewnętrznej jednostki wojskowej w związku z wykonywaniem czynności służbowych mogą użyć broni palnej lub ją wykorzystać.”.

Art. 9. W ustawie z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2025 r. poz. 902 i 1366 oraz z 2026 r. poz. 26) wprowadza się następujące zmiany:

1) w art. 5 w ust. 1 pkt 2a otrzymuje brzmienie:

„2a) rozpoznawanie, zapobieganie i wykrywanie zagrożeń godzących w bezpieczeństwo istotnych z punktu widzenia ciągłości funkcjonowania państwa systemów teleinformatycznych organów administracji publicznej lub systemu sieci teleinformatycznych objętych wykazem, o którym mowa w art. 6r ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2023 r. poz. 122, z późn. zm.[8)]), a także systemów teleinformatycznych operatorów infrastruktury krytycznej, o których mowa w art. 3 pkt 3a tej ustawy;”;

2) w art. 32a ust. 1 otrzymuje brzmienie:

„1. W celu zapobiegania, przeciwdziałania i zwalczania zdarzeń o charakterze terrorystycznym lub uprawdopodabniających popełnienie przestępstwa szpiegostwa, dotyczących istotnych z punktu widzenia ciągłości funkcjonowania państwa systemów teleinformatycznych organów administracji publicznej lub sieci teleinformatycznych objętych wykazem, o którym mowa w art. 6r ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, a także systemów teleinformatycznych operatorów infrastruktury krytycznej, o których mowa w art. 3 pkt 3a tej ustawy, lub danych przetwarzanych w tych systemach oraz rozpoznawania, zapobiegania i wykrywania przestępstw o charakterze terrorystycznym lub przestępstwa szpiegostwa w tym obszarze oraz ścigania ich sprawców, ABW może przeprowadzać ocenę bezpieczeństwa tych systemów teleinformatycznych, zwaną dalej „oceną bezpieczeństwa”.”;

3) w art. 32aa ust. 1 otrzymuje brzmienie:

„1. W celu zapobiegania, przeciwdziałania i zwalczania zdarzeń o charakterze terrorystycznym lub uprawdopodabniających popełnienie przestępstwa szpiegostwa, dotyczących istotnych z punktu widzenia ciągłości funkcjonowania państwa systemów teleinformatycznych organów administracji publicznej lub sieci teleinformatycznych objętych wykazem, o których mowa w art. 6r ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, a także systemów teleinformatycznych operatorów infrastruktury krytycznej, o których mowa w art. 3 pkt 3a tej ustawy, lub danych przetwarzanych w tych systemach oraz rozpoznawania, zapobiegania i wykrywania przestępstw o charakterze terrorystycznym lub przestępstwa szpiegostwa w tym obszarze oraz ścigania ich sprawców, ABW wdraża w tych podmiotach system wczesnego

---

[8)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2024 r. poz. 834, 1222, 1473, 1572 i 1907, z 2025 r. poz. 1795 oraz …

ostrzegania o zagrożeniach występujących w sieci Internet, zwany dalej „systemem ostrzegania”, prowadzi go i koordynuje jego funkcjonowanie.”.

Art. 10. W ustawie z dnia 28 marca 2003 r. o transporcie kolejowym (Dz. U. z 2025 r. poz. 1234 oraz z 2026 r. poz. 41) dodaje się art. 29g w brzmieniu:

„Art. 29g. 1. W sytuacji kryzysowej, jeżeli wymagają tego potrzeby obronności lub istotny interes bezpieczeństwa państwa, właściwy miejscowo wojewoda może, w drodze rozporządzenia porządkowego, po zasięgnięciu opinii zarządcy infrastruktury kolejowej, wprowadzić czasowe ograniczenia w dostępie do infrastruktury kolejowej, w tym całkowicie wyłączyć dostęp do infrastruktury kolejowej.

2. Rozporządzenie porządkowe w zakresie, o którym mowa w ust. 1, określa:

1) linie kolejowe, opisane zgodnie z wykazem linii kolejowych zawartym w regulaminie sieci, wraz ze wskazaniem kilometraża odcinków linii kolejowych, na których wprowadzono czasowe ograniczenia w dostępie do infrastruktury kolejowej, w tym całkowicie wyłączono dostęp do infrastruktury kolejowej;
2) rodzaj ograniczenia w dostępie do infrastruktury kolejowej, w tym wskazuje przewozy priorytetowe lub ładunki z pierwszeństwem dostępu do infrastruktury kolejowej oraz przejazdu;
3) okres, na który wprowadzono ograniczenia w dostępie do infrastruktury kolejowej, w tym całkowicie wyłączono dostęp do infrastruktury kolejowej;
4) koordynatora przewozów priorytetowych lub ładunków z pierwszeństwem dostępu do infrastruktury kolejowej oraz przejazdu na liniach kolejowych, o których mowa w pkt 1.

3. Rozporządzenie porządkowe, o którym mowa w ust. 1, może być ogłoszone w drodze obwieszczenia lub za pomocą środków komunikacji elektronicznej, lub w inny sposób zwyczajowo przyjęty na danym terenie.

4. Operatorzy obiektów infrastruktury usługowej zapewniają pierwszeństwo w obsłudze przewozom priorytetowym lub ładunkom z pierwszeństwem dostępu do infrastruktury kolejowej oraz przejazdu, w zakresie wskazanym przez koordynatora, o którym mowa w ust. 2 pkt 4.

5. Jeżeli w opinii, o której mowa w ust. 1, zarządca infrastruktury kolejowej wskazuje na konieczność wprowadzenia czasowego ograniczenia w dostępie do infrastruktury kolejowej, w tym całkowitego wyłączenia dostępu do infrastruktury kolejowej zlokalizowanej poza obszarem właściwości wojewody wydającego

rozporządzenie porządkowe, wojewoda przekazuje tę opinię pozostałym właściwym miejscowo wojewodom.”.

Art. 11. W ustawie z dnia 11 marca 2004 r. o ochronie zdrowia zwierząt oraz zwalczaniu chorób zakaźnych zwierząt (Dz. U. z 2023 r. poz. 1075 oraz z 2025 r. poz. 1795) dodaje się art. 47d–47g w brzmieniu:

„Art. 47d. 1. W przypadku nakazu odstrzału, o którym mowa w art. 46 ust. 3 pkt 8, jeżeli jest to niezbędne ze względu na rodzaj i skalę zagrożenia, minister właściwy do spraw wewnętrznych, na wniosek wojewody, może przekazać do jego dyspozycji doraźne zgrupowanie zadaniowe sformowane z policjantów, funkcjonariuszy Straży Granicznej lub funkcjonariuszy Państwowej Straży Pożarnej, którzy posiadają uprawnienia do wykonywania polowania, celem ich użycia do odstrzału sanitarnego zwierząt wolno żyjących (dzikich) na określonych obszarach.

2. Dowodzenie doraźnymi zgrupowaniami zadaniowymi, o których mowa w ust. 1, powierzane jest odpowiednio policjantowi, funkcjonariuszowi Straży Granicznej lub funkcjonariuszowi Państwowej Straży Pożarnej wskazanemu przez właściwego miejscowo komendanta odpowiednio Policji, Straży Granicznej lub Państwowej Straży Pożarnej, a w przypadku stworzenia doraźnego zgrupowania zadaniowego złożonego z policjantów, funkcjonariuszy Straży Granicznej lub funkcjonariuszy Państwowej Straży Pożarnej – policjantowi wskazanemu przez właściwego miejscowo komendanta Policji.

Art. 47e. 1. Jeżeli w sytuacji kryzysowej użycie innych sił i środków jest niemożliwe lub może okazać się niewystarczające, Minister Obrony Narodowej, na wniosek wojewody, może przekazać do jego dyspozycji doraźne zgrupowanie zadaniowe sformowane z żołnierzy, którzy posiadają uprawnienia do wykonywania polowania, celem użycia ich do odstrzału, o którym mowa w art. 46 ust. 3 pkt 8, zwierząt wolno żyjących (dzikich) na określonych obszarach.

2. Dowodzenie doraźnymi zgrupowaniami zadaniowymi, o których mowa w ust. 1, odbywa się na zasadach określonych w regulaminach wojskowych i według procedur obowiązujących w Siłach Zbrojnych Rzeczypospolitej Polskiej.

3. Użycie doraźnych zgrupowań zadaniowych w sytuacji kryzysowej nie może zagrozić zdolności Sił Zbrojnych do realizacji zadań wynikających z Konstytucji Rzeczypospolitej Polskiej i ratyfikowanych umów międzynarodowych.

Art. 47f. 1. W przypadkach, o których mowa w art. 47d i art. 47e, odpowiednio policjanci, funkcjonariusze Straży Granicznej, funkcjonariusze Państwowej Straży

Pożarnej i żołnierze używają broni myśliwskiej prywatnej lub użyczonej zgodnie z przepisami ustawy z dnia 21 maja 1999 r. o broni i amunicji (Dz. U. z 2024 r. poz. 485, z 2025 r. poz. 1795 oraz z 2026 r. poz. 187).

2. Odpowiedzialność za szkody wyrządzone przez policjantów, funkcjonariuszy Straży Granicznej, funkcjonariuszy Państwowej Straży Pożarnej i żołnierzy realizujących zadania, o których mowa w ust. 1, ponosi wojewoda.

3. W przypadkach, o których mowa w art. 47d i art. 47e:

1) nie stosuje się przepisów ustawy dotyczących ryczałtu;
2) policjanci, funkcjonariusze Straży Granicznej, funkcjonariusze Państwowej Straży Pożarnej i żołnierze współpracują z zarządcą lub dzierżawcą obwodu łowieckiego.

Art. 47g. W przypadkach, o których mowa w art. 47d i art. 47e, do obowiązków wojewody należy:

1) zapewnienie amunicji do broni, o której mowa w art. 47f ust. 1;
2) zwrot kosztów transportu, zakwaterowania i wyżywienia doraźnych zgrupowań zadaniowych; zwrot kosztów zakwaterowania lub wyżywienia nie przysługuje w przypadku zapewnienia w miejscu wykonywania czynności bezpłatnego zakwaterowania lub wyżywienia.”.

Art. 12. W ustawie z dnia 4 września 2008 r. o ochronie żeglugi i portów morskich (Dz. U. z 2024 r. poz. 597) wprowadza się następujące zmiany:

1) w art. 1 w ust. 3 w pkt 4 kropkę zastępuje się średnikiem i dodaje się punkt 5 w brzmieniu:
„5) terminalu morskiego przeładunku ropy i paliw ciekłych w Gdańsku.”;
2) w art. 24 ust. 5 otrzymuje brzmienie:
„5. W przypadku wprowadzenia poziomu ochrony 3 stosuje się odpowiednio art. 21 i art. 25 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U z 2023 r. poz. 122, z późn. zm.[9)]).”;
3) po art. 25 dodaje się art. 25a–25d w brzmieniu:
„Art. 25a. 1. W celu zapewnienia wsparcia wymiany informacji pomiędzy organami lub podmiotami realizującymi zadania w zakresie zapobiegania, ograniczania lub usuwania poważnego niebezpieczeństwa grożącego:
1) obiektom portowym i portom morskim oraz związanej z nimi infrastrukturze,

---

9) Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2024 r. poz. 834, 1222, 1473, 1572 i 1907, z 2025 r. poz. 1795 oraz …

2) obiektom, urządzeniom i instalacjom wchodzącym w skład infrastruktury zapewniającej dostęp do portów o podstawowym znaczeniu dla gospodarki narodowej,
3) zlokalizowanym na polskich obszarach morskich obiektom, urządzeniom i instalacjom wchodzącym w skład infrastruktury służącej do:
   a) wytwarzania lub przesyłania źródeł energii lub surowców energetycznych, w tym morskim farmom wiatrowym w rozumieniu art. 3 pkt 3 ustawy o promowaniu i zespołom urządzeń służącym do wyprowadzenia mocy w rozumieniu art. 3 pkt 13 ustawy o promowaniu, oraz podmorskim sieciom elektroenergetycznym i światłowodowym lub rurociągom, a także związanej z nimi infrastrukturze,
   b) telekomunikacji w rozumieniu ustawy z dnia 12 lipca 2024 r. – Prawo komunikacji elektronicznej (Dz. U. poz. 1221, z 2025 r. poz. 637 i 820 oraz z 2026 r. poz. 252 i …),
4) wykorzystywanym w wyłącznej strefie ekonomicznej sztucznym wyspom, konstrukcjom i urządzeniom przeznaczonym do gospodarczego badania i eksploatacji zasobów wyłącznej strefy ekonomicznej

– zwanych dalej „infrastrukturą morską” oraz statkom, a także zadania w zakresie ochrony granicy państwowej na morzu oraz ochrony życia lub zdrowia ludzi, mienia w znacznych rozmiarach lub środowiska zlokalizowanych na polskich obszarach morskich w rozumieniu ustawy z dnia 21 marca 1991 r. o obszarach morskich Rzeczypospolitej Polskiej i administracji morskiej, tworzy się Centrum Bezpieczeństwa Morskiego, zwane dalej „CBM”.

2. CBM umiejscowione jest we wskazanym przez Komendanta Głównego Straży Granicznej oddziale Straży Granicznej.

3. CBM kieruje wyznaczony przez Komendanta Głównego Straży Granicznej komendant oddziału Straży Granicznej lub jego zastępca, zwany dalej „Szefem CBM”.

4. Do zadań CBM należy:

1) bieżące monitorowanie zagrożeń,
2) wspieranie wymiany informacji pomiędzy organami lub podmiotami, o których mowa w art. 25b ust. 1,
3) wspieranie współpracy z właściwymi organami innych państw,

4) wspieranie procesu decyzyjnego właściwych organów lub podmiotów oraz podejmowanych przez nich działań,
5) opracowywanie raportów dotyczących zagrożeń

– w odniesieniu do żeglugi, infrastruktury morskiej, statków, granicy państwowej na morzu, życia lub zdrowia ludzi, mienia w znacznych rozmiarach lub środowiska na polskich obszarach morskich.

5. CBM realizuje zadania w systemie całodobowym przez 7 dni w tygodniu.

6. Koordynację wspólnej realizacji zadań określonych w ust. 4 zapewnia Szef CBM.

Art. 25b. 1. W ramach CBM współdziałają przedstawiciele Ministra Obrony Narodowej, Szefa Służby Kontrwywiadu Wojskowego, Szefa Agencji Bezpieczeństwa Wewnętrznego, Szefa Agencji Wywiadu, Szefa Służby Wywiadu Wojskowego, Komendanta Głównego Policji, Komendanta Głównego Państwowej Straży Pożarnej, Szefa Krajowej Administracji Skarbowej, Dyrektora Morskiej Służby Poszukiwania i Ratownictwa (Służby SAR), dyrektorów urzędów morskich oraz właściwych terytorialnie wojewodów i operatorów infrastruktury krytycznej, którzy wspólnie ze Strażą Graniczną realizują zadania określone w art. 25a ust. 4, na zasadach określonych w porozumieniu zawartym między właściwym organem lub podmiotem a Komendantem Głównym Straży Granicznej.

2. Wspólna realizacja zadań określonych w art. 25a ust. 4 w przypadku przedstawicieli:

1) Ministra Obrony Narodowej, Szefa Agencji Bezpieczeństwa Wewnętrznego, Dyrektora Morskiej Służby Poszukiwania i Ratownictwa (Służby SAR) oraz dyrektorów urzędów morskich – jest wykonywana w siedzibie CBM;
2) Szefa Agencji Wywiadu, Szefa Służby Kontrwywiadu Wojskowego, Szefa Służby Wywiadu Wojskowego, Komendanta Głównego Policji, Komendanta Głównego Państwowej Straży Pożarnej, Szefa Krajowej Administracji Skarbowej, właściwych terytorialnie wojewodów i operatorów infrastruktury krytycznej – jest wykonywana w siedzibie CBM lub w siedzibie organu lub podmiotu, którego jest przedstawicielem.

3. Komendant Główny Straży Granicznej występuje do organu lub podmiotu, o którym mowa w ust. 1, z wnioskiem o wyznaczenie przedstawicieli oraz zawarcie porozumienia.

4. Wniosek, o którym mowa w ust. 3, zawiera w szczególności:

1) zakres zadań i obowiązków oraz kwalifikacje, uprawnienia lub umiejętności wymagane do ich wykonywania;
2) wymagania w zakresie posiadania poświadczenia bezpieczeństwa upoważniającego do dostępu do informacji niejawnych i okresu jego ważności;
3) proponowany czas pracy albo służby przedstawicieli organu lub podmiotu, o którym mowa w ust. 1, z uwzględnieniem możliwości jej wykonywania w systemie zmianowym;
4) miejsce wykonywania zadań określonych w art. 25a ust. 4 przez przedstawicieli organu lub podmiotu, o którym mowa w ust. 1;
5) liczbę przedstawicieli organu lub podmiotu, o którym mowa w ust. 1, niezbędną do wykonywania zadań określonych w art. 25a ust. 4, w celu zapewnienia ciągłości działania CBM.

5. Wniosek, o którym mowa w ust. 3, może zawierać imię i nazwisko przedstawiciela, organu lub podmiotu, o którym mowa w ust. 1. Organ lub podmiot, o którym mowa w ust. 1, może odmówić wyznaczenia osoby, której dotyczy wniosek, jeżeli jest to uzasadnione potrzebami tego organu lub podmiotu.

6. Organ lub podmiot, o którym mowa w ust. 1, w terminie 7 dni od dnia otrzymania wniosku, o którym mowa w ust. 3, zawiadamia Komendanta Głównego Straży Granicznej o wyznaczonych przedstawicielach.

7. Porozumienie, o którym mowa w ust. 1, określa w szczególności:

1) datę zawarcia porozumienia;
2) miejsce wspólnego wykonywania zadań CBM;
3) imiona i nazwiska przedstawicieli;
4) stopnie przedstawicieli, w przypadku gdy są oni funkcjonariuszami albo żołnierzami;
5) numery poświadczeń bezpieczeństwa wydanych przedstawicielom, daty ich wydania i wystawcę takich poświadczeń oraz okres ważności i oznaczenie klauzuli upoważniających do przetwarzania informacji niejawnych;
6) zakres zadań i obowiązków przedstawicieli oraz sposób organizacji wykonywania tych zadań i obowiązków;
7) ustalony czas pracy albo służby;
8) osobę odpowiedzialną za organizację i koordynację wykonywanych zadań w CBM oraz monitorowanie ich realizacji.

8. W przypadku planowanej zmiany przedstawiciela organ lub podmiot, o którym mowa w ust. 1, wskazuje kolejnego przedstawiciela w celu zapewnienia ciągłości działania CBM. W takim przypadku dokonuje się zmiany zawartego porozumienia poprzez wskazanie nowego przedstawiciela.

9. Organ lub podmiot, o którym mowa w ust. 1, wypłaca swoim przedstawicielom uposażenie albo wynagrodzenie i inne świadczenia oraz należności pieniężne.

Art. 25c. 1. W szczególnie uzasadnionych przypadkach związanych z zagrożeniem wystąpienia poważnego niebezpieczeństwa, Szef CBM powołuje sztab koordynacyjny, w skład którego wchodzą przedstawiciele wyznaczeni przez organy lub podmioty, o których mowa w art. 25b ust. 1.

2. Do zadań sztabu koordynacyjnego należy dokonywanie aktualnej oceny stopnia zagrożenia infrastruktury morskiej, statków lub granicy państwowej na morzu oraz wydawania rekomendacji zmierzających do odpowiedniego zabezpieczenia tej infrastruktury, statków lub granicy.

Art. 25d. Komendant Główny Straży Granicznej, w terminie do dnia 31 marca każdego roku kalendarzowego, przedstawia ministrowi właściwemu do spraw wewnętrznych sprawozdanie z działania CBM w poprzednim roku kalendarzowym.”;

4) w art. 27 w ust. 1 po pkt 5 dodaje się pkt 6 w brzmieniu:

„6) terminalowi morskiego przeładunku ropy i paliw ciekłych w Gdańsku”;

5) po rozdziale 6 dodaje się rozdział 6a w brzmieniu:

„Rozdział 6a

Zapobieganie bezprawnemu wykonywaniu operacji z użyciem bezzałogowych obiektów pływających

Art. 28a. 1. Bezzałogowy obiekt pływający może zostać zniszczony, unieruchomiony albo może nad nim zostać przejęta kontrola, w przypadku gdy:

1) przebieg operacji lub działanie bezzałogowego obiektu pływającego:
   a) zagraża lub może zagrozić życiu lub zdrowiu ludzi lub zwierząt,
   b) stwarza lub może stworzyć zagrożenie dla chronionych obiektów, urządzeń lub obszarów,
   c) stwarza lub może stworzyć uzasadnione podejrzenie, że może zostać użyty jako środek ataku terrorystycznego,

d) stwarza lub może stworzyć zagrożenie bezpieczeństwa jednostki pływającej lub życia lub zdrowia załogi lub pasażerów znajdujących się na jej pokładzie,

e) utrudnia lub może utrudnić ruch w portach morskich lub powoduje lub może spowodować jego wstrzymanie lub ograniczenie;

2) bezzałogowy obiekt pływający wbrew zakazowi wykonuje operację na polskich obszarach morskich.

2. Do zniszczenia, unieruchomienia bezzałogowego obiektu pływającego albo przejęcia nad nim kontroli, w związku z realizacją zadań ustawowych, są uprawnieni na zasadach określonych w ustawie z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej (Dz. U. z 2026 r. poz. 244 i …) funkcjonariusze Policji, Straży Granicznej, Służby Ochrony Państwa oraz, zgodnie z zakresem właściwości miejscowej, pracownicy ochrony specjalistycznych uzbrojonych formacji ochronnych, o których 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 oraz …).

3. Do zniszczenia, unieruchomienia bezzałogowego obiektu pływającego albo przejęcia nad nim kontroli, w związku z realizacją zadań ustawowych, na terenie chronionych obiektów Sił Zbrojnych Rzeczypospolitej Polskiej oraz jednostek organizacyjnych podległych, podporządkowanych lub nadzorowanych przez Ministra Obrony Narodowej są uprawnieni na zasadach określonych w ustawie z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej żołnierze Żandarmerii Wojskowej oraz Sił Zbrojnych Rzeczypospolitej Polskiej.

4. Za szkody powstałe w wyniku zniszczenia, unieruchomienia albo przejęcia kontroli nad bezzałogowym obiektem pływającym w przypadkach, o których mowa w ust. 1, odpowiada właściciel lub operator lub armator bezzałogowego obiektu pływającego zniszczonego, unieruchomionego albo nad którym przejęto kontrolę.”.

Art. 13. W ustawie z dnia 18 marca 2010 r. o szczególnych uprawnieniach ministra właściwego do spraw aktywów państwowych oraz ich wykonywaniu w niektórych spółkach kapitałowych lub grupach kapitałowych prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych (Dz. U. z 2025 r. poz. 470) wprowadza się następujące zmiany:

1) w art. 1 ust. 1 otrzymuje brzmienie:

„1. Ustawa określa szczególne uprawnienia przysługujące ministrowi właściwemu do spraw aktywów państwowych w spółkach kapitałowych lub grupach kapitałowych,

w rozumieniu art. 3 ust. 1 pkt 44 ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2023 r. poz. 120, z późn. zm.[10)]), prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych, których mienie zostało ujawnione w wykazie, o którym mowa w art. 6r ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2023 r. poz. 122, z późn. zm.[11)]), zwanych dalej „spółkami”.”;

2) w art. 2:

a) ust. 3 otrzymuje brzmienie:

„3. Sprzeciw jest wyrażany w formie decyzji administracyjnej, w terminie 45 dni od dnia otrzymania przez ministra właściwego do spraw aktywów państwowych od pełnomocnika do spraw ochrony infrastruktury krytycznej, o którym mowa w art. 5, informacji o podjęciu przez organy spółki uchwały lub dokonaniu przez zarząd spółki czynności prawnej, o której mowa w ust. 1 i 2, jednak nie później niż w terminie 60 dni od dnia ich dokonania.”,

b) po ust. 3 dodaje się ust. 3a w brzmieniu:

„3a. Sprzeciw jest wyrażany po zasięgnięciu opinii odpowiednio ministra właściwego do spraw energii lub ministra właściwego do spraw gospodarki surowcami energetycznymi. Opinię wydaje się w terminie 10 dni od dnia otrzymania wniosku o jej wydanie. Niewyrażenie opinii w tym terminie uważa się za brak uwag.”,

c) ust. 5 otrzymuje brzmienie:

„5. W przypadku złożenia wniosku o ponowne rozpatrzenie sprawy termin na jej załatwienie wynosi 30 dni od dnia otrzymania wniosku.”,

d) w ust. 6 pkt 1 otrzymuje brzmienie:

„1) minister właściwy do spraw aktywów państwowych przekazuje skargę do właściwego sądu administracyjnego wraz z aktami sprawy i odpowiedzią na skargę w terminie 30 dni od dnia jej wniesienia przez stronę;”,

e) ust. 8 otrzymuje brzmienie:

[10)] 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.

[11)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2024 r. poz. 834, 1222, 1473, 1572 i 1907, z 2025 r. poz. 1795 oraz …

„8. W sprawach nieuregulowanych w ust. 1–7 do postępowania w sprawie sprzeciwu stosuje się przepisy ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (Dz. U. z 2025 r. poz. 1691).”;

3) w art. 4 ust. 2 otrzymuje brzmienie:

„2. Minister właściwy do spraw aktywów państwowych, po otrzymaniu od dyrektora Rządowego Centrum Bezpieczeństwa informacji o ujęciu spółki w wykazie lub wyciągu, o którym mowa w ust. 1, powiadamia spółkę o ujęciu w wykazie składników jej mienia, o których mowa w art. 1 ust. 1 i 2.”;

4) w art. 5:

a) ust. 1 otrzymuje brzmienie:

„1. Zarząd spółki, w porozumieniu z ministrem właściwym do spraw aktywów państwowych oraz dyrektorem Rządowego Centrum Bezpieczeństwa, powołuje i odwołuje pełnomocnika do spraw ochrony infrastruktury krytycznej oraz jego zastępcę, przy czym powołanie pełnomocnika następuje w terminie 30 dni, a powołanie jego zastępcy w terminie 60 dni od dnia otrzymania powiadomienia, o którym mowa w art. 4 ust. 2.”,

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

„1a. Minister właściwy do spraw aktywów państwowych niezwłocznie informuje odpowiednio ministra właściwego do spraw energii lub ministra właściwego do spraw gospodarki surowcami energetycznymi o powołaniu lub odwołaniu pełnomocnika do spraw infrastruktury krytycznej oraz jego zastępcy.”,

c) ust. 4 otrzymuje brzmienie:

„4. Pełnomocnik do spraw ochrony infrastruktury krytycznej może jednocześnie pełnić funkcję koordynatora ochrony infrastruktury krytycznej lub pełnomocnika bezpieczeństwa usługi kluczowej, o których mowa odpowiednio w art. 6zi ust. 1 i art. 6zzd ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym.”,

d) po ust. 5 dodaje się ust. 6 w brzmieniu:

„6. Do zastępcy pełnomocnika postanowienia art. 5 ust. 2–5 stosuje się odpowiednio.”;

5) w art. 6:

a) ust. 1 otrzymuje brzmienie:

„1. Zarząd spółki zobowiązany jest do przekazywania pełnomocnikowi do spraw ochrony infrastruktury krytycznej lub jego zastępcy dokumentów lub informacji o podjęciu uchwały lub o dokonaniu przez organy spółki czynności prawnych, o których mowa w art. 2 ust. 1 i 2, w terminie 3 dni od dnia ich podjęcia lub dokonania.”,

b) ust. 2 otrzymuje brzmienie:

„2. Zarząd spółki powiadamia pełnomocnika do spraw ochrony infrastruktury krytycznej lub jego zastępcę o każdym planowanym posiedzeniu dotyczącym spraw, o których mowa w art. 2 ust. 1 i 2.”,

c) w ust. 3 wstęp do wyliczenia otrzymuje brzmienie:

„3. Pełnomocnik do spraw ochrony infrastruktury krytycznej albo jego zastępca sporządza dla zarządu spółki oraz rady nadzorczej raport doraźny, okresowy, raport półroczny i roczny o stanie ochrony infrastruktury krytycznej. Raport doraźny sporządzany jest w terminie 1 dnia od zidentyfikowania zagrożenia lub wystąpienia sytuacji stwarzającej zagrożenie dla funkcjonowania, ciągłości działania oraz integralności infrastruktury krytycznej. Raport okresowy jest sporządzany co kwartał lub na żądanie zarządu spółki lub rady nadzorczej. Raport powinien zawierać informacje dotyczące ochrony infrastruktury krytycznej w zakresie:”,

d) po ust. 3 dodaje się ust. 3a w brzmieniu:

„3a. Raport roczny i półroczny zawierają informacje, o których mowa w ust. 3, poszerzone o:

1) rejestr stwierdzonych incydentów wraz z informacją o przeprowadzonych działaniach korygujących;
2) informację o przeprowadzonych kontrolach i audytach dotyczących ochrony infrastruktury krytycznej;
3) informację o posiadanych certyfikatach systemów i rozwiązań dotyczących ochrony infrastruktury krytycznej;”,

e) ust. 4 otrzymuje brzmienie:

„4. Raport doraźny oraz raport półroczny i roczny są przekazywane ministrowi właściwemu do spraw aktywów państwowych, dyrektorowi Rządowego Centrum Bezpieczeństwa oraz odpowiednio ministrowi właściwemu do spraw energii lub ministrowi właściwemu do spraw gospodarki surowcami energetycznymi. Jeżeli raporty są niepełne, zawierają nieścisłości lub nie przedstawiają dokładnie stanu

faktycznego w zakresie spraw w nim zawartych, pełnomocnik do spraw ochrony infrastruktury krytycznej lub jego zastępca jest zobowiązany, na wezwanie ministra właściwego do spraw aktywów państwowych lub dyrektora Rządowego Centrum Bezpieczeństwa, lub odpowiednio ministra właściwego do spraw energii lub ministra właściwego do spraw gospodarki surowcami energetycznymi, do uzupełnienia raportów we wskazanym zakresie i terminie.”,

f) ust. 5 otrzymuje brzmienie:

„5. Pełnomocnik do spraw ochrony infrastruktury krytycznej lub w razie jego nieobecności jego zastępca sporządza sprawozdania półroczne i roczne z wykonanych obowiązków, które składa ministrowi właściwemu do spraw aktywów państwowych, dyrektorowi Rządowego Centrum Bezpieczeństwa oraz odpowiednio ministrowi właściwemu do spraw energii lub ministrowi właściwemu do spraw gospodarki surowcami energetycznymi.”,

g) ust. 6 otrzymuje brzmienie:

„6. Pełnomocnik do spraw ochrony infrastruktury krytycznej lub w razie jego nieobecności jego zastępca, w terminie 4 dni od dnia otrzymania dokumentów lub informacji o podjęciu uchwały lub o dokonaniu przez organy spółki czynności prawnych, o których mowa w art. 2 ust. 1 i 2, przekazuje ministrowi właściwemu do spraw aktywów państwowych, dyrektorowi Rządowego Centrum Bezpieczeństwa oraz odpowiednio ministrowi właściwemu do spraw energii lub ministrowi właściwemu do spraw gospodarki surowcami energetycznymi pisemną informację w tej sprawie oraz stanowisko odnośnie do wniesienia sprzeciwu, wraz z jego uzasadnieniem. Stanowisko powinno zawierać informacje dotyczące faktów i okoliczności podjętych przez spółkę czynności prawnych, o których mowa w art. 2 ust. 1 i 2, wraz ze wskazaniem motywów podejmowanych działań i tła historycznego.”,

h) ust. 8 otrzymuje brzmienie:

„8. Prezes Rady Ministrów określi, w drodze rozporządzenia:

1) szczegółowy tryb powoływania i odwoływania pełnomocnika do spraw ochrony infrastruktury krytycznej oraz jego zastępcy,

2) sposób wykonywania obowiązku monitorowania działalności spółki w zakresie, o którym mowa w art. 2 ust. 1 i 2,

– uwzględniając konieczność efektywnego wykonywania szczególnych uprawnień ministra właściwego do spraw aktywów państwowych w spółkach kapitałowych lub grupach kapitałowych.”;

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

„Art. 7a. 1. Zarząd spółki może podlegać karze pieniężnej za nierealizowanie zadań:

1) o których mowa w art. 5 ust. 1 – w wysokości do 50 000 zł;

2) o których mowa w art. 6 ust. 1 – w wysokości do 100 000 zł;

3) o których mowa w art. 6 ust. 2 – w wysokości do 50 000 zł.

2. Jeżeli zarząd spółki uporczywie narusza przepisy ustawy, może podlegać karze w wysokości do 1 000 000 zł.

3. Kary pieniężne nakłada w drodze decyzji minister właściwy do spraw aktywów państwowych.

4. W przypadku nierealizowania przez pełnomocnika do spraw ochrony infrastruktury krytycznej, lub jego zastępcę, obowiązków wskazanych w art. 5 ust. 2, minister właściwy do spraw aktywów państwowych może uznać, że pełnomocnik przestał dawać rękojmię prawidłowego wykonywania obowiązków, o czym powiadamia zarząd spółki.

5. Zarząd spółki w terminie 30 dni od powiadomienia, o którym mowa w art. 7a ust. 4, zobowiązany jest do odwołania pełnomocnika w trybie określonym w art. 5 ust. 1 ustawy.”.

Art. 14. W ustawie z dnia 14 grudnia 2012 r. o odpadach (Dz. U. z 2023 r. poz. 1587, z późn. zm.[12)]) w art. 25 w ust. 6i pkt 2 otrzymuje brzmienie:

„2) stanowiącego element infrastruktury krytycznej ujętej w wykazie, o którym mowa w art. 6r ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2023 r. poz. 122, z późn. zm.[13)]);”.

Art. 15. W ustawie z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej (Dz. U. z 2026 r. poz. 244) wprowadza się następujące zmiany:

1) w art. 4:

a) w pkt 8 lit. b otrzymuje brzmienie:

[12)] 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, z 2025 r. poz. 1812 oraz z 2026 r. poz. 174.

[13)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2024 r. poz. 834, 1222, 1473, 1572 i 1907, z 2025 r. poz. 1795 oraz …

„b) obiekty, urządzenia, instalacje, sieci, systemy oraz usługi lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje, sieci, systemy oraz usługi ujęte w wykazie infrastruktury krytycznej, o którym mowa w art. 6r ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2023 r. poz. 122, z późn. zm.[14)]),”,

b) pkt 9 otrzymuje brzmienie:

„9) wykorzystaniu środka przymusu bezpośredniego – należy przez to rozumieć zastosowanie środka przymusu bezpośredniego:

a) wobec zwierzęcia,

b) w celu zatrzymania, zablokowania lub unieruchomienia pojazdu lub pokonania przeszkody,

c) w przypadku bezzałogowego statku powietrznego – w celu jego zniszczenia, unieruchomienia albo przejęcia kontroli nad jego lotem,

d) w przypadku bezzałogowego obiektu pływającego – w celu jego zniszczenia, unieruchomienia albo przejęcia nad nim kontroli,

e) w przypadku bezzałogowego obiektu lądowego – w celu jego zniszczenia, unieruchomienia albo przejęcia nad nim kontroli;”;

2) w art. 11 w pkt 15 kropkę zastępuje się średnikiem i dodaje się pkt 16 i 17 w brzmieniu:

„16) zniszczenia, unieruchomienia bezzałogowego obiektu pływającego albo przejęcia nad nim kontroli, w przypadkach, o których mowa w art. 28a ust. 1 ustawy z dnia 4 września 2008 r. o ochronie żeglugi i portów morskich (Dz. U. z 2024 r. poz. 597 oraz …);

17) zniszczenia, unieruchomienia bezzałogowego obiektu lądowego albo przejęcia nad nim kontroli, w przypadku gdy:

a) zagraża lub może zagrozić życiu lub zdrowiu ludzi lub zwierząt,

b) stwarza lub może stworzyć zagrożenie dla chronionych obiektów, urządzeń lub obszarów,

c) zakłóca lub może zakłócić przebieg zgromadzenia lub imprezy masowej albo zagraża bezpieczeństwu ich uczestników,

d) stwarza lub może stworzyć uzasadnione podejrzenie, że może zostać użyty jako środek ataku o charakterze terrorystycznym.”;

[14)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2024 r. poz. 834, 1222, 1473, 1572 i 1907, z 2025 r. poz. 1795 oraz …

3) w art. 12 w ust. 1 w pkt 21 kropkę zastępuje się średnikiem i dodaje się pkt 22 i 23 w brzmieniu:

„22) środki i urządzenia przeznaczone do zniszczenia, unieruchomienia bezzałogowego obiektu pływającego albo przejęcia nad nim kontroli;

23) środki i urządzenia przeznaczone do zniszczenia, unieruchomienia bezzałogowego obiektu lądowego albo przejęcia nad nim kontroli.”;

4) art. 23 otrzymuje brzmienie:

„Art. 23. 1. Pocisków niepenetracyjnych miotanych z broni palnej, broni pneumatycznej lub urządzeń do tego przeznaczonych można użyć lub wykorzystać w przypadkach, o których mowa w art. 11 pkt 2–5, 7–11, 13 i 15–17.

2. W przypadku zbiorowego zakłócenia porządku publicznego użycie pocisków niepenetracyjnych poprzedza się strzałem ostrzegawczym lub salwą ostrzegawczą w bezpiecznym kierunku, z wyjątkiem sytuacji, gdy miałoby to nastąpić w pomieszczeniach, obiektach aresztu śledczego, zakładu karnego, strzeżonego ośrodka lub aresztu dla cudzoziemców.

3. Pocisków niepenetracyjnych używa się w celu obezwładnienia osób lub wykorzystuje się w celu obezwładnienia zwierzęcia przez zadanie bólu fizycznego, przy czym nie celuje się w głowę lub szyję, oraz w celu zniszczenia albo unieruchomienia bezzałogowego statku powietrznego, bezzałogowego obiektu pływającego lub bezzałogowego obiektu lądowego.

4. Można użyć lub wykorzystać także pociski niepenetracyjne zawierające chemiczne środki obezwładniające lub barwiące.”;

5) w art. 33a dodaje się ust. 3 w brzmieniu:

„3. Środki i urządzenia przeznaczone do zniszczenia albo unieruchomienia bezzałogowego statku powietrznego albo przejęcia kontroli nad jego lotem, uniemożliwiające telekomunikację na określonym obszarze, mogą być zastosowane wyłącznie na zasadach określonych w przepisach odrębnych.”;

6) po art. 33a dodaje się art. 33b i 33c w brzmieniu:

„Art. 33b. 1. Środki i urządzenia przeznaczone do zniszczenia, unieruchomienia bezzałogowego obiektu pływającego albo przejęcia nad nim kontroli można wykorzystać w przypadku, o którym mowa w art. 11 pkt 16.

2. Zniszczenie, unieruchomienie bezzałogowego obiektu pływającego albo przejęcie nad nim kontroli może nastąpić przez wykorzystanie:

1) bezzałogowych statków powietrznych;
2) pocisków niepenetracyjnych lub innych przedmiotów miotanych za pomocą przeznaczonych do tego urządzeń oraz za pomocą broni palnej i broni pneumatycznej;
3) urządzeń emitujących skumulowaną wiązkę energii lub fal elektromagnetycznych;
4) urządzeń zakłócających działanie systemów pozycjonowania obiektu pływającego;
5) urządzeń zakłócających komunikację pomiędzy operatorem a obiektem pływającym;
6) urządzeń technicznych przymocowanych do dna morskiego i służących do ochrony fizycznej;
7) bezzałogowych obiektów pływających.

3. Środki i urządzenia przeznaczone do zniszczenia albo unieruchomienia bezzałogowego obiektu pływającego albo przejęcia nad nim kontroli, uniemożliwiające telekomunikację na określonym obszarze, mogą być zastosowane wyłącznie na zasadach określonych w przepisach odrębnych.

Art. 33c. 1. Środki i urządzenia przeznaczone do zniszczenia, unieruchomienia bezzałogowego obiektu lądowego albo przejęcia nad nim kontroli można wykorzystać w przypadku, o którym mowa w art. 11 pkt 17.

2. Zniszczenie, unieruchomienie bezzałogowego obiektu lądowego albo przejęcie nad nim kontroli może nastąpić przez wykorzystanie:

1) bezzałogowych statków powietrznych;
2) pocisków niepenetracyjnych lub innych przedmiotów miotanych za pomocą przeznaczonych do tego urządzeń oraz za pomocą broni palnej i broni pneumatycznej;
3) urządzeń emitujących skumulowaną wiązkę energii lub fal elektromagnetycznych;
4) urządzeń zakłócających działanie systemów pozycjonowania obiektu lądowego;
5) urządzeń zakłócających komunikację pomiędzy operatorem a obiektem lądowym;
6) bezzałogowych obiektów lądowych.

3. Środki i urządzenia przeznaczone do zniszczenia albo unieruchomienia bezzałogowego obiektu lądowego albo przejęcia nad nim kontroli, uniemożliwiające telekomunikację na określonym obszarze, mogą być zastosowane wyłącznie na zasadach określonych w przepisach odrębnych.”;

7) w art. 47 w pkt 7 kropkę zastępuje się średnikiem i dodaje się pkt 8 w brzmieniu:

„8) zniszczenia lub unieruchomienia bezzałogowego obiektu lądowego, w przypadkach, o których mowa w art. 11 pkt 17.”.

Art. 16. W ustawie z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (Dz. U. z 2025 r. poz. 194) wprowadza się następujące zmiany:

1) w art. 2 uchyla się pkt 3;

2) art. 4 otrzymuje brzmienie:

„Art. 4. 1. Organy administracji publicznej lub operatorzy infrastruktury krytycznej współpracują z organami, służbami i instytucjami właściwymi w sprawach bezpieczeństwa i zarządzania kryzysowego przy realizacji działań antyterrorystycznych.

2. Organy i podmioty, o których mowa w ust. 1, przekazują niezwłocznie Szefowi ABW będące w ich posiadaniu informacje dotyczące zagrożeń o charakterze terrorystycznym, w tym zagrożeń dla funkcjonowania systemów i sieci energetycznych, wodno-kanalizacyjnych, ciepłowniczych oraz teleinformatycznych istotnych z punktu widzenia bezpieczeństwa państwa.

3. W przypadku powzięcia informacji o możliwości wystąpienia zdarzenia o charakterze terrorystycznym zagrażającego infrastrukturze krytycznej, życiu lub zdrowiu ludzi, mieniu w znacznych rozmiarach, dziedzictwu narodowemu lub środowisku, Szef ABW może wydawać polecenia organom i podmiotom, o których mowa w ust. 1, z wyłączeniem podmiotów, o których mowa w art. 7, zagrożonym tymi zdarzeniami, mające na celu przeciwdziałanie zagrożeniom, ich usunięcie albo minimalizację, oraz przekazywać im informacje niezbędne do tego celu. Organy i podmioty, o których mowa w zdaniu pierwszym, informują Szefa ABW o podjętych działaniach w tym zakresie.

4. Szef ABW o podjętych działaniach, o których mowa w ust. 3, informuje niezwłocznie Ministra Koordynatora Służb Specjalnych, jeżeli został powołany.”;

3) w art. 12:

a) w ust. 1 pkt 1 i 2 otrzymują brzmienie:

„1) Policja – w obiektach infrastruktury krytycznej wskazanych przez Komendanta Głównego Policji w uzgodnieniu z Szefem ABW;

2) Żandarmeria Wojskowa – w obiektach stanowiących siedzibę urzędu obsługującego Ministra Obrony Narodowej oraz w obiektach należących do komórek i jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych albo administrowanych przez te

komórki i jednostki organizacyjne wskazanych przez Ministra Obrony Narodowej w uzgodnieniu z Szefem SKW.”,

b) po ust. 2 dodaje się ust. 3 w brzmieniu:

„3. Komendant Główny Policji i Szef ABW określą, w drodze porozumienia, tryb wskazywania obiektów infrastruktury krytycznej, o których mowa w ust. 1 pkt 1.”;

4) w art. 15 w ust. 9 wyraz „zadania” zastępuje się wyrazem „przedsięwzięcia”;

5) w art. 16 w ust. 1 pkt 4 otrzymuje brzmienie:

„4) dla określonych obiektów jednostek organizacyjnych administracji publicznej, prokuratury, sądów lub obiektów infrastruktury krytycznej;”;

6) w art. 17:

a) ust. 1 otrzymuje brzmienie:

„1. W przypadku wprowadzenia pierwszego lub drugiego stopnia alarmowego lub pierwszego lub drugiego stopnia alarmowego CRP w trybie art. 16 ust. 1, Szef ABW może powołać sztab koordynacyjny, w skład którego wchodzą przedstawiciele wyznaczeni przez podmioty, o których mowa w art. 5 ust. 1.”,

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

„1a. W przypadku wprowadzenia trzeciego lub czwartego stopnia alarmowego lub trzeciego lub czwartego stopnia alarmowego CRP, w trybie art. 16 ust. 1, Szef ABW powołuje sztab koordynacyjny, o którym mowa w ust. 1.”,

c) ust. 3 otrzymuje brzmienie:

„3. Do zadań sztabu koordynacyjnego należy:

1) rekomendowanie zmiany lub odwołania stopnia alarmowego lub stopnia alarmowego CRP;

2) dokonywanie oceny stopnia zagrożenia infrastruktury krytycznej zlokalizowanej na obszarze objętym obowiązywaniem stopnia alarmowego lub stopnia alarmowego CRP oraz wydawanie rekomendacji zmierzających do jej odpowiedniego zabezpieczenia;

3) rekomendowanie form i zakresu współdziałania podmiotów wchodzących w skład sztabu koordynacyjnego i biorących udział w jego pracach.”.

Art. 17. W ustawie z dnia 20 lipca 2017 r. – Prawo wodne (Dz. U. z 2025 r. poz. 960 i 1535) w art. 240 w ust. 3 pkt 24 otrzymuje brzmienie:

„24) współdziałają z wojewodami w zakresie opracowywania wojewódzkiego planu zarządzania ryzykiem oraz wojewódzkiego planu reagowania kryzysowego;”.

Art. 18. W ustawie z dnia 8 grudnia 2017 r. o Służbie Ochrony Państwa (Dz. U. z 2025 r. poz. 34, z późń. zm.[15)]) wprowadza się następujące zmiany:

1) w art. 37 ust. 1 i 2 otrzymują brzmienie:

„1. W przypadkach, o których mowa w art. 11 pkt 1–6 i 9–16 ustawy z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej (Dz. U. z 2026 r. poz. 244 i …), funkcjonariusz może użyć środków przymusu bezpośredniego, o których mowa w art. 12 ust. 1 pkt 1, pkt 2 lit. a, pkt 5, 7, 9, 11, pkt 12 lit. a, c i d, pkt 13 i 17–23 tej ustawy, lub wykorzystać te środki.

2. W przypadkach, o których mowa w art. 45 pkt 1 lit. a–c i e, pkt 2 i pkt 3 lit. a, z wyłączeniem pościgu za osobą, o której mowa w art. 45 pkt 1 lit. d, oraz w art. 47 pkt 1, pkt 2 lit. a i pkt 3–8 ustawy z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej, funkcjonariusz może użyć broni palnej lub ją wykorzystać.”;

2) w art. 39 ust. 1 otrzymuje brzmienie:

„1. Komendant SOP:

1) w celu realizacji zadań, o których mowa w art. 3 pkt 1, lub

2) w przypadkach, o których mowa:

a) w art. 156ze ust. 1 ustawy z dnia 3 lipca 2002 r. – Prawo lotnicze (Dz. U. z 2025 r. poz. 1431 i 1668 oraz z 2026 r. poz. 176), lub

b) w art. 28a ust. 1 ustawy z dnia 4 września 2008 r. o ochronie żeglugi i portów morskich (Dz. U. z 2024 r. poz. 597 oraz …), lub

c) w art. 11 pkt 17 ustawy z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej

– może podjąć decyzję o dopuszczalności zastosowania urządzeń uniemożliwiających telekomunikację na określonym obszarze przez czas niezbędny do wykonywania czynności przez SOP, z uwzględnieniem konieczności minimalizacji skutków braku możliwości korzystania z usług telekomunikacyjnych.”;

3) w art. 98 dodaje się ust. 3 w brzmieniu:

[15)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2024 r. poz. 1871 oraz z 2025 r. poz. 179, 718 i 1366 i 1823.

„3. W przypadku funkcjonariusza oddelegowanego do wykonywania zadań służbowych w urzędzie obsługującym ministra właściwego do spraw wewnętrznych albo w jednostce podległej lub nadzorowanej przez ministra właściwego do spraw wewnętrznych, należności, o których mowa w ust. 1, wypłaca komórka organizacyjna SOP właściwa w sprawach finansowych w uzgodnieniu z kierownikiem urzędu albo jednostki, do której funkcjonariusz został oddelegowany.”.

Art. 19. W ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2026 r. poz. 20 i 252) wprowadza się następujące zmiany:

1) w art. 10 w ust. 4 wyrazy „właścicielem, posiadaczem samoistnym albo posiadaczem zależnym obiektów, instalacji, urządzeń lub usług wchodzących w skład infrastruktury krytycznej, wymienionych w 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 oraz z 2024 r. poz. 834)” zastępuje się wyrazami „operatorem infrastruktury krytycznej, o którym mowa w art. 3 pkt 3a ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2023 r. poz. 122, z późn. zm.[16])”;
2) w art. 15 w ust. 7 w pkt 2 wyrazy „właścicielem, posiadaczem samoistnym albo posiadaczem zależnym obiektów, instalacji, urządzeń lub usług wchodzących w skład infrastruktury krytycznej, wymienionych w wykazie, o którym mowa w art. 5b ust. 7 pkt 1” zastępuje się wyrazami „operatorem infrastruktury krytycznej, o którym mowa w art. 3 pkt 3a”;
3) w art. 26:
   a) w ust. 2 wyrazy „właścicieli, posiadaczy samoistnych albo posiadaczy zależnych obiektów, instalacji, urządzeń lub usług wchodzących w skład infrastruktury krytycznej, wymienionych w wykazie, o którym mowa w art. 5b ust. 7 pkt 1” zastępuje się wyrazami „operatorów infrastruktury krytycznej, o których mowa w art. 3 pkt 3a”,
   b) w ust. 5 pkt 1 otrzymuje brzmienie:
      „1) podmioty podległe Ministrowi Obrony Narodowej lub przez niego nadzorowane, w tym podmioty, których systemy teleinformatyczne lub sieci

[16] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2024 r. poz. 834, 1222, 1473, 1572 i 1907, z 2025 r. poz. 1795 oraz …

teleinformatyczne objęte są wykazem, o których mowa w art. 6r ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym;”,

c) w ust. 7 pkt 5 i 6 otrzymują brzmienie:

„5) inne niż wymienione w pkt 1–4 oraz w ust. 5 podmioty, których systemy teleinformatyczne lub sieci teleinformatyczne objęte są wykazem, o którym mowa w art. 6i ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym;

6) podmioty, o których mowa w ust. 6, jeżeli incydent dotyczy systemów teleinformatycznych lub sieci teleinformatycznych objętych wykazami, o których mowa w art. 6i ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym.”,

d) w art. 46 po ust. 1 dodaje się ust. 1a w brzmieniu:

„1a. System, o którym mowa w ust. 1, zapewnia wymianę informacji między organami do spraw podmiotów krytycznych, o których mowa w art. 6v ustawy z dnia 27 kwietnia 2007 r. o zarządzaniu kryzysowym, dyrektorem Rządowego Centrum Bezpieczeństwa a podmiotami krytycznymi, o których mowa w art. 3 pkt 1a tej ustawy.”.

Art. 20. W ustawie z dnia 17 grudnia 2020 r. o rezerwach strategicznych (Dz. U. z 2024 r. poz. 1598 i 1907 oraz z 2026 r. poz. 203) wprowadza się następujące zmiany:

1) w art. 2:

a) pkt 1 otrzymuje brzmienie:

„1) infrastruktura krytyczna – infrastrukturę, o której mowa w art. 3 pkt 2 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2023 r. poz. 122, z późn. zm.[17)]);”,

b) po pkt 1 dodaje się pkt 1a i 1b w brzmieniu:

„1a) podmiot krytyczny – podmiot, o którym mowa w art. 3 pkt 1a ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym;

1b) usługa kluczowa – usługa, o której mowa w art. 3 pkt 1d ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym;”,

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

[17)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2024 r. poz. 834, 1222, 1473, 1572 i 1907, z 2025 r. poz. 1795 oraz …

„4a) wirtualne środowisko informatyczne – wydzielona przestrzeń wielosystemowa oparta o ograniczone zasoby fizyczne;”;

2) art. 4 otrzymuje brzmienie:

„Art. 4. Rezerwy strategiczne mogą stanowić surowce, materiały, urządzenia, maszyny, konstrukcje, elementy infrastruktury krytycznej, moc produkcyjna, moc usługowa, wirtualne środowisko informatyczne, fizyczne i wirtualne zasoby teleinformatyczne, produkty naftowe, produkty rolne i rolno-spożywcze, środki spożywcze i ich składniki, wyroby medyczne, produkty lecznicze, produkty lecznicze weterynaryjne oraz substancje czynne w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne (Dz. U. z 2025 r. poz. 750, z późn. zm.[18)]), materiały wybuchowe, broń, amunicja oraz ich istotne części, ładunki miotające oraz wyroby i technologie o przeznaczeniu wojskowym lub policyjnym w rozumieniu ustawy z dnia 13 czerwca 2019 r. o wykonywaniu działalności gospodarczej w zakresie wytwarzania i obrotu materiałami wybuchowymi, bronią, amunicją oraz wyrobami i technologią o przeznaczeniu wojskowym lub policyjnym (Dz. U. z 2023 r. poz. 1743), produkty biobójcze, a także inne produkty – niezbędne do realizacji celów, o których mowa w art. 3.”;

3) w art. 5 dotychczasową treść oznacza się jako ust. 2 i dodaje się ust. 1 w brzmieniu:

„Art. 5. 1. Agencja w imieniu własnym dokonuje zakupu asortymentu, o którym mowa w art. 4, z przeznaczeniem do rezerw strategicznych oraz zawiera umowy, o których mowa w art. 17 i art. 18, w celu utworzenia rezerw strategicznych.”;

4) art. 7 otrzymuje brzmienie:

„Art. 7. Do decyzji wydawanych przez ministra właściwego do spraw wewnętrznych w zakresie rezerw strategicznych oraz decyzji, o której mowa w art. 32 ust. 1, a także do decyzji wydawanych przez organy i podmioty, o których mowa w art. 8 ust. 2, w przypadku, o którym mowa w art. 29, nie stosuje się przepisów ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (Dz. U. z 2025 r. poz. 1691).”;

5) w art. 8:

a) w ust. 2 pkt 5 otrzymuje brzmienie:

„5) minister właściwy do spraw gospodarki surowcami energetycznymi;”,

---

[18)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2025 r. poz. 905, 924, 1416, 1537 i 1795.

b) w ust. 4 pkt 1–3 otrzymują brzmienie:

„1) ocenę ryzyka zidentyfikowanych zagrożeń, uwzględniającą sposoby i środki reagowania na te zagrożenia, zawartą w opracowanych planach zarządzania kryzysowego, o których mowa w art. 2 pkt 16 ustawy o zarządzaniu kryzysowym;

2) wnioski wynikające z wykonania postanowień Strategii Oporności Podmiotów Krytycznych, o której mowa w art. 6f ustawy o zarządzaniu kryzysowym, w zakresie sprawowania nadzoru nad infrastrukturą krytyczną oraz podmiotami krytycznymi zapewniającymi świadczenie usług kluczowych;

3) wykazy potrzeb wynikających z oceny ryzyka, dotyczących utworzenia rezerw strategicznych w danym asortymencie i ilości, w podziale na poszczególne lata wraz z uzasadnieniem;”;

6) w art. 9 w ust. 1 pkt 1 i 2 otrzymują brzmienie:

„1) wnioski dotyczące tworzenia, utrzymywania i likwidacji rezerw wynikające z oceny ryzyka zidentyfikowanych zagrożeń zawartej w Krajowej Ocenie Ryzyka, o której mowa w art. 6e ustawy o zarządzaniu kryzysowym, oraz wnioski, o których mowa w art. 8 ust. 4 pkt 2;

2) dane dotyczące asortymentów rezerw strategicznych i ich ilości, jakie należy utworzyć w poszczególnych latach wraz z uzasadnieniem;”;

7) w art. 10:

a) ust. 2 otrzymuje brzmienie:

„2. Minister właściwy do spraw wewnętrznych, po przyjęciu Programu przez Radę Ministrów, niezwłocznie przekazuje:

1) Program – Agencji i organom, o których mowa w art. 8 ust. 2 pkt 1–3;

2) wyciąg z Programu, zawierający informacje o rodzaju i ilości rezerw strategicznych ujętych w Programie, z podziałem na poszczególne lata – organom i podmiotom, o których mowa w art. 8 ust. 2 pkt 4–22.”,

b) dodaje się ust. 3 w brzmieniu:

„3. Przepis ust. 2 stosuje się odpowiednio w przypadku aktualizacji Programu.”;

8) w art. 11 w ust. 2 w pkt 1 lit. a i b otrzymują brzmienie:

„a) zakupu asortymentu w celu utworzenia rezerw strategicznych oraz odtworzenia udostępnionych rezerw strategicznych,

b) utrzymywania i przechowywania rezerw strategicznych, w tym ich zamiany, wymiany i konserwacji,”;

9) w art. 12 ust. 1 otrzymuje brzmienie:

„1. W budżecie państwa tworzy się rezerwę celową z przeznaczeniem na finansowanie działań ministra właściwego do spraw wewnętrznych w sytuacjach zagrożeń, o których mowa w art. 3, na skutek zdarzeń, których nie można było przewidzieć ani im przeciwdziałać, w szczególności na finansowanie kosztów:

1) udostępnienia rezerw strategicznych, w tym wydawania, przetransportowania i dystrybucji udostępnionych rezerw strategicznych do ostatecznych odbiorców;
2) innych usług niezbędnych do udostępnienia rezerw strategicznych ostatecznym odbiorcom;
3) przetworzenia i przetrzymania udostępnionych rezerw strategicznych, jeżeli jest to konieczne;
4) zakupu danego asortymentu rezerw lub usług w ramach udostępnienia rezerw utrzymywanych na podstawie umów, o których mowa w art. 17 i art. 18;
5) niezbędnych czynności Agencji i organów, na których rzecz rezerwy strategiczne udostępniono, oraz podmiotów, którym je wydano, w zakresie organizacji i realizacji udostępnienia rezerw strategicznych, na zasadach określonych w ustawie;
6) utworzenia i utrzymywania rezerw strategicznych nieobjętych Programem, o których mowa w art. 14;
7) odtworzenia udostępnionych rezerw strategicznych objętych Programem, o których mowa w art. 13;
8) realizacji zadań, o których mowa w art. 32.”;

10) w art. 13:

a) ust. 2 otrzymuje brzmienie:

„2. Decyzja o utworzeniu rezerw strategicznych określa w szczególności:

1) sposób utworzenia rezerw strategicznych przez Agencję;
2) rodzaj i ilość asortymentu rezerw strategicznych.”,

b) ust. 4 otrzymuje brzmienie:

„4. Wykonując decyzję o utworzeniu rezerw strategicznych, Agencja:

1) dokonuje nabycia określonej ilości asortymentu rezerw strategicznych;
2) przechowuje zakupiony asortyment rezerw strategicznych;

3) zawiera umowy, o których mowa w art. 17 lub w art. 18;

4) może przyjąć określony asortyment w formie darowizny z przeznaczeniem do rezerw strategicznych.”,

c) ust. 5 otrzymuje brzmienie:

„5. W przypadkach, w których nie mają zastosowania przepisy o zamówieniach publicznych, Agencja, dokonując zakupu asortymentu rezerw strategicznych lub usług związanych z utrzymywaniem rezerw strategicznych, lub zawierając umowy, o których mowa w art. 17 i art. 18, stosuje przejrzyste, niedyskryminacyjne i konkurencyjne warunki wyłaniania sprzedawcy tego asortymentu, usługi lub podmiotu, z którym zostanie zawarta umowa, o której mowa w art. 17 i art. 18, w szczególności:

1) przesyła zapytania ofertowe do podmiotów wykonujących działalność gospodarczą w zakresie produkcji, handlu, świadczenia określonych usług, w tym przechowywania, oraz dysponujących odpowiednią bazą magazynową i gwarantujących odpowiednią jakość poszukiwanego asortymentu rezerw strategicznych, a także zapewniających ochronę informacji niejawnych, zgodnie z odrębnymi przepisami;

2) zaprasza do negocjacji podmioty oferujące najkorzystniejsze ekonomicznie warunki sprzedaży, świadczenia usług i przechowywania asortymentu rezerw strategicznych, biorąc pod uwagę relację ceny do jakości;

3) przeprowadza negocjacje cenowe z uwzględnieniem cen rynkowych w zakresie zakupu określonej ilości asortymentu rezerw strategicznych lub zakupu określonych usług.”;

11) w art. 14 dodaje się ust. 3 w brzmieniu:

„3. Do decyzji, o której mowa w ust. 1, przepisy art. 13 ust. 2–6 stosuje się odpowiednio.”;

12) w art. 17 w ust. 2 pkt 1–3 otrzymują brzmienie:

„1) wysokość wynagrodzenia za utrzymywanie rezerw z możliwością ich zakupu lub najmu na rzecz Agencji;

2) zobowiązanie podmiotu, z którym zawarto umowę, do stałej gotowości sprzedaży lub najmu na rzecz Agencji asortymentu przechowywanych rezerw;

3) tryb i warunki, w tym cenę sprzedaży asortymentu będącego przedmiotem umowy na rzecz Agencji lub wysokość czynszu najmu tego asortymentu, do którego

uiszczenia będzie zobowiązana Agencja w przypadku wydania, przez upoważniony organ, decyzji o udostępnieniu rezerw strategicznych.”;

13) w art. 19:

a) w ust. 5:

– pkt 4 i 5 otrzymują brzmienie:

„4) wskazanie czy udostępnienie rezerw strategicznych następuje bez obowiązku zwrotu, z obowiązkiem zwrotu lub z obowiązkiem zwrotu niewykorzystanej części udostępnionych rezerw strategicznych;

5) inne szczególne warunki udostępnienia rezerw strategicznych, w tym w szczególności dotyczące obowiązku przetransportowania rezerw, montażu, zainstalowania lub ich przetworzenia lub obowiązku pokrycia kosztów przeglądów, demontażu, jeżeli jest to konieczne ze względu na właściwości udostępnionego asortymentu rezerw strategicznych lub jest uzasadnione innymi względami;”,

– dodaje się pkt 6 i 7 w brzmieniu:

„6) określenie, czy udostępnione bez obowiązku zwrotu rezerwy strategiczne podlegają odtworzeniu wraz ze wskazaniem ilości oraz źródeł finansowania;

7) określenie źródła finansowania kosztów udostępnienia.”,

b) dodaje się ust. 9–11 w brzmieniu:

„9. W przypadku wydania decyzji o udostępnieniu rezerw strategicznych bez obowiązku zwrotu własność asortymentu rezerw strategicznych przechodzi na organ lub podmiot, któremu rezerwy strategiczne zostały wydane z chwilą jego wydania.

10. W przypadku wydania decyzji o udostępnieniu rezerw strategicznych z obowiązkiem zwrotu utrzymanie wydanych rezerw strategicznych w należytym stanie, w tym dokonywanie wymaganych przeglądów, konserwacji i napraw, obciąża, podmiot lub organ, któremu rezerwy strategiczne zostały wydane.

11. Do zakupu usług transportowych oraz innych usług logistycznych związanych z wykonaniem decyzji o udostępnieniu rezerw strategicznych nie stosuje się przepisów ustawy z dnia 11 września 2019 r. – Prawo zamówień

publicznych (Dz. U. z 2024 r. poz. 1320, z późn. zm.[19)]), jeżeli wartość zamówienia jest mniejsza niż progi unijne, o których mowa art. 3 ust. 1 tej ustawy.”;

14) w art. 20 w ust. 2 pkt 6 otrzymuje brzmienie:

„6) zwraca Agencji niewykorzystaną część udostępnionych rezerw strategicznych, jeżeli zostały udostępnione z obowiązkiem zwrotu niewykorzystanej części;”;

15) w art. 21:

a) ust. 1 otrzymuje brzmienie:

„1. Minister właściwy do spraw wewnętrznych może, w drodze decyzji, udostępnić określony specjalistyczny asortyment techniczny rezerw strategicznych, mając na względzie potrzebę przeciwdziałania lub usuwania skutków klęski żywiołowej lub sytuacji kryzysowej lub wsparcia realizacji celów społecznych lub przedsięwzięć gospodarczych, w szczególności związanych z odtworzeniem, budową, modernizacją lub remontem infrastruktury. Przepisy art. 19 ust. 2 i 4 oraz ust. 5 pkt 1–3 stosuje się odpowiednio.”,

b) ust. 3 otrzymuje brzmienie:

„3. Udostępnienie specjalistycznego asortymentu technicznego rezerw strategicznych jest dokonywane nieodpłatnie na rzecz państwowych jednostek organizacyjnych, jednostek samorządu terytorialnego lub utworzonych przez nie jednostek organizacyjnych w przypadku wystąpienia klęski żywiołowej lub sytuacji kryzysowej lub w celu zaspokojenia potrzeb społecznych lub gospodarczych, w szczególności związanych z odtworzeniem, budową, modernizacją lub remontem infrastruktury.”;

16) art. 22 otrzymuje brzmienie:

„Art. 22. 1. Agencja może odpłatnie udostępnić określony specjalistyczny asortyment techniczny rezerw strategicznych na rzecz jednostek samorządu terytorialnego, utworzonych przez nie jednostek organizacyjnych, służb, inspekcji lub innych jednostek, o których mowa w art. 8 ust. 2 pkt 22, oraz na rzecz przedsiębiorców mając na względzie potrzebę wsparcia w realizacji celów społecznych lub przedsięwzięć gospodarczych.

2. Udostępnienie specjalistycznego asortymentu technicznego rezerw strategicznych jest dokonywane na wniosek podmiotów określonych w ust. 1.

[19)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2025 r. poz. 620, 769, 794, 1165, 1173 i 1235 oraz z 2026 r. poz. 252.

3. Specjalistyczny asortyment techniczny rezerw strategicznych, o którym mowa w ust. 1, jest udostępniany na podstawie umowy zawartej na czas oznaczony między Agencją a podmiotem, o którym mowa w ust. 1.

4. Umowa, o której mowa w ust. 3, określa w szczególności warunki udostępnienia specjalistycznego asortymentu technicznego rezerw strategicznych oraz jego zwrotu.”;

17) w art. 23 ust. 5 otrzymuje brzmienie:

„5. Umowa, o której mowa w ust. 4, określa w szczególności warunki udostępnienia specjalistycznego asortymentu medycznego rezerw strategicznych oraz jego zwrotu.”;

18) po art. 23 dodaje się art. 23a w brzmieniu:

„Art. 23a. 1. Minister właściwy do spraw wewnętrznych może, w drodze decyzji, udostępnić wirtualne środowisko informatyczne oraz fizyczne lub wirtualne zasoby informatyczne, mając na względzie potrzebę wsparcia realizacji celów związanych z cyberbezpieczeństwem państwa oraz konieczność odtworzenia zasobów cyfrowych. Przepisy art. 19 ust. 2 i 4 oraz ust. 5 pkt 1–3 stosuje się odpowiednio.

2. Decyzję, o której mowa w ust. 1, wykonuje Agencja.

3. Udostępnienie, o którym mowa w ust. 1, jest dokonywane odpłatnie na rzecz państwowych jednostek organizacyjnych, jednostek samorządu terytorialnego lub utworzonych przez nie jednostek organizacyjnych w przypadku wystąpienia zagrożenia cyberbezpieczeństwa państwa lub konieczności odtworzenia zasobów cyfrowych.

4. Wirtualne środowisko informatyczne oraz fizyczne lub wirtualne zasoby informatyczne są udostępniane na podstawie umowy zawartej na czas oznaczony pomiędzy Agencją a podmiotem, o którym mowa w ust. 3.

5. Umowa, o której mowa w ust. 4, w szczególności warunki udostępnienia asortymentu określonego w ust. 1 oraz jego zwrotu.”;

19) art. 24 otrzymuje brzmienie:

„Art. 24. Minister właściwy do spraw wewnętrznych określi, w drodze rozporządzenia, szczegółową procedurę udostępnienia rezerw strategicznych, w tym czasowego, zwrotnego udostępnienia specjalistycznego asortymentu technicznego rezerw strategicznych oraz specjalistycznego asortymentu medycznego rezerw strategicznych, procedurę zwrotu asortymentu rezerw strategicznych, oraz szczegółowe czynności przy udostępnieniu lub wydaniu rezerw strategicznych, uwzględniając konieczność zapewnienia prawidłowej i efektywnej realizacji zadań Agencji.”;

20) w art. 27a w ust. 1 wprowadzenie do wyliczenia otrzymuje brzmienie:

„1. Minister właściwy do spraw wewnętrznych może zlikwidować, w drodze decyzji, określony asortyment rezerw strategicznych, ze względu na konieczność:”;

21) uchyla się art. 28;

22) art. 29:

a) ust. 2 otrzymuje brzmienie:

„2. W przypadkach, o których mowa w ust. 1, organ lub podmiot powierzający Agencji określone zadanie wskazuje rodzaj i ilość asortymentu, zakres jego przechowania, w tym czas tego przechowania, oraz organy lub podmioty, którym dany asortyment zostanie wydany oraz warunki wydania, a także określa wysokość środków finansowych przeznaczonych na finansowanie zadania.”,

b) po ust. 3 dodaje się ust. 3a i 3b w brzmieniu:

„3a. Środki finansowe na realizację powierzonego zadania oraz na pokrycie kosztów, o których mowa w ust. 3, organ lub podmiot powierzający Agencji określone zadanie przekazuje Agencji na podstawie zawartego z nią porozumienia.

3b. Środki finansowe, o których mowa w ust. 3a, nie stanowią przychodu Agencji, a ich przekazanie nie wymaga dokonywania zmian w planie finansowym Agencji.”;

23) po art. 29 dodaje się art. 29a w brzmieniu:

„Art. 29a. 1. Agencja, za zgodą ministra właściwego do spraw wewnętrznych, może wykonywać zadania związane z:

1) przeciwdziałaniem wystąpieniu zagrożenia bezpieczeństwa i obronności państwa, porządku i zdrowia publicznego, klęski żywiołowej lub sytuacji kryzysowej;

2) udzielaniem pomocy humanitarnej ludności znajdującej się w sytuacji zagrożenia życia lub zdrowia

– na podstawie przepisów prawa międzynarodowego publicznego, procedur organizacji międzynarodowych oraz porozumień tworzących wiążące zobowiązanie wobec Agencji.

2. Agencja może realizować zadania, o których mowa w ust. 1, po zapewnieniu środków finansowych na ich realizację, w tym na pokrycie wydatków niekwalifikowanych, zgodnie z ustawą o finansach publicznych.”;

24) w art. 31:

a) w ust. 1:

– pkt 3 otrzymuje brzmienie:

„3) wykonywanie decyzji organów lub podmiotów, o których mowa w art. 8 ust. 2, dotyczących zakupu, przechowywania, dystrybucji i wydawania określonych asortymentów towarów zgodnie z zasadami określonymi w rozdziale 6;”,

– po pkt 8 dodaje się pkt 8a w brzmieniu:

„8a) wykonywanie zadań, o których mowa w art. 29a ust. 1;”,

– pkt 10 i 11 otrzymują brzmienie:

„10) opracowywanie informacji o asortymencie rezerw strategicznych, ilości i wartości rezerw strategicznych oraz ich finansowaniu, wykorzystaniu i rozmieszczeniu, w terminach do dnia 15 września każdego roku za I półrocze i do dnia 31 marca każdego roku za rok poprzedni;

11) przekazywanie Ministrowi Obrony Narodowej, ministrowi właściwemu do spraw transportu, ministrowi właściwemu do spraw wewnętrznych i Szefowi Agencji Bezpieczeństwa Wewnętrznego informacji o ilości i rozmieszczeniu rezerw strategicznych, ujętych w Programie w terminach do dnia 15 września każdego roku za I półrocze i do dnia 31 marca każdego roku za rok poprzedni;”,

– w pkt 13 kropkę zastępuje się średnikiem i dodaje się pkt 14 w brzmieniu:

„14) prowadzenie działalności informacyjnej, promocyjnej i edukacyjnej w zakresie zadań Agencji.”,

b) ust. 2 otrzymuje brzmienie:

„2. Do czynności realizowanych przez Agencję w ramach zadań, o których mowa w ust. 1 pkt 5, nie stosuje się przepisów art. 38–41 ustawy z dnia 16 grudnia 2016 r. o zasadach zarządzania mieniem państwowym (Dz. U. z 2024 r. poz. 125, z późn. zm.[20)]).”;

25) art. 32 otrzymuje brzmienie:

„Art. 32. 1. Minister właściwy do spraw wewnętrznych może powierzyć Agencji, w drodze decyzji, realizację innych zadań niż określone w art. 31, na terytorium Rzeczypospolitej Polskiej lub w porozumieniu z ministrem właściwym do spraw zagranicznych poza jej granicami, związanych z:

[20)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2024 r. poz. 834, 1823, 1897 i 1940 praz z 2026 r. poz. 160.

1) wystąpieniem zagrożenia bezpieczeństwa i obronności państwa, porządku i zdrowia publicznego, klęski żywiołowej lub sytuacji kryzysowej;
2) wypełnieniem zobowiązania międzynarodowego albo udzieleniem pomocy lub wsparcia:
   a) podmiotowi prawa międzynarodowego publicznego,
   b) podmiotowi krajowemu, zagranicznemu lub międzynarodowemu podejmującemu działania w zakresie niesienia pomocy humanitarnej lub usuwania skutków sytuacji kryzysowej

– w szczególności w przypadkach określonych w pkt 1.

2. Realizując zadania, o których mowa w ust. 1, Agencja jest uprawniona w szczególności do:

1) nabywania, zbywania, transportowania, przechowywania, wydawania oraz do wywozu poza terytorium Rzeczypospolitej Polskiej i przywozu z terytorium innego państwa określonego asortymentu;
2) nabywania oraz świadczenia usług, w szczególności usług o charakterze logistycznym, transportowym i magazynowym, na terytorium Rzeczypospolitej Polskiej lub poza jej granicami;
3) zlecania wykonania robót budowlanych oraz usług związanych z ich wykonaniem;
4) przyjmowania i przekazywania darowizn.

3. Powierzając zadania, o których mowa w ust. 1, minister właściwy do spraw wewnętrznych zapewnia Agencji na ten cel odpowiednie środki finansowe.

4. Wydając decyzję, o której mowa w ust. 1, minister właściwy do spraw wewnętrznych może nadać jej rygor natychmiastowej wykonalności. Decyzja nie wymaga uzasadnienia.

5. Do udzielania zamówień niezbędnych do realizacji decyzji, o której mowa w ust. 1, nie stosuje się przepisów ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych, jeżeli wartość zamówienia jest mniejsza niż progi unijne, o których mowa art. 3 ust. 1 tej ustawy.

6. Agencja, w terminie 30 dni od dnia udzielenia zamówienia, o którym mowa w ust. 5, zamieszcza w Biuletynie Zamówień Publicznych informację o udzieleniu tego zamówienia, w której podaje:

1) datę i miejsce zawarcia umowy lub informację o zawarciu umowy drogą elektroniczną,

2) opis przedmiotu umowy, z wyszczególnieniem odpowiednio ilości rzeczy lub innych dóbr oraz zakresu usług,
3) cenę albo cenę maksymalną, jeżeli cena nie jest znana w chwili zamieszczenia ogłoszenia,
4) wskazanie okoliczności faktycznych uzasadniających udzielenie zamówienia bez zastosowania przepisów ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych,
5) nazwę (firmę) podmiotu albo imię i nazwisko osoby, z którymi została zawarta umowa

– z wyłączeniem przypadków, w których udzielenie zamówienia wiąże się z korzystaniem z informacji niejawnych.”;

26) w art. 36 dodaje się ust. 5 w brzmieniu:

„5. Przepisów ust. 1–4 nie stosuje się do naboru wewnętrznego spośród pracowników Agencji do zatrudnienia na wolne stanowiska pracy w Agencji.”;

27) art. 40 otrzymuje brzmienie:

„Art. 40. Pracownicy Agencji zatrudnieni:
1) na stanowisku głównego księgowego,
2) na stanowisku zastępcy dyrektora biura lub na stanowisku równorzędnym,
3) na stanowisku kierownika działu lub na stanowisku równorzędnym,
4) na stanowisku kierownika składnicy lub na stanowisku równorzędnym

– składają Prezesowi Agencji oświadczenia o stanie majątkowym na zasadach, w trybie i w terminach określonych w przepisach ustawy z dnia 21 sierpnia 1997 r. o ograniczeniu prowadzenia działalności gospodarczej przez osoby pełniące funkcje publiczne oraz podlegają ograniczeniom w prowadzeniu działalności gospodarczej, takim jak pracownicy agencji państwowych, o których mowa w art. 2 pkt 10 ustawy z dnia 21 sierpnia 1997 r. o ograniczeniu prowadzenia działalności gospodarczej przez osoby pełniące funkcje publiczne (Dz. U. z 2025 r. poz. 499).”;

28) po art. 40 dodaje się art. 40a w brzmieniu:

„Art. 40a. Agencja wykonuje obowiązek, o którym mowa w art. 13 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) (Dz. Urz. UE L 119 z 04.05.2016,

str. 1, z późn. zm. [21]), zwanego dalej „rozporządzeniem 2016/679”, przez udostępnienie informacji, o których mowa w art. 13 ust. 1 i 2 rozporządzenia 2016/679, na swojej stronie internetowej lub w Biuletynie Informacji Publicznej na stronie podmiotowej Agencji. W takim przypadku Agencja, podczas pozyskiwania danych osobowych, informuje osobę, której dane dotyczą, o miejscu udostępnienia tych informacji.”;

29) w art. 41:

a) w ust. 2 pkt 2 otrzymuje brzmienie:

„2) dotacje celowe na realizację zadań, o których mowa w art. 12 ust. 1;”,

b) w ust. 2 w pkt 9 kropkę zastępuje się średnikiem i dodaje się pkt 10 w brzmieniu:

„10) środki pochodzące z budżetu Unii Europejskiej.”,

c) ust. 3 otrzymuje brzmienie:

„3. Przychody, o których mowa w ust. 2 pkt 4–7, przeznacza się na realizację zadań Agencji, o których mowa w art. 31 i art. 32, oraz na bieżącą działalność Agencji, w tym wynagrodzenia jej pracowników.”,

d) po ust. 3a dodaje się ust. 3b w brzmieniu:

„3b. Przychody Agencji, o których mowa w ust. 2 pkt 10, przeznacza się na realizację zadań Agencji, o których mowa w art. 31 ust. 1, w szczególności w pkt 8a.”;

30) w art. 42:

a) w ust. 1 w pkt 3 lit. b otrzymuje brzmienie:

„b) realizacji zadań określonych w ustawie oraz w ustawie o zapasach ropy naftowej, produktów naftowych i gazu ziemnego, z uwzględnieniem:

– kosztów realizacji tych zadań przez inne podmioty,

– zakupu towarów i usług;”,

b) ust. 3 otrzymuje brzmienie:

„3. Agencja, w terminie 30 dni od ogłoszenia ustawy budżetowej na dany rok, przekazuje ministrowi właściwemu do spraw wewnętrznych plan rzeczowy rezerw strategicznych stanowiący załącznik do planu finansowego Agencji.”;

31) w art. 44 ust. 1 otrzymuje brzmienie:

„1. Należności i wierzytelności Agencji mające charakter cywilnoprawny, w szczególności z tytułu wykonywania zadań, o których mowa w art. 31 ust. 1 pkt 1, 2,

---

[21]) Zmiany niniejszego rozporządzenia zostały ogłoszone w Dz. Urz. UE L 127 z 23.05.2018, str. 2 i Dz. Urz. UE L 074 z 04.03.2021, str. 35.

4–8 i 13, mogą być umarzane w całości albo w części lub ich spłata może być odraczana, lub rozkładana na raty.”;

32) w art. 46 w ust. 1 dodaje się pkt 1a w brzmieniu:

„1a) minister właściwy do spraw gospodarki surowcami energetycznymi – w zakresie należności i wierzytelności wynikających z wykonywania zadań, o których mowa w art. 31 ust. 1 pkt 8, z zastrzeżeniem pkt 1;”;

33) po art. 46 dodaje się art. 46a w brzmieniu:

„Art. 46a. Przepisów art. 44–46 nie stosuje się do zawarcia ugody na podstawie art. 54a ustawy o finansach publicznych.”.

Art. 21. 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, z 2025 r. poz. 1017 oraz z 2026 r. poz. 252) w art. 2 w ust. 4 po pkt 1a dodaje się pkt 1b w brzmieniu:

„1b) wpływy z kar pieniężnych, o których mowa w art. 6zzo ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2023 r. poz. 122, z późn. zm.[22)]);”.

Art. 22. W ustawie z dnia 12 lipca 2024 r – Prawo komunikacji elektronicznej (Dz. U. z 2024 r. poz. 1221, z 2025 r. poz. 637 i 820 oraz z 2026 r. poz. 252) wprowadza się następujące zmiany:

1) uchyla się art. 42;

2) po art. 67 dodaje się art. 67a w brzmieniu:

„Art. 67a. 1. Prezes UKE, w uzgodnieniu z ministrem właściwym do spraw wewnętrznych, zapewnia odpowiednie częstotliwości do realizacji zadań z zakresu komunikacji głosowej i transmisji danych do zapewnienia bezpiecznej radiowej łączności mobilnej w celu zapewnienia ciągłości i bezpieczeństwa funkcjonowania administracji państwowej oraz ochrony ludności i obrony cywilnej.

2. Podmiot będący przedsiębiorcą telekomunikacyjnym lub podmiot prowadzący działalność telekomunikacyjną, o którym mowa w art. 79 ustawy z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej (Dz. U. poz. 1907, z 2025 r. poz. 1705 oraz …), któremu minister właściwy do spraw wewnętrznych zlecił zadania związane z organizacją, budową, utrzymaniem i modernizacją Systemu Bezpiecznej Łączności Państwowej, wykorzystuje częstotliwości do wykonywania zadań, o których mowa w ust.

[22)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2024 r. poz. 834, 1222, 1473, 1572 i 1907, z 2025 r. poz. 1795 oraz …

1, na podstawie decyzji o rezerwacji częstotliwości wydanej przez Prezesa UKE po uzgodnieniu z ministrem właściwym do spraw wewnętrznych.

3. Do rezerwacji częstotliwości, o której mowa w ust. 1, przepisu art. 104 ust. 3 nie stosuje się.”.

Art. 23. W ustawie z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej (Dz. U. poz. 1907 oraz z 2025 r. poz. 1705) wprowadza się następujące zmiany:

1) w art. 5 ust. 2 otrzymuje brzmienie:

„2. Podmioty ochrony ludności i obrony cywilnej są obowiązane do współpracy z organami ochrony ludności i obrony cywilnej, stosownie do swoich możliwości, kompetencji, obszaru działania oraz zakresu działania ujętego w planach zarządzania kryzysowego, o których mowa w art. 6g ust. 2 oraz art. 6j ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, i planach ciągłości działania.”;

2) w art. 15 w ust. 1 pkt 6 otrzymuje brzmienie:

„6) analizowanie wniosków z ocen ryzyka mających wpływ na bezpieczeństwo i ochronę ludności i obronę cywilną, o których mowa w Krajowej Ocenie Ryzyka, o której mowa w art. 6e ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, i informacji pochodzących z raportów Rządowego Centrum Bezpieczeństwa oraz centrów służb podległych mu i nadzorowanych przez niego, a także przedstawianie propozycji rozwiązań w tym zakresie;”;

3) w art. 38 wprowadzenie do wyliczenia otrzymuje brzmienie:

„Organy ochrony ludności i Dyrektor Rządowego Centrum Bezpieczeństwa uwzględniają w planach, o których mowa w art. 6g ust. 2 oraz art. 6j ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym:”;

4) art. 40 otrzymuje brzmienie:

„Art. 40. 1. Dyrektor Rządowego Centrum Bezpieczeństwa opracowuje krajowy plan ewakuacji ludności we współpracy z Szefem Sztabu Generalnego Wojska Polskiego.

2. Krajowy plan ewakuacji opracowuje się na podstawie wojewódzkich planów ewakuacji ludności.

3. Krajowy plan ewakuacji oraz wojewódzkie plany ewakuacji opracowuje się na okres 3 lat.

4. Plany, o których mowa w ust. 3, mogą być aktualizowane w przypadku zmian dotyczących sytuacji, o których mowa w art. 39 ust. 1.

5. Krajowy plan ewakuacji jest zatwierdzany przez ministra właściwego do spraw wewnętrznych.”;

5) art. 44 otrzymuje brzmienie:

„Art. 44. Wojewódzki plan ewakuacji ludności stanowi załącznik funkcjonalny do wojewódzkiego planu reagowania kryzysowego. Wkłady, o których mowa w art. 43, stanowią załączniki funkcjonalne do planów reagowania kryzysowego odpowiednio gminy i powiatu.”;

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

„Art. 79a. 1. Zlecenie zadań związanych z organizacją budową, utrzymaniem i modernizacją SBŁP przedsiębiorcy spełniającemu łącznie warunki, o których mowa w art. 79, może nastąpić w drodze decyzji administracyjnej, wydawanej przez ministra właściwego do spraw wewnętrznych.

2. Wykonywanie zadań, w zakresie określonym w ust. 1, następuje na podstawie umowy zawartej pomiędzy przedsiębiorcą oraz ministrem właściwym do spraw wewnętrznych.

3. W umowie, o której mowa w ust. 2, określa się w szczególności zakres zadań, warunki finansowania i sposób współpracy z operatorem SBŁP.”;

7) w art. 206 dotychczasową treść oznacza się jako ust. 1 i dodaje się ust. 2 w brzmieniu:

„2. Postanowień ust. 1 nie stosuje się dla zamierzenia budowlanego, wobec którego przed dniem wejścia w życie niniejszej ustawy złożono wniosek o wydanie decyzji o środowiskowych uwarunkowaniach zgody na realizację przedsięwzięcia.”.

Art. 24. 1. Krajową Ocenę Ryzyka, o której mowa w art. 6e ust. 1 ustawy zmienianej w art. 1, w brzmieniu nadanym niniejszą ustawą, Rada Ministrów przyjmuje po raz pierwszy w terminie 6 miesięcy od dnia wejścia w życie niniejszej ustawy.

2. Strategię odporności podmiotów krytycznych, o której mowa w art. 6f ust. 1 ustawy zmienianej w art. 1, w brzmieniu nadanym niniejszą ustawą, Rada Ministrów przyjmuje po raz pierwszy w terminie 6 miesięcy od dnia wejścia w życie niniejszej ustawy.

Art. 25. 1. Krajowy Plan Zarządzania Ryzykiem, o którym mowa w art. 6g ust. 2 pkt 1 ustawy zmienianej w art. 1, w brzmieniu nadanym niniejszą ustawą, Rada Ministrów przyjmuje po raz pierwszy w terminie 12 miesięcy od dnia wejścia w życie niniejszej ustawy.

2. Plany zarządzania ryzykiem, o których mowa w art. 6g ust. 2 pkt 2–5 ustawy zmienianej w art. 1, w brzmieniu nadanym niniejszą ustawą, są zatwierdzane po raz pierwszy w terminie 3 miesięcy od dnia przyjęcia Krajowego Planu Zarządzania Ryzykiem.

3. Powiatowe plany zarządzania ryzykiem, o których mowa w art. 6g ust. 2 pkt 6 ustawy zmienianej w art. 1, w brzmieniu nadanym niniejszą ustawą, są zatwierdzane po raz pierwszy w terminie 3 miesięcy od dnia przyjęcia planu zarządzania ryzykiem właściwego wojewody.

4. Gminne plany zarządzania ryzykiem, o których mowa w art. 6g ust. 2 pkt 7 ustawy zmienianej w art. 1, w brzmieniu nadanym niniejszą ustawą, są zatwierdzane po raz pierwszy w terminie 3 miesięcy od dnia przyjęcia planu zarządzania ryzykiem właściwego starosty.

5. Krajowy Plan Reagowania Kryzysowego, o którym mowa w art. 6j ust. 1 pkt 1 ustawy zmienianej w art. 1, Rada Ministrów przyjmuje po raz pierwszy w terminie 9 miesięcy od dnia przyjęcia Krajowego Planu Zarządzania Ryzykiem.

6. Plany reagowania kryzysowego, o których mowa w art. 6j ust. 1 pkt 2–5 ustawy zmienianej w art. 1, w brzmieniu nadanym niniejszą ustawą, są zatwierdzane po raz pierwszy w terminie 3 miesięcy od dnia przyjęcia Krajowego Planu Reagowania Kryzysowego.

7. Powiatowe plany reagowania kryzysowego, o których mowa w art. 6j ust. 1 pkt 6 ustawy zmienianej w art. 1, w brzmieniu nadanym niniejszą ustawą, są zatwierdzane po raz pierwszy w terminie 3 miesięcy od dnia przyjęcia planu reagowania kryzysowego właściwego wojewody.

8. Gminne plany reagowania kryzysowego, o których mowa w art. 6j ust. 1 pkt 7 ustawy zmienianej w art. 1, w brzmieniu nadanym niniejszą ustawą, są zatwierdzane po raz pierwszy w terminie 3 miesięcy od dnia przyjęcia planu reagowania kryzysowego właściwego starosty.

9. Plany zarządzania kryzysowego zatwierdzone na podstawie ustawy zmienianej w art. 1, w brzmieniu dotychczasowym, pozostają w mocy do czasu zatwierdzenia planów, o których mowa w ust. 1–8, i mogą być w tym czasie aktualizowane.

Art. 26. 1. Szczegółowe kryteria pozwalające wyodrębnić obiekty, instalacje, urządzenia i usługi, o których mowa w art. 5b ust. 2 pkt 3 ustawy zmienianej w art. 1, w brzmieniu dotychczasowym, pozostają w mocy do czasu sporządzenia kryteriów, wydanych na podstawie art. 6r ust. 5 ustawy zmienianej w art. 1 i mogą być w tym czasie aktualizowane.

2. Kryteria, o których mowa w art. 6r ust. 5 ustawy zmienianej w art. 1, w brzmieniu nadanym niniejszą ustawą, zostaną sporządzone po raz pierwszy w terminie 3 miesięcy od dnia wejścia w życie niniejszej ustawy.

Art. 27. 1. Jednolity wykaz obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, o którym mowa w art. 5b ust. 7 pkt 1 ustawy zmienianej w art. 1, w brzmieniu dotychczasowym, pozostaje w mocy do czasu sporządzenia wykazu, o którym mowa w art. 6r ust. 1 ustawy zmienianej w art. 1, w brzmieniu nadanym niniejszą ustawą, i może być w tym czasie aktualizowany.

2. Plany ochrony infrastruktury krytycznej, o których mowa w art. 6 ust. 5 ustawy zmienianej w art. 1, w brzmieniu dotychczasowym, pozostają w mocy do czasu ujęcia infrastruktury krytycznej w wykazie, o którym mowa w art. 6r ust. 1 ustawy zmienianej w art. 1, w brzmieniu nadanym niniejszą ustawą, oraz opracowania dokumentacji ochrony infrastruktury krytycznej, o której mowa w art. 6zf ust. 1 ustawy zmienianej w art. 1, w brzmieniu nadanym niniejszą ustawą, i mogą być w tym czasie aktualizowane.

Art. 28. 1. Właściciele, posiadacze samoistni i zależni obiektów, instalacji, urządzeń i usług ujętych w jednolitym wykazie, o którym mowa w art. 5b ust. 7 pkt 1 ustawy zmienianej w art. 1, w brzmieniu dotychczasowym, realizują zadania w zakresie ochrony infrastruktury krytycznej na podstawie art. 6 ustawy zmienianej w art. 1, w brzmieniu dotychczasowym, do czasu ujęcia w wykazie infrastruktury krytycznej, o którym mowa w art. 6r ust. 1 ustawy zmienianej w art. 1, w brzmieniu nadanym niniejszą ustawą.

2. Ministrowie kierujący działami administracji rządowej, kierownicy urzędów centralnych oraz wojewodowie, w zakresie swoich właściwości, na podstawie przepisów dotychczasowych, realizują zadania w zakresie ochrony infrastruktury krytycznej ujętej w wykazie, o którym mowa w art. 5b ust. 7 pkt 1 ustawy zmienianej w art. 1, w brzmieniu dotychczasowym, do czasu sporządzenia wykazu infrastruktury krytycznej, o którym mowa w art. 6r ust. 1 ustawy zmienianej w art. 1, w brzmieniu nadanym niniejszą ustawą.

Art. 29. Organy do spraw podmiotów krytycznych, o których mowa w art. 6zk ust. 1 ustawy zmienianej w art. 1, w brzmieniu nadanym niniejszą ustawą, po raz pierwszy identyfikują podmioty krytyczne i wpisują je do wykazu podmiotów krytycznych w terminie 9 miesięcy od dnia wejścia w życie niniejszej ustawy.

Art. 30. 1. Pojedynczy Punkt Kontaktowy, o którym mowa w art. 6zm ust. 1 ustawy zmienianej w art. 1, w brzmieniu nadanym niniejszą ustawą, po raz pierwszy opracowuje i przekazuje Komisji Europejskiej oraz Grupie do spraw Odporności Podmiotów Krytycznych sprawozdanie dotyczące incydentów istotnych zgłaszanych przez podmioty krytyczne mających wpływ na ciągłość świadczonych przez nich usług kluczowych na terytorium

Rzeczypospolitej Polskiej oraz ciągłość świadczonych usług kluczowych w państwach członkowskich Unii Europejskiej w terminie do dnia 17 lipca 2028 r.

2. Pojedynczy Punkt Kontaktowy, o którym mowa w art. 6zm ust. 1 ustawy zmienianej w art. 1, w brzmieniu nadanym niniejszą ustawą, po raz pierwszy przekazuje Komisji Europejskiej informacje o przepisach dotyczących kar pieniężnych nie później niż w ciągu 7 dni od dnia wejścia w życie ustawy.

3. Pojedynczy Punkt Kontaktowy, o którym mowa w art. 6zm ust. 1 ustawy zmienianej w art. 1, w brzmieniu nadanym niniejszą ustawą, przekazuje Komisji Europejskiej dane kontaktowe wyznaczonych organów do spraw podmiotów krytycznych, Pojedynczego Punktu Kontaktowego oraz wskazuje zakres realizowanych zadań, w terminie trzech miesięcy od dnia wejścia w życie ustawy.

Art. 31. Utrzymanie wykazu podmiotów krytycznych prowadzonego w systemie, o którym mowa w art. 46 ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, jest finansowane z części budżetowej, której dysponentem jest minister właściwy do spraw informatyzacji.

2. Minister właściwy do spraw informatyzacji może powierzyć realizację zadania utrzymania wykazu podmiotów krytycznych jednostce podległej albo przez niego nadzorowanej. Jednostka ta otrzymuje dotację celową na realizację zadania utrzymania wykazu podmiotów krytycznych.

Art. 32. 1. W terminie 30 dni od dnia wejścia w życie niniejszej ustawy Prezes Narodowego Banku Polskiego przekazuje Komisji Nadzoru Finansowego zestawienie podmiotów podlegających nadzorowi Komisji Nadzoru Finansowego umieszczonych w prowadzonym przez siebie wykazie, o którym mowa w art. 5 ust. 3 ustawy zmienianej w art. 7, w brzmieniu dotychczasowym.

2. W terminie 45 dni od dnia wejścia w życie niniejszej ustawy w wykazie, o którym mowa w art. 5 ust. 3 ustawy zmienianej w art. 7, w brzmieniu nadanym niniejszą ustawą, prowadzonym przez Komisję Nadzoru Finansowego umieszcza się podmioty zgodnie z zestawieniem, o którym mowa w ust. 1.

3. W przypadku, o którym mowa w ust. 2, umieszczenie podmiotu w wykazie, o którym mowa w art. 5 ust. 3 ustawy zmienianej w art. 7, w brzmieniu nadanym niniejszą ustawą, prowadzonym przez Komisję Nadzoru Finansowego nie wymaga decyzji administracyjnej.

4. Po umieszczeniu podmiotów w prowadzonym przez siebie wykazie, o którym mowa w art. 5 ust. 3 ustawy zmienianej w art. 7, w brzmieniu nadanym niniejszą ustawą, Komisja Nadzoru Finansowego niezwłocznie:

1) informuje o tym umieszczone podmioty oraz Prezesa Narodowego Banku Polskiego;
2) przesyła ten wykaz do właściwych terytorialnie wojewodów.

5. Po otrzymaniu informacji, o której mowa w ust. 4 pkt 1, Prezes Narodowego Banku Polskiego usuwa podmioty umieszczone w wykazie prowadzonym przez Komisję Nadzoru Finansowego z prowadzonego przez siebie wykazu, o którym mowa w art. 5 ust. 3 ustawy zmienianej w art. 7, w brzmieniu dotychczasowym. Usunięcie podmiotów, o którym mowa w zdaniu pierwszym, nie wymaga decyzji administracyjnej.

Art. 33. 1. Do postępowań w sprawie sprzeciwu wobec uchwał organu spółki lub innych dokonywanych przez zarząd spółki czynności prawnych, o których mowa w art. 2 ust. 1 i 2 ustawy zmienianej w art. 13, w brzmieniu dotychczasowym, wszczętych i niezakończonych przed dniem wejścia w życie niniejszej ustawy, w zakresie terminów, stosuje się przepisy dotychczasowe.

2. Raport półroczny oraz raport roczny o stanie ochrony infrastruktury krytycznej, o których mowa w art. 6 ust. 3 ustawy zmienianej w art. 13, w brzmieniu nadanym niniejszą ustawą, składa się po raz pierwszy odpowiednio za pierwsze półrocze 2026 r. oraz za rok 2026.

3. Przepisy wykonawcze wydane na podstawie art. 6 ust. 8 ustawy zmienianej w art. 13, w brzmieniu dotychczasowym, zachowują moc do dnia wejścia w życie przepisów wykonawczych wydanych na podstawie art. 6 ust. 8 ustawy zmienianej w art. 13, w brzmieniu nadanym niniejszą ustawą, nie dłużej jednak niż przez 6 miesięcy od dnia wejścia w życie niniejszej ustawy.

Art. 34. Szczegółowa procedura udostępnienia rezerw strategicznych, o której mowa w art. 24 ustawy zmienianej w art. 20, w brzmieniu dotychczasowym, zachowuje moc do dnia wejścia w życie przepisów wykonawczych wydanych na podstawie art. 24 ustawy zmienianej w art. 20, w brzmieniu nadanym niniejszą ustawą, nie dłużej jednak niż przez 6 miesięcy od dnia wejścia w życie niniejszej ustawy.

Art. 35. W terminie 30 dni od dnia wejścia w życie niniejszej ustawy wojewoda wypełnia obowiązek informacyjny, o którym mowa w art. 5 ust. 8 ustawy zmienianej w art. 7, w brzmieniu nadanym niniejszą ustawą, względem dotychczas prowadzonej ewidencji.

Art. 36. 1. Komendant Główny Straży Granicznej w terminie 7 dni od dnia wejścia w życie niniejszej ustawy wyznacza spośród oficerów Straży Granicznej Pełnomocnika Komendanta Głównego Straży Granicznej do spraw utworzenia Centrum Bezpieczeństwa Morskiego, zwanego dalej „Pełnomocnikiem”, w celu podjęcia czynności przygotowawczych i organizacyjnych niezbędnych do rozpoczęcia funkcjonowania Centrum Bezpieczeństwa Morskiego, w szczególności:

1) wskazania lokalizacji i pomieszczeń;
2) wyposażenia w niezbędny sprzęt;
3) zapewnienia funkcjonalności i komplementarności odpowiednich systemów teleinformatycznych i stanowisk pracy;
4) wspierania procesu wyznaczania przedstawicieli innych organów lub podmiotów do wykonywania zadań CBM.

2. Czynności, o których mowa w ust. 1, Pełnomocnik realizuje we współpracy i przy wsparciu organów lub podmiotów, o których mowa w art. 25b ust. 1 ustawy zmienianej w art. 12.

3. Pełnomocnik kończy swoją działalność z dniem utworzenia Centrum Bezpieczeństwa Morskiego.

Art. 37. Do finansowania należności, o których mowa w art. 36k ust. 3a ustawy zmienianej w art. 3 niniejszej ustawy, w art. 41i ust. 3 ustawy zmienianej w art. 4 niniejszej ustawy, w art. 37r ust. 3 ustawy zmienianej w art. 6 niniejszej ustawy oraz w art. 98 ust. 3 ustawy zmienianej w art. 18 niniejszej ustawy, oddelegowanych funkcjonariuszy, którzy w dniu wejścia w życie ustawy wykonywali zadania w urzędzie obsługującym ministra właściwego do spraw wewnętrznych albo w jednostce podległej lub nadzorowanej przez ministra właściwego do spraw wewnętrznych, stosuje się przepisy w brzmieniu nadanym niniejszą ustawą.

Art. 38. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 20 – gospodarka, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2026 r. – 586 tys. zł;
2) w 2027 r. – 611 tys. zł;
3) w 2028 r. – 626 tys. zł;
4) w 2029 r. – 642 tys. zł;
5) w 2030 r. – 658 tys. zł;

6) w 2031 r. – 710 tys. zł;
7) w 2032 r. – 691 tys. zł;
8) w 2033 r. – 708 tys. zł;
9) w 2034 r. – 726 tys. zł;
10) w 2035 r. – 744 tys. zł.

2. 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 oraz odpowiada za wdrożenie mechanizmu korygującego, o którym mowa w ust. 3.

3. W przypadku przekroczenia lub zagrożenia przekroczeniem przyjętego na dany rok budżetowy maksymalnego limitu wydatków, o którym mowa w ust. 1, zastosowany zostanie mechanizm korygujący polegający na ograniczeniu kosztów nowo powstałych stanowisk pracy.

Art. 39. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 21 – gospodarka morska, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:
1) w 2026 r. – 2.149 tys. zł;
2) w 2027 r. – 2.241 tys. zł;
3) w 2028 r. – 2.297 tys. zł;
4) w 2029 r. – 2.352 tys. zł;
5) w 2030 r. – 2.411 tys. zł;
6) w 2031 r. – 2.603 tys. zł;
7) w 2032 r. – 2.533 tys. zł;
8) w 2033 r. – 2.596 tys. zł;
9) w 2034 r. – 2.661 tys. zł;
10) w 2035 r. – 2.728 tys. zł.

2. Minister właściwy do spraw gospodarki morskiej 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 oraz odpowiada za wdrożenie mechanizmu korygującego, o którym mowa w ust. 3.

3. W przypadku przekroczenia lub zagrożenia przekroczeniem przyjętego na dany rok budżetowy maksymalnego limitu wydatków, o którym mowa w ust. 1, zastosowany zostanie

mechanizm korygujący polegający na ograniczeniu kosztów nowo powstałych stanowisk pracy.

Art. 40. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 22 – gospodarka wodna, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2026 r. – 586 tys. zł;
2) w 2027 r. – 611 tys. zł;
3) w 2028 r. – 626 tys. zł;
4) w 2029 r. – 642 tys. zł;
5) w 2030 r. – 658 tys. zł;
6) w 2031 r. – 710 tys. zł;
7) w 2032 r. – 691 tys. zł;
8) w 2033 r. – 708 tys. zł;
9) w 2034 r. – 726 tys. zł;
10) w 2035 r. – 744 tys. zł.

2. Minister właściwy do spraw gospodarki wodnej 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 oraz odpowiada za wdrożenie mechanizmu korygującego, o którym mowa w ust. 3.

3. W przypadku przekroczenia lub zagrożenia przekroczeniem przyjętego na dany rok budżetowy maksymalnego limitu wydatków, o którym mowa w ust. 1, zastosowany zostanie mechanizm korygujący polegający na ograniczeniu kosztów nowo powstałych stanowisk pracy.

Art. 41. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 27 – informatyzacja, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2026 r. – 2.461 tys. zł;
2) w 2027 r. – 1.093 tys. zł;
3) w 2028 r. – 1.123 tys. zł;
4) w 2029 r. – 1.153 tys. zł;
5) w 2030 r. – 1.185 tys. zł;
6) w 2031 r. – 1.253 tys. zł;
7) w 2032 r. – 1.250 tys. zł;

8) w 2033 r. – 1.284 tys. zł;
9) w 2034 r. – 1.319 tys. zł;
10) w 2035 r. – 1.355 tys. zł.

2. Minister właściwy do spraw informatyzacji 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 oraz odpowiada za wdrożenie mechanizmu korygującego, o którym mowa w ust. 3.

3. W przypadku przekroczenia lub zagrożenia przekroczeniem przyjętego na dany rok budżetowy maksymalnego limitu wydatków, o którym mowa w ust. 1, zastosowany zostanie mechanizm korygujący polegający na ograniczeniu kosztów:

1) nowo powstałych stanowisk pracy;
2) funkcjonowania wykazu podmiotów krytycznych prowadzonego w systemie, o którym mowa w art. 46 ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

Art. 42. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 32 – rolnictwo, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2026 r. – 586 tys. zł;
2) w 2027 r. – 611 tys. zł;
3) w 2028 r. – 626 tys. zł;
4) w 2029 r. – 642 tys. zł;
5) w 2030 r. – 658 tys. zł;
6) w 2031 r. – 710 tys. zł;
7) w 2032 r. – 691 tys. zł;
8) w 2033 r. – 708 tys. zł;
9) w 2034 r. – 726 tys. zł;
10) w 2035 r. – 744 tys. zł.

2. Minister właściwy do spraw rolnictwa 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 oraz odpowiada za wdrożenie mechanizmu korygującego, o którym mowa w ust. 3.

3. W przypadku przekroczenia lub zagrożenia przekroczeniem przyjętego na dany rok budżetowy maksymalnego limitu wydatków, o którym mowa w ust. 1, zastosowany zostanie mechanizm korygujący polegający na ograniczeniu kosztów nowo powstałych stanowisk pracy.

Art. 43. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 37 – sprawiedliwość, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2026 r. – 195 tys. zł;
2) w 2027 r. – 204 tys. zł;
3) w 2028 r. – 209 tys. zł;
4) w 2029 r. – 214 tys. zł;
5) w 2030 r. – 219 tys. zł;
6) w 2031 r. – 237 tys. zł;
7) w 2032 r. – 230 tys. zł;
8) w 2033 r. – 236 tys. zł;
9) w 2034 r. – 242 tys. zł;
10) w 2035 r. – 248 tys. zł.

2. Minister Sprawiedliwości 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 oraz odpowiada za wdrożenie mechanizmu korygującego, o którym mowa w ust. 3.

3. W przypadku przekroczenia lub zagrożenia przekroczeniem przyjętego na dany rok budżetowy maksymalnego limitu wydatków, o którym mowa w ust. 1, zastosowany zostanie mechanizm korygujący polegający na ograniczeniu kosztów nowo powstałego stanowiska pracy.

Art. 44. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 39 – transport, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2026 r. – 586 tys. zł;
2) w 2027 r. – 611 tys. zł;
3) w 2028 r. – 626 tys. zł;
4) w 2029 r. – 642 tys. zł;
5) w 2030 r. – 658 tys. zł;
6) w 2031 r. – 710 tys. zł;

7) w 2032 r. – 691 tys. zł;
8) w 2033 r. – 708 tys. zł;
9) w 2034 r. – 726 tys. zł;
10) w 2035 r. – 744 tys. zł.

2. Minister właściwy do spraw transportu 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 oraz odpowiada za wdrożenie mechanizmu korygującego, o którym mowa w ust. 3.

3. W przypadku przekroczenia lub zagrożenia przekroczeniem przyjętego na dany rok budżetowy maksymalnego limitu wydatków, o którym mowa w ust. 1, zastosowany zostanie mechanizm korygujący polegający na ograniczeniu kosztów nowo powstałych stanowisk pracy.

Art. 45. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 42 – sprawy wewnętrzne, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:
1) w 2026 r. – 10.081 tys. zł;
2) w 2027 r. – 7.444 tys. zł;
3) w 2028 r. – 7.619 tys. zł;
4) w 2029 r. – 7.792 tys. zł;
5) w 2030 r. – 7.975 tys. zł;
6) w 2031 r. – 8.500 tys. zł;
7) w 2032 r. – 8.357 tys. zł;
8) w 2033 r. – 8.554 tys. zł;
9) w 2034 r. – 8.757 tys. zł;
10) w 2035 r. – 8.965 tys. zł.

2. Minister właściwy do spraw wewnętrznych 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 oraz odpowiada za wdrożenie mechanizmu korygującego, o którym mowa w ust. 3.

3. W przypadku przekroczenia lub zagrożenia przekroczeniem przyjętego na dany rok budżetowy maksymalnego limitu wydatków, o którym mowa w ust. 1, zastosowany zostanie mechanizm korygujący polegający na ograniczeniu kosztów:

1) nowo powstałych stanowisk pracy;
2) ograniczeniu finansowania działalności Rządowego Centrum Bezpieczeństwa w zakresie:
   a) prowadzenia Pojedynczego Punktu Kontaktowego,
   b) prowadzenia wykazu infrastruktury krytycznej oraz wykazu potencjalnej infrastruktury krytycznej,
   c) prowadzenia wykazu podmiotów krytycznych;
3) ograniczeniu finansowania tworzenia i działalności Centrum Bezpieczeństwa Morskiego.

4. Wdrożenie mechanizmu korygującego, o którym mowa w ust. 3 pkt 1 i 2, następuje w uzgodnieniu z Prezesem Rady Ministrów.

Art. 46. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 47 – energia, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2026 r. – 586 tys. zł;
2) w 2027 r. – 611 tys. zł;
3) w 2028 r. – 626 tys. zł;
4) w 2029 r. – 642 tys. zł;
5) w 2030 r. – 658 tys. zł;
6) w 2031 r. – 710 tys. zł;
7) w 2032 r. – 691 tys. zł;
8) w 2033 r. – 708 tys. zł;
9) w 2034 r. – 726 tys. zł;
10) w 2035 r. – 744 tys. zł.

2. Minister właściwy do spraw energii 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 oraz odpowiada za wdrożenie mechanizmu korygującego, o którym mowa w ust. 3.

3. W przypadku przekroczenia lub zagrożenia przekroczeniem przyjętego na dany rok budżetowy maksymalnego limitu wydatków, o którym mowa w ust. 1, zastosowany zostanie mechanizm korygujący polegający na ograniczeniu kosztów nowo powstałych stanowisk pracy.

Art. 47. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 48 – gospodarka surowcami energetycznymi, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2026 r. – 586 tys. zł;
2) w 2027 r. – 611 tys. zł;
3) w 2028 r. – 626 tys. zł;
4) w 2029 r. – 642 tys. zł;
5) w 2030 r. – 658 tys. zł;
6) w 2031 r. – 710 tys. zł;
7) w 2032 r. – 691 tys. zł;
8) w 2033 r. – 708 tys. zł;
9) w 2034 r. – 726 tys. zł;
10) w 2035 r. – 744 tys. zł.

2. Minister właściwy do spraw gospodarki surowcami energetycznymi 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 oraz odpowiada za wdrożenie mechanizmu korygującego, o którym mowa w ust. 3.

3. W przypadku przekroczenia lub zagrożenia przekroczeniem przyjętego na dany rok budżetowy maksymalnego limitu wydatków, o którym mowa w ust. 1, zastosowany zostanie mechanizm korygujący polegający na ograniczeniu kosztów nowo powstałych stanowisk pracy.

Art. 48. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 51 – klimat, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2026 r. – 586 tys. zł;
2) w 2027 r. – 611 tys. zł;
3) w 2028 r. – 626 tys. zł;
4) w 2029 r. – 642 tys. zł;
5) w 2030 r. – 658 tys. zł;
6) w 2031 r. – 710 tys. zł;
7) w 2032 r. – 691 tys. zł;
8) w 2033 r. – 708 tys. zł;
9) w 2034 r. – 726 tys. zł;

10) w 2035 r. – 744 tys. zł.

2. Minister właściwy do spraw klimatu 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 oraz odpowiada za wdrożenie mechanizmu korygującego, o którym mowa w ust. 3.

3. W przypadku przekroczenia lub zagrożenia przekroczeniem przyjętego na dany rok budżetowy maksymalnego limitu wydatków, o którym mowa w ust. 1, zastosowany zostanie mechanizm korygujący polegający na ograniczeniu kosztów nowo powstałych stanowisk pracy.

Art. 49. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 69 – żegluga śródlądowa, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2026 r. – 586 tys. zł;
2) w 2027 r. – 611 tys. zł;
3) w 2028 r. – 626 tys. zł;
4) w 2029 r. – 642 tys. zł;
5) w 2030 r. – 658 tys. zł;
6) w 2031 r. – 710 tys. zł;
7) w 2032 r. – 691 tys. zł;
8) w 2033 r. – 708 tys. zł;
9) w 2034 r. – 726 tys. zł;
10) w 2035 r. – 744 tys. zł.

2. Minister właściwy do spraw żeglugi śródlądowej 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 oraz odpowiada za wdrożenie mechanizmu korygującego, o którym mowa w ust. 3.

3. W przypadku przekroczenia lub zagrożenia przekroczeniem przyjętego na dany rok budżetowy maksymalnego limitu wydatków, o którym mowa w ust. 1, zastosowany zostanie mechanizm korygujący polegający na ograniczeniu kosztów nowo powstałych stanowisk pracy.

Art. 50. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 76 – Urząd Komunikacji Elektronicznej, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2026 r. – 586 tys. zł;
2) w 2027 r. – 611 tys. zł;
3) w 2028 r. – 626 tys. zł;
4) w 2029 r. – 642 tys. zł;
5) w 2030 r. – 658 tys. zł;
6) w 2031 r. – 710 tys. zł;
7) w 2032 r. – 691 tys. zł;
8) w 2033 r. – 708 tys. zł;
9) w 2034 r. – 726 tys. zł;
10) w 2035 r. – 744 tys. zł.

2. Prezes Urzędu Komunikacji Elektronicznej 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 oraz odpowiada za wdrożenie mechanizmu korygującego, o którym mowa w ust. 3.

3. W przypadku przekroczenia lub zagrożenia przekroczeniem przyjętego na dany rok budżetowy maksymalnego limitu wydatków, o którym mowa w ust. 1, zastosowany zostanie mechanizm korygujący polegający na ograniczeniu kosztów nowo powstałych stanowisk pracy.

Art. 51. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 85/02 – województwo dolnośląskie, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2026 r. – 426 tys. zł;
2) w 2027 r. – 433 tys. zł;
3) w 2028 r. – 444 tys. zł;
4) w 2029 r. – 454 tys. zł;
5) w 2030 r. – 466 tys. zł;
6) w 2031 r. – 513 tys. zł;
7) w 2032 r. – 489 tys. zł;
8) w 2033 r. – 502 tys. zł;

9) w 2034 r. – 514 tys. zł;
10) w 2035 r. – 527 tys. zł.

2. Wojewoda dolnośląski 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 oraz odpowiada za wdrożenie mechanizmu korygującego, o którym mowa w ust. 3.

3. W przypadku przekroczenia lub zagrożenia przekroczeniem przyjętego na dany rok budżetowy maksymalnego limitu wydatków, o którym mowa w ust. 1, zastosowany zostanie mechanizm korygujący polegający na ograniczeniu kosztów nowo powstałych stanowisk pracy.

Art. 52. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 85/04 – województwo kujawsko-pomorskie, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2026 r. – 426 tys. zł;
2) w 2027 r. – 433 tys. zł;
3) w 2028 r. – 444 tys. zł;
4) w 2029 r. – 454 tys. zł;
5) w 2030 r. – 466 tys. zł;
6) w 2031 r. – 513 tys. zł;
7) w 2032 r. – 489 tys. zł;
8) w 2033 r. – 502 tys. zł;
9) w 2034 r. – 514 tys. zł;
10) w 2035 r. – 527 tys. zł.

2. Wojewoda kujawsko-pomorski 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 oraz odpowiada za wdrożenie mechanizmu korygującego, o którym mowa w ust. 3.

3. W przypadku przekroczenia lub zagrożenia przekroczeniem przyjętego na dany rok budżetowy maksymalnego limitu wydatków, o którym mowa w ust. 1, zastosowany zostanie mechanizm korygujący polegający na ograniczeniu kosztów nowo powstałych stanowisk pracy.

Art. 53. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 85/06 – województwo lubelskie, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2026 r. – 426 tys. zł;
2) w 2027 r. – 433 tys. zł;
3) w 2028 r. – 444 tys. zł;
4) w 2029 r. – 454 tys. zł;
5) w 2030 r. – 466 tys. zł;
6) w 2031 r. – 513 tys. zł;
7) w 2032 r. – 489 tys. zł;
8) w 2033 r. – 502 tys. zł;
9) w 2034 r. – 514 tys. zł;
10) w 2035 r. – 527 tys. zł.

2. Wojewoda lubelski 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 oraz odpowiada za wdrożenie mechanizmu korygującego, o którym mowa w ust. 3.

3. W przypadku przekroczenia lub zagrożenia przekroczeniem przyjętego na dany rok budżetowy maksymalnego limitu wydatków, o którym mowa w ust. 1, zastosowany zostanie mechanizm korygujący polegający na ograniczeniu kosztów nowo powstałych stanowisk pracy.

Art. 54. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 85/08 – województwo lubuskie, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2026 r. – 426 tys. zł;
2) w 2027 r. – 433 tys. zł;
3) w 2028 r. – 444 tys. zł;
4) w 2029 r. – 454 tys. zł;
5) w 2030 r. – 466 tys. zł;
6) w 2031 r. – 513 tys. zł;
7) w 2032 r. – 489 tys. zł;
8) w 2033 r. – 502 tys. zł;
9) w 2034 r. – 514 tys. zł;

10) w 2035 r. – 527 tys. zł.

2. Wojewoda lubuski 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 oraz odpowiada za wdrożenie mechanizmu korygującego, o którym mowa w ust. 3.

3. W przypadku przekroczenia lub zagrożenia przekroczeniem przyjętego na dany rok budżetowy maksymalnego limitu wydatków, o którym mowa w ust. 1, zastosowany zostanie mechanizm korygujący polegający na ograniczeniu kosztów nowo powstałych stanowisk pracy.

Art. 55. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 85/10 – województwo łódzkie, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2026 r. – 426 tys. zł;
2) w 2027 r. – 433 tys. zł;
3) w 2028 r. – 444 tys. zł;
4) w 2029 r. – 454 tys. zł;
5) w 2030 r. – 466 tys. zł;
6) w 2031 r. – 513 tys. zł;
7) w 2032 r. – 489 tys. zł;
8) w 2033 r. – 502 tys. zł;
9) w 2034 r. – 514 tys. zł;
10) w 2035 r. – 527 tys. zł.

2. Wojewoda łódzki 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 oraz odpowiada za wdrożenie mechanizmu korygującego, o którym mowa w ust. 3.

3. W przypadku przekroczenia lub zagrożenia przekroczeniem przyjętego na dany rok budżetowy maksymalnego limitu wydatków, o którym mowa w ust. 1, zastosowany zostanie mechanizm korygujący polegający na ograniczeniu kosztów nowo powstałych stanowisk pracy.

Art. 56. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 85/12 – województwo małopolskie, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2026 r. – 426 tys. zł;
2) w 2027 r. – 433 tys. zł;
3) w 2028 r. – 444 tys. zł;
4) w 2029 r. – 454 tys. zł;
5) w 2030 r. – 466 tys. zł;
6) w 2031 r. – 513 tys. zł;
7) w 2032 r. – 489 tys. zł;
8) w 2033 r. – 502 tys. zł;
9) w 2034 r. – 514 tys. zł;
10) w 2035 r. – 527 tys. zł.

2. Wojewoda małopolski 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 oraz odpowiada za wdrożenie mechanizmu korygującego, o którym mowa w ust. 3.

3. W przypadku przekroczenia lub zagrożenia przekroczeniem przyjętego na dany rok budżetowy maksymalnego limitu wydatków, o którym mowa w ust. 1, zastosowany zostanie mechanizm korygujący polegający na ograniczeniu kosztów nowo powstałych stanowisk pracy.

Art. 57. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 85/14 – województwo mazowieckie, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2026 r. – 426 tys. zł;
2) w 2027 r. – 433 tys. zł;
3) w 2028 r. – 444 tys. zł;
4) w 2029 r. – 454 tys. zł;
5) w 2030 r. – 466 tys. zł;
6) w 2031 r. – 513 tys. zł;
7) w 2032 r. – 489 tys. zł;
8) w 2033 r. – 502 tys. zł;
9) w 2034 r. – 514 tys. zł;

10) w 2035 r. – 527 tys. zł.

2. Wojewoda mazowiecki 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 oraz odpowiada za wdrożenie mechanizmu korygującego, o którym mowa w ust. 3.

3. W przypadku przekroczenia lub zagrożenia przekroczeniem przyjętego na dany rok budżetowy maksymalnego limitu wydatków, o którym mowa w ust. 1, zastosowany zostanie mechanizm korygujący polegający na ograniczeniu kosztów nowo powstałych stanowisk pracy.

Art. 58. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 85/16 – województwo opolskie, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2026 r. – 426 tys. zł;
2) w 2027 r. – 433 tys. zł;
3) w 2028 r. – 444 tys. zł;
4) w 2029 r. – 454 tys. zł;
5) w 2030 r. – 466 tys. zł;
6) w 2031 r. – 513 tys. zł;
7) w 2032 r. – 489 tys. zł;
8) w 2033 r. – 502 tys. zł;
9) w 2034 r. – 514 tys. zł;
10) w 2035 r. – 527 tys. zł.

2. Wojewoda opolski 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 oraz odpowiada za wdrożenie mechanizmu korygującego, o którym mowa w ust. 3.

3. W przypadku przekroczenia lub zagrożenia przekroczeniem przyjętego na dany rok budżetowy maksymalnego limitu wydatków, o którym mowa w ust. 1, zastosowany zostanie mechanizm korygujący polegający na ograniczeniu kosztów nowo powstałych stanowisk pracy.

Art. 59. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 85/18 – województwo podkarpackie, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2026 r. – 426 tys. zł;
2) w 2027 r. – 433 tys. zł;
3) w 2028 r. – 444 tys. zł;
4) w 2029 r. – 454 tys. zł;
5) w 2030 r. – 466 tys. zł;
6) w 2031 r. – 513 tys. zł;
7) w 2032 r. – 489 tys. zł;
8) w 2033 r. – 502 tys. zł;
9) w 2034 r. – 514 tys. zł;
10) w 2035 r. – 527 tys. zł.

2. Wojewoda podkarpacki 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 oraz odpowiada za wdrożenie mechanizmu korygującego, o którym mowa w ust. 3.

3. W przypadku przekroczenia lub zagrożenia przekroczeniem przyjętego na dany rok budżetowy maksymalnego limitu wydatków, o którym mowa w ust. 1, zastosowany zostanie mechanizm korygujący polegający na ograniczeniu kosztów nowo powstałych stanowisk pracy.

Art. 60. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 85/20 – województwo podlaskie, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2026 r. – 426 tys. zł;
2) w 2027 r. – 433 tys. zł;
3) w 2028 r. – 444 tys. zł;
4) w 2029 r. – 454 tys. zł;
5) w 2030 r. – 466 tys. zł;
6) w 2031 r. – 513 tys. zł;
7) w 2032 r. – 489 tys. zł;
8) w 2033 r. – 502 tys. zł;
9) w 2034 r. – 514 tys. zł;

10) w 2035 r. – 527 tys. zł.

2. Wojewoda podlaski 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 oraz odpowiada za wdrożenie mechanizmu korygującego, o którym mowa w ust. 3.

3. W przypadku przekroczenia lub zagrożenia przekroczeniem przyjętego na dany rok budżetowy maksymalnego limitu wydatków, o którym mowa w ust. 1, zastosowany zostanie mechanizm korygujący polegający na ograniczeniu kosztów nowo powstałych stanowisk pracy.

Art. 61. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 85/22 – województwo pomorskie, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2026 r. – 426 tys. zł;
2) w 2027 r. – 433 tys. zł;
3) w 2028 r. – 444 tys. zł;
4) w 2029 r. – 454 tys. zł;
5) w 2030 r. – 466 tys. zł;
6) w 2031 r. – 513 tys. zł;
7) w 2032 r. – 489 tys. zł;
8) w 2033 r. – 502 tys. zł;
9) w 2034 r. – 514 tys. zł;
10) w 2035 r. – 527 tys. zł.

2. Wojewoda pomorski 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 oraz odpowiada za wdrożenie mechanizmu korygującego, o którym mowa w ust. 3.

3. W przypadku przekroczenia lub zagrożenia przekroczeniem przyjętego na dany rok budżetowy maksymalnego limitu wydatków, o którym mowa w ust. 1, zastosowany zostanie mechanizm korygujący polegający na ograniczeniu kosztów nowo powstałych stanowisk pracy.

Art. 62. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 85/24 – województwo śląskie, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2026 r. – 426 tys. zł;
2) w 2027 r. – 433 tys. zł;
3) w 2028 r. – 444 tys. zł;
4) w 2029 r. – 454 tys. zł;
5) w 2030 r. – 466 tys. zł;
6) w 2031 r. – 513 tys. zł;
7) w 2032 r. – 489 tys. zł;
8) w 2033 r. – 502 tys. zł;
9) w 2034 r. – 514 tys. zł;
10) w 2035 r. – 527 tys. zł.

2. Wojewoda śląski 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 oraz odpowiada za wdrożenie mechanizmu korygującego, o którym mowa w ust. 3.

3. W przypadku przekroczenia lub zagrożenia przekroczeniem przyjętego na dany rok budżetowy maksymalnego limitu wydatków, o którym mowa w ust. 1, zastosowany zostanie mechanizm korygujący polegający na ograniczeniu kosztów nowo powstałych stanowisk pracy.

Art. 63. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 85/26 – województwo świętokrzyskie, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2026 r. – 426 tys. zł;
2) w 2027 r. – 433 tys. zł;
3) w 2028 r. – 444 tys. zł;
4) w 2029 r. – 454 tys. zł;
5) w 2030 r. – 466 tys. zł;
6) w 2031 r. – 513 tys. zł;
7) w 2032 r. – 489 tys. zł;
8) w 2033 r. – 502 tys. zł;
9) w 2034 r. – 514 tys. zł;

10) w 2035 r. – 527 tys. zł.

2. Wojewoda świętokrzyski 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 oraz odpowiada za wdrożenie mechanizmu korygującego, o którym mowa w ust. 3.

3. W przypadku przekroczenia lub zagrożenia przekroczeniem przyjętego na dany rok budżetowy maksymalnego limitu wydatków, o którym mowa w ust. 1, zastosowany zostanie mechanizm korygujący polegający na ograniczeniu kosztów nowo powstałych stanowisk pracy.

Art. 64. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 85/28 – województwo warmińsko-mazurskie, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2026 r. – 426 tys. zł;
2) w 2027 r. – 433 tys. zł;
3) w 2028 r. – 444 tys. zł;
4) w 2029 r. – 454 tys. zł;
5) w 2030 r. – 466 tys. zł;
6) w 2031 r. – 513 tys. zł;
7) w 2032 r. – 489 tys. zł;
8) w 2033 r. – 502 tys. zł;
9) w 2034 r. – 514 tys. zł;
10) w 2035 r. – 527 tys. zł.

2. Wojewoda warmińsko-mazurski 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 oraz odpowiada za wdrożenie mechanizmu korygującego, o którym mowa w ust. 3.

3. W przypadku przekroczenia lub zagrożenia przekroczeniem przyjętego na dany rok budżetowy maksymalnego limitu wydatków, o którym mowa w ust. 1, zastosowany zostanie mechanizm korygujący polegający na ograniczeniu kosztów nowo powstałych stanowisk pracy.

Art. 65. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 85/30 – województwo wielkopolskie, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2026 r. – 426 tys. zł;
2) w 2027 r. – 433 tys. zł;
3) w 2028 r. – 444 tys. zł;
4) w 2029 r. – 454 tys. zł;
5) w 2030 r. – 466 tys. zł;
6) w 2031 r. – 513 tys. zł;
7) w 2032 r. – 489 tys. zł;
8) w 2033 r. – 502 tys. zł;
9) w 2034 r. – 514 tys. zł;
10) w 2035 r. – 527 tys. zł.

2. Wojewoda wielkopolski 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 oraz odpowiada za wdrożenie mechanizmu korygującego, o którym mowa w ust. 3.

3. W przypadku przekroczenia lub zagrożenia przekroczeniem przyjętego na dany rok budżetowy maksymalnego limitu wydatków, o którym mowa w ust. 1, zastosowany zostanie mechanizm korygujący polegający na ograniczeniu kosztów nowo powstałych stanowisk pracy.

Art. 66. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 85/32 – województwo zachodniopomorskie, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2026 r. – 426 tys. zł;
2) w 2027 r. – 433 tys. zł;
3) w 2028 r. – 444 tys. zł;
4) w 2029 r. – 454 tys. zł;
5) w 2030 r. – 466 tys. zł;
6) w 2031 r. – 513 tys. zł;
7) w 2032 r. – 489 tys. zł;
8) w 2033 r. – 502 tys. zł;
9) w 2034 r. – 514 tys. zł;

10) w 2035 r. – 527 tys. zł.

2. Wojewoda zachodniopomorski 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 oraz odpowiada za wdrożenie mechanizmu korygującego, o którym mowa w ust. 3.

3. W przypadku przekroczenia lub zagrożenia przekroczeniem przyjętego na dany rok budżetowy maksymalnego limitu wydatków, o którym mowa w ust. 1, zastosowany zostanie mechanizm korygujący polegający na ograniczeniu kosztów nowo powstałych stanowisk pracy.

Art. 67. Ustawa wchodzi w życie po upływie 14 dni od dnia ogłoszenia, z wyjątkiem art. 12 pkt 3, który wchodzi w życie po upływie 6 miesięcy od dnia ogłoszenia.

Załącznik
do ustawy
z dnia
(Dz. U. poz.)

Sektory, podsektory i kategorie podmiotów

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 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, świadczący usługę, o której mowa w art. 3 pkt 6e tej ustawy.
		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.
		Uczestnicy rynku świadczący usługę, o której mowa w art. 3 pkt 59 i pkt 59a ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne.
	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.
	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.
	Wodór	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 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 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 dystrybucji wodoru.
	Energetyka jądrowa	Podmiot będący operatorem obiektu energetyki jądrowej i inwestorem, 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.
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.
		Zarządzający lotniskiem, o którym mowa w art. 2 pkt 7 ustawy z dnia 3 lipca 2002 r. – Prawo lotnicze.
		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, z wyłączeniem zarządców wyłącznie infrastruktury nieczynnej, o której mowa w art. 4 pkt 1 lit. b tej ustawy, infrastruktury prywatnej, o której mowa w art. 4 pkt 1 lit. c, 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 funkcje 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, 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.
		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.
		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.
	Transport publiczny	Podmioty, o których mowa w art. 4 ust. 8 ustawy z dnia 16 grudnia 2010 r. o publicznym transporcie zbiorowym.

	Transport drogowy	Organy, o których mowa w art. 19 ust. 2, 5 i 5a ustawy z dnia 21 marca 1985 r. o drogach publicznych, z wyłączeniem podmiotów publicznych, dla których zarządzanie ruchem lub obsługa inteligentnych systemów transportowych stanowią inną niż istotna część ich ogólnej działalności.
		Podmioty, o których mowa w art. 43a ust. 1 ustawy z dnia 21 marca 1985 r. o drogach publicznych.
Bankowość i infrastruktura rynków finansowych		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.
		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.
		Administratorzy kluczowych wskaźników referencyjnych.

		Centralny depozyt papierów wartościowych, 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.
		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.
		Giełda towarowa w rozumieniu art. 2 pkt 1 ustawy z dnia 26 października 2000 r. o giełdach towarowych.
		Izba rozliczeniowa, o której mowa w art. 67 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe.
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.
		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.
		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.
		Podmioty udzielające świadczeń opieki zdrowotnej, w rozumieniu art. 133 ustawy o

		świadczeniach opieki zdrowotnej finansowanych ze środków publicznych.
		Jednostki organizacyjne podległe lub nadzorowane przez ministra kierującego działem administracji rządowej zdrowie.
		Urzędy obsługujące centralne organy nadzorowane przez ministra właściwego do spraw zdrowia.
	Produkcja, dystrybucja, obrót i magazynowanie substancji czynnych, produktów leczniczych i wyrobów medycznych	Urzędy obsługujące organy Państwowej 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.
		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.
		Przedsiębiorca prowadzący działalność polegającą na prowadzeniu hurtowni farmaceutycznej w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne.
		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.
		Wytwórca lub importer produktu leczniczego w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne.
		Wytwórca, importer lub dystrybutor 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.
		Przedsiębiorca prowadzący działalność w formie apteki ogólnodostępnej w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne.
		Jednostki organizacyjne podległe lub nadzorowane przez ministra kierującego

		działem administracji rządowej zdrowie.
		Urzędy obsługujące centralne organy nadzorowane przez ministra właściwego do spraw zdrowia.
		Jednostki notyfikowane, jednostki oceniające zgodność, producenci, o których mowa w ustawie z dnia 7 kwietnia 2022 r. o wyrobach medycznych.
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 z wyłączeniem podmiotów, dla których dostarczanie wody przeznaczonej do spożycia przez ludzi 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.
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 usług chmurowych.
		Dostawca usług ośrodka przetwarzania danych.
		Dostawca sieci dostarczania treści.
		Dostawca usług zaufania.
		Podmiot świadczący usługę rejestracji nazw domen.
	Komunikacja elektroniczna	Przedsiębiorca komunikacji elektronicznej.
Administracja publiczna	Podmioty publiczne	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 z wyłączeniem jednostek organizacyjnych podległych ministrowi właściwemu do spraw budżetu, finansów publicznych i instytucji finansowych lub przez niego nadzorowanych, urzędu obsługującego tego ministra oraz spółki celowej utworzonej do wykonywania niektórych zadań dotyczących informatyzacji w zakresie działów administracji rządowej budżet i finanse publiczne.
		Jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 3, 5, 6, 8, 9, 11 i 12 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych, z wyłączeniem jednostek organizacyjnych obsługujących jednostki samorządu terytorialnego.
		Podmiot, o którym mowa w art. 96 ust. 1 ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych.

		Instytuty badawcze.
		Urząd Dozoru Technicznego.
		Polska Agencja Żeglugi Powietrznej.
		Polskie Centrum Akredytacji.
		Urząd Komisji Nadzoru Finansowego.
		Polska Agencja Prasowa.
		Polska Wytwórnia Papierów Wartościowych.
		Państwowe Gospodarstwo Wodne Wody Polskie, o którym mowa w ustawie z dnia 20 lipca 2017 r. – Prawo wodne.
		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.
		Podmioty zarządzające lub odpowiedzialne za stan techniczny oraz sprawność infrastruktury przeciwpowodziowej, budowli hydrotechnicznych i pozostałych obiektów o charakterze inżynierskim.
		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.
	Finanse publiczne	Centrum Informatyki Resortu Finansów.
		Spółka celowa, 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 obsługujący ministra właściwego do spraw budżetu, finansów publicznych i instytucji finansowych.
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.
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.
Zarządzanie usługami ICT		Dostawca usług zarządzanych.
Produkcja, wytwarzanie i		Przedsiębiorstwo zajmujące się produkcją substancji oraz wytwarzaniem i dystrybucją

dystrybucja chemikaliów		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.
		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.
Usługi pocztowe		Operator pocztowy, o którym mowa w art. 3 pkt 12 ustawy z dnia 23 listopada 2012 r. –

		Prawo pocztowe.
Gospodarowanie odpadami	Zbieranie odpadów	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 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.
	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 wraz z nadzorem nad wymienionymi działaniami, a także późniejsze postępowanie z miejscami	Przedsiębiorstwa świadczące usługi w rozumieniu ustawy z dnia 14 grudnia 2012 r. o odpadach, polegające na przetwarzaniu odpadów, wraz z nadzorem nad wymienionymi działaniami, a także podmioty świadczące usługi z późniejszym postępowaniem z miejscami unieszkodliwiania odpadów, zobowiązane do

	unieszkodliwiania odpadów	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.

UZASADNIENIE

Wstęp, ogólna charakterystyka proponowanych regulacji

Projektowane rozwiązania mają na celu:

- ✓ wzmocnienie systemu zarządzania kryzysowego poprzez wprowadzenie rozwiązań zapewniających efektywne zarządzanie ryzykiem, z uwzględnieniem postanowień Decyzji Parlamentu Europejskiego i Rady nr 1313/2013/EU z dnia 17 grudnia 2013 r. w sprawie Unijnego Mechanizmu Ochrony Ludności (Dz. Urz. UE L 347 z 20.12.2013, str. 924, L 250 z 04.10.2018, str. 1 oraz L 77A z 20.03.2019, str. 1), zwanej dalej „UMOL";
- ✓ wdrożenie 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 333 z 27.12.2022, str. 164), zwanej dalej „dyrektywą 2022/2557";
- ✓ wzmocnienie ochrony infrastruktury krytycznej, w szczególności niezbędnej do świadczenia tzw. usług kluczowych przez podmioty krytyczne;
- ✓ wdrożenie rozwiązań umożliwiających wzmocnienie ochrony najważniejszych dla państwa obszarów, obiektów i urządzeń, w szczególności infrastruktury morskiej.

Posiadanie planów zarządzania ryzykiem jest o tyle istotne, iż są one niezbędne do spełnienia tzw. warunkowości ex ante w perspektywie finansowej UE na lata 2021–2027, co ma przełożenie na możliwość pozyskiwania środków finansowych w ramach polityki spójności z Europejskiego Funduszu Rozwoju Regionalnego, Funduszu Spójności oraz Europejskiego Funduszu Morskiego i Rybackiego.

Opracowanie dokumentów planistycznych w obszarze zarządzania ryzykiem jest bowiem bezpośrednio powiązane z jednym z warunków podstawowych perspektywy finansowej, który mówi o „osiągnięciu skutecznych ram zarządzania ryzykiem". Wskazuje się wprost na konieczność opracowania planu zarządzania ryzykiem na szczeblu krajowym lub regionalnym, powiązanego ze strategiami adaptacji do zmian klimatu. Ponadto państwa członkowskie opracowują oceny ryzyka na szczeblu krajowym lub niższym oraz udostępniają Komisji Europejskiej tzw. streszczenie istotnych elementów tych ocen.

Obowiązujące obecnie w tym obszarze regulacje ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym nie pozwalają w pełni odzwierciedlać w planach zarządzania kryzysowego kwestii dotyczących zarządzania ryzykiem. Istnieje zatem konieczność

opracowywania planów zarządzania ryzykiem, na szczeblu krajowym lub odpowiednio niższym, wskazanie podmiotów odpowiedzialnych za ich opracowanie, zakresu merytorycznego takiego planu oraz określenie cyklu planowania.

Koniecznym stała się więc modyfikacja dotychczasowych rozwiązań w kierunku zapewnienia podstaw prawnych i organizacyjnych dotyczących kwestii zarządzania ryzykiem, co znajdzie odzwierciedlenie w projekcie w rozwiązaniach dotyczących dokumentów strategicznych w zakresie oceny ryzyka oraz treści planów zarządzania kryzysowego. Nowe regulacje pozwolą również na efektywne przekazywanie dokumentów o charakterze sprawozdawczym Komisji Europejskiej, m.in. „Streszczenia istotnych elementów krajowej oceny ryzyka" oraz „Streszczenia istotnych elementów krajowej oceny zdolności zarządzania ryzykiem".

W zakresie kwestii zarządzania ryzykiem, z uwzględnieniem postanowień UMOL, przewiduje się wdrożenie zintegrowanego podejścia do zarządzania ryzykiem, obejmującego cały cykl zarządzania, od oceny ryzyka poprzez przygotowanie planów zarządzania nim oraz wdrażanie środków zapobiegawczych i zapewniających gotowość do ich użycia.

Przewiduje się opracowanie na szczeblu centralnym dokumentu rządowego, tzw. Krajowej Oceny Ryzyka, który zastąpi obecnie funkcjonujący Raport o zagrożeniach bezpieczeństwa narodowego. Dotychczasowe doświadczenia wykazują, że Raport o zagrożeniach bezpieczeństwa narodowego jest dokumentem nadmiernie obszernym, mającym charakter quasi cyklicznej oceny zidentyfikowanych zagrożeń, a jednocześnie nie przekładającym się na procesy planistyczne dotyczące zarządzania ryzykiem.

Krajowa Ocena Ryzyka będzie funkcjonalnym dokumentem zawierającym zidentyfikowane zagrożenia o różnym charakterze, w tym mogące spowodować katastrofę naturalną lub awarię techniczną, zagrożenia hybrydowe, cyberbezpieczeństwa, o charakterze terrorystycznym, jak również inne mogące spowodować znaczące negatywne skutki dla ludności, gospodarki lub dóbr kultury oraz ocenę ryzyk wynikających z tych zagrożeń, pozwalającą określić cele strategiczne i priorytety na rzecz ich ograniczania. Istotne jest bowiem zrozumienie, że dopiero prawidłowo przeprowadzona ocena ryzyka, identyfikuje zagrożenia i obszary, w których konieczne jest podjęcie działań, w tym zwiększenie nakładów finansowych na realizację przedsięwzięć ograniczających.

Dodatkowo Krajowa Ocena Ryzyka jako dokument o charakterze strategicznym będzie odnosić się do zagrożeń niezidentyfikowane jednoznacznie, które mogą wystąpić w przyszłości.

Krajowa Ocena Ryzyka – w obszarze planowania cywilnego – wykorzystywana będzie wykorzystywana na potrzeby opracowania Krajowego Planu Zarządzania Kryzysowego oraz planów zarządzania kryzysowego ministrów, kierowników urzędów centralnych, wojewodów. Plany zarządzania kryzysowego na szczeblu powiatu oraz gminy będą mogły uwzględniać treści zawarte w Krajowej Ocenie Ryzyka.

W przypadku planów zarządzania kryzysowego – opracowywane do tej pory plany zarządzania kryzysowego podzielone zostaną na plany zarządzania ryzykiem oraz plany reagowania kryzysowego, tj.:

- ✓ plany zarządzania ryzykiem w odniesieniu do działań uczestników zarządzania kryzysowego w zakresie zapobiegania sytuacji kryzysowej oraz przygotowywania do przejmowania nad nią kontroli,
- ✓ plany reagowania kryzysowego w odniesieniu do działań uczestników zarządzania kryzysowego w zakresie reagowania w przypadku wystąpienia sytuacji kryzysowej oraz usuwaniu jej skutków.

Konieczne będzie dostosowanie terminologii do regulacji unijnych, co stworzy efektywne narzędzia do prowadzenia oceny ryzyka i zarządzania nim. Jednocześnie zostaną ujednolicone terminy cyklów planistycznych krajowych z unijnymi. Obowiązujące przepisy krajowe przewidują cykl 2-letni, podczas gdy unijne regulacje wskazują na 3-letnie cykle planistyczne. Nowy cykl planistyczny będzie obejmował więc 3 lata.

Wdrożenie rozwiązań zawartych w dyrektywie 2022/2557 ma zapewnić ciągłości świadczenia usług kluczowych realizowanych w sektorach lub podsektorach w niej wskazanych.

U podstaw zmiany podejścia do tematyki infrastruktury krytycznej oraz usług realizowanych za jej pomocą należy uznać ewoluujące zagrożenia hybrydowe i terrorystyczne, współzależności między konkretną infrastrukturą a sektorami, na co wpływa m.in. globalizacja, zmiany związane z klimatem, które pociągają za sobą ekstremalne zjawiska pogodowe oraz fragmentację rynku wewnętrznego w zakresie uznawania podmiotów za krytyczne. Tym samym rozwiązania polegające na ochrony pojedynczych składników infrastruktury okazują się w wielu przypadkach niewystarczające, aby zapobiec zakłóceniom świadczenia usług niezbędnych dla państwa, jak i obywateli.

Przewidywane rozwiązania w tym zakresie dotyczą:

- ✓ identyfikacji usług kluczowych świadczonych przez operatorów infrastruktury krytycznej z uwzględnieniem potencjalnych skutków zakłócenia usług;
- ✓ minimalizacji skutków zakłócenia usług poprzez wprowadzenie procesów oceny i zarządzania ryzykiem;
- ✓ modyfikacji obecnych rozwiązań w zakresie ochrony infrastruktury krytycznej, która jest niezbędnym elementem świadczenia usług kluczowych przez podmioty krytyczne;
- ✓ identyfikacji i wyznaczanie podmiotów krytycznych (w tym podmiotów krytycznych o szczególnym znaczeniu europejskim) w podziale na tzw. sektory i podsektory, o których mowa w dyrektywie 2022/2557, jak również regulacje w zakresie nadzoru nad podmiotami krytycznymi oraz egzekwowania przepisów;
- ✓ obowiązków opracowania krajowej strategii w zakresie zwiększenia odporności podmiotów krytycznych;
- ✓ obowiązków podmiotów krytycznych mające na celu zwiększenie ich odporności i zdolności do świadczenia usług kluczowych niezbędnych dla utrzymania funkcji społecznych lub niezbędnej działalności gospodarczej;
- ✓ wskazanie organów odpowiedzialnych za prawidłowe stosowanie, jak również egzekwowanie przepisów na szczeblu krajowym oraz na poziomie sektorowym;
- ✓ wyznaczenie tzw. pojedynczego punktu kontaktowego zapewniającego współpracę transgraniczną z pojedynczymi punktami kontaktowymi innych państw członkowskich oraz z powoływaną na mocy dyrektywy 2022/2557 tzw. Grupą ds. Odporności Podmiotów Krytycznych;
- ✓ określenia mechanizmów wsparcia podmiotów krytycznych obejmujących opracowanie wytycznych oraz metodyk, pomoc w organizacji ćwiczeń mających na celu sprawdzenie odporności podmiotów krytycznych, jak również zapewnienie doradztwa i szkoleń personelu tychże podmiotów;
- ✓ zapewnienia mechanizmów sporządzania ocen ryzyka podmiotów krytycznych, stanowiących m.in. podstawę do projektowania i wdrażania środków dla zwiększenia odporności;

- ✓ określenia środków, które muszą być wprowadzone przez podmioty krytyczne dla zwiększenia ich odporności obejmujących środki techniczne, środki bezpieczeństwa oraz środki organizacyjne;
- ✓ wskazania mechanizmów sporządzania planów zwiększania odporności podmiotów krytycznych lub wskazania innych, tożsamych co do treści dokumentów;
- ✓ wskazania mechanizmów wymiany informacji między podmiotami krytycznymi a właściwymi organami m.in. w zakresie zgłaszania zdarzeń zakłócających funkcjonowanie świadczenia usług przez podmioty krytyczne, jak również na rzecz bieżącego monitorowania zdarzeń lub zagrożeń mogących mieć wpływ na świadczenie usług przez podmioty krytyczne;
- ✓ mechanizmów koordynacji tzw. misji doradczych realizowanych przez Komisję Europejską w odniesieniu do podmiotów krytycznych o szczególnym znaczeniu europejskim;
- ✓ mechanizmów przeprowadzania audytów lub kontroli podmiotów krytycznych;
- ✓ wskazanie sankcji mających zastosowanie w przypadku naruszeń przepisów krajowych przyjętych na podstawie dyrektywy 2022/2557.

Jak wskazano powyżej, konieczna jest „modyfikacja obecnych rozwiązań w zakresie ochrony infrastruktury krytycznej, która jest niezbędnym elementem świadczenia usług kluczowych przez podmioty krytyczne".

Wdrożenie rozwiązań zawartych w dyrektywie 2022/2557 nie może odbyć się bez redefiniowania regulacji dotyczących infrastruktury krytycznej, która jest niezbędna do świadczenia usług kluczowych przez podmioty krytyczne, o których traktuje ta dyrektywa.

W przypadku usług kluczowych – należy je chronić kompleksowo – nie tylko przez pryzmat pojedynczych obiektów, czy też urządzeń. W projekcie przyjęto założenie, iż nie każdą infrastrukturę krytyczną da się wykorzystać do świadczenia usługi kluczowej w rozumieniu dyrektywy 2022/2557, lecz każda usługa kluczowa „wymaga" infrastruktury krytycznej do jej świadczenia.

Dlatego też część spośród operatorów infrastruktury krytycznej, tj. właścicieli lub posiadaczy m.in. obiektów, urządzeń oraz instalacji lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji, które zostały wpisane do wykazu infrastruktury krytycznej, będzie mogła

uzyskać status podmiotu krytycznego na podstawie mechanizmu wskazanego w projektowanej regulacji.

W projekcie założono wzmocnienie mechanizmów ochrony każdej infrastruktury krytycznej, niezależenie od tego, czy stanowi ona element świadczenia usługi kluczowej, czy też nie. Wzięto pod uwagę, iż infrastruktura krytyczna to rdzeń sprawnego funkcjonowania państwa, zaspokajania potrzeb obywateli, w tym wspólnot o charakterze lokalnym.

Należy pamiętać, iż opracowanie kompleksowych mechanizmów zapewniających bezpieczeństwo funkcjonującej infrastrukturze krytycznej, ma obecnie bezpośredni związek z sytuacją geopolityczną Rzeczypospolitej Polskiej, w szczególności w związku z konfliktem zbrojnym na Ukrainie oraz zagrożeniami hybrydowymi towarzyszącymi temu konfliktowi.

Wprowadzenie i oznaczenie rozdziałów

Mając na względzie konieczność wdrożenia projektowanych rozwiązań w ustawie z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (dalej „ustawa z.k.”), projektowana regulacja wprowadza rozdziały do tej ustawy w celu zachowania czytelności zawartych w niej regulacji.

Zakres stosowania ustawy (art. 1 pkt 3 ustawy nowelizującej)

Zakres zmian dotyczy również konieczności zmiany zakresu przedmiotowego, jak i podmiotowego ustawy z.k. Obok organów właściwych w sprawach zarządzania kryzysowego pojawią się organy właściwe do spraw podmiotów krytycznych, którym ustawa z.k. wskaże zadania i obowiązki oraz określi zasady ich finansowania. Ustawa z.k. zostanie również rozszerzona o kwestie związane z tzw. usługami kluczowymi świadczonymi przez podmioty krytyczne.

Projektowane rozwiązania zawierają również wyłączenia od stosowania przepisów ustawy z.k. Regulacji w zakresie infrastruktury krytycznej, usług kluczowych i podmiotów krytycznych nie stosuje się do organów oraz jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych.

Regulacji w zakresie usług kluczowych i podmiotów krytycznych nie stosuje się również do podmiotów, które w zakresie swojej działalności prowadzą postępowania przygotowawcze, o których mowa w art. 297 ustawy z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego.

Słowniczek (art. 1 pkt 4 ustawy nowelizującej)

W projektowanych zmianach do słowniczka ustawy o zarządzaniu kryzysowym wskazać należy na:

- ✓ definicję sytuacji kryzysowej, zostanie uzupełniona o kwestie dotyczące dziedzictwa kulturowego. Projekt nowelizacji w definicji sytuacji kryzysowej uwzględnia postanowienia decyzji Parlamentu Europejskiego i Rady nr 1313/2013/EU z dnia 17 grudnia 2013 r. w sprawie Unijnego Mechanizmu Ochrony Ludności, która w art. 2 określa, że „Ochrona zapewniana w ramach unijnego mechanizmu obejmuje przede wszystkim ludzi, lecz także środowisko naturalne i mienie, w tym dziedzictwo kulturowe, i chroni je przed wszystkimi rodzajami klęsk żywiołowych i katastrof spowodowanych przez człowieka, w tym następstwami ataków terrorystycznych".

  Ponadto decyzja Parlamentu Europejskiego i Rady 2019/420 z dnia 13 marca 2019 r. zmieniająca decyzję nr 1313/2013/UE w sprawie Unijnego Mechanizmu Ochrony Ludności rozszerzyła katalog zagrożeń, jak też działań podejmowanych w sytuacji wystąpienia klęsk żywiołowych i katastrof spowodowanych przez człowieka. Brak regulacji dotyczących ochrony dziedzictwa kulturowego mógłby powodować, iż problematyka ta nie zostanie włączona do budowanego obecnie systemu przygotowań na zdarzenia nadzwyczajne, w szczególności w administracji publicznej różnych szczebli, między innymi poprzez podejmowane działania planistyczno-organizacyjne, szkoleniowe i kontrolne. Ponadto pozbawia instytucje kultury, w których zgromadzone są zbiory, a które stanowią dziedzictwo narodowe, z korzystania z zasobów ludzkich i sprzętowych, podmiotów wyspecjalizowanych w prowadzeniu akcji ratowniczych.

  Uzupełnienie dotychczasowej treści definicji o wskazanie istoty zakłóceń funkcjonowania organów administracji publicznej związane jest z faktem, iż przepisy ustawy o zarządzaniu kryzysowym przede wszystkim statuują oraz wskazują obowiązki i kompetencje organów administracji publicznej w ramach systemu zarządzania kryzysowego. Ich niezakłócona działalność jest gwarantem działań podejmowanych na rzecz szeroko rozumianej ochrony ludności;

- ✓ szereg definicji bazujących na definicjach zawartych w dyrektywie 2022/2557, w tym definicję podmiotu krytycznego, w którym przyjmuje się, iż podmiotem krytycznym w rozumieniu ustawy co do zasady jest operator infrastruktury krytycznej wpisanego do

wykazu podmiotów krytycznych, realizującego co najmniej jedną usługę kluczową, prowadzącego działalność w sektorze lub podsektorze wymienionym w załączniku do ustawy i prowadzącego działalność na terytorium Rzeczypospolitej Polskiej lub na obszarach morskich Rzeczypospolitej Polskiej.

Dyrektywa 2022/2557 wymaga infrastruktury krytycznej do świadczenia usługi kluczowej – tak więc najprostszym rozwiązaniem uwzględniającym obecny stan faktyczny i dotychczasową praktykę – jest wybór podmiotów krytycznych spośród operatorów infrastruktury krytycznej. Tak skonstruowana definicja uwzględnia obecny dorobek w zakresie ochrony infrastruktury krytycznej, który jest pomocny w implementacji dyrektywy 2022/2557. Obok definicji podmiotu krytycznego, słowniczek w tym obszarze zawiera definicje podmiotu krytycznego o szczególnym znaczeniu europejskim, który został zdefiniowany jako podmiot krytyczny świadczący co najmniej jedną usługę kluczową, spośród usług kluczowych wskazanych w przepisach rozporządzenia delegowanego wydanego na podstawie art. 5 ust. 1 dyrektywy 2022/2557, na rzecz co najmniej sześciu państw członkowskich Unii Europejskiej lub w co najmniej sześciu państwach członkowskich Unii Europejskiej, uznany za taki podmiot przez Komisję Europejską. Podmiotowi krytycznemu o szczególnym znaczeniu europejskim poświęcono odrębny rozdział w projektowanej ustawie;

- ✓ definicję usługi kluczowej – czyli usługę, która ma decydujące znaczenie dla utrzymania niezbędnych funkcji społecznych, niezbędnej działalności gospodarczej, zdrowia i bezpieczeństwa publicznego lub środowiska, wskazaną w przepisach aktu wykonawczego wydanego na podstawie projektowanego art. 6zp ust. 3 pkt 1;
- ✓ pojęcie odporności podmiotu krytycznego, przez które należy rozumieć zdolność do zapobiegania incydentowi, ochrony przed incydentem realizowanej w drodze zaplanowanych działań, z wykorzystaniem posiadanych zasobów, reagowania w przypadku wystąpienia incydentu i jego absorbowania oraz adaptacji i usuwania skutków incydentu, w tym odtwarzania infrastruktury krytycznej niezbędnej do świadczenia usługi kluczowej. Brzmienie definicji łączy w sobie wypracowane rozwiązania w zakresie ochrony infrastruktury krytycznej z nowym podejściem w zakresie ochrony prezentowanym w dyrektywie 2022/2557. Pojawiające się w definicji odporności pojęcie incydentu również zostało zdefiniowane w słowniczku w

podziale na incydent, przez który rozumiemy każde zdarzenie mające lub mogące mieć niekorzystny wpływ na świadczenie usługi kluczowej, oraz tzw. incydent istotny – czyli incydent, który powoduje lub może spowodować istotne obniżenie jakości lub przerwanie ciągłości świadczenia usługi kluczowej. W treści projektu wskazano działania związane z koniecznością obsługi tzw. incydentów istotnych, których progi Rada Ministrów wskaże w rozporządzeniu w odniesieniu do poszczególnych usług kluczowych;

- ✓ zdefiniowane pojęcie zagrożenia hybrydowego rozumianego jako kombinację wrogich działań realizowanych przy zastosowaniu środków politycznych, gospodarczych, dyplomatycznych, informacyjnych, militarnych lub innych, które nie stanowią agresji militarnej w ujęciu prawa międzynarodowego. Postanowiono również zdefiniować tzw. zagrożenie antagonistyczne, które jest rodzajem zagrożenia hybrydowego ukierunkowanego przeciwko usługom kluczowym i infrastrukturze krytycznej niezbędnej do świadczenia tych usług, realizowanego w sposób celowy i świadomy oraz bez względu na motywację postępowania sprawców;
- ✓ definicję infrastruktury krytycznej, która czerpie z obecnych rozwiązań i łączy je z podejściem zawartym w dyrektywie 2022/2557. Infrastruktura krytyczna w tym rozumieniu to obiekt, urządzenie, instalacja, sieć, system oraz usługa lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje, sieci, systemy oraz usługi niezbędne do realizacji ważnych interesów państwa, w tym zapewnienia funkcjonowania organów administracji publicznej, zapewnienia funkcjonowania przedsiębiorstw, zaspokajania oraz utrzymywania potrzeb obywateli, w tym potrzeb o charakterze lokalnym oraz zapewnienia świadczenia usług kluczowych. Dodatkowo projekt zawiera definicję potencjalnej infrastruktury krytycznej, czyli ww. elementów, będących w fazie projektowania lub budowy, które po ich zakończeniu mogą być niezbędne do realizacji celów tożsamych z celami przypisanymi dla infrastruktury krytycznej;
- ✓ zdefiniowano na użytek planistyki w zarządzaniu kryzysowym kwestie planów. I tak przez plany zarządzania kryzysowego rozumiemy plany zarządzania ryzykiem oraz plany reagowania kryzysowego;

  Plany zarządzania ryzykiem to Krajowy Plan Zarządzania Ryzykiem, plany zarządzania ryzykiem ministrów kierujących działami administracji rządowej i

kierowników urzędów centralnych oraz wojewódzkie, powiatowe i gminne plany zarządzania ryzykiem.

Natomiast plany reagowania kryzysowego to Krajowy Plan Reagowania Kryzysowego, plany reagowania kryzysowego ministrów kierujących działami administracji rządowej i kierowników urzędów centralnych oraz wojewódzkie, powiatowe i gminne plany reagowania kryzysowego;

- ✓ szereg definicji dotyczących pojęcia ryzyka, definiujących samo pojęcie ryzyka, ocenę ryzyka oraz zarządzanie ryzykiem, a które są niezbędne do opracowania planów zarządzania kryzysowego, jak również wdrażania rozwiązań dyrektywy CER w zakresie oceny ryzyka dla podmiotów krytycznych.

Dokumenty strategiczne (art. 1 pkt 7 ustawy nowelizującej)

Projekt wprowadza w ustawie z.k. rozdział „Dokumenty strategiczne". Do dokumentów strategicznych zalicza się tzw. Krajową Ocenę Ryzyka (zastępującą obecny Raport o zagrożeniach bezpieczeństwa narodowego) oraz Strategię Odporności Podmiotów Krytycznych, zastępującą Narodowy Program Ochrony Infrastruktury Krytycznej, a obejmującą zarówno kwestie infrastruktury krytycznej, jak i podmiotów krytycznych mających świadczyć usługi kluczowe.

Krajowa Ocena Ryzyka (projektowany art. 6e)

„Działania państw członkowskich mające na celu identyfikację podmiotów krytycznych i przyczynienie się do zapewniania ich odporności powinny być zgodne z podejściem opierającym się na analizie ryzyka skoncentrowanym na podmiotach najważniejszych dla pełnienia niezbędnych funkcji społecznych lub prowadzenia niezbędnej działalności gospodarczej. W celu zapewnienia takiego ukierunkowanego podejścia każde państwo członkowskie powinno przeprowadzić – w zharmonizowanych ramach – ocenę istotnych czynników ryzyka, naturalnych i spowodowanych przez człowieka, w tym tych o charakterze międzysektorowym lub transgranicznym, które mogą wpływać na świadczenie usług kluczowych, z uwzględnieniem wypadków, klęsk żywiołowych, stanów zagrożenia zdrowia publicznego, takich jak pandemie, oraz zagrożeń hybrydowych lub innych zagrożeń związanych z konfliktem, w tym przestępstw terrorystycznych, infiltracji przestępczej i

sabotażu (…). Wyniki ocen ryzyka państw członkowskich należy wykorzystać do celów identyfikacji podmiotów krytycznych i wspierania tych podmiotów w spełnianiu odnoszących się do nich wymogów dotyczących odporności.”.

Krajowa Ocena Ryzyka będzie opracowywana cyklicznie w celu dokonywania oceny ryzyka zidentyfikowanych zagrożeń. Będzie ona przyjmowana przez Radę Ministrów w drodze uchwały. Krajowa Ocena Ryzyka będzie punktem wyjścia dla programowania wielu procesów, gdyż Krajową Ocena Ryzyka uwzględnia się w:

- ✓ planach zarządzania kryzysowego na wszystkich szczeblach zarządzania kryzysowego;
- ✓ procesach identyfikacji podmiotów krytycznych;
- ✓ opracowywaniu ocen ryzyka dla podmiotów krytycznych oraz wdrażaniu przez podmioty krytyczne środków w zakresie zwiększenia ich odporności;
- ✓ innych dokumentach opracowywanych przez organy administracji publicznej w zakresie zarządzania kryzysowego.

Krajowa Ocena Ryzyka (dalej „KOR”) w założeniu ma zawierać zidentyfikowane istotne zagrożenia oraz zagrożenia niezidentyfikowane jednoznacznie, które mogą wystąpić w przyszłości. Do zidentyfikowanych istotnych zagrożeniami zaliczamy zagrożenia stanowiące katastrofę naturalną lub awarię techniczną w rozumieniu przepisów ustawy z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej, zagrożenia hybrydowe, cyberbezpieczeństwa, o charakterze terrorystycznym, zagrożenia mogące spowodować niedostępność usług kluczowych, jak również inne mogące spowodować znaczące negatywne skutki dla ludności, gospodarki lub dóbr kultury.

Ponadto KOR ma zawierać ocenę ryzyka wystąpienia zidentyfikowanych istotnych zagrożeń, przy opracowywaniu której – zgodnie z KOR – bierze się pod uwagę m.in. powiązania między zagrożeniami wynikające z oddziaływań transgranicznych, zależności międzysektorowych i zmian klimatu, ogólną ocenę ryzyka przeprowadzoną na podstawie art. 6 ust. 1 decyzji nr 1313/2013/UE oraz inne istotne oceny ryzyka przeprowadzone zgodnie z wymogami właściwych sektorowych aktów Unii Europejskiej.

Przy ocenie ryzyka dla podmiotów krytycznych uwzględnia się dodatkowo rodzaje usług kluczowych, zidentyfikowane zagrożenia antagonistyczne, istotne ryzyka wynikające ze stopnia wzajemnej zależności między sektorami określonymi w załączniku do ustawy, wpływ znaczącego zakłócenia w jednym sektorze na inne sektory, w tym wszelkie istotne czynniki

ryzyka dla obywateli i rynku wewnętrznego, wpływ, jaki znaczące zakłócenie w jednym sektorze może mieć wpływ na inne sektory, w tym wszelkie istotne czynniki ryzyka dla obywateli i rynku wewnętrznego oraz informacje dotyczące incydentów zgłaszanych przez podmioty krytyczne świadczące usługi kluczowe.

Na potrzeby opracowania projektu KOR – Dyrektor Centrum wydaje wytyczne do jego opracowania, które przekazuje ministrom kierującym działami administracji rządowej, Szefowi Agencji Bezpieczeństwa Wewnętrznego, Szefowi Agencji Wywiadu, Szefowi Centralnego Biura Antykorupcyjnego, wojewodom, Pełnomocnikowi Rządu do spraw Cyberbezpieczeństwa oraz innym podmiotom, jeżeli jest to konieczne.

Na podstawie wytycznych ww. podmioty, w zakresie swoich właściwości, opracowują propozycje do ujęcia w projekcie KOR i przekazują je Dyrektorowi Centrum we wskazanym przez niego terminie. Propozycje przekazywane są wraz z danymi stanowiącymi podstawę do ich przygotowania, z wyłączeniem informacji niejawnych. Dyrektor Centrum może wystąpić do tych podmiotów o przekazanie dodatkowych propozycji, jeżeli uzna, że ich umieszczenie w KOR jest niezbędne. Dyrektor Centrum uzasadnia wystąpienie przekazania dodatkowych propozycji.

Regulacja przewiduje, iż propozycje przekazane przez ministra kierującego działem administracji rządowej uwzględniają propozycje kierownika urzędu centralnego podległego temu ministrowi lub przez niego nadzorowanego. W tym celu kierownik urzędu centralnego podległy ministrowi kierującego działem administracji rządowej lub przez niego nadzorowany opracowuje i przekazuje wkład do propozycji ministra kierującego działem administracji rządowej.

Dyrektor Centrum przedkłada projekt KOR przedkłada się nie rzadziej niż raz na trzy lata.

Dodatkowo – w ramach sprawozdawczości – zgodnie z wymogami decyzji nr 1313/2013/UE Dyrektor Centrum, na podstawie KOR, opracowuje i udostępnia Komisji Europejskiej streszczenie istotnych elementów oceny ryzyka, o której mowa w art. 6 ust. 1 lit. a tejże decyzji.

Ponadto Dyrektor Centrum – na podstawie KOR – opracowuje i udostępnia Komisji Europejskiej informacje dotyczące rodzajów ryzyka w odniesieniu do sektorów i podsektorów, o których mowa w załączniku do ustawy.

Krajowa Strategia Odporności Podmiotów Krytycznych (projektowany art. 6f)

Drugim dokumentem strategicznym przewidzianym w projekcie jest dokument wymagany dyrektywą CER. „W celu zapewnienia kompleksowego podejścia do odporności podmiotów krytycznych każde państwo członkowskie powinno dysponować strategią mającą na celu zwiększenie odporności podmiotów krytycznych (…). Strategie powinny określać cele strategiczne i środki z zakresu polityki, które należy wdrożyć. Dla zachowania spójności i efektywności strategia powinna zostać opracowana w taki sposób, aby sprawnie zintegrować istniejące polityki, w miarę możliwości opierając się na odpowiednich istniejących strategiach krajowych i sektorowych, planach lub podobnych dokumentach. Aby wypracować kompleksowe podejście, państwa członkowskie powinny zapewnić, aby ich strategie przewidywały ramy polityczne umożliwiające zwiększoną koordynację między właściwymi organami na mocy niniejszej dyrektywy i właściwymi organami na mocy dyrektywy (UE) 2022/2555, w kontekście wymiany informacji na temat ryzyk w cyberprzestrzeni, cyberzagrożeń i cyberincydentów oraz ryzyk, zagrożeń i incydentów poza cyberprzestrzenią oraz w kontekście wykonywania zadań nadzorczych. Przy określaniu swoich strategii państwa członkowskie powinny należycie uwzględnić hybrydowy charakter zagrożeń dotyczących podmiotów krytycznych.”.

W celu zwiększenia odporności podmiotów krytycznych opracowuje się Krajową Strategię Odporności Podmiotów Krytycznych (dalej: „KSOPK”), która Rada Ministrów przyjmuje, w drodze uchwały.

KSOPK określa cele strategiczne i priorytety w zakresie zapewnienia niezakłóconego świadczenia usług kluczowych przez podmioty krytyczne oraz niezakłóconego funkcjonowania infrastruktury krytycznej.

Dodatkowo KSOPK ma określić zakresy działań oraz formy działań służące osiąganiu celów strategicznych i priorytetów przez organy właściwe w sprawach podmiotów krytycznych, oraz organy identyfikujące infrastrukturę krytyczną, jak również inne podmioty, które mają być zaangażowane w realizację KSOPK.

Ponadto KSOPK zawierać będzie opisy procesów identyfikujących podmioty krytyczne, środków niezbędnych do zwiększenia ogólnej odporności podmiotów krytycznych, środków mających na celu ułatwienie wypełniania obowiązków wynikających z rozdziału III dyrektywy 2022/2557 przez małe i średnie przedsiębiorstwa, w rozumieniu załącznika do zalecenia Komisji 2003/361/W, które zostały zidentyfikowane jako podmioty krytyczne.

Dodatkowo KSOPK określa zakres koordynacji działań organów do spraw podmiotów krytycznych i organów właściwych do spraw cyberbezpieczeństwa, o których mowa w ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

W celu opracowania projektu KSOPK – Dyrektor Centrum wydaje wytyczne do jej opracowania i przekazuje ministrom kierującym działami administracji rządowej, Szefowi Agencji Bezpieczeństwa Wewnętrznego, Szefowi Agencji Wywiadu, Szefowi Centralnego Biura Antykorupcyjnego, Komisji Nadzoru Finansowego, wojewodom oraz innym podmiotom, jeżeli jest to konieczne.

Organy i podmioty, w zakresie swoich właściwości, opracowują z uwzględnieniem wytycznych propozycje do ujęcia w projekcie KSOPK i przekazują je Dyrektorowi Centrum we wskazanym przez niego terminie. Propozycje przekazywane są z danymi stanowiącymi podstawę do ich przygotowania, z wyłączeniem informacji niejawnych. W przypadku konieczności pozyskania dodatkowych informacji – Dyrektor Centrum może wystąpić do organów i podmiotów przygotowujących propozycje do projektu Strategii o przekazanie dodatkowych propozycji, jeżeli uzna, że ich umieszczenie w KSOPK jest niezbędne.

W przypadku propozycji przekazywanych przez ministra kierującego działem administracji rządowej – obejmują one propozycje kierownika urzędu centralnego podległego temu ministrowi lub przez niego nadzorowanego. Natomiast po stronie kierownika urzędu centralnego podległy ministrowi kierującego działem administracji rządowej lub przez niego nadzorowany pozostaje opracowanie i przekazanie wkład do propozycji ministra kierującego działem administracji rządowej.

Na etapie projektowania KSOPK – Dyrektor Centrum kieruje projekt KSOPK do 30-dniowych konsultacji publicznych, z przeprowadzenia których sporządza raport, wskazując główne tezy zawarte w stanowiskach zgłoszonych do projektu KSOPK oraz odniesienie się do nich. Raport będzie każdorazowo udostępniany na stronie podmiotowej Biuletynu Informacji Publicznej Centrum.

Dyrektor Centrum przedkłada Radzie Ministrów projekt KSOPK nie rzadziej niż raz na trzy lata. Dyrektor Centrum udostępnia Komisji Europejskiej przyjętą przez Radę Ministrów KSOPK najpóźniej w terminie trzech miesięcy od jej przyjęcia (jej znaczące aktualizacje – jeżeli będą – również).

Ponadto Dyrektor Centrum monitoruje wdrażanie KSOPK oraz w terminie do dnia 31 marca każdego roku przedkłada Radzie Ministrów sprawozdanie z jej wdrażania za poprzedni rok.

Plany zarządzania kryzysowego (art. 1 pkt 7 ustawy nowelizującej)

Projekt zakłada – w celu realizacji zadań z zakresu planowania cywilnego – opracowywanie planów zarządzania kryzysowego na wszystkich szczeblach zarządzania kryzysowego, w podziale na plany zarządzania ryzykiem oraz plany reagowania kryzysowego.

Plany zarządzania ryzykiem (projektowane art. 6g–6i)

Projekt – definiując plany zarządzania ryzykiem – wskazuje wspólne elementy tych planów. Plany zarządzania ryzykiem zawierają bowiem takie same elementy na wszystkich szczeblach zarządzania kryzysowego.

Wspólna pozostaje część zarządzania ryzykiem, która na wszystkich szczeblach zawiera następujące elementy:

- ✓ cele strategiczne;
- ✓ opis zasad współdziałania między podmiotami wskazanymi w siatce bezpieczeństwa;
- ✓ uporządkowaną listę działań na rzecz ograniczenia ryzyka katastrof w zakresie organizacyjnym, technicznym i finansowym, z uwzględnieniem:
    - o hierarchii działań,
    - o ram czasowych ich realizacji,
    - o podmiotów wiodących oraz współpracujących przy ich wykonywaniu,
    - o sposobów finansowania oraz wysokości nakładów finansowych,
    - o oceny osiągniętych efektów oraz wniosków z wdrożonych działań.

Plany zarządzania ryzykiem opracowują:

- ✓ dyrektor Centrum – Krajowy Plan Zarządzania Ryzykiem („KPZR”);
- ✓ minister kierujący działem administracji rządowej – plan zarządzania ryzykiem ministra kierującego działem administracji rządowej;
- ✓ Szef Agencji Bezpieczeństwa Wewnętrznego, Szef Agencji Wywiadu oraz Szef Centralnego Biura Antykorupcyjnego – plan zarządzania ryzykiem odpowiednio Szefa Agencji Bezpieczeństwa Wewnętrznego, Szefa Agencji Wywiadu oraz Szefa Centralnego Biura Antykorupcyjnego;

- ✓ kierownik urzędu centralnego wskazany przez ministra kierującego działem administracji rządowej, któremu podlega lub jest przez tego ministra nadzorowany – plan zarządzania ryzykiem kierownika urzędu centralnego;
- ✓ wojewoda – wojewódzki plan zarządzania ryzykiem;
- ✓ starosta – powiatowy plan zarządzania ryzykiem;
- ✓ wójt (burmistrz, prezydent miasta) – gminny plan zarządzania ryzykiem.

Punktem odniesienia do opracowywania planów zarządzania ryzykiem są przede wszystkim zagrożenia wskazane w KOR.

W celu opracowania projektu KPZR – Dyrektor Centrum wydaje wytyczne do jego opracowania i przekazuje ministrom kierującym działami administracji rządowej, Szefowi Agencji Bezpieczeństwa Wewnętrznego, Szefowi Agencji Wywiadu oraz Szefowi Centralnego Biura Antykorupcyjnego, wojewodom oraz innym podmiotom, jeżeli jest to konieczne.

Ww. organy i podmioty opracowują z uwzględnieniem wytycznych propozycje do ujęcia w projekcie KPZR i przekazują je Dyrektorowi Centrum we wskazanym przez niego terminie, przekazując jednocześnie dane stanowiące podstawę do przygotowania propozycji, z wyłączeniem informacji niejawnych.

Dyrektor Centrum może wystąpić do organów i podmiotów przygotowujących propozycje do projektu o przekazanie dodatkowych propozycji, jeżeli uzna, że ich umieszczenie w KPZR będzie niezbędne.

Propozycje przekazane przez ministra kierującego działem administracji rządowej uwzględniają propozycje kierownika urzędu centralnego podległego temu ministrowi lub przez niego nadzorowanego, a kierownik urzędu centralnego podległy ministrowi kierującego działem administracji rządowej lub przez niego nadzorowany opracowuje dlatego ministra stosowny wkład do propozycji.

Dyrektor Centrum przedkłada Radzie Ministrów projekt KPZR nie rzadziej niż raz na trzy lata. Rada Ministrów przyjmuje KPZR w drodze uchwały, a następnie Dyrektor Centrum udostępnia KPZR na stronie podmiotowej Biuletynu Informacji Publicznej Centrum.

W ramach unijnej sprawozdawczości – na podstawie KPZR Dyrektor Centrum opracowuje i udostępnia Komisji Europejskiej tzw. streszczenie istotnych elementów krajowej oceny zdolności zarządzania ryzykiem, o której mowa w art. 6 ust. 1 lit. b decyzji 1313/2013/UE.

W przypadku planu zarządzania ryzykiem ministra kierującego działem administracji rządowej – plan ten obejmuje własny plan zarządzania ryzykiem ministra oraz plany zarządzania kryzysowego kierowników urzędów centralnych podległych temu ministrowi lub przez niego nadzorowanych.

Niemniej jednak minister kierujący działem administracji, w zakresie swojej właściwości, może wskazać kierownika urzędu centralnego podległego lub nadzorowanego, który będzie zobowiązany do opracowania własnego planu zarządzania ryzykiem.

W przypadku planu zarządzania ryzykiem Ministra Obrony Narodowej – uwzględnia się w tym planie zarządzania ryzykiem Szefa Służby Kontrwywiadu Wojskowego oraz Szefa Służby Wywiadu Wojskowego.

Projektowane przepisy o charakterze proceduralnym przewidują usystematyzowany proces uzgadniania i zatwierdzania planów zarządzania ryzykiem.

Minister kierujący działem administracji rządowej, Szef Agencji Bezpieczeństwa Wewnętrznego, Szef Agencji Wywiadu, Szef Centralnego Biura Antykorupcyjnego:

- ✓ uzgadnia projekt planu zarządzania ryzykiem z dyrektorem Centrum pod względem spójności z KPZR;
- ✓ zatwierdza uzgodniony plan zarządzania ryzykiem;
- ✓ przekazuje kopię zatwierdzonego planu zarządzania ryzykiem dyrektorowi Centrum.

Kierownik urzędu centralnego, wskazany przez ministra do opracowania własnego planu, o którym mowa w ust. 2:

- ✓ uzgadnia projekt planu zarządzania ryzykiem z ministrem kierującym działem administracji rządowej, któremu podlega lub przez którego jest nadzorowany;
- ✓ uzgadnia projekt planu zarządzania ryzykiem z dyrektorem Centrum pod względem spójności z KPZR;
- ✓ zatwierdza uzgodniony plan zarządzania ryzykiem;
- ✓ przekazuje kopię zatwierdzonego planu zarządzania ryzykiem właściwemu ministrowi oraz dyrektorowi Centrum.

W przypadku wojewody:

- ✓ przekazuje projekt wojewódzkiego planu zarządzania ryzykiem do zatwierdzenia ministrowi właściwemu do spraw administracji publicznej;

- ✓ przekazuje zatwierdzony wojewódzki plan zarządzania ryzykiem do wiadomości dyrektorowi Centrum.

Starosta przekazuje projekt powiatowego planu zarządzania ryzykiem do zatwierdzenia właściwemu wojewodzie, natomiast wójt (burmistrz, prezydent miasta) przekazuje projekt gminnego planu zarządzania ryzykiem do zatwierdzenia właściwemu staroście.

Plany reagowania kryzysowego (art. 6j–6n)

Plany reagowania kryzysowego opracowują:

- ✓ dyrektor Centrum – Krajowy Plan Zarządzania Ryzykiem ("KPRK");
- ✓ minister kierujący działem administracji rządowej – plan reagowania kryzysowego ministra kierującego działem administracji rządowej;
- ✓ Szef Agencji Bezpieczeństwa Wewnętrznego, Szef Agencji Wywiadu oraz Szef Centralnego Biura Antykorupcyjnego – plan reagowania kryzysowego odpowiednio Szefa Agencji Bezpieczeństwa Wewnętrznego, Szefa Agencji Wywiadu oraz Szefa Centralnego Biura Antykorupcyjnego;
- ✓ kierownik urzędu centralnego wskazany przez ministra kierującego działem administracji rządowej, któremu podlega lub jest przez tego ministra nadzorowany – plan reagowania kryzysowego kierownika urzędu centralnego;
- ✓ wojewoda – wojewódzki plan reagowania kryzysowego;
- ✓ starosta – powiatowy plan reagowania kryzysowego;
- ✓ wójt (burmistrz, prezydent miasta) – gminny plan reagowania kryzysowego.

Każdy z ww. planów rozpisany jest odmiennie dla każdego z poziomów zarządzania kryzysowego.

Krajowy Plan Reagowania Kryzysowego zawiera:

- ✓ określenie zadań i obowiązków uczestników zarządzania kryzysowego w formie siatki bezpieczeństwa w zakresie reagowania w przypadku wystąpienia sytuacji kryzysowej oraz usuwania jej skutków;
- ✓ zasady współdziałania między uczestnikami, w tym dotyczące wymiany informacji w relacjach krajowych i międzynarodowych;
- ✓ zestawienie sił i środków planowanych do wykorzystania w sytuacjach kryzysowych;
- ✓ zestawienie modułów zadaniowych pogrupowanych w katalogi;

- ✓ załączniki określające:
    - organizację systemu monitorowania zagrożeń, ostrzegania i alarmowania,
    - organizację łączności,
    - zasady informowania ludności o zagrożeniach i sposobach postępowania na wypadek zagrożeń,
    - zasady oraz tryb oceniania i dokumentowania strat i szkód,
    - procedury uruchamiania rezerw strategicznych,
    - procedury reagowania kryzysowego – standardowe procedury operacyjne,
    - priorytety w zakresie ochrony oraz odtwarzania infrastruktury krytycznej.

Dyrektor Centrum we współpracy z ministrami kierującymi działami administracji rządowej, kierownikami urzędów centralnych oraz wojewodami opracowuje projekt KPRK.

Dyrektor Centrum przedkłada projekt KPRK Radzie Ministrów nie rzadziej niż raz na trzy lata. Rada Ministrów przyjmuje KPRK w drodze uchwały.

Plan reagowania kryzysowego ministra kierującego działem administracji rządowej, Szefa Agencji Bezpieczeństwa Wewnętrznego, Szefa Agencji Wywiadu, Szefa Centralnego Biura Antykorupcyjnego oraz kierownika urzędu centralnego podległego ministrowi kierującemu działem administracji rządowej lub przez niego nadzorowanego zawiera:

- ✓ określenie zadań i obowiązków uczestników zarządzania kryzysowego w formie siatki bezpieczeństwa w zakresie reagowania w przypadku wystąpienia sytuacji kryzysowej oraz usuwania jej skutków;
- ✓ określenie zadań w zakresie monitorowania zagrożeń;
- ✓ zestawienie przedsięwzięć realizowanych w ramach przypisanych katalogów i modułów zadaniowych wraz z ich opisem;
- ✓ określenie organizacji realizacji zadań z zakresu ochrony infrastruktury krytycznej lub zapewnienia ciągłości świadczenia usług kluczowych.

Co do zasady plan reagowania kryzysowego ministra kierującego działem administracji rządowej obejmuje plany reagowania kryzysowego kierowników urzędów centralnych podległych temu ministrowi lub przez niego nadzorowanych.

Minister kierujący działem administracji, w zakresie swojej właściwości, wskazuje kierowników urzędów centralnych podległych lub nadzorowanych, którzy są zobowiązanych do opracowania własnych planów reagowania kryzysowego.

W przypadku planu reagowania kryzysowego Ministra Obrony Narodowej jego integralną treścią są treści planów reagowania kryzysowego Szefa Służby Kontrwywiadu Wojskowego oraz Szefa Służby Wywiadu Wojskowego.

Przepisy o charakterze proceduralnym wskazują, iż minister kierujący działem administracji rządowej, Szef Agencji Bezpieczeństwa Wewnętrznego, Szef Agencji Wywiadu, Szef Centralnego Biura Antykorupcyjnego:

- ✓ uzgadnia projekt planu reagowania kryzysowego z Dyrektorem Centrum pod względem spójności z KPRK;
- ✓ zatwierdza uzgodniony z Dyrektorem Centrum plan reagowania kryzysowego;
- ✓ przekazuje zatwierdzony plan reagowania kryzysowego do wiadomości Dyrektorowi Centrum.

W przypadku kierownika urzędu centralnego, który opracowuje plan samodzielnie, uzgadnia on projekt planu reagowania kryzysowego z właściwym ministrem oraz uzgadnia projekt planu z Dyrektorem Centrum pod względem spójności z KPRK, zatwierdza uzgodniony plan zarządzania kryzysowego, a następnie przekazuje zatwierdzony plan zarządzania kryzysowego do wiadomości właściwemu ministrowi oraz Dyrektorem Centrum.

Plan reagowania kryzysowego opracowywany przez wojewodę składa się standardowo z części reagowania kryzysowego obejmującej wspólne elementy z planami wyższego rzędu oraz dodatkowo zestawienia przedsięwzięć minimalizujących skutki zakłócenia funkcjonowania infrastruktury krytycznej dla ludności na terenie województwa wraz z ich opisem. Wojewoda opracowuje projekt swojego planu, przekazuje projekt wojewódzkiego planu reagowania kryzysowego do zatwierdzenia ministrowi właściwemu do spraw administracji publicznej, a następnie przekazuje zatwierdzony wojewódzki plan reagowania kryzysowego do wiadomości Dyrektorowi Centrum.

Powiatowy plan reagowania kryzysowego oraz gminny plan reagowania kryzysowego składa się standardowo z części reagowania kryzysowego obejmujących wspólne elementy z planami wyższego rzędu, a dodatkowo zawiera zestawienie przedsięwzięć minimalizujących skutki zakłócenia funkcjonowania infrastruktury krytycznej dla ludności na terenie właściwej jednostki samorządu terytorialnego, wraz z ich opisem.

Opracowany projekt planu starosta przekazuje do zatwierdzenia właściwemu wojewodzie. Natomiast wójt (burmistrz, prezydent miasta) przekazuje projekt gminnego planu reagowania kryzysowego do zatwierdzenia właściwemu staroście.

Ww. plany – zgodnie z projektem ustawy – podlegają systematycznej aktualizacji w cyklu planowania nie dłuższym niż trzy lata.

Infrastruktura krytyczna (art. 1 pkt 7 ustawy nowelizującej)

Zadania dotyczące infrastruktury krytycznej (projektowany art. 6p–6q)

„Chociaż pewne środki istniejące na poziomie (…) krajowym mają na celu wspieranie ochrony infrastruktury krytycznej w Unii, należy zrobić więcej, aby lepiej przygotować podmioty będące operatorami takiej infrastruktury do reagowania na ryzyko dla ich funkcjonowania, które mogłoby prowadzić do zakłóceń w świadczeniu usług kluczowych. Należy również zrobić więcej, aby lepiej przygotować takie podmioty na dynamiczny krajobraz zagrożeń, obejmujący m.in. ewoluujące zagrożenia hybrydowe i terrorystyczne, i na rosnące współzależności między infrastrukturą a sektorami. Ponadto istnieje zwiększone fizyczne ryzyko związane z klęskami żywiołowymi i zmianą klimatu, która zwiększa częstotliwość i skalę ekstremalnych zdarzeń pogodowych i wywołuje długoterminowe zmiany średnich warunków klimatycznych, co może ograniczyć zdolności, skuteczność i okres eksploatacji niektórych rodzajów infrastruktury, jeżeli nie zostaną wdrożone środki z zakresu przystosowania się do zmiany klimatu.”.

Projektowana regulacja przewiduje, iż zadania w zakresie infrastruktury krytycznej obejmują:

- ✓ identyfikację oraz wyznaczanie infrastruktury krytycznej;
- ✓ gromadzenie i przetwarzanie informacji dotyczących zagrożeń infrastruktury krytycznej;
- ✓ opracowywanie i wdrażanie procedur na wypadek wystąpienia zagrożeń infrastruktury krytycznej;
- ✓ odtwarzanie infrastruktury krytycznej;
- ✓ współpracę między organami administracji publicznej a operatorami infrastruktury krytycznej w zakresie ochrony infrastruktury krytycznej.

Organami właściwymi w sprawie identyfikacji infrastruktury krytycznej oraz współpracy z operatorami infrastruktury krytycznej, w zakresie swoich właściwości, są ministrowie kierujący działami administracji rządowej, wojewodowie oraz Komisja Nadzoru Finansowego. Wykonują oni swoje zadania we współpracy z Dyrektorem Centrum.

Minister kierujący działem administracji rządowej, wojewoda, Komisja Nadzoru Finansowego, w zakresie swojej właściwości, oraz Dyrektor Centrum, zapewniają bieżącą współpracę z operatorem infrastruktury krytycznej, w szczególności przez:

- ✓ prowadzenie bieżącej wymiany informacji na temat bieżących zagrożeń;
- ✓ organizowanie spotkań dotyczących dobrych praktyk w zakresie ochrony infrastruktury krytycznej, w tym konferencji, seminariów lub forów;
- ✓ udzielanie wsparcia merytorycznego operatorom infrastruktury krytycznej:
  - o w zakresie wdrażania dobrych praktyk oraz niezbędnych rozwiązań dotyczących ochrony infrastruktury krytycznej,
  - o w celu zapewnienia właściwego funkcjonowania infrastruktury krytycznej, jej ochrony lub odbudowy,
  - o w sytuacji kryzysowej lub w przypadku możliwości wystąpienia sytuacji kryzysowej.

Identyfikowanie infrastruktury krytycznej (projektowane art. 6r–6x)

Obecne regulacje w zakresie m.in. identyfikowania infrastruktury krytycznej są „rozproszone" między przepisy ustawy, aktu wykonawczego do ustawy dotyczącego Narodowego Programu Ochrony Infrastruktury Krytycznej oraz sam Narodowy Program. Proponowane regulacje porządkują kwestie infrastruktury krytycznej wskazując czytelnie regulacje obejmujące:

Dyrektor Centrum prowadzi wykaz infrastruktury krytycznej w celu:

- ✓ identyfikacji obiektu, urządzenia oraz instalacji lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji oraz sieci, systemów lub usług jako infrastruktury krytycznej;
- ✓ zapewnienia realizacji zadań w zakresie ochrony infrastruktury krytycznej.

Wykaz prowadzony przez Dyrektora Centrum zawiera:

- ✓ nazwę i lokalizację infrastruktury krytycznej, w tym wskazanie infrastruktury krytycznej niezbędnej do świadczenia usług kluczowych;
- ✓ dane operatora infrastruktury krytycznej, w tym siedzibę i adres oraz numer identyfikacji podatkowej (NIP), jeżeli został nadany;
- ✓ wskazanie organu identyfikującego infrastrukturę krytyczną.

Wykaz prowadzony jest w postaci elektronicznej, a do wykazu stosuje się przepisy ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych.

Aby obiekt, urządzenie oraz instalacja lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje oraz sieć, system lub usługa mogły być wpisane do wykazu, muszą spełniać kryteria, które określa uchwałą Rada Ministrów. Kryteria w uchwale będą podzielone na kryteria sektorowe i przekrojowe, a wytycznymi do wydania tego rozporządzenia będzie ich znaczenie dla realizacji interesów państwa, funkcjonowania przedsiębiorców, zaspokajania potrzeb obywateli, w tym potrzeb o charakterze lokalnym oraz zapewnienie świadczenia usług kluczowych. Do uchwały zastosowanie będą miały przepisy ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych.

Dyrektor Centrum dokonuje wpisu do wykazu infrastruktury krytycznej na podstawie wniosku złożonego, w zakresie swojej właściwości, przez ministra kierującego działem administracji rządowej, właściwego miejscowo wojewodę oraz Komisję Nadzoru Finansowego.

Minister kierujący działem administracji rządowej we współpracy z Dyrektorem Centrum identyfikuje obiekt, urządzenie, instalację lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje oraz sieć, system lub usługę mogące stanowić infrastrukturę krytyczną.

W przypadku identyfikacji prowadzonej przez ministra kierującego działem administracji rządowej, obiekt, urządzenie oraz instalacja lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje oraz sieć, system lub usługa zostają wpisane do wykazu infrastruktury krytycznej, jeżeli spełniają łącznie kryterium sektorowe, oraz co najmniej jedno z kryteriów przekrojowych.

W celu ustalenia stanu faktycznego minister kierujący działem administracji rządowej może wystąpić do właściciela lub posiadacza obiektu, urządzenia, instalacji lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji oraz sieci, systemu lub usługi o udzielenie informacji, które umożliwią ocenę, czy spełniają one warunki do uznania ich za infrastrukturę krytyczną, przekazując dokumenty niezbędne do udzielenia informacji. Minister kierujący działem administracji rządowej w wystąpieniu wskazuje termin udzielenia informacji, który nie może być krótszy niż 14 dni, licząc od dnia otrzymania wystąpienia przez podmiot.

Minister kierujący działem administracji rządowej składa do Dyrektora Centrum wniosek o wpis obiektu, urządzenia, instalacji lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji oraz sieci, systemu lub usługi do wykazu infrastruktury krytycznej. Wniosek zawiera informacje obejmujące:

- ✓ nazwę i lokalizację obiektu, urządzenia oraz instalacji lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji oraz sieci, systemu lub usługi;
- ✓ dane właściciela lub posiadacza obiektu, urządzenia oraz instalacji lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji oraz sieci, systemu lub usługi, w tym siedzibę i adres oraz numer identyfikacji podatkowej (NIP), jeżeli został nadany.

Podobnie jak ministrowie kierujący działami administracji rządowej – również wojewodowie, we współpracy z Dyrektorem Centrum, identyfikują obiekty, urządzenia, instalacje lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje oraz sieci, systemy lub usługi mogące stanowić infrastrukturę krytyczną na terenie województwa.

W przypadku identyfikacji prowadzonej przez wojewodę, obiekt, urządzenie oraz instalacja lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje oraz sieć, system lub usługa mogą zostać wpisane do wykazu infrastruktury krytycznej, jeżeli spełniają co najmniej jedno z kryteriów przekrojowych. Proces weryfikacji przez wojewodę właściciela lub posiadacza, który może zostać ujęty w wykazie oraz jego wpisu do wykazu jest analogiczny do procesu prowadzonego przez ministra.

Analogicznie do ww. organów mogących identyfikować infrastrukturę krytyczną – Komisja Nadzoru Finansowego, w zakresie swojej właściwości, we współpracy z Dyrektorem Centrum, identyfikuje obiekt, urządzenie, instalację lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje oraz sieć, system lub usługę mogące stanowić infrastrukturę krytyczną.

W przypadku identyfikacji prowadzonej przez Komisję Nadzoru Finansowego, obiekt, urządzenie oraz instalacja lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje oraz sieć, system lub usługa mogą zostać wpisane do wykazu infrastruktury krytycznej, jeżeli spełniają łącznie kryterium sektorowe oraz co najmniej jedno z kryteriów przekrojowych. Proces weryfikacji właściciela lub posiadacza, który może zostać ujęty w wykazie oraz jego wpisu do wykazu jest analogiczny do procesu prowadzonego przez ministra.

Dyrektor Centrum – prowadzący wykaz – informuje właściciela lub posiadacza obiektu, urządzenia, instalacji lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji oraz sieci, systemu lub usługi o dokonaniu wpisu do wykazu infrastruktury krytycznej oraz obowiązkach z tym związanych w terminie 30 dni od wpisu do wykazu. Informacje o realizacji czynności w tym zakresie przekazuje organowi wnioskującemu o wpis do wykazu.

W celu zapewnienia przejrzystości procesów związanych z identyfikacją infrastruktury krytycznej organy identyfikujące oraz Dyrektor Centrum, prowadzą bieżącą wymianę

informacji dotyczących realizacji czynności w zakresie identyfikacji obiektów, urządzeń oraz instalacji lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji oraz sieci, systemów lub usług, które mogą zostać wpisane do wykazu infrastruktury krytycznej.

Identyfikowanie potencjalnej infrastruktury krytycznej (projektowane art. 6y–6zd)

Dyrektor Centrum prowadzi wykaz potencjalnej infrastruktury krytycznej w celu identyfikacji obiektu, urządzenia oraz instalacji lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji oraz sieci, systemu lub usługi, będących na etapie projektowania lub budowy jako potencjalnej infrastruktury krytycznej oraz zapewnienia realizacji zadań w zakresie ochrony potencjalnej infrastruktury krytycznej.

Wykaz zawiera:

- ✓ nazwę i lokalizację potencjalnej infrastruktury krytycznej;
- ✓ dane podmiotu będącego inwestorem, w rozumieniu ustawy z dnia 7 lipca 1994 r. – Prawo budowlane (Dz. U. z 2025 r. poz. 418, z późn. zm.), prowadzącego prace projektowe lub budowlane dotyczące potencjalnej infrastruktury krytycznej, w tym siedzibę i adres oraz numer identyfikacji podatkowej (NIP), jeżeli został nadany;
- ✓ wskazanie organu identyfikującego potencjalną infrastrukturę krytyczną.

Wykaz prowadzony jest w postaci elektronicznej. Do wykazu stosuje się przepisy ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych.

Obiekt, urządzenie oraz instalacja lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje oraz sieci, systemy lub usługi, które są na etapie projektowania lub budowy mogą zostać wpisane do wykazu, w przypadku gdy z założeń projektowanych wynika, że spełnia kryteria przewidziane dla infrastruktury krytycznej.

Dyrektor Centrum dokonuje wpisu do wykazu potencjalnej infrastruktury krytycznej na podstawie wniosku złożonego przez ministra kierującego działem administracji rządowej, właściwego miejscowo wojewodę lub Komisję Nadzoru Finansowego.

Minister kierujący działem administracji rządowej, wojewoda oraz Komisja Nadzoru Finansowego we współpracy z Dyrektorem Centrum oraz inwestorem identyfikuje potencjalną infrastrukturę krytyczną.

Regulacje dotyczące kryteriów identyfikowania oraz procedury w zakresie identyfikowania są tożsame z regulacjami dotyczącymi infrastruktury krytycznej.

Dyrektor Centrum informuje inwestora o dokonaniu wpisu do wykazu potencjalnej infrastruktury krytycznej oraz obowiązkach z tym związanych w terminie 30 dni od wpisu do wykazu.

Właściwy organ, odpowiedzialny za identyfikację wraz z Dyrektorem Centrum, przedstawiają inwestorowi informacje oraz dokumenty pozwalające na uwzględnienie wymogów dotyczących infrastruktury krytycznej w dokumentacji projektowej lub podczas realizacji inwestycji oraz zapewniają bieżącą współpracę w zakresie ochrony infrastruktury krytycznej.

Dodatkowo projekt wskazuje, iż podmioty identyfikują potencjalną infrastrukturę krytyczną oraz dyrektor Centrum, prowadzą bieżącą wymianę informacji dotyczących realizacji czynności w zakresie identyfikacji obiektów, urządzeń, instalacji, sieci, systemów oraz usług lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji, sieci, systemów oraz usług będących w fazie projektowania lub budowy, które mogą zostać wpisane do wykazu potencjalnej infrastruktury krytycznej. Przepis zapewnia tym samym podstawy do wymiany informacji dotyczących czynności realizowanych w ramach identyfikacji potencjalnej infrastruktury krytycznej, finalnie prowadzących do jej ujmowania w wykazie.

Wdrażanie rozwiązań w zakresie ochrony infrastruktury krytycznej (projektowany art. 6ze)

Zgodnie z projektowanymi rozwiązaniami operator infrastruktury krytycznej zapewnia jej ochronę. W ramach działań związanych z ochroną przewiduje się prowadzenie systematycznej analizy zagrożeń dla infrastruktury krytycznej oraz wdrażanie adekwatnych do przeprowadzonej analizy zagrożeń rozwiązania w zakresie:

- ✓ bezpieczeństwa fizycznego, w tym ochrony fizycznej oraz zabezpieczeń technicznych uwzględniających kontrolę dostępu;
- ✓ bezpieczeństwa technicznego;
- ✓ bezpieczeństwa osobowego dotyczącego pracowników i dostawców zewnętrznych;
- ✓ cyberbezpieczeństwa;
- ✓ bezpieczeństwa prawnego;

- ✓ ciągłości działania i odtwarzania, w tym utrzymywania własnych systemów rezerwowych zapewniających bezpieczeństwo i podtrzymujących funkcjonowanie infrastruktury krytycznej do czasu jej pełnego odtworzenia.

Operator infrastruktury krytycznej przeprowadza po raz pierwszy analizę zagrożeń w terminie 6 miesięcy od dnia otrzymania informacji o dokonaniu wpisu do wykazu infrastruktury krytycznej.

Operator infrastruktury krytycznej wdraża rozwiązania w terminie 6 miesięcy od dnia przeprowadzenia po raz pierwszy analizy zagrożeń, a następnie stosowanie do potrzeb, w zależności od wyników przeprowadzonej analizy zagrożeń.

Ponadto operator infrastruktury krytycznej ma obowiązek prowadzenia bieżącej współpracy z organami zarządzania kryzysowego, służbami, stażami i inspekcjami oraz Dyrektorem Centrum w zakresie przekazywanie i odbieranie informacji o zagrożeniach zakłócających lub mogących zakłócić funkcjonowanie infrastruktury krytycznej lub spodziewanych przerwach lub zakłóceniach w funkcjonowaniu infrastruktury krytycznej.

Obowiązkiem operatora jest również zapewnienie zdolności do ochrony informacji niejawnych, w przypadku gdy jest konieczne do realizacji przedsięwzięć związanych z ochroną infrastruktury krytycznej.

Wdrażanie ww. rozwiązań w zakresie bezpieczeństwa infrastruktury krytycznej ma się odbywać z uwzględnieniem tzw. minimalnych wymagań odnoszących się do poszczególnych obszarów bezpieczeństwa. Projekt wskazuje, iż Rada Ministrów określi, w drodze rozporządzenia, minimalne wymagania w zakresie bezpieczeństwa fizycznego, technicznego, osobowego, cyberbezpieczeństwa, prawnego oraz ciągłości działania, niezbędne do wdrażania rozwiązań w ww. obszarach. Jako wytyczne do wydania rozporządzania przewiduje się: rekomendacje o charakterze specjalistycznym w zakresie ochrony infrastruktury krytycznej, lokalizację i charakterystykę infrastruktury krytycznej oraz potrzebę podejmowania działań zapewniających bezpieczeństwo infrastruktury krytycznej.

Przy wdrażaniu minimalnych wymagań operator infrastruktury krytycznej, opracowując i zawierając umowy, żąda od usługodawców certyfikatów potwierdzających posiadanie właściwych kompetencji i uprawnień niezbędnych do ich realizacji oraz potwierdzenia zdolności do ochrony informacji niejawnych oraz stosowania przepisów o ochronie informacji niejawnych, jeżeli opracowanie, przygotowanie i wykonanie umowy wiążą się dostępem do informacji niejawnych.

Dokumentacja ochrony infrastruktury krytycznej (projektowany art. 6zf)

Realizacja zadań w zakresie ochrony infrastruktury krytycznej wymaga stosownej dokumentacji w tym zakresie. Dlatego też operator infrastruktury krytycznej opracowuje, stosuje i na bieżąco aktualizuje dokumentację ochrony infrastruktury krytycznej zawierającą:

- ✓ charakterystykę infrastruktury krytycznej oraz analizę zagrożeń dla tej infrastruktury;
- ✓ opis zastosowanych, adekwatnie do przeprowadzonej analizy zagrożeń, rozwiązań w poszczególnych obszarach bezpieczeństwa, wskazanych powyżej;
- ✓ procedury obejmujące działania w sytuacji zagrożenia lub zakłócenia funkcjonowania infrastruktury krytycznej, zapewnienie ciągłości funkcjonowania infrastruktury krytycznej oraz umożliwiające odtwarzanie infrastruktury krytycznej.

Operator infrastruktury krytycznej w terminie 15 miesięcy od uzyskania informacji o dokonaniu wpisu do wykazu infrastruktury krytycznej przedkłada oświadczenie o opracowaniu dokumentacji ochrony infrastruktury krytycznej, odpowiednio do organów, które dokonały identyfikacji infrastruktury krytycznej, oraz do Dyrektora Centrum.

Opracowaną dokumentację operator infrastruktury krytycznej wykorzystuje na własne potrzeby, a jej przekazanie właściwym organom oraz Dyrektorowi Centrum następuje wyłącznie na ich żądanie.

Raport o stanie ochrony infrastruktury krytycznej (projektowany art. 6zg)

Do obowiązków operatora infrastruktury krytycznej należy również prowadzenie sprawozdawczości w zakresie jej ochrony. Operator infrastruktury krytycznej sporządza, w terminie do dnia 31 marca każdego roku raport o stanie ochrony infrastruktury krytycznej za rok ubiegły.

Raport o stanie ochrony infrastruktury krytycznej zawiera w szczególności informacje dotyczące jej ochrony w obszarach bezpieczeństwa fizycznego, bezpieczeństwa technicznego, bezpieczeństwa osobowego, cyberbezpieczeństwa, bezpieczeństwa prawnego, ciągłości działania i odtwarzania.

Raport o stanie ochrony infrastruktury krytycznej sporządza się z uwzględnieniem analizy zagrożeń dla infrastruktury krytycznej, wdrożonych adekwatnych do analizy zagrożeń

rozwiązań, wskazania innych zagrożeń (nieujętych w analizie), które zakłóciły lub mogły zakłócić funkcjonowanie infrastruktury krytycznej, jak również wskazania działań podjętych przez operatora infrastruktury krytycznej w przypadkach wystąpienia zagrożeń.

Dodatkowo Raport zawiera wyniki przeprowadzonych kontroli i audytów odnoszących się do wdrożonych rozwiązań w poszczególnych obszarach bezpieczeństwa infrastruktury krytycznej.

Raport przekazywany jest odpowiednio do organów, które dokonały identyfikacji infrastruktury krytycznej operatora, oraz na żądanie Dyrektora Centrum lub Szefa Agencji Bezpieczeństwa Wewnętrznego.

Rozwiązania w zakresie zapewnienia bezpieczeństwa osobowego (projektowany art. 6zh)

W celu zapewnienia bezpieczeństwa osobowego – tak jak ma to miejsce obecnie – operator infrastruktury krytycznej żąda od określonych grup pracowników (lub kandydatów na pracowników) przedłożenia informacji dotyczących karalności, w tym informacji, czy ich dane osobowe są zgromadzone w Krajowym Rejestrze Karnym. W określonych przypadkach operator infrastruktury krytycznej żąda od pracownika danych biometrycznych w postaci odcisków linii papilarnych palców, głosu, obrazu rogówki, sieci żył palców lub biometrii twarzy – które są odpowiednie do wdrożonych środków kontroli dostępu niezbędnych dla ochrony szczególnie ważnych informacji o bezpieczeństwie infrastruktury krytycznej lub dostępu do stref, obiektów lub pomieszczeń wymagających szczególnej kontroli.

Koordynator ochrony infrastruktury krytycznej (projektowany art. 6zi)

W celu realizacji zadań – operator infrastruktury krytycznej wyznacza tzw. koordynatora ochrony infrastruktury krytycznej oraz zastępcę koordynatora ochrony infrastruktury krytycznej.

Operator infrastruktury krytycznej wyznacza koordynatora ochrony infrastruktury krytycznej oraz zastępcę koordynatora ochrony infrastruktury krytycznej w terminie 30 dni od dnia otrzymania informacji o ujęciu w wykazie infrastruktury krytycznej. Zastępca koordynatora infrastruktury krytycznej zastępuje koordynatora w czasie jego nieobecności lub czasowej niemożności wykonywania przez niego obowiązków.

Koordynatorem ochrony infrastruktury krytycznej – zgodnie z projektowanymi regulacjami – może być osoba, która:

- ✓ jest pracownikiem operatora infrastruktury krytycznej albo żołnierzem lub funkcjonariuszem pełniącym służbę w jednostce organizacyjnej będącej operatorem infrastruktury krytycznej;
- ✓ korzysta z pełni praw publicznych;
- ✓ posiada wiedzę, umiejętności i doświadczenie w zakresie zarządzania bezpieczeństwem, z uwzględnieniem przedmiotu działalności operatora infrastruktury krytycznej;
- ✓ nie była skazana prawomocnym wyrokiem za umyślne przestępstwo lub umyślne przestępstwo skarbowe;
- ✓ spełnia wymagania bezpieczeństwa osobowego w zakresie dostępu do informacji niejawnych.

Aby skutecznie realizować powierzone obowiązki – koordynator ochrony infrastruktury krytycznej podlega bezpośrednio organowi zarządzającemu operatora infrastruktury krytycznej. Ponadto operator infrastruktury krytycznej zapewnia koordynatorowi ochrony infrastruktury krytycznej organizacyjne i techniczne warunki realizacji zadań, w tym dostęp do niezbędnych dokumentów i informacji.

Uprawnienia operatora infrastruktury krytycznej w zakresie ochrony posiadanej infrastruktury krytycznej przed bezzałogowymi statkami powietrznymi oraz bezzałogowymi obiektami pływającymi lub lądowymi (projektowany art. 6zj)

Projekt przewiduje, iż operator w celu zapewnienia ochrony infrastruktury krytycznej w przypadkach, o których mowa w przepisach ustawy – Prawo lotnicze, ustawy o ochronie żeglugi i portów morskich lub w przypadkach wskazanych z ustawie o środkach przymusu bezpośredniego i broni palnej może podjąć decyzję o dopuszczalności zastosowania urządzeń, uniemożliwiających telekomunikację na określonym obszarze przez czas niezbędny do wykonywania czynności przez pracowników ochrony specjalistycznych uzbrojonych formacji ochronnych, z uwzględnieniem konieczności minimalizacji skutków braku możliwości korzystania z usług telekomunikacyjnych.

Projekt przewiduje obowiązek operatora infrastruktury krytycznej do informowania Prezesa Urzędu Komunikacji Elektronicznej o możliwości zastosowania urządzeń uniemożliwiających telekomunikację na określonym obszarze, jak również o zastosowaniu tychże urządzeń.

W przypadku obowiązku informowania Ministra Obrony Narodowej (kierownika jednostki organizacyjnej podległej Ministrowi Obrony Narodowej właściwej w sprawach zarządzenia częstotliwościami) wynika to z faktu, iż zgodnie z art. 71 ustawy z dnia 12 lipca 2024 r. – Prawo komunikacji elektronicznej Minister Obrony Narodowej w uzgodnieniu z zainteresowanym użytkownikiem rządowym koordynuje wykorzystanie częstotliwości przez użytkowników rządowych w zakresach częstotliwości będących w użytkowaniu rządowym, w tym ich rozdziału między poszczególnych użytkowników rządowych. Natomiast zgodnie z § 4 ust. 1 decyzji Nr 144/MON z dnia 7 listopada 2024 r. w sprawie zarządzania widmem częstotliwości radiowych w resorcie obrony narodowej (Dz. Urz. Min. Obr. Nar. poz. 179) Minister Obrony Narodowej realizację powyższego zadania powierzył Dyrektorowi Wojskowego Biura Zarządzania Częstotliwościami (WBZC).

Uwzględniając znaczenie informacji przekazywanych przez operatora infrastruktury krytycznej, o których mowa w projektowanym art. 6zj ustawy o zarządzaniu kryzysowym dla realizacji powyższych zadań, resort obrony narodowej proponuje, by kierownik jednostki organizacyjnej podległej Ministrowi Obrony Narodowej właściwej w sprawach zarządzania częstotliwościami obok Prezesa Urzędu Komunikacji Elektronicznej był informowany o zamiarze zastosowania lub o zastosowaniu urządzeń uniemożliwiających telekomunikację na określonym obszarze. Zasadnym jest również doprecyzowanie zakresu informacji, jakich będzie zobowiązany udzielić operator infrastruktury krytycznej i uwzględnienie wśród nich podstawowych parametrów technicznych planowanych do zastosowania lub zastosowanych urządzeń, niezbędnych do oceny wpływu na inne systemy radioelektroniczne, w tym w szczególności te przeznaczone do zapewnienia bezpieczeństwa państwa.

W przypadku gdy będzie to niezbędne dla zapewnienia obronności i bezpieczeństwa państwa (np. w przypadku stwierdzenia nieakceptowalnego poziomu ryzyka zakłócenia lub obezwładnienia systemów radioelektronicznych służących zapewnieniu bezpieczeństwa państwa), Minister Obrony Narodowej będzie mógł nakazać operatorowi infrastruktury krytycznej zaprzestanie lub zmianę sposobu używania urządzenia uniemożliwiającego telekomunikację w konkretnej lokalizacji, informując jednocześnie o tym fakcie dyrektora Rządowego Centrum Bezpieczeństwa oraz właściwego komendanta wojewódzkiego Policji.

Realizację powyższego zadania Minister Obrony Narodowej będzie mógł również powierzyć kierownikowi komórki organizacyjnej lub jednostki organizacyjnej podległej Ministrowi Obrony Narodowej lub przez niego nadzorowanej właściwej w sprawach zarządzania częstotliwościami (WBZC).

Podmioty krytyczne (art. 1 pkt 7 ustawy nowelizującej)

Organy do spraw podmiotów krytycznych (projektowane art. 6zk–6zl)

„Państwa członkowskie powinny wyznaczyć lub ustanowić organy odpowiedzialne za nadzór nad stosowaniem przepisów (…) i, w stosownych przypadkach, za ich egzekwowanie oraz zapewnić, aby organy te dysponowały odpowiednimi uprawnieniami i zasobami. Z uwagi na różnice pomiędzy krajowymi strukturami zarządzania, w celu zabezpieczenia obowiązujących ustaleń sektorowych lub działania unijnych organów nadzorczych i regulacyjnych, a także w celu unikania powielania działań, państwa członkowskie powinny móc wyznaczać lub ustanowić więcej niż jeden właściwy organ. W przypadku gdy państwa członkowskie wyznaczają lub ustanawiają więcej niż jeden właściwy organ, powinny one wyraźnie rozgraniczyć odpowiednie zadania tych organów oraz zapewnić, aby organy te współpracowały ze sobą w sposób płynny i skuteczny.”.

Organami do spraw podmiotów krytycznych są:

- ✓ minister właściwy do spraw energii dla sektora energii, z wyłączeniem podsektorów wydobywania kopalin, ropy i paliw, gazu, energetyki jądrowej, wodoru, dla których organem jest minister właściwy do spraw gospodarki surowcami energetycznymi;
- ✓ minister właściwy do spraw transportu dla sektora transportu z wyłączeniem podsektora transportu wodnego, gdzie organami są minister właściwy do spraw gospodarki morskiej oraz minister właściwy do spraw żeglugi śródlądowej;
- ✓ Komisja Nadzoru Finansowego dla sektora bankowości oraz infrastruktury rynków finansowych;
- ✓ minister właściwy do spraw zdrowia dla sektora zdrowia;
- ✓ minister właściwy do spraw gospodarki wodnej dla sektora zaopatrzenia w wodę pitną i jej dystrybucję oraz sektora zbiorowego odprowadzania ścieków;
- ✓ minister właściwy do spraw informatyzacji dla sektora infrastruktury cyfrowej z wyłączeniem podsektora komunikacji elektronicznej dla którego organem jest Prezes Urzędu Komunikacji Elektronicznej;

- ✓ minister właściwy do spraw administracji publicznej dla sektora administracji publicznej w sektorze podmiotów publicznych z wyłączeniem podsektora finansów publicznych, dla którego organem jest minister właściwy do spraw finansów publicznych;
- ✓ minister właściwy do spraw gospodarki dla sektora przestrzeni kosmicznej;
- ✓ minister właściwy do spraw rolnictwa dla sektora produkcji, przetwarzania i dystrybucji żywności;
- ✓ minister właściwy do spraw informatyzacji dla sektora zarządzania usługami ICT;
- ✓ minister właściwy do spraw gospodarki dla sektora produkcji, wytwarzania i dystrybucji chemikaliów;
- ✓ Prezes Urzędu Komunikacji Elektronicznej dla sektora usług pocztowych;
- ✓ minister właściwy do spraw klimatu dla sektora gospodarowania odpadami.

Do zadań organu do spraw podmiotów krytycznych należy:

- ✓ prowadzenie bieżącej analizy operatorów infrastruktury krytycznej pod kątem uznania ich za podmiot krytyczny w danym sektorze lub podsektorze;
- ✓ prowadzenie bieżącej analizy podmiotów krytycznych w danym sektorze lub podsektorze pod kątem niespełniania warunków kwalifikujących dany podmiot jako podmiot krytyczny;
- ✓ składanie wniosków o dokonanie wpisu do wykazu podmiotów krytycznych oraz wykreślenia z tego wykazu;
- ✓ prowadzenie bieżącej wymiany informacji oraz współpracę w zakresie obsługi incydentów;
- ✓ monitorowanie stosowanie przepisów ustawy przez podmioty krytyczne;
- ✓ prowadzenie kontroli podmiotów krytycznych;
- ✓ prowadzenie działań informacyjnych dotyczących dobrych praktyk, działań edukacyjnych i kampanii na rzecz poszerzania wiedzy i budowania odporności podmiotów krytycznych;
- ✓ uczestniczenie w planowaniu i organizowaniu ćwiczeń podmiotów krytycznych oraz udział w tego typu ćwiczeniach;
- ✓ współpraca z innymi organami do spraw podmiotów krytycznych oraz organami właściwymi do spraw cyberbezpieczeństwa, o których mowa w ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;

- ✓ współpraca, za pośrednictwem Pojedynczego Punktu Kontaktowego z odpowiednimi organami państw członkowskich;
- ✓ nakładanie kar pieniężnych na podmiot krytyczny.

Pojedynczy Punkt Kontaktowy (projektowane art. 6zm–6zn)

Projekt zakłada ustanowienie Pojedynczego Punktu Kontaktowego, który wykonuje funkcję łącznikową w celu zapewnienia współpracy transgranicznej z pojedynczymi punktami kontaktowymi innych państw członkowskich i z Grupą ds. Odporności Podmiotów Krytycznych. Ponadto przyjmuje się, iż Pojedynczy Punkt Kontaktowy będzie wykonywał również funkcję łącznikową z Komisją i zapewniał współpracę z państwami trzecimi.

Dyrektor Centrum prowadzi Pojedynczy Punkt Kontaktowy do którego zadań należy:

- ✓ odbieranie zgłoszeń incydentów istotnych z pojedynczych punktów kontaktowych w innych państwach członkowskich Unii Europejskiej;
- ✓ przekazywanie zgłoszeń incydentów istotnych dotyczących innych państw członkowskich Unii Europejskiej do pojedynczych punktów kontaktowych tych państw;
- ✓ opracowywanie i przekazywanie Komisji Europejskiej oraz Grupie do spraw Odporności Podmiotów Krytycznych sprawozdań dotyczących incydentów istotnych zgłaszanych przez podmioty krytyczne mających wpływ na ciągłość świadczonych przez nich usług kluczowych na terytorium Rzeczypospolitej Polskiej oraz ciągłość świadczonych usług kluczowych w państwach członkowskich Unii Europejskiej;
- ✓ zapewnienie reprezentacji Rzeczypospolitej Polskiej w Grupie do spraw Odporności Podmiotów Krytycznych;
- ✓ zapewnienie współpracy z Komisją Europejską w obszarze zapewnienia bezpieczeństwa świadczenia usług kluczowych;
- ✓ koordynacja współpracy między organami do spraw podmiotów krytycznych i organami administracji publicznej w Rzeczypospolitej Polskiej z odpowiednimi organami w państwach członkowskich Unii Europejskiej;
- ✓ zapewnienie wymiany informacji na potrzeby Grupy Współpracy, o której mowa w dyrektywie (UE) 2022/2555 oraz organów właściwych do spraw cyberbezpieczeństwa;

- ✓ współpracuje z pojedynczym punktem kontaktowym, o którym mowa w ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

Pojedynczy Punkt Kontaktowy przekazuje Grupie do spraw Odporności Podmiotów Krytycznych:

- ✓ informacje na temat infrastruktury krytycznej zlokalizowanej na terytorium Rzeczypospolitej Polskiej służącej realizacji usług kluczowych w innych państwach członkowskich;
- ✓ dobre praktyki związane ze zgłaszaniem i obsługą incydentów istotnych;
- ✓ propozycje do programu prac Grupy do spraw Odporności Podmiotów Krytycznych;
- ✓ dobre praktyki krajowe dotyczące podnoszenia świadomości, szkoleń, badań i rozwoju w obszarze zapewnienia ciągłości świadczenia usług kluczowych;
- ✓ dobre praktyki w odniesieniu do identyfikowania podmiotów krytycznych, w tym w odniesieniu do występujących w dwóch lub większej liczbie państw członkowskich Unii Europejskiej zależności dotyczących ryzyka i incydentów.

Dane przekazywane Grupie do spraw Odporności Podmiotów Krytycznych nie mogą obejmować informacji, które dotyczą bezpieczeństwa narodowego oraz porządku publicznego.

Pojedynczy Punkt Kontaktowy przekazuje organom do spraw podmiotów krytycznych oraz innym organom administracji publicznej zgodnie z ich właściwością informacje pochodzące z Grupy do spraw Odporności Podmiotów Krytycznych dotyczące:

- ✓ analiz i ocen krajowych strategii państw członkowskich Unii Europejskiej w zakresie odporności podmiotów krytycznych, a także dobrych praktyk w obszarze zapewnienia świadczenia usług kluczowych;
- ✓ wytycznych o charakterze strategicznym w obszarze zapewnienia świadczenia usług kluczowych;
- ✓ dobrych praktyk w zakresie wymiany informacji związanych ze zgłaszaniem w Unii Europejskiej incydentów istotnych przez podmioty krytyczne;
- ✓ dobrych praktyk w krajach członkowskich Unii Europejskiej dotyczących innowacji badań i rozwoju w zakresie budowania odporności podmiotów krytycznych;
- ✓ dobrych praktyk w zakresie identyfikowania podmiotów krytycznych przez państwa członkowskie Unii Europejskiej, w tym w odniesieniu do transgranicznych i międzysektorowych zależności, dotyczących ryzyka i incydentów.

Pojedynczy Punkt Kontaktowy przekazuje Komisji Europejskiej:

- ✓ niezwłocznie informacje o:
    - o wyznaczonych organach do spraw podmiotów krytycznych, Pojedynczym Punkcie Kontaktowym, ich zadaniach oraz późniejszych zmianach w tym zakresie,
    - o przepisach dotyczących kar pieniężnych;
- ✓ informacje umożliwiające ocenę wdrażania dyrektywy 2022/2557, obejmujące w szczególności:
    - o środki umożliwiające identyfikację podmiotów krytycznych,
    - o wykaz usług kluczowych,
    - o liczbę zidentyfikowanych podmiotów krytycznych w każdym sektorze, o którym mowa w załączniku do ustawy, oraz wskazanie ich znaczenia w odniesieniu do tego sektora,
    - o progi istotności skutku zakłócającego dla świadczonej usługi kluczowej brane pod uwagę przy kwalifikowaniu podmiotów jako podmiotów krytycznych;
- ✓ informacje o zadaniach organów właściwych w sprawach podmiotów krytycznych;
- ✓ informacje o środkach mających na celu zwiększenie odporności podmiotów krytycznych.

Organy do spraw podmiotów krytycznych, za pośrednictwem Pojedynczego Punktu Kontaktowego, prowadzą konsultacje i bieżącą wymianę informacji z właściwymi organami państw członkowskich, w przypadku gdy podmioty krytyczne:

- ✓ korzystają z infrastruktury krytycznej, która jest fizycznie połączona na terytorium co najmniej dwóch państw członkowskich;
- ✓ są częścią struktur przedsiębiorstw połączonych lub powiązanych z podmiotami krytycznymi w innych państwach członkowskich;
- ✓ zostały zidentyfikowane jako podmioty krytyczne w jednym państwie członkowskim i świadczą usługi kluczowe na rzecz innych państw członkowskich lub w innych państwach członkowskich.

Identyfikowanie podmiotów krytycznych (projektowane art. 6zo–6zr)

Dyrektor Centrum prowadzi wykaz podmiotów krytycznych w celu identyfikacji pomiotów krytycznych oraz umożliwienia prowadzenia czynności nadzorczych nad podmiotami krytycznymi.

Wykaz podmiotów krytycznych zawiera:

- ✓ nazwę (firmę) podmiotu krytycznego;
- ✓ siedzibę i adres oraz adres do doręczeń elektronicznych;
- ✓ numer identyfikacji podatkowej (NIP), jeżeli został nadany;
- ✓ nazwę usługi kluczowej, zgodną z wykazem usług kluczowych;
- ✓ wskazanie sektora, podsektora i kategorii podmiotu;
- ✓ datę rozpoczęcia świadczenia usługi kluczowej;
- ✓ informację wskazującą, w których państwach członkowskich Unii Europejskiej podmiot został uznany za podmiot świadczący usługę kluczową;
- ✓ datę zakończenia świadczenia usługi kluczowej;
- ✓ datę wykreślenia z wykazu podmiotów krytycznych.

Wykaz podmiotów krytycznych prowadzony jest w systemie teleinformatycznym, o którym mowa w art. 46 ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

Operator infrastruktury krytycznej zostaje wpisany do wykazu podmiotów krytycznych w przypadku gdy świadczy co najmniej jedną usługę kluczową oraz incydent miałby istotny skutek zakłócający dla świadczenia usługi kluczowej.

Istotność skutku zakłócającego incydentu dla świadczenia usługi kluczowej, o którym mowa w ust. 1 pkt 2, jest określana na podstawie progów istotności skutku zakłócającego, które Rada Ministrów określi, w drodze rozporządzenia. Progi określa się w zależności od:

- ✓ liczby użytkowników zależnych od usługi kluczowej świadczonej przez dany podmiot;
- ✓ stopnia, w jakim inne sektory lub podsektory, o których mowa w załączniku do ustawy, są zależne od usługi świadczonej przez ten podmiot;
- ✓ wpływu, jaki incydent – jeżeli chodzi o jego skalę i czas trwania – mógłby mieć na działalność gospodarczą i społeczną, środowisko, bezpieczeństwo publicznej lub na zdrowie ludności;
- ✓ udziału podmiotu krytycznego w rynku w odniesieniu do świadczonej usługi kluczowej;
- ✓ obszaru geograficznego, którego mógłby dotyczyć incydent;
- ✓ znaczenia podmiotu w utrzymywaniu wystarczającego poziomu świadczenia usługi kluczowej przy uwzględnieniu dostępności alternatywnych sposobów jej świadczenia;
- ✓ innych czynników charakterystycznych dla danego sektora lub podsektora, jeżeli występują.

W celu podjęcia decyzji o dokonaniu wpisu do wykazu podmiotów krytycznych organ do spraw podmiotów krytycznych występuje do operatora infrastruktury krytycznej o udzielenie informacji, które umożliwią wstępną ocenę, czy spełnia warunki do uznania za podmiot krytyczny, w szczególności w zakresie spełniania warunków uznania za podmiot krytyczny oraz wskazania infrastruktury krytycznej niezbędnej do świadczenia usługi kluczowej.

Organ do spraw podmiotów krytycznych w wystąpieniu przekazuje operatorowi infrastruktury krytycznej dokumenty w zakresie niezbędnym do udzielenia informacji oraz wskazuje termin udzielenia informacji, nie krótszy niż 14 dni, licząc od dnia otrzymania wystąpienia przez operatora infrastruktury krytycznej.

Operator infrastruktury krytycznej przekazuje organowi do spraw podmiotów krytycznych informacje żądane w wystąpieniu, wskazując jednocześnie infrastrukturę krytyczną niezbędną do świadczenia usługi kluczowej, w tym infrastrukturę krytyczną innego operatora lub obiekt, urządzenie, instalację lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje oraz sieci, systemy lub usługi, którego właściciel lub posiadacz nie jest operatorem infrastruktury krytycznej.

Organ do spraw podmiotów krytycznych składa wniosek o wpis do wykazu podmiotów krytycznych zawierający dane niezbędne do uzyskania wpisu. Wpis operatora infrastruktury krytycznej do wykazu podmiotów krytycznych dokonuje się automatycznie z chwilą złożenia wniosku w systemie teleinformatycznym, o którym mowa w art. 46 ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

Organ do spraw podmiotów krytycznych niezwłocznie informuje operatora infrastruktury krytycznej o dokonania wpisu do wykazu podmiotów krytycznych oraz obowiązkach z tym związanych. Informację w tym zakresie organ do spraw podmiotów krytycznych przekazuje Dyrektorowi Centrum.

Podmiot krytyczny w przypadku zakończenia świadczenia usługi kluczowej niezwłocznie informuje właściwy organ do spraw podmiotów krytycznych o tym fakcie. W przypadku zakończenia świadczenia usługi kluczowej przez podmiot krytyczny, organ do spraw podmiotów krytycznych składa wniosek o wykreślenie podmiotu krytycznego. Wykreślenie podmiotu krytycznego z wykazu dokonuje się automatycznie z chwilą złożenia wniosku w systemie teleinformatycznym, o którym mowa w art. 46 ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

Ponadto organ do spraw podmiotów krytycznych niezwłocznie informuje podmiot krytyczny o wykreśleniu z wykazu i dacie wykreślenia. Informację w tym zakresie organ do spraw podmiotów krytycznych przekazuje Dyrektorowi Centrum.

Rozwiązania służące zapewnieniu odporności podmiotu krytycznego (art. 1 pkt 7 ustawy nowelizującej)

Wdrażanie rozwiązań w zakresie ochrony podmiotu krytycznego (projektowany art. 6zt)

Podmiot krytyczny wdraża zintegrowany system zarządzania bezpieczeństwem świadczenia usługi kluczowej zapewniający prowadzenie oceny ryzyka (którą przeprowadza po raz pierwszy ocenę ryzyka w terminie 9 miesięcy od otrzymania informacji o ujęciu w wykazie podmiotów krytycznych) oraz wdrożenie odpowiednich i proporcjonalnych do wyników oceny ryzyka rozwiązań organizacyjno-technicznych (w terminie 3 miesięcy od dnia przeprowadzenia po raz pierwszy oceny ryzyka, a następnie stosownie do potrzeb), w zależności od wyników oceny ryzyka, obejmujących:

- ✓ polityki zarządzania ryzykiem;
- ✓ zapewnienie bezpieczeństwa fizycznego, w tym ochrony fizycznej budynków i terenów należących do podmiotu krytycznego oraz zabezpieczeń technicznych, uwzględniających kontrolę dostępu;
- ✓ ochronę infrastruktury krytycznej niezbędnej do świadczenia usługi kluczowej, zgodnie z wymogami ochrony infrastruktury krytycznej;
- ✓ bezpieczeństwo osobowe dotyczące pracowników i dostawców zewnętrznych;
- ✓ cyberbezpieczeństwo, zgodnie z wymogami dotyczącymi podmiotów kluczowych, o których mowa w przepisach ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;
- ✓ bezpieczeństwo prawne świadczenia usługi kluczowej;
- ✓ zapewnienie ciągłości działania i odtwarzania, w tym utrzymywania własnych systemów rezerwowych zapewniających bezpieczeństwo i podtrzymujących funkcjonowanie świadczenia usługi kluczowej do czasu jej pełnego odtworzenia;
- ✓ zdolność do ochrony informacji niejawnych w niezbędnym zakresie do zapewnienia świadczenia usługi kluczowej;

- ✓ prowadzenie szkoleń i ćwiczeń personelu w celu jego przygotowania na różnego rodzaju zagrożenia i incydenty;
- ✓ realizację okresowych audytów i certyfikacji.

Ponadto – do obowiązków podmiotu krytycznego należy:

- ✓ zapewnienie bieżącej współpracę z właściwymi organami zarządzania kryzysowego oraz służbami, strażami i inspekcjami dotyczącą wymiany informacji o zagrożeniach i incydentach zakłócających lub mogących zakłócić funkcjonowanie usługi kluczowej oraz sposobu postępowania w przypadku takiego zdarzenia;
- ✓ gromadzenie informacji o zagrożeniach i incydentach zakłócających lub mogących zakłócić świadczenie usługi kluczowej;
- ✓ zarządzanie incydentami;
- ✓ stosowanie środków zapobiegających i ograniczających wpływ incydentów na świadczenie usługi kluczowej.

W celu jak najbardziej efektywnego wdrożenia rozwiązań organizacyjno-technicznych Rada Ministrów określi w drodze rozporządzenia wykaz norm oraz wytycznych do ich stosowania, które podmiot krytyczny uwzględnia przy ich wdrażaniu, mając na względzie zarządzanie bezpieczeństwem informacji, zarządzanie ciągłością działania usługi kluczowej oraz zapewnienie bezpieczeństwa fizycznego, w tym ochrony fizycznej oraz zabezpieczeń technicznych, uwzględniających kontrolę dostępu.

Dodatkowo – projekt przewiduje, iż organ do spraw podmiotów krytycznych może opracować, odrębnie dla nadzorowanego sektora lub podsektora i udostępnić 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), które podmiot krytyczny uwzględnia przy wdrażaniu rozwiązań organizacyjno-technicznych wskazanych w ust. 1 pkt 2.

Ponadto – w celu wdrożenia rozwiązań organizacyjno-technicznych podmiot krytyczny uwzględnia specyfikacje techniczne określone w aktach wykonawczych Komisji Europejskiej, wydanych na podstawie art. 13 ust. 6 dyrektywy 2022/2557.

W ramach opracowywania i zawierania umów zapewniających wdrożenie rozwiązań organizacyjno-technicznych, podmiot krytyczny żąda od usługodawców stosownych certyfikatów potwierdzających posiadanie właściwych kompetencji i uprawnień niezbędnych

do ich realizacji oraz potwierdzenia zdolności do ochrony informacji niejawnych oraz stosowania przepisów o ochronie informacji niejawnych, jeżeli opracowanie, przygotowanie i wykonanie umowy wiążą się dostępem do informacji niejawnych.

Dokumentacja wdrażanych rozwiązań w zakresie ochrony podmiotu krytycznego (projektowany art. 6zu)

W celu odpowiedniej dokumentacji wdrażanych rozwiązań w zakresie bezpieczeństwa świadczenia usługi kluczowej – podmiot krytyczny opracowuje, stosuje i aktualizuje dokumentację zintegrowanego systemu zarządzania bezpieczeństwem świadczenia usługi kluczowej, którą stanowią:

- ✓ dokumentacja dotycząca systemu zarządzania bezpieczeństwem informacji;
- ✓ dokumentacja systemu zarządzania ciągłością działania usługi kluczowej;
- ✓ dokumentacja ochrony fizycznej oraz zabezpieczeń technicznych oraz bezpieczeństwa osobowego;
- ✓ dokumentacja ochrony infrastruktury krytycznej;
- ✓ inne dokumenty uwzgledniające rodzaj świadczonej usługi kluczowej.

Podmiot krytyczny po raz pierwszy sporządza dokumentację w terminie 15 miesięcy od otrzymania informacji o ujęciu w wykazie podmiotów krytycznych, a następnie stosownie do potrzeb dokonuje jej aktualizacji. Podmiot krytyczny jest obowiązany do ustanowienia nadzoru nad dokumentacją zapewniającego dostępność dokumentów wyłącznie dla osób upoważnionych, zgodnie z realizowanymi przez nie zadaniami oraz ochronę dokumentów przed uszkodzeniem, zniszczeniem, utratą, nieuprawnionym dostępem, niewłaściwym użyciem lub utratą integralności.

Obsługa incydentów (projektowane art. 6zv–6zx)

W odniesieniu do incydentów – podmiot krytyczny:

- ✓ zapewnia obsługę incydentów;
- ✓ zapewnia dostęp do informacji o zarejestrowanych incydentach organowi do spraw podmiotów krytycznych oraz Dyrektorowi Centrum;
- ✓ klasyfikuje incydent jako istotny, na podstawie progów uznawania incydentu za istotny;

- ✓ zgłasza incydent istotny niezwłocznie, nie później niż w terminie 24 godzin od momentu jego wystąpienia lub wykrycia do:
    - o właściwego organu do spraw podmiotów krytycznych oraz Dyrektora Centrum,
    - o Szefa Agencji Bezpieczeństwa Wewnętrznego,
    - o podmiotu, w ramach którego funkcjonuje Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT) poziomu krajowego;
- ✓ współdziała podczas obsługi incydentu istotnego z właściwym organem do spraw podmiotów krytycznych lub Dyrektorem Centrum;
- ✓ informuje właściwy organ do spraw podmiotów krytycznych oraz Dyrektora Centrum o usunięciu incydentu istotnego.

Zgłaszanie incydentów istotnych dokonuje się za pomocą systemu, o którym mowa w art. 46 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. W przypadku braku możliwości dokonania zgłoszenia w systemie, o którym mowa w art. 46 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

Rada Ministrów określi, w drodze rozporządzenia, progi uznania incydentu za istotny według zdarzenia w poszczególnych sektorach i podsektorach określonych w załączniku do ustawy, w zależności od liczby użytkowników dotkniętych zakłóceniem, czasu trwania zakłócenia usługi kluczowej, obszaru geograficznego, którego dotyczy zakłócenie oraz innych czynników charakterystycznych dla danego sektora lub podsektora, jeżeli występują. Rada Ministrów, wydając rozporządzenie, określi co najmniej jeden próg uznania incydentu za incydent istotny dla każdego zdarzenia, kierując się potrzebą zapewnienia ochrony przed zagrożeniami życia lub zdrowia ludzi, znacznymi stratami majątkowymi oraz zagrożeniem obniżenia jakości świadczonej usługi kluczowej.

Oprócz incydentów istotnych – podmiot krytyczny może przekazywać właściwym organom do spraw podmiotów krytycznych oraz Dyrektorowi Centrum informacje dotyczące incydentów innych niż istotne oraz informacji o zagrożeniach dla niezakłóconego świadczenia usługi kluczowej.

Audyt (projektowany art. 6zz–6zza)

Podmiot krytyczny przeprowadza na własny koszt, co najmniej raz na 3 lata, audyt zintegrowanego systemu zarządzania bezpieczeństwem świadczenia usługi kluczowej, w zakresie zarządzania bezpieczeństwem informacji, zarządzania ciągłością działania usługi kluczowej, zapewnienia bezpieczeństwa fizycznego, w tym ochrony fizycznej budynków

i terenów należących do podmiotu krytycznego oraz zabezpieczeń technicznych, uwzględniających kontrolę dostępu.

W przypadku wystąpienia incydentu istotnego, organ do spraw podmiotów krytycznych może nakazać podmiotowi krytycznemu przeprowadzenie zewnętrznego audytu, w drodze decyzji, wraz z określeniem terminu przekazania kopii raportu z przeprowadzonego audytu i wskazaniem kategorii podmiotów do przeprowadzenia audytu. Organ do spraw podmiotów krytycznych może również określić zakres audytu. Dodatkowo – decyzja nakazująca przeprowadzenie zewnętrznego audytu podlega natychmiastowemu wykonaniu.

Audyt może być prowadzony przez jednostkę certyfikującą lub co najmniej dwóch audytorów, w tym jednego z ukończonym szkoleniem audytora wiodącego, posiadających stosowne certyfikaty. Rada Ministrów określi, w drodze rozporządzenia, wymogi dla osób lub podmiotów przeprowadzających audyt, w tym zakres wymaganej wiedzy specjalistycznej oraz wymagane doświadczenie w dziedzinie objętej audytem, mając na względzie zapewnienie skutecznego i rzetelnego przeprowadzania audytu

Dodatkowym wymogiem dla audytujących jest konieczność spełniania wymagań bezpieczeństwa osobowego i przemysłowego w zakresie dostępu do informacji niejawnych o klauzuli „poufne”. Z wymogu posiadania dostępu do informacji niejawnych o klauzuli "poufne" zwolnieni są audytorzy, w przypadku gdy są oni pracownikami podmiotu krytycznego.

Na podstawie zebranych dokumentów i dowodów jednostka certyfikująca lub audytorzy sporządzają raport z przeprowadzonego audytu i przekazują je podmiotowi krytycznemu wraz z dokumentacją z przeprowadzonego audytu. Obowiązek przeprowadzenia audytu uznaje się za spełniony w przypadku posiadania przez podmiot krytyczny certyfikatów, które potwierdzają wdrożenie rozwiązań w zakresie bezpieczeństwa świadczenia usługi kluczowej w oparciu o stosowne normy.

Podmiot krytyczny przedstawia kopię raportu z przeprowadzonego audytu lub certyfikatu właściwemu organowi do spraw podmiotów krytycznych w terminie 7 dni roboczych od dnia jego otrzymania lub Dyrektorowi Centrum na jego uzasadniony wniosek. Kopię raportu z przeprowadzonego audytu lub certyfikatu, o którym mowa w ust. 6, przekazuje się za pomocą systemu, o którym mowa w art. 46 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. W przypadku braku możliwości przekazania kopii audytu lub certyfikatu, o którym mowa w ust. 7, za pomocą systemu, o którym mowa w art. 46 ustawy

z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, przekazanie następuje na piśmie utrwalonym w postaci elektronicznej, opatrzonym kwalifikowanym podpisem elektronicznym, podpisem osobistym albo podpisem zaufanym.

Podnoszenie świadomości personelu podmiotu krytycznego (projektowany art. 6zzb)

Podmiot krytyczny zapewnia udział struktur organizacyjnych lub pracowników niezbędnych do zapewnienia niezakłóconego świadczenia usługi kluczowej w szkoleniach i ćwiczeniach, w tym m.in. w ćwiczeniach z zakresu obrony cywilnej ochrony ludności przeciwdziałania zagrożeniom o charakterze terrorystycznym, spraw obronnych oraz zarządzania kryzysowego. Podmiot krytyczny we współpracy z właściwym organem do spraw podmiotów krytycznych lub Dyrektorem Centrum planuje i organizuje udział w szkoleniach i ćwiczeniach.

Bezpieczeństwo osobowe świadczenia usługi kluczowej (projektowany art. 6zzc)

Podmiot krytyczny, w celu zapewnienia ochrony ciągłości świadczenia usługi kluczowej, może prowadzić sprawdzenie przeszłości w przypadku swojego pracownika lub kandydata na pracownika oraz osoby świadczącej usługę na rzecz podmiotu krytycznego, niebędącej pracownikiem podmiotu krytycznego.

Podmiot krytyczny może prowadzić sprawdzenie przeszłości w odniesieniu do:

- ✓ pracownika podmiotu krytycznego lub kandydata na pracownika:
  - pełniącego newralgiczną rolę bezpośrednio w strukturze organizacyjnej podmiotu krytycznego lub działając na jego rzecz, w tym:
    - reprezentującego podmiot krytyczny samodzielnie lub łącznie z innymi osobami na podstawie statutu, umowy lub innego aktu założycielskiego,
    - pełniącego funkcje kierownicze lub koordynacyjne,
  - posiadającego bezpośredni lub zdalny dostęp do budynków i terenów podmiotu krytycznego, obiegu informacji lub systemów kontroli, w szczególności związanych z bezpieczeństwem podmiotu krytycznego,
  - realizującego audyt;
- ✓ osoby świadczącej usługę na rzecz podmiotu krytycznego, niebędącej pracownikiem podmiotu krytycznego, posiadającej bezpośredni lub zdalny dostęp do budynków

i terenów podmiotu krytycznego, obiegu informacji lub systemów kontroli, w szczególności związanych z bezpieczeństwem podmiotu krytycznego.

Sprawdzenie przeszłości osób będących pracownikami podmiotu krytycznego obejmuje:

- ✓ potwierdzenie tożsamości;
- ✓ ocenę informacji pozyskanych z rejestrów karnych pod kątem przestępstw, które mogą mieć znaczenie dla zajmowanego stanowiska, ubiegania się o to stanowisko lub świadczenia usług na rzecz podmiotu krytycznego.

Podmiot krytyczny w celu:

- ✓ potwierdzenia tożsamości:
  - o żąda przedłożenia ważnego dowodu osobistego lub ważnego dokumentu paszportowego tej osoby oraz podania nazwiska rodowego i poprzednio noszonego nazwiska, jeżeli było zmieniane, oraz nazwisk, imion, dat i miejsc urodzenia rodziców,
  - o wnioskuje do organu dowolnej gminy o udostępnienie danych jednostkowych zawartych w rejestrze PESEL oraz o udostępnienie danych w trybie jednostkowym z Rejestru Dowodów Osobistych;
- ✓ dokonania oceny informacji pozyskanych z rejestrów karnych:
  - o pozyskuje informację z Krajowego Rejestru Karnego w zakresie skazań za przestępstwa umyślne ścigane z oskarżenia publicznego oraz umyślne przestępstwa skarbowe;
  - o występuje do Biura Informacyjnego Krajowego Rejestru Karnego z wnioskiem o wystąpienie do organów centralnych państw członkowskich Unii Europejskiej państwa obywatelstwa osoby podlegającej sprawdzeniu przeszłości z zapytaniem o udzielenie informacji o osobie, w przypadku gdy osoba podlegająca sprawdzeniu ma obywatelstwo państwa członkowskiego innego niż Rzeczpospolita Polska.

Natomiast w przypadku osoby świadczącej usługę na rzecz podmiotu krytycznego, niebędącej jego pracownikiem – podmiot krytyczny ma prawo żądać:

- ✓ przedłożenia przez tę osobę ważnego dowodu osobistego lub ważnego dokumentu paszportowego tej osoby oraz podania nazwiska rodowego i poprzednio noszonego nazwiska, jeżeli było zmieniane, oraz nazwisk, imion, dat i miejsc urodzenia rodziców;

- ✓ przedłożenia przez tę osobę informacji z Krajowego Rejestru Karnego w zakresie skazań za przestępstwa umyślne ścigane z oskarżenia publicznego oraz umyślne przestępstwa skarbowe.

Podmiot krytyczny uwzględnia negatywny wynik sprawdzenia przeszłości w zakresie powierzania zadań osobom podlegającym sprawdzeniu, w szczególności w przypadku skazania prawomocnym wyrokiem na karę pozbawienia wolności za przestępstwo umyślne ścigane z oskarżenia publicznego, także popełnione za granicą, lub umyślne przestępstwo skarbowe, jeżeli czyn, za który nastąpiło skazanie wywołuje uzasadnione wątpliwości w zakresie powierzenia realizacji tych zadań.

Sprawdzenia przeszłości nie prowadzi się w odniesieniu do osoby będącej pracownikiem lub kandydatem na pracownika, która samodzielnie przedłożyła wymagane dokumenty albo posiada co najmniej poświadczenie bezpieczeństwa o klauzuli "poufne".

Pełnomocnik bezpieczeństwa usługi kluczowej (projektowany art. 6zzd)

W celu efektywnej realizacji zadań związanych z bezpieczeństwem świadczenia usługi kluczowej – podmiot krytyczny wyznacza pełnomocnika bezpieczeństwa usługi kluczowej oraz zastępcę pełnomocnika usługi kluczowej.

Podmiot krytyczny wyznacza pełnomocnika bezpieczeństwa usługi kluczowej oraz zastępcę pełnomocnika usługi kluczowej w terminie 30 dni od dnia otrzymania informacji o ujęciu w wykazie podmiotów krytycznych. Zastępca pełnomocnika bezpieczeństwa usługi kluczowej zastępuje pełnomocnika w czasie jego nieobecności lub czasowej niemożności wykonywania przez niego obowiązków.

Pełnomocnik bezpieczeństwa usługi kluczowej:

- ✓ jest pracownikiem podmiotu krytycznego albo żołnierzem lub funkcjonariuszem pełniącym służbę w jednostce organizacyjnej będącej podmiotem krytycznym;
- ✓ korzysta z pełni praw publicznych;
- ✓ posiada wiedzę, umiejętności i doświadczenie w zakresie zarządzania bezpieczeństwem, z uwzględnieniem przedmiotu działalności podmiotu świadczące usługę kluczową;
- ✓ nie był skazany prawomocnym wyrokiem za umyślne przestępstwo lub umyślne przestępstwo skarbowe;

- ✓ spełnia wymagania bezpieczeństwa osobowego w zakresie dostępu do informacji niejawnych o klauzuli „poufne”.

Pełnomocnik bezpieczeństwa usługi kluczowej podlega bezpośrednio organowi zarządzającemu podmiotu krytycznego, a podmiot krytyczny zapewnia pełnomocnikowi bezpieczeństwa usługi kluczowej organizacyjne i techniczne warunki realizacji zadań, w tym dostęp do niezbędnych dokumentów i informacji.

O wyznaczeniu pełnomocnika bezpieczeństwa usługi kluczowej podmiot krytyczny informuje niezwłocznie właściwy organ do spraw podmiotów krytycznych oraz Dyrektora Centrum, przekazując dane tej osoby obejmujące imię i nazwisko, numer telefonu oraz adres poczty elektronicznej.

Podmiot krytyczny o szczególnym znaczeniu europejskim (projektowane art. 6zzf–6zzh)

Podmiot krytyczny informuje właściwy organ do spraw podmiotów krytycznych oraz Pojedynczy Punkt Kontaktowy o fakcie świadczenia co najmniej jednej usługi kluczowej spośród usług kluczowych wskazanych w przepisach rozporządzenia delegowanego wydanego na podstawie art. 5 ust. 1 dyrektywy 2022/2557, lub podobnej usługi kluczowej, na rzecz co najmniej sześciu państw członkowskich Unii Europejskiej lub w co najmniej sześciu państwach członkowskich Unii Europejskiej. W przypadku uzyskania takiej informacji właściwy organ do spraw podmiotów krytycznych, za pośrednictwem Pojedynczego Punktu Kontaktowego informuje Komisję Europejską o potencjalnym podmiocie krytycznym o szczególnym znaczeniu europejskim, przekazując stosowne dane identyfikujące ten podmiot.

Organ do spraw podmiotów krytycznych, za pośrednictwem Pojedynczego Punktu Kontaktowego, inicjuje i prowadzi konsultacje z Komisją Europejską oraz właściwymi organami państw członkowskich Unii Europejskiej w celu ustalenia, czy podmiot krytyczny świadczący usługę kluczową na terytorium Rzeczypospolitej Polskiej, świadczy ją na rzecz co najmniej sześciu państw członkowskich Unii Europejskiej lub w co najmniej sześciu państwach członkowskich Unii Europejskiej. W przypadku uznania przez Komisję Europejska takiego podmiotu krytycznego za podmiot krytyczny o szczególnym znaczeniu europejskim, organ do spraw podmiotów krytycznych informuje podmiot krytyczny, o tym fakcie oraz obowiązkach z tym związanych.

Organ do spraw podmiotów krytycznych, za pośrednictwem Pojedynczego Punktu Kontaktowego, zapewnia współpracę z Komisją Europejską oraz właściwymi organami państwa członkowskiego, na rzecz którego lub w którym jest świadczona usługa kluczowa, w tym prowadzi wymianę informacji w zakresie oceny ryzyka podmiotu krytycznego o szczególnym znaczeniu europejskim, wdrażania odpowiednich i proporcjonalnych do wyników oceny ryzyka rozwiązań organizacyjno-technicznych służących zapewnieniu odporności tego podmiotu, działań z zakresu nadzoru oraz egzekwowania przepisów ustawy przez właściwy organ do spraw podmiotów krytycznych.

Właściwy organ do spraw podmiotów krytycznych, za pośrednictwem Pojedynczego Punktu Kontaktowego, zapewnia współpracę z Komisją Europejską w zakresie zapewnienia obsługi misji doradczej, w tym:

- ✓ konsultuje program misji doradczej;
- ✓ koordynuje realizację czynności związanych z dostępem przedstawicieli misji doradczej do informacji oraz budynków, terenów i infrastruktury krytycznej podmiotu krytycznego o szczególnym znaczeniu europejskim;
- ✓ przeprowadza analizę sprawozdania z ustaleń misji doradczej.

Właściwy organ do spraw podmiotów krytycznych za pośrednictwem Pojedynczego Punktu Kontaktowego:

- ✓ po dokonaniu analizy sprawozdania z ustaleń misji doradczej, przedkłada Komisji Europejskiej informację o stopniu wdrożenia rozwiązań organizacyjno-technicznych służących zapewnieniu odporności podmiotu krytycznego o szczególnym znaczeniu europejskim lub przedkłada rekomendacje w zakresie zwiększenia odporności tego podmiotu, w celu wydania przez Komisję Europejską opinii dotyczącej wywiązywania się z nałożonych obowiązków przez ten podmiot lub wskazującej środki, które można wprowadzić, aby zwiększyć odporność tego podmiotu;
- ✓ przekazuje opinię podmiotowi krytycznemu o szczególnym znaczeniu europejskim oraz zapewnia wsparcie w przypadku konieczności wdrożenia dodatkowych środków zwiększających odporność;
- ✓ informuje Komisję Europejską oraz właściwe organy państwa członkowskiego, na rzecz którego lub w którym jest świadczona usługa kluczowa, o środkach zwiększających odporność, wprowadzonych z uwzględnieniem opinii albo informację o braku konieczności wprowadzania tych środków.

Nadzór i kontrola podmiotów krytycznych (projektowane art. 6zzi–6zzn)

Nadzór w zakresie stosowania przepisów ustawy sprawują organy do spraw podmiotów krytycznych w zakresie spełniania przez podmioty krytyczne wymogów bezpieczeństwa dotyczących świadczenia usług kluczowych oraz wykonywania przez podmioty krytyczne obowiązków wynikających z ustawy dotyczących przeciwdziałania zagrożeniom dla świadczonych usług kluczowych i zgłaszania incydentów istotnych.

W ramach nadzoru organ do spraw podmiotów krytycznych:

- ✓ prowadzi kontrole podmiotów krytycznych;
- ✓ zleca audyt zintegrowanego systemu zarządzania bezpieczeństwem świadczenia usługi kluczowej, w przypadku wystąpienia incydentu istotnego;
- ✓ nakłada kary pieniężne na podmioty krytyczne.

Do kontroli realizowanej wobec podmiotów:

- ✓ będących przedsiębiorcami – stosuje się przepisy rozdziału 5 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców;
- ✓ niebędących przedsiębiorcami – stosuje się przepisy ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej określające zasady i tryb przeprowadzania kontroli.

Dodatkowo przepisy określają czynności kontrolne wobec podmiotów będących przedsiębiorcami.

Osoba prowadząca czynności kontrolne wobec podmiotów będących przedsiębiorcami ma prawo do:

- ✓ swobodnego wstępu i poruszania się po terenie podmiotu kontrolowanego;
- ✓ wglądu do dokumentów dotyczących działalności podmiotu kontrolowanego, pobierania za pokwitowaniem oraz zabezpieczania dokumentów związanych z zakresem kontroli, z zachowaniem przepisów o tajemnicy prawnie chronionej;
- ✓ sporządzania, a w razie potrzeby żądania sporządzenia, niezbędnych do kontroli kopii, odpisów lub wyciągów z dokumentów oraz zestawień lub obliczeń;
- ✓ przetwarzania danych osobowych w zakresie niezbędnym do realizacji celu kontroli;
- ✓ żądania złożenia ustnych lub pisemnych wyjaśnień w sprawach dotyczących zakresu kontroli;

- ✓ przeprowadzania oględzin urządzeń, nośników oraz systemów informacyjnych.

W celu zapewnienia niezakłóconego przebiegu kontroli – kontrolowane podmioty zapewniają osobie prowadzącej czynności kontrolne warunki niezbędne do sprawnego przeprowadzenia kontroli, w szczególności przez zapewnienie niezwłocznego przedstawienia żądanych dokumentów, terminowego udzielania ustnych i pisemnych wyjaśnień w sprawach objętych kontrolą, udostępniania niezbędnych urządzeń technicznych, a także sporządzania we własnym zakresie kopii lub wydruków dokumentów oraz informacji zgromadzonych na nośnikach, w urządzeniach lub w systemach informacyjnych.

Jeżeli na podstawie informacji zgromadzonych w protokole kontroli organ do spraw podmiotów krytycznych uzna, że mogło dojść do naruszenia przepisów ustawy przez podmiot kontrolowany, przekazuje zalecenia pokontrolne dotyczące usunięcia nieprawidłowości, wskazując jednocześnie termin usunięcia nieprawidłowości. Przy określaniu terminu usunięcia nieprawidłowości organ do spraw podmiotów krytycznych bierze pod uwagę zakres i rodzaj stwierdzonych nieprawidłowości.

Od zaleceń pokontrolnych nie przysługują środki odwoławcze. Podmiot kontrolowany, w wyznaczonym terminie, informuje organ do spraw podmiotów krytycznych o sposobie wykonania zaleceń.

Przepisy o karach pieniężnych dla podmiotów krytycznych (projektowane art. 6zzo–6zzr)

Projekt przewiduje katalog kar za brak realizacji obowiązków wynikających z projektowanej ustawy. Karze podlega podmiot krytyczny, który m.in.:

- ✓ nie przeprowadza oceny ryzyka;
- ✓ nie wdraża rozwiązań organizacyjno-technicznych;
- ✓ nie prowadzi dokumentacji dotyczącej bezpieczeństwa świadczenia usługi kluczowej;
- ✓ nie zgłasza incydentów istotnych;
- ✓ nie przeprowadza audytu;
- ✓ nie wyznacza pełnomocnika bezpieczeństwa usługi kluczowej lub zastępcy pełnomocnika bezpieczeństwa usługi kluczowej;
- ✓ uniemożliwia lub utrudnia wykonywanie kontroli;

- ✓ nie wykonał w wyznaczonym terminie zaleceń pokontrolnych, o których mowa w art. 6zzn ust. 1;
- ✓ nie wdrożył rozwiązań dotyczących ochrony infrastruktury krytycznej w odniesieniu do infrastruktury krytycznej niezbędnej do świadczenia usługi kluczowej;
- ✓ nie opracował dokumentacji ochrony infrastruktury krytycznej w odniesieniu do infrastruktury krytycznej niezbędnej do świadczenia usługi kluczowej.

Kary pieniężne nakładają, w drodze decyzji, właściwe organy do spraw podmiotów krytycznych. Wpływy z tytułu kar pieniężnych, o których mowa w art. 6zzo, 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, z późn. zm.).

W przypadku naruszenia przepisów ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa przez podmiot krytyczny będący jednocześnie podmiotem kluczowym w rozumieniu przepisów tej ustawy, karę pieniężną na ten podmiot nakłada organ właściwy do spraw cyberbezpieczeństwa. Do ustalenia wysokości kary pieniężnej w tym przypadku stosuje się przepisy ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

Jednocześnie przepisy wskazują na obowiązek organu właściwego do spraw cyberbezpieczeństwa niezwłocznego informowania organu do spraw podmiotów krytycznych, sprawujący nadzór nad podmiotem o wszczęciu wobec tego podmiotu postępowania w sprawie nałożenia kary pieniężnej, naruszeniu dokonanym przez podmiot wraz z kwalifikacją prawną oraz wysokości nałożonej na ten podmiot kary lub odstąpieniu od jej nałożenia. Tym samym organ do spraw podmiotów krytycznych nie wszczyna postępowania w sprawie nałożenia kary pieniężnej jeżeli postępowanie w przedmiocie tego naruszenia prowadzi organ właściwy do spraw cyberbezpieczeństwa.

Organ do spraw podmiotów krytycznych, podejmując decyzję o nałożeniu kary pieniężnej i ustalając jej wysokość, bierze pod uwagę:

- ✓ wagę naruszenie i znaczenie naruszonych przepisów ustawy;
- ✓ czasu trwania naruszenia;
- ✓ wcześniejszych naruszeń ze strony danego podmiotu krytycznego;
- ✓ spowodowane szkody majątkowe i niemajątkowe, w tym wpływ na użytkowników usługi oraz na inne usługi kluczowe;
- ✓ środki zastosowane przez podmiot w celu ograniczenia szkód;

- ✓ umyślny lub nieumyślny charakter czynu ze strony sprawcy naruszenia;
- ✓ stopień współpracy podmiotu krytycznego z organem do spraw podmiotów krytycznych.

Podejmując decyzję, organ uwzględnia również wysokość przychodu uzyskanego z działalności gospodarczej w roku obrotowym poprzedzającym wymierzenie kary pieniężnej lub możliwości finansowe podmiotu krytycznego będącego podmiotem publicznym.

W związku z toczącym się postępowaniem w sprawie nałożenia kary pieniężnej, organ do spraw podmiotów krytycznych może żądać od podmiotu krytycznego przekazania we wskazanym terminie, nie dłuższym niż 14 dni od dnia otrzymania żądania, informacji niezbędnych do określenia wymiaru kary pieniężnej.

W przypadku nieprzekazania informacji, o których mowa w ust. 2, lub przekazania informacji uniemożliwiających ustalenie podstawy wymiaru kary pieniężnej, organ do spraw podmiotów krytycznych ustala podstawę wymiaru kary pieniężnej w sposób szacunkowy, uwzględniając wielkość podmiotu krytycznego, specyfikę działalności tego podmiotu oraz ogólnodostępne dane finansowe.

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 odrębny rachunek bankowy wskazany przez organ właściwy do spraw podmiotów krytycznych w decyzji o wymierzeniu kary pieniężnej. Kara pieniężna nieuiszczona w terminie wraz z odsetkami podlega ściągnięciu w trybie określonym w przepisach o postępowaniu egzekucyjnym w administracji.

Organ właściwy do spraw podmiotów krytycznych może odstąpić od nałożenia kary pieniężnej, jeżeli waga naruszenia i znaczenie naruszonych przepisów jest znikome, a podmiot krytyczny zaprzestał naruszania prawa lub naprawił wyrządzoną szkodę.

W zakresie nieuregulowanym w niniejszym rozdziale stosuje się odpowiednio przepisy działu IVa ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego.

Przepisy szczególne dotyczące niektórych podmiotów krytycznych (projektowane art. 6zzt i art. 6zzu)

Projekt ustawy przewiduje wyłączenia stosowania przepisów – tj. do podmiotów krytycznych z sektora bankowości i infrastruktury rynków finansowych nie stosuje się

przepisów rozdziałów 11–14, z wyjątkiem art. 6zt ust. 1 pkt 1, art. 6zt ust. 1 pkt 2 lit. b–d, f, h oraz i, art. 6zt pkt 3, art. 6zt ust. 2–11, art. 6zu ust. 1 i ust. 2 pkt 3, 4 i 6, art. 6zu ust. 3–6, art. 6zx, art. 6zy, art. 6zzb i art. 6zzd.

Natomiast do podmiotów krytycznych z sektora infrastruktury cyfrowej nie stosuje się przepisów rozdziałów 11–14 projektowanej ustawy.

Pozostałe najważniejsze zmiany w ustawie o zarządzaniu kryzysowym

- ✓ (art. 1 pkt 8 ustawy nowelizującej) propozycja dokonania zmian w zakresie poleceń Prezesa Rady Ministrów, o których mowa w art. 7a ustawy o zarządzaniu kryzysowym jest propozycją dostosowującą do nowych uregulowań w zakresie usług kluczowych. W zmienianych przepisach przedmiotem poleceń będzie nie tylko zapewnienie właściwego funkcjonowania, ochrony, wzmocnienia oraz odbudowy infrastruktury krytycznej lecz również zapewnienie niezakłóconego świadczenia usługi kluczowej;
- ✓ (art. 1 pkt 10 ustawy nowelizującej) propozycja obejmuje wskazanie m.in. zadań Rządowego Centrum Bezpieczeństwa przewidzianych do realizacji w ustawie z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej. W art. 22 tejże ustawy wskazano, iż do zadań Rządowego Centrum Bezpieczeństwa należy:
    - monitorowanie zagrożeń oraz powiadamianie, ostrzeganie i alarmowanie ludności o zagrożeniach,
    - realizacja zobowiązań wynikających z uczestnictwa Rzeczypospolitej Polskiej w Organizacji Traktatu Północnoatlantyckiego i Unii Europejskiej w zakresie budowania odporności państwa na zagrożenia,
    - opracowanie krajowego planu ewakuacji i koordynowanie sporządzania przez wojewodów wojewódzkich planów ewakuacji ludności,
    - zapewnianie wymiany informacji związanych z ochroną ludności i obroną cywilną na potrzeby Prezesa Rady Ministrów, Rady Ministrów i ministra właściwego do spraw wewnętrznych,
    - realizacja innych zadań z zakresu ochrony ludności i obrony cywilnej powierzonych przez ministra właściwego do spraw wewnętrznych,

- zapewnienie wymiany informacji na potrzeby realizacji zadań ochrony ludności i obrony cywilnej,
- zapewnienie wymiany informacji w ramach międzynarodowej współpracy w obszarze ludności i zobowiązań sojuszniczych,
- współdziałanie z organami ochrony ludności.

- ✓ (art. 1 pkt 11 ustawy nowelizującej) dodanie art. 11b ma na celu przede wszystkim dostosowanie przepisów do stanu faktycznego. Centrum w praktyce realizuje zadania w zakresie planowania cywilnego wynikającego z członkostwa w Organizacji Traktatu Północnoatlantyckiego, Centrum, w tym koordynuje udział przedstawicieli Rzeczypospolitej Polskiej w pracach prowadzonych na forum NATO (np. Komitetu Odporności NATO) oraz zapewnia wsparcie merytoryczne prowadzonych prac czy też uruchamiania przedsięwzięcia i procedur systemu zarządzania kryzysowego NATO;
- ✓ (art. 1 pkt 12 i 13 ustawy nowelizującej) zmiany w art. 12 oraz 14 ustawy o zarządzaniu kryzysowym są dostosowaniem do zmian w zakresie planów zarządzania kryzysowego, wynikających z dostosowania do zmiana w obszarze planistyki zarządzania kryzysowego;
- ✓ (art. 1 pkt 14 ustawy nowelizującej) propozycje zmian polega na doprecyzowaniu jednego z zadań Sił Zbrojnych Rzeczypospolitej Polskiej realizowanego na rzecz zarzadzania kryzysowego;
- ✓ (art. 1 pkt 15 ustawy nowelizującej) uchylane przepisy zostają przeniesione do ustawy ustawie z dnia 11 marca 2004 r. o ochronie zdrowia zwierząt oraz zwalczaniu chorób zakaźnych zwierząt. Regulacje w zakresie możliwości tworzenia doraźnych zgrupowań zadaniowych formowanych z policjantów, funkcjonariuszy Straży Granicznej lub funkcjonariuszy Państwowej Straży Pożarnej, którzy posiadają uprawnienia do wykonywania polowania, celem ich użycia do odstrzału sanitarnego zwierząt wolno żyjących (dzikich) na określonych obszarach powinny być materią tejże ustawy, a nie ustawy o zarządzaniu kryzysowym;
- ✓ (art. 1 pkt 17 ustawy nowelizującej) doprecyzowuje przeznaczenie środków finansowych na rzecz jednostek samorządu terytorialnego. Zgodnie z postulatami strony samorządowej Środki finansowe z rezerwy celowej tworzonej na potrzeby zarządzania kryzysowego mogą być przeznaczone na realizację przedsięwzięć związanych z zarządzaniem ryzykiem, reagowaniem w przypadku wystąpienia sytuacji kryzysowej oraz usuwaniem jej skutków i

odtwarzaniem zasobów, z uwzględnieniem planowanych działań z zakresu ochrony ludności i obrony cywilnej. Projektowana regulacja przewiduje możliwość, aby środki z rezerwy celowej mogły być przeznaczane na pomoc finansową udzielaną innym jednostkom samorządu terytorialnego na realizację przez te jednostki przedsięwzięć z zakresu zarządzania kryzysowego;

- ✓ (art. 1 pkt 16, 18 i 19 ustawy nowelizującej) zmiany mają charakter porządkowy.

Zmiany w innych ustawach (art. 2–23 ustawy nowelizującej)

- ✓ ustawa z dnia 21 marca 1985 r. o drogach publicznych (Dz. U. z 2025 r. poz. 889).[1]

  Z uwagi na konieczność szybkiego zapewnienia możliwości przemieszczania się wojsk, innych zasobów niezbędnych dla Sił Zbrojnych RP, a także w celu transportowania sprzętu wojskowego lub amunicji, żywności, produktów leczniczych i wyrobów medycznych, wody pitnej i innych środków humanitarnych itp. do miejsca docelowego, w tym na przejścia graniczne, konieczne jest uruchomienie narzędzia prawnego umożliwiającego niezwłoczne zapewnienie pełnej, niezakłóconej przepustowości niektórych odcinków dróg publicznych lub linii kolejowych w ściśle oznaczonym czasie, a także zapewnienie pierwszeństwa rozładunku i załadunku określonym przewozom i ładunkom. Aktualna sytuacja geopolityczna, w szczególności położenie geograficzne RP i graniczenie z państwem, którego terytorium objęte jest działaniami wojennymi, zmusza do zabezpieczenia obronności i istotnego interesu bezpieczeństwa państwa, na wypadek konieczności pilnego i niezakłóconego transportu kontyngentów wojskowych lub humanitarnych w określone miejsce przeznaczenia, w szczególności strategiczne z punktu widzenia obronności i ochrony życia i zdrowia ludzkiego, a także ewakuację ludności cywilnej z obszarów objętych zagrożeniem.

  Należy wskazać, iż w sytuacji bieżącego funkcjonowania państwa może powstać konieczność zapewnienia niezwłocznej reakcji państwa na określone zagrożenia hybrydowe. Jednocześnie wprowadzone czasowe ograniczenia w korzystaniu z dróg publicznych czy zamknięcie dróg publicznych na niektórych odcinkach powinno

[1] Analogiczna propozycja dotyczy również linii kolejowych – vide zmiana w ustawie o transporcie kolejowym.

uwzględniać konieczność zapewnienia obywatelom przemieszczenia się w dowolnych kierunkach innymi alternatywnymi drogami, np. o charakterze lokalnym.

Zasadnym jest zobowiązanie właściwego miejscowo wojewodę do przekazania informacji o konieczności podjęcia działań również przez innego wojewodę, jeżeli w toku procedowania rozporządzenia porządkowego uzyska on informację o konieczności wprowadzenia czasowego ograniczenia w dostępie do przepustowości lub całkowitego wyłączenia z udostępniania infrastruktury kolejowej dla linii kolejowych znajdujących się poza obszarem jego właściwości.

Uzasadnionym jest także wprowadzenie koordynatora przewozu dla wszystkich zarządców infrastruktury oraz licencjonowanych przewoźników kolejowych dla określonych przewozów. W zakresie sposobu publikacji rozporządzeń porządkowych wskazano, iż mogą być publikowane w drodze obwieszczenia lub za pomocą środków komunikacji elektronicznej (np. sms ALERT RCB) lub w inny sposób zwyczajowo przyjęty na danym terenie (np. tablice informacyjne). Dzień takiego opublikowania jest dniem ogłoszenia;

- ✓ ustawa z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2025 r. poz. 636, z późn. zm.).

Proponowana zmiana w art. 16 tej ustawy jest konsekwencją wprowadzenia zmian do ustawy o środkach przymusu bezpośredniego i broni palnej.

Dodatkowo projekt obejmuje propozycję art. 18c ustawy o Policji, w której wskazano, iż Komendant Główny Policji, Komendant CBŚP, Komendant CBZC lub komendant wojewódzki Policji mogą w określonych przypadkach podjąć decyzję o dopuszczalności zastosowania przez Policję urządzeń uniemożliwiających telekomunikację na określonym obszarze, przez czas niezbędny do wyeliminowania zagrożenia lub jego skutków, z uwzględnieniem konieczności minimalizacji skutków braku możliwości korzystania z usług telekomunikacyjnych.

Natomiast propozycja dodania w art. 36k ust. 3a precyzuje kwestię wypłaty należności funkcjonariuszy Policji oddelegowanych do wykonywania zadań służbowych w urzędzie obsługującym ministra właściwego do spraw wewnętrznych albo w jednostce podległej lub nadzorowanej przez ministra właściwego do spraw wewnętrznych – jednoznacznie wskazując, iż stosowne należności wypłaca jednostka organizacyjna Policji, w której policjant pełnił służbę bezpośrednio przed oddelegowaniem. Zadania związane z zarządzaniem kryzysowym, ochroną ludności lub obroną cywilną to zadania realizowane na rzecz całego Państwa, we współpracy wielu służb. Przyjęcie zasady, że koszty ponosi

jednostka, która deleguje funkcjonariusza – w ocenie wnioskodawcy – wzmocni odpowiedzialność i zaangażowania służb w realizację wspólnych celów. Za wprowadzeniem proponowanego rozwiązania przemawia również wspieranie racjonalnego gospodarowania zasobami kadrowymi i zachowanie spójności budżetowej.

- ✓ ustawa z dnia 12 października 1990 r. o Straży Granicznej (Dz. U. z 2025 r. poz. 914, z późn. zm.).

  Propozycja dodania w art. 1 ustawy o Straży Granicznej ust. 3c związana jest z realizacją nowych zadania, jakim jest koordynacja działań podejmowanych przez podmioty realizujące zadania w ramach Centrum Bezpieczeństwa Morskiego, o którym mowa w art. 25a ustawy z dnia 4 września 2008 r. o ochronie żeglugi i portów morskich.

  Dodatkowo projekt obejmuje propozycję art. 10c ustawy o Straży Granicznej, w której wskazano, iż Komendant Główny Straży Granicznej, Komendant BSWSG lub komendant oddziału Straży Granicznej mogą w określonych przypadkach podjąć decyzję o dopuszczalności zastosowania urządzeń uniemożliwiających telekomunikację na określonym obszarze, przez czas niezbędny do wykonywania czynności przez Straż Graniczną, z uwzględnieniem konieczności minimalizacji skutków braku możliwości korzystania z usług telekomunikacyjnych.

  Propozycja zmiany w art. 23 ustawy o Straży Granicznej jest konsekwencją wprowadzenia zmian do ustawy o środkach przymusu bezpośredniego i broni palnej.

  Natomiast propozycja dodania w art. 41i ust. 1a precyzuje kwestię wypłaty należności funkcjonariuszy Straży Granicznej oddelegowanych do wykonywania zadań służbowych w urzędzie obsługującym ministra właściwego do spraw wewnętrznych albo w jednostce podległej lub nadzorowanej przez ministra właściwego do spraw wewnętrznych – jednoznacznie wskazując, iż stosowne należności wypłaca jednostka organizacyjna, w której funkcjonariusz pełnił służbę bezpośrednio przed oddelegowaniem. Zadania związane z zarządzaniem kryzysowym, ochroną ludności lub obroną cywilną to zadania realizowane na rzecz całego Państwa, we współpracy wielu służb. Przyjęcie zasady, że koszty ponosi jednostka, która deleguje funkcjonariusza – w ocenie wnioskodawcy – wzmocni odpowiedzialność i zaangażowania służb w realizację wspólnych celów. Za wprowadzeniem proponowanego rozwiązania przemawia również wspieranie racjonalnego gospodarowania zasobami kadrowymi i zachowanie spójności budżetowej;

- ✓ ustawa z dnia 24 sierpnia 1991 r. o ochronie przeciwpożarowej (Dz. U. z 2025 r. poz. 188). Dostosowanie przepisu tej ustawy do projektowanych zmian w zarządzaniu kryzysowym przez wskazanie korelacji planów ratowniczych z planami reagowania kryzysowego;
- ✓ ustawa z dnia 24 sierpnia 1991 r. o Państwowej Straży Pożarnej (Dz. U. z 2025 r poz. 1312, z późn. zm.).

  Propozycja dodania w art. 37r ustawy o Państwowej Straży Pożarnej ust. 1a precyzuje kwestię wypłaty należności strażaków PSP oddelegowanych do wykonywania zadań służbowych w urzędzie obsługującym ministra właściwego do spraw wewnętrznych albo w jednostce podległej lub nadzorowanej przez ministra właściwego do spraw wewnętrznych – jednoznacznie wskazując, iż stosowne należności wypłaca jednostka organizacyjna PSP, w której strażak pełnił służbę bezpośrednio przed oddelegowaniem. Zadania związane z zarządzaniem kryzysowym, ochroną ludności lub obroną cywilną to zadania realizowane na rzecz całego Państwa, we współpracy wielu służb. Przyjęcie zasady, że koszty ponosi jednostka, która deleguje funkcjonariusza – w ocenie wnioskodawcy – wzmocni odpowiedzialność i zaangażowanie służb w realizację wspólnych celów. Za wprowadzeniem proponowanego rozwiązania przemawia również wspieranie racjonalnego gospodarowania zasobami kadrowymi i zachowanie spójności budżetowej;
- ✓ ustawa z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz. U. z 2025 r. poz. 532).

  Proponowane zmiany wpisują się w cele projektu ustawy o zmianie ustawy o zarządzaniu kryzysowym oraz niektórych innych ustaw, co wynika z faktu, że odnoszą się do zwiększenia ochrony infrastruktury kluczowej w zakresie bezpieczeństwa publicznego, a równocześnie stanowią odpowiedź na wnioski Najwyższej Izby Kontroli sformułowane po zakończeniu kontroli wybranych przedsiębiorstw wykonujących zadania gmin w zakresie zaspakajania zbiorowych potrzeb mieszkańców odnośnie dostawy wody, ciepła i usuwaniu ścieków komunalnych, które to wnioski zostały skierowane bezpośrednio do ministra właściwego do spraw wewnętrznych. Najwyższa Izba Kontroli zawnioskowała o dokonanie kompleksowej oceny ustawy o ochronie osób i mienia, w tym również jej uspójnienia z ustawą o zarządzaniu kryzysowym w kierunku wzmocnienia ochrony tych obiektów przed zagrożeniem nieuprawnioną ingerencją. W opinii NIK nieprecyzyjne przepisy powodują, że obecny poziom ich zabezpieczenia jest niewystarczający. Brak jest również bieżącej wymiany informacji i ewidencjonowania istniejącej tego rodzaju

infrastruktury na poziomie województwa. W związku z powyższym, proponuje się zastąpienie występujących w art. 5 ust. 2 pkt 3 lit. a ustawy o ochronie osób i mienia wyrazów „aglomeracji miejskich" pojęciem „powiatów lub miast na prawach powiatu". W ten sposób doprecyzowana zostanie kwestia, jakie obiekty i urządzenia powinny być uwzględniane w tym katalogu. Pojęcie „aglomeracja miejska" nie jest prawnie zdefiniowane, co powoduje trudności w jednolitym stosowaniu tego przepisu. Dodatkowo proponuje się dodanie przepisu, w którym starostowie i prezydenci miast na prawach powiatów będą przekazywali stosowne informacje wojewodom na temat zakładów, obiektów i urządzeń.

Dodatkowo w ustawie o ochronie osób i mienia proponuje się zmiany przepisów w zakresie ochrony najważniejszych dla państwa obszarów, obiektów i urządzeń, tj. zmiany do art. 5 ustawy, które mają usprawnić zapewnienie tej ochrony.

W pierwszej kolejności proponuje się zmianę do art. 5 ust. 2 pkt 5, która dostosowuje ten przepis do nowej siatki pojęciowej wprowadzanej przedmiotową nowelizacją, jednocześnie zapewniając wyeliminowanie trudności, które mogłyby powstać w sytuacji równoległego stosowania znowelizowanej ustawy o zarządzaniu kryzysowym oraz ustawy o ochronie osób i mienia w tym zakresie.

Ponadto proponuje się dodanie Komisji Nadzoru Finansowego do katalogu podmiotów zobowiązanych do prowadzenia wykazów obszarów, obiektów i urządzeń podlegających obowiązkowej ochronie. Zgodnie z obowiązującym art. 5 ust. 3 ustawy o ochronie osób i mienia Prezes Narodowego Banku Polskiego prowadzi taki wykaz w odniesieniu do banków. Natomiast nie zachodzą żadne przesłanki, aby uznać, że w wykazie prowadzonym przez Prezesa Narodowego Banku Polskiego mogą być umieszczane jakiekolwiek inne podmioty procesujące wartości pieniężne w znacznych ilościach, takie jak np. spółdzielcze kasy oszczędnościowo-kredytowe.

Rezultatem tych zmian jest konieczność wprowadzenia przepisów dostosowujących, które pozwolą na uniknięcie sytuacji, w której ten sam podmiot (bank) będzie znajdował się zarówno w wykazie prowadzonym przez Prezesa Narodowego Banku Polskiego, jak i w wykazie prowadzonym przez Komisję Nadzoru Finansowego.

Ponadto w celu wyeliminowania obserwowanych opóźnień w zakresie realizacji obowiązku przesyłania do właściwych terytorialnie wojewodów aktualnych wykazów obszarów, obiektów i urządzeń podlegających obowiązkowej ochronie, projektowane

zmiany do art. 5 ww. ustawy przewidują określenie terminu realizacji przedmiotowego zadania. Z powyższym rozwiązaniem powiązane jest wprowadzenie wymogu niezwłocznej aktualizacji prowadzonej przez wojewodę ewidencji. Pozwoli to na sprawny przepływ bieżących informacji, co warunkuje możliwość zapewnienia odpowiedniej ochrony obszarom, obiektom i urządzeniom kluczowym dla bezpieczeństwa państwa.

Jednocześnie proponuje się dodanie art. 5a, co ma na celu zapewnienie stosowania określonych w tej ustawie środków ochrony fizycznej i zabezpieczenia technicznego od strony wody poza granicami obiektów podlegających obowiązkowej ochronie. Równolegle proponuje się rozszerzenie uprawnień pracowników ochrony o możliwość podejmowania dodatkowych działań względem infrastruktury portowej w celu zapewnienia jej większego poziomu zabezpieczenia – zmiany do art. 36 ustawy).

Projektowane regulacje w tym zakresie uzupełniają przepisy dotyczące sankcji możliwych do stosowania do osób, które jako nieuprawnione przebywają na terenie obszarów lub obiektów podlegających obowiązkowej ochronie, nie stosują się do żądań ich opuszczenia, czy też uniemożliwiają korzystanie m.in. z obszarów lub obiektów podlegających obowiązkowej ochronie.

- ✓ ustawa z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych (Dz. U. z 2026 r. poz. 159).

  Konsekwencja wprowadzenia zmian do ustawy o środkach przymusu bezpośredniego i broni palnej są zmiany w ustawach pragmatycznych poszczególnych służb, tj. w ustawie o Policji, ustawie o Straży Granicznej, ustawie o Żandarmerii Wojskowej i wojskowych organach porządkowych oraz w ustawie o Służbie Ochrony Państwa;

- ✓ ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2025 r. poz. 902, z późn. zm.) – zmiany wynikowe – zmiana definicji infrastruktury krytycznej oraz systematyki ustawy o zarządzaniu kryzysowym;

- ✓ ustawa z dnia 28 marca 2003 r. o transporcie kolejowym (Dz. U. z 2025 r. poz. 1234, z późn. zm.) – uzasadnienie wprowadzenia zmian jest analogiczne do zakresu zmian proponowanych w ustawie o drogach publicznych;

- ✓ ustawa z dnia 11 marca 2004 r. o ochronie zdrowia zwierząt oraz zwalczaniu chorób zakaźnych zwierząt (Dz. U. z 2023 r. poz. 1075, z późn. zm.) – „przeniesienie" przepisów

dotyczących „zorganizowanego sanitarnego odstrzału dzików” z przepisów ustawy o zarządzaniu kryzysowym (art. 25a–25d ustawy z.k.);

- ✓ ustawa z dnia 4 września 2008 r. o ochronie żeglugi i portów morskich (Dz. U. z 2024 r. poz. 597).

W ustawie o ochronie żeglugi i portów morskich proponuje się w pierwszej kolejności rozszerzenie zasad ochrony na terminal morskiego przeładunku ropy i paliw ciekłych w Gdańsku (Naftoport).

Ponadto proponuje się dodanie kolejnego rozdziału dotyczącego zapobieganiu bezprawnemu wykonywaniu operacji z użyciem bezzałogowych obiektów pływających. Proponowane rozwiązania w tym zakresie są wzorowane na propozycjach zmian do ustawy – Prawo lotnicze w ramach prac nad projektem ustawy o zmianie ustawy – Prawo lotnicze oraz niektórych innych ustaw (UC19). Proponuje się opisanie w ustawie o ochronie żeglugi i portów morskich przypadków, w których możliwe jest zniszczenie, unieruchomienie lub przejmowanie kontroli nad bezzałogowym obiektem pływającym. Regulacje w tym zakresie są niezbędne ze względów bezpieczeństwa osób i miejsc, nad którymi mogą być wprowadzane stałe lub czasowe ograniczone możliwości operacji takimi urządzeniami, albo gdy obecność takiego statku jest zakazana. Dodatkowo wskazuje się, że za szkody powstałe w wyniku zniszczenia, unieruchomienia albo przejęcia kontroli nad bezzałogowym statkiem pływającym we wskazanych przypadkach odpowiada właściciel lub operator lub armator statku.

Konsekwencją ww. zmian są zmiany do ustawy o środkach przymusu bezpośredniego i broni palnej oraz zmiany w ustawach pragmatycznych poszczególnych służb (*vide* ustawa o Policji, Straży Granicznej, Służbie Ochrony Państwa, Żandarmerii Wojskowej).

Projektowane zmiany do ustawy o ochronie żeglugi i portów morskich w zakresie dodawanych art. 25a–25d mają na celu ustanowienie podstawy prawnej do powołania i funkcjonowania Centrum Bezpieczeństwa Morskiego (CBM).

Należy zauważyć, że w dobie podwyższonego zagrożenia szeroko rozumianymi atakami hybrydowymi ze strony Federacji Rosyjskiej oraz Białorusi, o czym świadczą m.in. próby uszkodzenia rurociągów (Nord Stream i Balticconnector), kabli energetycznych (SvePol) i telekomunikacyjnych (C-Lion1, NordBalt, E-Finest), poważnym wyzwaniem dla bezpieczeństwa Polski staje się ochrona infrastruktury morskiej. Instalacje energetyczne, rurociągi i porty morskie wyspecjalizowane do przeładunku paliw płynnych są kluczowymi

instrumentami dla zapewnienia nieprzerwanych dostaw ropy i gazu do Polski. Co więcej, w najbliższych latach realizowane będą nowe strategiczne inwestycje, mające na celu zwiększenie bezpieczeństwa energetycznego Polski, takie jak elektrownia jądrowa oraz morskie farmy wiatrowe. Planowana jest również rozbudowa terminalu regazyfikacyjnego skroplonego gazu ziemnego w Świnoujściu, portów morskich w Gdańsku, Gdyni i Szczecinie-Świnoujściu, a także budowa pływającego terminalu LNG (FSRU) w Zatoce Gdańskiej, które dzięki tym inwestycjom zwiększą przepustowość i zdolności logistyczne Polski dla transportu morskiego.

W tym kontekście niezbędnym jest więc podjęcie działań mających na celu zwiększenie poziomu ochrony infrastruktury morskiej. To z kolei będzie możliwe jedynie w przypadku zapewnienia stałego monitoringu i bieżącej oceny sytuacji dla tej infrastruktury, usprawnianie reakcji służb na potencjalne zdarzenia oraz zapewnienie efektywnego zarządzania kryzysowego z użyciem nowoczesnej technologii informacyjnej.

Powołanie Centrum Bezpieczeństwa Morskiego będzie stanowiło wyraz międzysektorowego i wieloinstytucjonalnego podejścia w odniesieniu do ochrony szeroko rozumianej infrastruktury morskiej, której wymiernym efektem będzie zwiększenie odporności tej infrastruktury na wszelkiego rodzaju ataki, w tym o charakterze hybrydowym. W związku z tym do zadań CBM będzie należało m.in. bieżące monitorowanie zagrożeń oraz wspieranie współpracy, w tym wymiany informacji, pomiędzy służbami i podmiotami realizującymi zadania w zakresie ochrony infrastruktury morskiej, statków, granicy państwa na morzu, a także ochrony życia lub zdrowia ludzi, mienia i środowiska znajdujących się na polskich obszarach morskich w tym w wyłącznej strefie ekonomicznej.

Projekt ustawy przewiduje, że CBM będzie umiejscowione we wskazanym przez Komendanta Głównego Straży Granicznej oddziale Straży Granicznej i kierowana przez funkcjonariuszy tej formacji, natomiast do niej oddelegowani będą przedstawiciele innych służb oraz podmiotów właściwych do zapewnienia realizacji poszczególnych zadań CBM. W myśl projektowanych przepisów zadania te CBM będzie realizowało w sposób ciągły, tj. w systemie całodobowym 7 dni w tygodniu. Natomiast w szczególnie uzasadnionych przypadkach związanych z pojawieniem się zagrożenia dla infrastruktury morskiej, w ramach CBM będzie dodatkowo powoływany sztab koordynacyjny, do zadań którego należeć będzie dokonywanie aktualnej oceny stopnia zagrożenia infrastruktury morskiej,

statków lub granicy państwa na morzu oraz wydawania rekomendacji zmierzających do odpowiedniego zabezpieczenia tej infrastruktury, statków lub granicy.

Założeniem projektodawcy jest usprawnienie, obecnie rozproszonego instytucjonalnie, systemu monitorowania zagrożeń i oceny bezpieczeństwa na wodach terytorialnych Morza Bałtyckiego, a tym samym zwiększenia zdolności operacyjnych i przyspieszenia reakcji służb. Z kolei powierzenie Straży Granicznej funkcji koordynacyjnej dla tej struktury wydaje się zasadne z uwagi na fakt, że formacja ta już obecnie realizuje szereg zadań wpisujących się w proponowaną koncepcję CBM. Straż Graniczna, poprzez Morski Oddział SG, chroni granicę państwową na morzu, sprawuje nadzór nad eksploatacją polskich obszarów morskich, zabezpiecza obiekty portowe od strony wody przed dostępem nieuprawnionych jednostek pływających, ochrania niektóre obiekty infrastruktury krytycznej, a także strzeże dostępu do strefy ustanowionej wokół terminala regazyfikacyjnego skroplonego gazu ziemnego w Świnoujściu.

Propozycje obejmują również podstawy prawne działań w odniesieniu do zapobiegania bezprawnemu wykonywaniu operacji z użyciem bezzałogowych obiektów pływających.

Bezzałogowe obiekty pływające będą mogły być zniszczone, unieruchomione albo może nad nim zostać przejęta kontrola, w przypadku gdy działanie bezzałogowego obiektu pływającego zagraża lub może zagrozić życiu lub zdrowiu ludzi lub zwierząt, stwarza lub może stworzyć zagrożenie dla chronionych obiektów, urządzeń lub obszarów, stwarza lub może stworzyć uzasadnione podejrzenie, że może zostać użyty jako środek ataku terrorystycznego, stwarza lub może stworzyć zagrożenie bezpieczeństwa jednostki pływającej lub życia lub zdrowia załogi lub pasażerów znajdujących się na jej pokładzie, lub utrudnia lub może utrudnić ruch w portach morskich lub powoduje lub może spowodować jego wstrzymanie lub ograniczenie. Innym przypadkiem na jaki wskazują projektowane przepisy jest wykonywanie operacji w polskich obszarach morskich wbrew zakazowi przez bezzałogowy obiekt pływający.

Co do zasady przepisy dają podstawę do zniszczenia, unieruchomienia bezzałogowego obiektu pływającego albo przejęcia nad nim kontroli przez funkcjonariuszy Policji, Straży Granicznej, Służby Ochrony Państwa oraz, zgodnie z zakresem właściwości miejscowej, pracowników ochrony specjalistycznych uzbrojonych formacji ochronnych.

Natomiast do zniszczenia, unieruchomienia bezzałogowego obiektu pływającego albo przejęcia nad nim kontroli na terenie chronionych obiektów Sił Zbrojnych

Rzeczypospolitej Polskiej oraz jednostek organizacyjnych podległych, podporządkowanych lub nadzorowanych przez Ministra Obrony Narodowej są uprawnieni żołnierze Żandarmerii Wojskowej oraz Sił Zbrojnych Rzeczypospolitej Polskiej.

Projekt przewiduje, iż za szkody powstałe w wyniku zniszczenia, unieruchomienia albo przejęcia kontroli nad bezzałogowym obiektem pływającym w przypadkach wskazanych w projektowanych przepisach odpowiada właściciel lub operator lub armator bezzałogowego obiektu pływającego zniszczonego, unieruchomionego albo nad którym przejęto kontrolę;

- ✓ ustawa z dnia 18 marca 2010 r. o szczególnych uprawnieniach ministra właściwego do spraw aktywów państwowych oraz ich wykonywaniu w niektórych spółkach kapitałowych lub grupach kapitałowych prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych (Dz. U. z 2025 r. poz. 470).

  Minister właściwy do spraw aktywów państwowych wykonuje uprawnienia wynikające z ustawy *o szczególnych uprawnieniach* wobec wszystkich podmiotów jej podlegających, tj. spółek prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych, których mienie zostało ujawnione w prowadzonym przez Dyrektora Rządowego Centrum Bezpieczeństwa jednolitym wykazie obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej z podziałem na systemy (dalej: „wykaz"). Do spółek tych należą, podmioty, w których Skarb Państwa posiada udziały i wykonuje prawa przysługujące z posiadanych akcji, oraz podmioty całkowicie prywatne.

  Szacuje się, że wraz z implementacją dyrektywy 2022/2557 do krajowego porządku prawnego jednolity wykaz, po przeprowadzeniu stosownej kwalifikacji, zostanie uzupełniony w znaczącej mierze podmiotami prywatnymi, wobec których minister aktywów państwowych nie będzie posiadał narzędzi dyscyplinujących i egzekwujących realizację postanowień ustawy *o szczególnych uprawnieniach*. Taki stan rzeczy wpłynie negatywnie na ochronę infrastruktury krytycznej, w tym infrastruktury kluczowej dla bezpieczeństwa państwa i jego obywateli oraz służącej zapewnieniu sprawnego funkcjonowania organów administracji publicznej a także instytucji i przedsiębiorców.

  Projektowana nowelizacja ustawy stawia sobie za cel wzmocnienie systemu ochrony infrastruktury krytycznej. Proponowane zmiany skupiają się przede wszystkim na czterech kluczowych aspektach dotyczących usankcjonowania obowiązku powoływania zastępcy Pełnomocnika do spraw ochrony infrastruktury krytycznej, zapewnienia ministrowi

właściwemu do spraw aktywów państwowych narzędzi dyscyplinujących zarządy spółek oraz Pełnomocników i ich zastępców, wydłużenie terminów przysługujących na rozpatrzenie spraw, a także zmianę sposobu i cyklu raportowania.

W celu zapewnienia ciągłości procesów realizowanych przez Pełnomocnika do spraw ochrony infrastruktury krytycznej (dalej: „Pełnomocnik OIK"), proponuje się w art. 5 ust. 1 zobowiązanie zarządów spółek do powoływania zastępcy Pełnomocnika OIK. Projektowane przepisy zakładają, że tryb powoływania i odwoływania oraz kompetencje i obowiązki zastępcy Pełnomocnika OIK będą analogiczne do zadań realizowanych przez Pełnomocnika OIK, z zastrzeżeniem, że zastępca Pełnomocnika OIK będzie powoływany w terminie 60 dni od dnia otrzymania przez zarząd spółki informacji o ujęciu składników jej mienia w wykazie (Pełnomocnik OIK powoływany jest w terminie 30 dni). Taki stan rzeczy pozwoli na zapewnienie przez Pełnomocnika OIK odpowiedniego wsparcia zarządowi spółki w zakresie pozyskania odpowiedniego, spełniającego kryteria formalne, kandydata na to stanowisko. Kluczowym zadaniem zastępcy Pełnomocnika OIK będzie zapewnienie zastępstwa, ale także wsparcie procesów i zadań realizowanych w spółce z zakresu bezpieczeństwa infrastruktury krytycznej.

Obecnie, w przypadku nieobecności pełnomocnika w pracy spowodowanej urlopem, chorobą lub innymi losowymi okolicznościami, których nie sposób przewidzieć, zastępstwo zapewniane jest przez inne osoby najczęściej pracujące w pionie bezpieczeństwa, których kompetencje pozostają niezweryfikowane. Nieoficjalni zastępcy nie posiadają narzędzi pozwalających np. na uczestnictwo w posiedzeniach organów spółki dotyczących infrastruktury krytycznej oraz nie posiadają prawa do żądania od organów spółki udzielenia informacji oraz wyjaśnień, a tym samym nie zapewniają rzetelnego wykonywania obowiązków należących do Pełnomocnika OIK, a w konsekwencji nie dają rękojmi do prawidłowego realizowania przepisów ustawy. Z uwagi na fakt, że zgodnie z art. 5 ust 2 ustawy *o szczególnych uprawnieniach* Pełnomocnik OIK jest pracownikiem spółki, tj. podlega przepisom Kodeksu pracy wraz z wszelkimi wynikającymi z tego faktu prawami i obowiązkami, niezbędne jest, w ocenie Ministerstwa, stworzenie warunków do zapewnienia Pełnomocnikowi OIK stosownego zastępstwa oraz zapewnienie ciągłości realizacji zadań ustawowych Pełnomocnika OIK.

Proponowane zmiany, w ocenie Ministerstwa Aktywów Państwowych, pozwolą na zapewnienie ciągłości realizowanych procesów oraz pozytywnie wpłyną na realizację

zadań Pełnomocnika OIK w zakresie zapewnienia bezpieczeństwa infrastruktury krytycznej. Zakłada się, że tryb powoływania i odwoływania zastępcy Pełnomocnika OIK, jego szczegółowe zadania oraz podległość służbowa zostaną dookreślone w ramach nowelizacji rozporządzenia Prezesa Rady Ministrów dnia 26 kwietnia 2021 r. *w sprawie pełnomocnika do spraw ochrony infrastruktury krytycznej*.

W ramach proponowanych zmian kolejnym istotnym aspektem jest zapewnienie ministrowi właściwemu do spraw aktywów państwowych odpowiednich narzędzi dyscyplinujących zarządy spółek oraz Pełnomocników OIK i ich zastępców. Ideą projektowanego art. 7a jest stworzenie warunków prawnych umożliwiających nałożenie kary finansowej na zarząd spółki w przypadku niepowołania Pełnomocnika OIK i jego zastępcy oraz w sytuacji braku współpracy zarządu spółki z Pełnomocnikiem OIK i jego zastępcą. Działania zarządu spółki polegające na nieprzekazywaniu dokumentów lub informacji o podjęciu uchwały lub o dokonaniu przez organy spółki czynności prawnych, o których mowa w ustawie *o szczególnych uprawnieniach*, lub nieinformowanie Pełnomocnika OIK i jego zastępcy o każdym planowanym posiedzeniu organów spółki, dotyczącym spraw, o których mowa w ustawie *o szczególnych uprawnieniach*, w znaczny sposób utrudnia, a w konsekwencji uniemożliwia prawidłową realizację ustawowych zadań Pełnomocnika OIK i jego zastępcy, co stanowi zagrożenie dla bezpieczeństwa infrastruktury krytycznej. W przypadku uporczywego naruszania przepisów ustawy przewiduje się również możliwość nałożenia kary finansowej. W projektowanych przepisach celowo użyto określenia, że „zarząd spółki może podlegać karze", z uwagi na fakt, że karanie, jako czynność, nie jest celem bezpośrednim proponowanego przepisu, a ma stanowić wyłącznie narzędzie dyscyplinujące poprzez samą możliwość nałożenia kary finansowej. W szczególności spółki, w których Skarb Państwa nie posiada udziałów oraz nie wykonuje praw z akcji mogą podejmować próby uchylenia się od realizacji zadań określonych w ustawie *o szczególnych uprawnieniach*, a tym samym sprowadzić potencjalne zagrożenie dla infrastruktury krytycznej.

Podobnie jak ma to miejsce w przypadku zarządu spółki, proponuje się również uzupełnienie ustawy *o szczególnych uprawnieniach* o narzędzia dyscyplinujące Pełnomocnika OIK oraz jego zastępcę. Zakłada się możliwość, w przypadku nierealizowania przez Pełnomocnika OIK lub jego zastępcę zadań ustawowych, uznania przez Ministra, że Pełnomocnik OIK przestał dawać rękojmię prawidłowego wykonywania obowiązków. W myśl proponowanych przepisów zarząd spółki, w terminie 30 dni od dnia

powiadomienia o uznaniu przez Ministra, że Pełnomocnik OIK lub jego zastępca przestał dawać rękojmie prawidłowej realizacji zadań ustawowych, byłby zobowiązany do odwołania Pełnomocnika OIK lub jego zastępcy w trybie określonym w art. 5 ust. 1 ustawy *o szczególnych uprawnieniach*.

Trzecim kluczowym aspektem nowelizacji ustawy *o szczególnych uprawnieniach* jest wydłużenie w art. 2 ust. 3 terminów przysługujących ministrowi właściwemu do spraw aktywów państwowych na zgłoszenia sprzeciwu wobec określonych czynności spółki stanowiących zagrożenie dla funkcjonowania, ciągłości działania oraz integralności infrastruktury krytycznej – z 14 do 45 dni od dnia otrzymania przez ministra właściwego do spraw aktywów państwowych od Pełnomocnika OIK informacji o podjęciu przez organy spółki uchwały oraz z 30 do 60 dni w przypadku dokonania tych czynności przez zarząd spółki. Dotychczasowe doświadczenia wskazują, że 14 dniowy termin na dokonanie wszechstronnej i kompleksowej oceny planowanych przez spółkę czynności w kontekście zagrożenia dla funkcjonowania, ciągłości działania oraz integralności infrastruktury krytycznej, a także przeprowadzenie postępowania i wydanie decyzji administracyjnej, w często skomplikowanych i złożonych sprawach, jest zbyt krótki. Wydłużając terminy w art. 2 ust. 3 przysługujące na rozpatrzenie sprawy, proponuje się również w art. 2 ust. 3a wydłużenie terminu z 7 do 10 dni, który przysługuje ministrowi właściwemu do spraw energii lub ministrowi właściwemu do spraw gospodarki surowcami energetycznymi, w zakresie wyrażenia opinii dotyczącej określonych ustawowo czynności spółki, które mogą stwarzać zagrożenie dla infrastruktury krytycznej. Analogicznie proponuje się w art. 2 ust. 5 wydłużenie terminu z 14 do 30 dni przysługującego na ponowne rozpatrzenie sprawy oraz w art. 2 ust. 6 pkt 1 i pkt 2 wydłużenie terminu z 14 do 30 dni, w którym minister właściwy do spraw aktywów państwowych zobowiązany jest do przekazania do właściwego sądu administracyjnego skargi na decyzję wraz z aktami sprawy oraz odpowiedzią na skargę, oraz w którym sąd administracyjny wyznacza rozprawę na dzień przypadający w terminie 30 dni od dnia przekazania skargi. Zasadniczym celem wydłużenia terminów jest zapewnienie warunków umożliwiających dokonanie wszechstronnej oceny planowanych przez spółkę czynności oraz zapewnienie czasu niezbędnego do analizy dokumentacji, pozyskania dodatkowych informacji i wyjaśnień oraz właściwej oceny, czy czynności prawne i materialne podejmowane przez spółkę stwarzają zagrożenie dla funkcjonowania, ciągłości działania oraz integralności infrastruktury krytycznej.

Czwartą istotną zmianą w projektowanej nowelizacji ustawy *o szczególnych uprawnieniach* jest modyfikacja cyklu raportowania. W dotychczasowym brzmieniu ustawy, Pełnomocnik OIK zobowiązany jest do opracowywania raportów kwartalnych i sprawozdań kwartalnych z wykonanych obowiązków, które przekazywane są ministrowi właściwemu do spraw aktywów państwowych, Dyrektorowi Rządowego Centrum Bezpieczeństwa oraz odpowiednio ministrowi właściwemu do spraw energii lub ministrowi właściwemu do spraw gospodarki surowcami energetycznymi. W przypadku uzupełnienia wykazu o dodatkowe podmioty w sektorze infrastruktury krytycznej zaopatrzenia w energię, surowce energetyczne i paliwa, znacznemu zwiększeniu ulegnie zaangażowanie pracowników analizujących raporty, co może doprowadzić do niewydolności oraz uniemożliwić właściwe monitorowanie zjawisk mogących stanowić zagrożenie dla infrastruktury krytycznej, a tym ograniczyć przydatność i zminimalizować rzeczywistą rolę raportów.

Zmiana w art. 6 ust. 3 polega na dookreśleniu, że Pełnomocnik OIK lub jego zastępca sporządza dla zarządu spółki oraz rady nadzorczej raport doraźny, raport okresowy, raport półroczny i raport roczny o stanie ochrony infrastruktury krytycznej. W ocenie ministerstwa propozycja RCB dotycząca ograniczenia raportowania wyłącznie do raportu rocznego może doprowadzić do sytuacji, w której zarząd spółki będzie miał ograniczone narzędzia kontroli działań realizowanych na rzecz zapewnienia bezpieczeństwa i ochrony infrastruktury krytycznej. Proponuje się przeformatowanie sposobu i cyklu raportowania wprowadzając raport doraźny – sporządzany w przypadku zidentyfikowania zagrożenia lub wystąpienia sytuacji stwarzającej zagrożenie dla funkcjonowania, ciągłości działania oraz integralności infrastruktury krytycznej, raporty okresowe – sporządzane co kwartał lub na żądanie zarządu spółki, a także raport roczny i półroczny. W myśl proponowanego art. 6 ust. 3a raporty roczne i półroczne zostałyby rozszerzone w stosunku do raportów kwartalnych o rejestr stwierdzonych incydentów wraz z informacją o przeprowadzonych działaniach korygujących, informacje dotyczące przeprowadzonych kontroli i audytów dotyczących ochrony infrastruktury krytycznej oraz o informacje dotyczące posiadanych certyfikatów systemów i rozwiązań dotyczących ochrony infrastruktury krytycznej. Zmiana w art. 6 ust. 4 polega na wskazaniu, że ministrowi właściwemu do spraw aktywów państwowych, Dyrektorowi Rządowego Centrum Bezpieczeństwa oraz odpowiednio ministrowi właściwemu do spraw energii lub ministrowi właściwemu do spraw gospodarki surowcami energetycznymi przekazywane byłyby wyłącznie raporty doraźne oraz raporty

roczne i półroczne, co ograniczyłoby ilość wpływających raportów oraz zwiększyłoby ich wartość merytoryczną.

Zmiana zawarta w art. 4 ust. 2 polega na technicznym doprecyzowaniu, że minister właściwy do spraw aktywów państwowych, po otrzymaniu stosownej informacji od Dyrektora Rządowego Centrum Bezpieczeństwa lub po otrzymaniu wyciągu z wykazu, powiadania spółkę o ujęciu składników jej mienia, o których mowa w art. 1 ust. 1 i 2, w jednolitym wykazie. W świetle obecnie obowiązujących przepisów minister właściwy do spraw aktywów państwowych ma obowiązek powiadomić spółkę o ujęciu składników jej mienia w wykazie dopiero po otrzymaniu od Dyrektora RCB wyciągu z wykazu, co wydłuża proces o konieczność aktualizacji przez RCB wykazu, sporządzenia z niego wyciągu i przekazania go ministrowi właściwemu do spraw aktywów państwowych.

Zmiany zaproponowane w art. 5 ust. 1a, art. 6 ust. 1 i 2 oraz w art. 6 ust. 5 i 6 stanowią konsekwencję zmiany zaproponowanej w art. 5 ust. 1 dotyczącej usankcjonowania powoływania zastępcy Pełnomocnika OIN i w swoim meritum sprowadzają się do wskazania, że zastępca Pełnomocnika OIN miałby takie same obowiązki i prawa wynikające z realizacji ustawy jak Pełnomocnik OIN. Planowany do dodania w art. 5 ust. 6 ma na celu dookreślenie zadań zastępcy Pełnomocnika OIN.

Zmiana w art. 6 ust 8 stanowi delegację ustawową zobowiązującą do określenia w drodze rozporządzenia szczegółowego trybu powoływania i odwoływania pełnomocnika do spraw ochrony infrastruktury krytycznej oraz jego zastępcy. W rozporządzeniu konieczne będzie dookreślenie podległości służbowej zastępcy Pełnomocnika oraz jego zadań.

Pozostałe zmiany mają charakter redakcyjny i techniczny, polegają na aktualizacji publikatorów oraz dostosowaniu nowelizacji ustawy *o szczególnych uprawnieniach* do nowelizowanej ustawy *o zarządzaniu kryzysowym*;

- ✓ ustawa z dnia 14 grudnia 2012 r. o odpadach (Dz. U. z 2023 r. poz. 1587, z późn. zm.) – zmiana wynikowa – zmiana definicji infrastruktury krytycznej oraz systematyki ustawy o zarządzaniu kryzysowym;
- ✓ ustawa z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej (Dz. U. z 2026 r. poz. 244) – zmiana wynikowa – zmiana definicji infrastruktury krytycznej oraz systematyki ustawy o zarządzaniu kryzysowym.

W proponowanych zmianach proponuje się ponadto dodanie do ustawy o środkach przymusu bezpośredniego i broni palnej w definicji wykorzystania środka przymusu bezpośredniego również bezzałogowego obiektu pływającego oraz bezzałogowego obiektu lądowego. Ponadto proponuje się dodanie przepisów, które umożliwią niszczenie, unieruchamiania i przejmowania kontroli nad tymi bezzałogowymi obiektami.

Konsekwentnie proponuje się stosowne rozszerzenie katalogu działań i środków umożliwiających zastosowania środków przymusu bezpośredniego do takich obiektów, a w przypadku bezzałogowych obiektów lądowych również wykorzystania broni palnej.

Ponadto dodaje się propozycję uzupełnienia dotychczasowych zmian w zakresie ustawy *o środkach przymusu bezpośredniego i broni palnej* związaną z potrzebą stworzenia odpowiednich uwarunkowań do realizacji zadań w obszarze zapewnienia bezpieczeństwa infrastruktury krytycznej poprzez umożliwienie używania pocisków niepenetracyjnych zawierających środki obezwładniające lub barwiące i wystrzeliwane z broni pneumatycznej. Wykorzystanie tego rodzaju środków przymusu bezpośredniego ma charakter odstraszający, a nie inwazyjny, a także ułatwia proces identyfikacji osób biorących udział w nielegalnych działaniach wymierzonych w szczególności w bezpieczeństwo obiektów i urządzeń infrastruktury krytycznej.

Konsekwencją zmian do ustawy o środkach przymusu bezpośredniego i broni palnej oraz zmiany w ustawach pragmatycznych poszczególnych służb (*vide* ustawa o Policji, Straży Granicznej, Służbie Ochrony Państwa, Żandarmerii Wojskowej;

- ✓ ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (Dz. U. z 2025 r. poz. 194) – uchylenie w art. 2 pkt 3 oraz zmiany w art. 4 ust. 1 i 2 oraz w art. 16 ust. 1 pkt 4 mają na celu dostosowanie przepisów ustawy o działaniach antyterrorystycznych do wprowadzanego przedmiotową nowelizacją nowego aparatu pojęciowego, który opiera się w dużej mierze na definicjach zawartych w dyrektywie CER.

  Wskazać należy, że projekt ustawy o zmianie ustawy o zarządzaniu kryzysowym oraz niektórych innych ustaw redefiniuje pojęcie infrastruktury krytycznej jako infrastruktury służącej zapewnieniu funkcjonowania organów administracji publicznej, zapewnieniu funkcjonowania przedsiębiorców, zaspokajaniu potrzeb obywateli, w tym zapewniającej świadczenie wspomnianych usług kluczowych. Tym samym, po wprowadzeniu tak brzmiącej definicji infrastruktury krytycznej" brak jest uzasadnienia dla utrzymania

odrębnej definicji „infrastruktury administracji publicznej” i jej stosowanie w ustawie o działaniach antyterrorystycznych.

Ponadto w celu zwiększenia poziomu zabezpieczenia infrastruktury krytycznej zasadne jest również dokonanie zmian w samej ustawie o działaniach antyterrorystycznych, tj.:

W art. 4 ust. 3 poprzez rozszerzenie uprawnienia Szefa ABW do wydawania poleceń operatorom infrastruktury krytycznej w odniesieniu do ich systemów teleinformatycznych również w przypadku możliwości wystąpienia przestępstwa z art. 224a ustawy z dnia 6 czerwca 1997 r. – Kodeks karny (Dz. U. z 2025 r. poz. 383, z późn. zm.), tj. w przypadkach tzw. fałszywych alarmów o podłożeniu materiałów wybuchowych. Propozycja dodania przepisu ma na celu zwiększenie stopnia skuteczności filtrowania domen z tzw. „blacklisty”, a tym samym ograniczenie negatywnych skutków fałszywych alarmów o podłożeniu materiałów lub urządzeń wybuchowych.

W art. 12 ust. 1 poprzez usprawnienie wykonywanych przez Policję działań sprawdzających zabezpieczenia infrastruktury krytycznej w przypadku wprowadzenia stopni alarmowych. W związku z tym proponuje się ograniczenie obowiązku dokonywania przedmiotowych sprawdzeń tylko do obiektów wskazanych przez Komendanta Głównego Policji w uzgodnieniu z Szefem ABW. Obecnie obowiązek ten dotyczy wszystkich obiektów infrastruktury krytycznej i obowiązuje począwszy od wprowadzenia drugiego stopnia alarmowego, kiedy nie jest znany dokładny cel zamachu. W rezultacie sprawdzenia te w przypadku części obiektów nie znajdują uzasadnienia, a jedynie powodują istotne zaangażowanie sił i środków Policji, które w takich przypadkach powinny być przesunięte na wybrane (faktycznie zagrożone) obiekty infrastruktury krytycznej.

W art. 17 poprzez usprawnienie funkcjonowania sztabu koordynacyjnego Szefa ABW, który to sztab jest powoływany w przypadku wprowadzenia stopnia alarmowego. W pierwszej kolejności proponuje się wprowadzenie fakultatywności powoływania przez Szefa ABW sztabu koordynacyjnego w przypadku wprowadzenia pierwszego lub drugiego stopnia alarmowego. Mając na uwadze, że pierwszy stopień alarmowy ma charakter tylko ogólnego ostrzeżenia, z kolei drugi stopień alarmowy może zostać wprowadzony w przypadku zwiększonego zagrożenia, ale gdy konkretny cel ataku nie został zidentyfikowany, zasadność powołania sztabu koordynacyjnego w takich przypadkach powinna wynikać z bieżącej oceny, a nie każdorazowo stanowić ustawowy obowiązek Szefa ABW.

Po drugie proponuje się rozszerzenie katalogu zadań przedmiotowego sztabu poprzez dodanie zadania polegającego na dokonywaniu oceny zagrożenia obiektów infrastruktury krytycznej zlokalizowanych na obszarze objętym obowiązywaniem stopnia alarmowego lub stopnia alarmowego CRP oraz wydawaniu rekomendacji zmierzających do odpowiedniego zabezpieczenia tej infrastruktury.

Mając na uwadze, że zakres przedmiotowy proponowanych zmian dotyczy usprawnienia działań służb (sztabu koordynacyjnego) w przypadku wprowadzenia stopnia alarmowego przy jednoczesnym rozszerzeniu katalogu zadań tego gremium o dokonywanie oceny stopnia zagrożenia infrastruktury krytycznej, propozycje te wpisują się w zakres przedmiotowy projektu ustawy o zmianie ustawy o zarządzaniu kryzysowym oraz niektórych innych ustaw, gdyż mają na celu wzmocnienie ochrony infrastruktury krytycznej podczas obowiązywania stopnia alarmowego;

- ✓ ustawa z dnia 20 lipca 2017 r. – Prawo wodne (Dz. U. z 2025 r. poz. 960, z późn. zm.) – zmiana w art. 240 w ust. 3 w pkt 24 jest dostosowaniem planów wojewódzkich do terminologii nowej planistyki w ustawie o zarządzaniu kryzysowym;
- ✓ ustawa z dnia 8 grudnia 2017 r. o Służbie Ochrony Państwa (Dz. U. z 2025 r. poz. 34, z późn. zm.).

Propozycje w ustawie o Służbie Ochrony Państwa są konsekwencją zmian w ustawie o środkach przymusu bezpośredniego i broni palnej.

Ponadto, zgodnie z propozycją brzmienia art. 39 ustawy o SOP, Komendant SOP może w określonych przypadkach podjąć decyzję o dopuszczalności zastosowania urządzeń uniemożliwiających telekomunikację na określonym obszarze przez czas niezbędny do wykonywania czynności przez SOP, z uwzględnieniem konieczności minimalizacji skutków braku możliwości korzystania z usług telekomunikacyjnych.

Dodatkowo zmiana w art. 98 ustawy o SOP dotyczy kwestii precyzuje wypłaty należności w przypadku funkcjonariuszy SOP oddelegowanych do wykonywania zadań służbowych związanych z zarządzaniem kryzysowym, ochroną ludności lub obroną cywilną w urzędzie obsługującym ministra właściwego do spraw wewnętrznych albo w jednostce podległej lub nadzorowanej przez ministra właściwego do spraw wewnętrznych. Przepis jednoznacznie wskazuje, że należności wypłaca komórka organizacyjna SOP właściwa w sprawach finansowych. Zadania związane z zarządzaniem kryzysowym, ochroną ludności lub obroną cywilną to zadania realizowane na rzecz całego Państwa, we współpracy wielu służb.

Przyjęcie zasady, że koszty ponosi jednostka, która deleguje funkcjonariusza – w ocenie wnioskodawcy – wzmocni odpowiedzialność i zaangażowanie służb w realizację wspólnych celów. Za wprowadzeniem proponowanego rozwiązania przemawia również wspieranie racjonalnego gospodarowania zasobami kadrowymi i zachowanie spójności budżetowej;

- ✓ ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2026 r. poz. 20, z późn. zm.) – zmiany wynikowe – zmiana definicji infrastruktury krytycznej oraz systematyki ustawy o zarządzaniu kryzysowym;
- ✓ ustawa z dnia 17 grudnia 2020 r. o rezerwach strategicznych (Dz. U. z 2024 r. poz. 1598, z późn. zm.).

Projektowane rozwiązania są ukierunkowane na poprawę obowiązujących procedur, usprawnienie przepływu informacji pomiędzy poszczególnymi podmiotami uczestniczącymi w systemie rezerw strategicznych. Ponadto projektowane zmiany mają zapewnić zwiększenie efektywności i szybkości działania Agencji w sytuacjach kryzysowych, w szczególności w związku z włączeniem Agencji do systemu obrony cywilnej i ochrony ludności – przez dostosowanie przepisów ustawy do dynamicznie zmieniających się oczekiwań organów władzy wykonawczej zaangażowanych w procesy zarządzania kryzysowego oraz zapewniania porządku publicznego i bezpieczeństwa narodowego. Proponowane zmiany stworzą podstawy do rozwinięcia nowych kompetencji Agencji w obszarach: tworzenia i utrzymywania nowych rodzajów rezerw strategicznych oraz w zakresie uczestnictwa Agencji w procedurach związanych z międzynarodowymi mechanizmami przewidzianymi na wypadek sytuacji kryzysowych oraz zwiększenia elastyczności i sprawności w działaniach Agencji przez zmodyfikowanie instytucji zadań powierzonych w celu szybkiego i sprawnego reagowania w sytuacjach kryzysowych.

Projektowane zmiany idą w kilku kierunkach. Po pierwsze mają doprecyzować krąg podmiotów uczestniczących w opracowywaniu projektu RPRS w kolejnych jego edycjach. Po drugie, mają zwiększyć elastyczność działań RARS, kładąc nacisk na zwiększenie efektywności realizowanych zadań ustawowych w warunkach nie tyle krajowego, co z założenia międzynarodowego środowiska bezpieczeństwa. Po trzecie wreszcie, intencją projektowanych poprawek jest rewizja obowiązków informacyjnych RARS, które z przyczyn praktycznych nie mogą stanowić dla ich adresatów źródła informacji o długotrwałej przydatności. Wynika to bezpośrednio z faktu, że w większości obszarów

rezerw strategicznych występuje duża dynamika dotycząca zarówno stanów rezerw strategicznych, jak również pewna zmienność miejsc ich przechowywania.

Z jednej strony wiąże się to z szerokim udziałem przedsiębiorców w systemie rezerw strategicznych, co rodzi konieczność uwzględniania przeobrażeń rynku, zarówno okresowych, jak i wynikających z nieprzewidzianych aberracji w funkcjonowaniu gospodarki. Z drugiej strony przesądza o tym bardzo duża aktywność RARS, która w 2020 r. stała się agencją w sposób stały wspomagającą reagowanie kryzysowe w warunkach nakładania się na siebie i długotrwałego współistnienia różnych zagrożeń.

Niezależnie od powyższego, podstawą wielu sformułowanych propozycji przepisów były doświadczenia RARS z lat 2020–24 związane z zarządzaniem rezerwami strategicznymi, procesem ich udostępniania, transportu i dystrybucji.

Proponowana zmiana do art. 2 polega na dodaniu nowej definicji ustawowej wirtualnego środowiska informatycznego. Wprowadzenie definicji związane jest z wprowadzeniem w art. 4 rezerw strategicznych nowego rodzaju oraz usunięciem niektórych rodzajów.

Mając na uwadze ogromne znaczenie bezpieczeństwa i dostępności informacji oraz danych przechowywanych w systemach informatycznych dla bezpieczeństwa i obronności państwa, zasadnym jest tworzenie rezerw strategicznych w obszarze utrzymywania wirtualnego środowiska informatycznego, które mogłoby być wykorzystywane w sytuacjach kryzysowych związanych z niepożądanymi działaniami w cyberprzestrzeni państwa i jego instytucji.

Z katalogu rezerw strategicznych usunięto zwierzęta gospodarskie, gdyż utrzymywanie takich rezerw strategicznych wiąże się ze szczególną trudnością. Usunięto także rezerwy strategiczne w postaci mocy produkcyjnej i mocy usługowej. Nie wyklucza to wszakże zawarcia umów w sprawie utrzymywania takich zdolności, w szczególności na podstawie art. 18.

Zmiany w art. 5 polegają na doprecyzowaniu roli Agencji w obrocie cywilnoprawnym przy zawieraniu umów dotyczących rezerw strategicznych. Rezerwy strategiczne stanowią wyodrębniony majątek Skarbu Państwa. Agencja zaś posiada odrębną od Skarbu Państwa osobowość prawną. Dotychczasowe przepisy nie pozwalają na jednoznaczne przesądzenie, czy Agencja pełni rolę ustawowego zastępcy Skarbu Państwa przy nabywaniu asortymentu do rezerw strategicznych, czy też nabywa ów asortyment w imieniu własnym, a następnie utrzymuje je jako rezerwy strategiczne stanowiące majątek Skarbu Państwa. Zapewnienie

prawidłowej reprezentacji podmiotu realizującego zadania ustawowe w dziedzinie bezpieczeństwa państwa ma kluczowe znaczenie dla ich wykonania. Za zjawisko niepożądane należy uznać występowanie niejednoznaczności w tej kwestii.

Proponowana zmiana art. 8 ust. 2 polega na włączeniu do kręgu podmiotów ministra właściwego do spraw gospodarki surowcami energetycznymi w proces przygotowania RPRS.

Ze względu na dużą dynamikę dotyczącą zarówno stanów rezerw strategicznych, jak i zmienności miejsc ich przechowywania, nie wydaje się konieczne utrzymanie ustawowego obowiązku wskazywania przez podmiot uczestniczący w przygotowaniu RPRS planowanego przeznaczenia oraz miejsca przechowywania specjalistycznego asortymentu technicznego rezerw strategicznych. Ostatecznie zadanie jego utrzymania spoczywa na Agencji, która jest podmiotem najlepiej zorientowanym w zakresie własnych zdolności przechowania, zaś planowane przeznaczenie może być rozmaite. Zdecydowanie efektywniejsze byłoby przekazanie przez takie podmioty uzasadnienia zakupu takiego asortymentu. Z tego względu proponuje się zmianę w art. 8 ust. 4 pkt 3 oraz art. 9 ust. 1 pkt 2 ustawy.

Zaproponowana w art. 10 ust. 2 zmiana będzie skutkować zawężeniem dystrybucji programu do kluczowych podmiotów szczebla centralnego. Zasadnym jest, aby na poziom wojewódzki trafiały jedynie wyciągi przygotowane przez ministra właściwego do spraw wewnętrznych, zawierające węższy zakres informacji niż dla organów szczebla centralnego. Nie ma potrzeby tak szerokiej dystrybucji elementów opisowych RPRS, w tym dotyczących zagrożeń, czy szczegółowych założeń. RPRS jest dokumentem o charakterze niejawnym, a zatem znajomość jego treści powinna być ograniczona jedynie do niezbędnego kręgu podmiotów. Ponadto kwestie dotyczące potencjalnych zagrożeń są udostępniane szczeblowi wojewódzkiemu m.in. w formie Raportu o zagrożeniach bezpieczeństwa narodowego.

Zmiany w art. 11 wynikają z potrzeby precyzyjnego określenia, że zarówno przyznawane Agencji dotacje celowe, jak i dotacje podmiotowe, przewidują niezbędne do poniesienia przez Agencję koszty w terminie ich zapłaty, a nie w terminie udzielenia konkretnej dotacji.

W art. 11 ust. 2 pkt 1 lit. a postuluje się uwzględnienie nie tylko kosztów zakupu asortymentu w celu utworzenia rezerw strategicznych, ale także kosztów odtworzenia już utworzonych, lecz udostępnionych rezerw strategicznych. Pozwoli to na sprawną realizację

zadania związanego z utrzymywaniem rezerw strategicznych w przypadku, gdy asortyment nie będzie już dostępny jako rezerwa strategiczna z uwagi na jego udostępnienie. Rezerwy strategiczne ze swego założenia mają być gotowe do użycia, zaś brak zapewnienia środków na ich odtworzenie rodzi zagrożenie braku dostępności, a w konsekwencji braku przygotowania do neutralizacji zagrożeń uwzględnionych w RPRS.

Proponowane zmiany w art. 11 ust. 2 pkt 1 lit. b zakładają przeznaczenie dotacji celowych nie tylko na przechowywanie rezerw, lecz przede wszystkim na ich utrzymywanie, zgodnie z limitami określonymi w RPRS. Utrzymywanie jest pojęciem szerszym niż przechowywanie, gdyż obejmuje również koszty serwisowania i przeglądów, niezbędnych do poniesienia w przypadku niektórych z utrzymywanych rezerw strategicznych w celu zachowania ich w gotowości do użycia.

Proponowane zmiany w art. 12 ustawy mają na celu rozwianie ewentualnych rozbieżności interpretacyjnych dotyczących możliwości finansowania z rezerwy celowej kosztów zaistniałych w związku ze sprzedażą towarów, ich wyprodukowaniem i sprzedażą lub sprzedażą usług na rzecz Agencji utrzymywanych rezerw na podstawie umów, o których mowa w art. 17 i art. 18 ustawy o rezerwach strategicznych. Zasadnym jest także przewidzenie środków na odtworzenie udostępnionych rezerw objętych Programem. Ponadto proponowane zmiany uwzględniają także potencjalne koszty nie tylko tworzenia, ale i utrzymywania rezerw strategicznych, a także dadzą podstawę do finansowania zadań zleconych na podstawie projektowanego art. 32.

Zmiany postulowane w art. 13 ust. 2 mają na celu doprecyzowanie treści decyzji o utworzeniu rezerw strategicznych. Ze względu na przewidziane w ustawie o rezerwach strategicznych różne możliwości prawne utworzenia rezerw strategicznych za słuszne należy uznać wybranie konkretnego sposobu w decyzji organu ją wydającego. To właśnie ten organ ma najszerszą wiedzę na temat zaistniałej potrzeby i okoliczności faktycznych związanych z zaistnieniem potrzeby utworzenia rezerwy strategicznej. Ma to istotne znaczenie, gdyż niektóre tryby tworzenia rezerw strategicznych przewidują wyłączenie stosowania przepisów o zamówieniach publicznych. Organ wydający decyzję nie powinien zatem pozostawiać żadnych wątpliwości co do trybu, w jakim rezerwa strategiczna ma zostać utworzona.

Art. 13 ust. 4 zezwoli Agencji na utworzenie rezerwy strategicznej poprzez przyjęcie darowizny określonego asortymentu. W obowiązujących przepisach nie ma takiej

możliwości, co należy ocenić za nieuzasadnione ograniczenie sposobu utworzenia rezerw strategicznych. Przyjęcie darowizny jest przy tym rozwiązaniem korzystnym finansowo, gdyż jest to świadczenie na rzecz majątku publicznego pod tytułem darmym. Agencja jako jednostka sektora finansów publicznych obowiązana jest realizować zadania w sposób m.in. oszczędny i celowy.

Zmiana w art. 13 ust. 5 koncentruje się na uwzględnieniu nie tylko zakupu asortymentu rezerw strategicznych, ale także na usługach związanych z ich utrzymywaniem. Znaczna część asortymentu mogącego potencjalnie służyć jako rezerwy strategiczne to towary wielokrotnego użytku. Dla utrzymania ich w gotowości do użycia wymagane jest zapewnienie niezbędnych przeglądów, napraw, czy aktualizacji. Świadczenie tych usług związane jest z obowiązkiem zachowania podobnej poufności, jak w przypadku zakupu asortymentu do rezerw strategicznych, ze względu na potencjalne powzięcie informacji co do ich ilości, typu, stanu, czy miejsca przechowywania. Z tego względu udzielenie zamówienia na usługi związane z utrzymywaniem rezerw strategicznych powinno nastąpić w sposób podobny do udzielenia zamówienia na zakup asortymentu do rezerw strategicznych.

Dodanie art. 14 ust. 3 pozwala na zapełnienie luki ustawowej. W odniesieniu do rezerw strategicznych tworzonych na podstawie art. 14 ustawy, dotychczasowe przepisy nie przewidują żadnej procedury ich utworzenia. Ze względu na fakt, że są to zamówienia przedmiotowo dotyczące rezerw strategicznych, postuluje się odpowiednie stosowanie art. 13 ust. 2–6 ustawy.

Proponowana zmiana w art. 17 ust. 2 pkt 2 ma charakter czysto techniczny polegający na dostosowaniu stosowanej terminologii do instytucji najmu w art. 659 ustawy z dnia 23 kwietnia 1964 r. – Kodeks cywilny.

Propozycja nowego brzmienia art. 19 ust. 5 pkt 4 i pkt 5 ma charakter porządkowy, wskazując jednoznacznie trzy istniejące ścieżki udostępnienia rezerw strategicznych:

1) udostępnienie bez obowiązku zwrotu;

2) udostępnienie z obowiązkiem zwrotu;

3) udostępnienie z obowiązkiem zwrotu w zakresie niewykorzystanym oraz rozszerzenie innych warunków udostępnienia rezerw.

Projektowane art. 19 ust. 9 i 10 są wynikiem dotychczasowych doświadczeń Agencji nabytych m.in. w związku podejmowaniem czynności związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych. Na tym tle zaistniała potrzeba uregulowania prawa własności asortymentu rezerw (urządzeń, sprzętu wielorazowego użytku) udostępnionego bez obowiązku zwrotu. Jednocześnie w przypadku zastrzeżenia obowiązku zwrotu, mając na względzie charakter rezerw strategicznych i konieczność zapewnienia ich gotowości do dalszego użycia, wydaje się uzasadnione obciążenie podmiotu, któremu rezerwy zostały wydane, obowiązkiem utrzymywania go w należytym stanie. Taki podmiot ma największą wiedzę na temat okoliczności faktycznych związanych z korzystaniem z udostępnionej mu rezerwy strategicznej oraz jej stanu.

Projektowany art. 19 ust. 11 uzasadniony jest charakterem zamówień dotyczących usług transportowych i innych usług logistycznych związanych z wykonaniem decyzji o udostępnieniu rezerw strategicznych. Decyzje o udostępnieniu rezerw strategicznych podlegają natychmiastowemu wykonaniu przez Agencję. Wydawane są one każdorazowo w sytuacjach faktycznego zagrożenia bezpieczeństwa państwa. Zamówienia te, ze swej istoty i nadrzędnego celu, wymykają się spod procedur przewidzianych przepisami o zamówieniach publicznych. Z powyższych względów ich udzielanie winno korzystać ze zwolnienia odpowiadającego obowiązującemu przepisowi art. 13 ust. 6 ustawy.

Zmiana art. 20 ust. 2 pkt 6 ma charakter porządkujący. Obowiązek zwrotu udostępnionych rezerw strategicznych w części niewykorzystanej nie jest automatyczny. Powstaje jedynie, gdy przewiduje to decyzja ministra właściwego do spraw wewnętrznych o udostępnieniu danej rezerwy, co wynika ze specyfiki udostępnianych rezerw.

W przepisach art. 21–22 doprecyzowano zasady udostępniania specjalistycznego asortymentu technicznego rezerw strategicznych, mając na celu zapewnienie efektywności przy realizacji zadań publicznych.

Projektowany art. 23 ust. 5 uzupełnia dotychczasowe przepisy o obowiązek określenia w umowie warunków zwrotu specjalistycznego asortymentu medycznego rezerw strategicznych. W przypadku udostępnienia bezzwrotnego nie znajdzie on zastosowania.

Projektowany art. 23a stanowi pochodną wprowadzenia szczególnego rodzaju rezerw strategicznych, tj. wirtualnego środowiska informatycznego. Udostępnienie rezerw strategicznych tego rodzaju wykazuje się znaczącą odmiennością od pozostałych typów

rezerw strategicznych. Możliwe jest bowiem świadczenie usług związanych z wirtualnym środowiskiem informatycznym bez fizycznego udostępnienia sprzętu. Przepis ten ma na celu stworzenie mechanizmu udostępniania rezerw strategicznych w obszarze informatycznym, mając na względzie wyzwania współczesnego świata i konieczność realizacji zadań związanych z bezpieczeństwem państwa także w obszarze cyfrowym.

Udostępnienie rezerw strategicznych jest czynnością, która obejmuje m.in. szereg czynności techniczno-organizacyjnych podejmowanych przez różne podmioty. Interesariuszami procesu udostępnienia są przede wszystkim Agencja jako podmiot udostępniający, podmiot, na rzecz którego następuje udostępnienie oraz podmiot, na rzecz którego rezerwy strategiczne mają być wydane (mogą to być różne podmioty). Ze względu na wielość podmiotów sugeruje się, aby procedura udostępnienia rezerw strategicznych przyjęła formę przepisów prawa powszechnie obowiązującego. W obecnym stanie prawnym Agencja nie ma żadnych możliwości prawnych do skłonienia innych podmiotów do postępowania zgodnie z procedurą zatwierdzoną przez ministra właściwego do spraw wewnętrznych, co rodzi poważne ryzyko jej niestosowania. W obrocie prawnym nie powinny istnieć przepisy, które w zasadzie nie kreują wiążącej normy. Jednocześnie warto zauważyć, że ze względu na cel udostępnienia oraz nierzadko znaczną wartość rezerw strategicznych zasadne wydaje się ustalenie jednolitej procedury udostępnienia wiążącej wszystkich interesariuszy. Z tego względu za najwłaściwszy sposób uznano wprowadzenie w art. 24 delegacji ustawowej dla ministra właściwego do spraw wewnętrznych do wydania rozporządzenia w tej kwestii.

Proponowane brzmienie art. 29 doprecyzowuje tryb realizowania przez Agencję zadań zleconych przez inne podmioty poza systemem rezerw strategicznych. Zmiany dotyczą przede wszystkim doprecyzowania zasad przekazywania środków finansowych na realizację zadań zleconych.

Przepisy dodawanego art. 29a określają sposób realizacji nowych kompetencji Agencji związanych z uczestnictwem w mechanizmach pomocowych m.in. organizacji międzynarodowych, jak np. Unijny Mechanizm Ochrony Ludności. Od lat obserwuje się rozwój inicjatyw mających na celu zacieśnienie współpracy w obszarze niesienia pomocom obywatelom Unii Europejskiej w sytuacjach kryzysowych. Projektowane przepisy pozwolą Agencji brać udział w realizowaniu przedsięwzięć związanych z bezpieczeństwem państwa oraz udzielaniem pomocy humanitarnej także na szczeblu międzynarodowym. Ze względu

na istotność tych zadań, podejmowanie tych działań możliwe jest po uzyskaniu uprzedniej zgody ministra właściwego do spraw wewnętrznych jako organu nadzoru nad Agencją.

Zmiany wprowadzone w art. 31 ust. 1 są konsekwencją wprowadzenia nowych kompetencji Agencji i stanowią uzupełnienie dotychczasowego katalogu zadań Agencji. Biorąc pod uwagę dotychczasowe doświadczenia, ze względów celowościowych zmieniono także datę przekazywania informacji o ilości i rozmieszczeniu rezerw strategicznych ujętych w Programie.

W art. 31 ust. 2 doprecyzowano zakres wyłączenia przepisów ustawy o zasadach zarządzania mieniem państwowym. W celu efektywnego realizowania zadań w zakresie utrzymywania rezerw strategicznych i zarządzania nieruchomościami, wprowadza się wyłączenie przepisów art. 38–41 ustawy z dnia 16 grudnia 2016 r. o zasadach zarządzania mieniem państwowym. Rezerwy strategiczne ze swej istoty nie są tworzone jako zasoby majątkowe, które spowodują w przyszłości wpływ korzyści ekonomicznych. Ich likwidacja odbywa się w sposób określony w ustawie o rezerwach strategicznych. Przepisy te mają charakter szczególny wobec ustawy o zasadach zarządzania mieniem państwowym. Jednakże w przypadkach, w których Agencja nie wykorzystuje magazynów rezerw strategicznych do przechowywania w nich rezerw, powstaje możliwość wykorzystania ich na cele komercyjne (najem, dzierżawa). Konieczność uzyskania zgody właściwego organu na dokonanie takiej czynności bardzo ogranicza, a czasem uniemożliwia efektywne wykorzystywanie tych nieruchomości. Uzyskanie zgody wymaga zawsze określonego czasu, a kontrahent Agencji, który chce skorzystać z powierzchni magazynowych, oczekuje szybkiej decyzji i szybkiego zawarcia określonej umowy. Oczekiwanie na zgodę właściwego organu może skutkować utratą kontrahenta. Utrzymywanie powierzchni magazynowych, które nie są czasowo zajęte w celu przechowywania rezerw strategicznych, generuje znaczące koszty po stronie Agencji, które można zredukować przez oddanie określonych powierzchni magazynowych w najem lub w dzierżawę.

Licznie pojawiające się w ostatnim czasie na terenie Rzeczypospolitej sytuacje szczególnego zagrożenia bezpieczeństwa państwa ujawniły potrzebę zapewnienia pewnej elastyczności w reagowaniu na nie. Służyć temu ma znowelizowany art. 32 ustawy, zgodnie z którym możliwe jest powierzenie Agencji innych zadań, związanych jednakże z wystąpieniem określonych zagrożeń wymienionych w sposób enumeratywny. Agencja jest wyspecjalizowaną agencją wykonawczą utworzoną w celu wypełniania zadań ustawowych

w obszarze bezpieczeństwa państwa, a zatem jednostką posiadającą doświadczenie w realizacji przedsięwzięć tego rodzaju. Realizacja takich zadań może wiązać się z koniecznością udzielania zamówień. Z uwagi na szczególne okoliczności towarzyszące takim zamówieniom oraz konieczność zapewnienia niezawodnej realizacji zadań, uzasadnione jest wyłączenie tych zamówień z reżimu przepisów o zamówieniach publicznych. Jednocześnie zapewniono realizację obowiązku informacyjnego przez publikację w Biuletynie Zamówień Publicznych.

Zmiana w art. 36 ma umożliwić Agencji, w pierwszej kolejności, zatrudnianie pracowników na wolne stanowiska pracy w ramach naborów wewnętrznych z wyłączeniem przepisów ust. 1–4 tego artykułu. Zmiana ta będzie zapewniała efektywne zarządzanie zasobami ludzkimi.

Obecnie obowiązujące przepisy dotyczące ograniczeń w prowadzeniu działalności gospodarczej w sposób nadmierny naruszają konstytucyjne uprawnienia pracowników Agencji. Brak jest merytorycznego uzasadnienia podtrzymania w dotychczasowym brzmieniu art. 40 ustawy o rezerwach strategicznych, w tym tak szerokiego kręgu osób podlegających ograniczeniom w prowadzeniu działalności gospodarczej oraz zobowiązanych do składania oświadczeń o stanie majątkowym.

Projektowany art. 40a umożliwi Agencji efektywną realizację obowiązków wynikających 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). Należy pamiętać, że Agencja jako podmiot wykonujący zadania państwa przetwarza znaczne zasoby danych osobowych, zaś wprowadzenie projektowanego przepisu nie wpłynie na obniżenie standardu ich ochrony.

Dodanie w art. 41 ust. 2 pkt 10 jest związane z dodaniem nowych źródeł przychodów związanych z nowymi kompetencjami w zakresie realizowanych zadań o charakterze międzynarodowym oraz w zakresie tworzenia rezerw strategicznych na polecenie Ministra Zdrowia.

Zaproponowano nową treść art. 42 ust. 3 z uwagi na zagadnienia związane z planowaniem finansowym Agencji jako jednostki sektora finansów publicznych. Plan rzeczowy rezerw strategicznych stanowi część planu finansowego Agencji i zawiera stany na początek roku

budżetowego, a zatem powinien być sporządzony na podstawie faktycznych stanów początkowych.

Zmiana proponowana w art. 44 ust. 1 ma umożliwić Agencji umorzenie lub rozłożenie na raty wszystkich należności i wierzytelności mających charakter cywilnoprawny przysługujących Agencji. W obecnym stanie prawnym możliwe jest to tylko w odniesieniu do wybranych należności i wierzytelności.

Proponowany art. 46a ma uchylić wątpliwości prawne co do możliwości zawarcia przez Agencję ugody w sprawie spornej należności cywilnoprawnej. Pomimo szczegółowego uregulowania kwestii umarzania należności w ustawie o rezerwach, brak jest przepisów dotyczących zawarcia ugody. Mając na względzie postulaty Prokuratorii Generalnej Rzeczypospolitej Polskiej w zakresie ugodowego rozwiązywania sporów przez jednostki sektora finansów publicznych, zaproponowano wprowadzenie wyraźnego odwołania do art. 54a ustawy o finansach publicznych;

- ✓ ustawa z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa – uzupełnienie wpływów do Funduszu Cyberbezpieczeństwa o wpływy z kar pieniężnych, o których mowa w art. 6zzo ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym;
- ✓ ustawa z dnia 12 lipca 2024 r. – Prawo komunikacji elektronicznej (Dz. U. z 2024 r. poz. 1221 z późn. zm.).

Zmiany obejmują uchylenie art. 42, co ma związek ze zmianami wprowadzonymi w projektowanych przepisach ustawy o Policji, Straży Granicznej, Służbie Ochrony Państwa oraz ustawy o zarządzaniu kryzysowym dotyczącymi możliwości zastosowania urządzeń uniemożliwiających telekomunikację na określonym obszarze, przez czas niezbędny do wyeliminowania zagrożenia lub jego skutków, z uwzględnieniem konieczności minimalizacji skutków braku możliwości korzystania z usług telekomunikacyjnych.

Dodatkowo – propozycja zawarta w projektowanym art. 67a wskazuje, iż Prezes UKE, w uzgodnieniu z ministrem właściwym do spraw wewnętrznych, zapewnia odpowiednie częstotliwości do realizacji zadań z zakresu komunikacji głosowej i transmisji danych do zapewnienia bezpiecznej radiowej łączności mobilnej w celu: zapewnienia ciągłości i bezpieczeństwa funkcjonowania administracji państwowej oraz ochrony ludności i obrony cywilnej. Do rezerwacji częstotliwości nie stosuje się przepisów dotyczących postępowania selekcyjnego obejmującego konkurs, przetarg lub akcję. Proponowane

rozwiązanie zagwarantuje Ministrowi Spraw Wewnętrznych i Administracji realizację zadań własnych jako operatora, o którym mowa w art. 74 ust. 2 ustawy z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej oraz w służbach i jednostkach podległych Ministrowi Spraw Wewnętrznych i Administracji lub przez niego nadzorowanych przy realizacji zadań związanych z ochroną ludności i obrony cywilnej.

- ✓ ustawa z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej (Dz. U. poz. 1907, z późn. zm.) – propozycje zmian mają skorelować projektowane rozwiązania w zakresie planistyki zarządzania kryzysowego oraz planistyki dotyczącej ochrony ludności i obrony cywilnej. Regulacja ma zapewnić również udział Szefa Sztabu Generalnego Wojska Polskiego w opracowaniu krajowego planu ewakuacji ludności.

  W celu zapewnienia niezakłóconego funkcjonowania SŁBP – projektowany przepis art. 79a przewiduje, że zlecenie zadań związanych z organizacją budową, utrzymaniem i modernizacją SBŁP określonej kategorii przedsiębiorcom może nastąpić w drodze decyzji administracyjnej, wydawanej przez ministra właściwego do spraw wewnętrznych. Wykonywanie tych zadań, w zakresie określonym następuje na podstawie umowy zawartej pomiędzy przedsiębiorcę oraz ministrem właściwym do spraw wewnętrznych, w której określa się w szczególności zakres zadań, warunki finansowania i sposób współpracy. Dodanie art. 79a umożliwi skuteczną realizację ustawowych zadań przez Ministra Spraw Wewnętrznych i Administracji będącego operatorem SBŁP przy organizowaniu systemu, którego celem jest zapewnienie ciągłości i bezpieczeństwa funkcjonowania administracji państwowej oraz ochrony ludności i obrony cywilnej.

  Propozycja dodania ust. 2 w art. 206 – projektowany przepis zmierza do zapewnienia ochrony interesów prawnych podmiotów, które przed dniem wejścia w życie ustawy o ochronie ludności i obronie cywilnej złożyły wniosek o wydanie decyzji o środowiskowych uwarunkowaniach dla zamierzenia budowlanego. Decyzja o środowiskowych uwarunkowaniach stanowi jeden z kluczowych etapów procedury inwestycyjnej. Sam fakt dotarcia przez inwestora do tego stadium wskazuje, że proces inwestycyjny znajduje się już na bardzo zaawansowanym etapie przygotowania, wiąże się z poniesieniem istotnych nakładów finansowych, przygotowaniem dokumentacji i przeprowadzeniem licznych analiz środowiskowych. Objęcie przedmiotowych spraw nową regulacją, która weszła w życie po zainicjowaniu procedury, prowadziłoby do poważnych komplikacji prawnych, ryzyka wydłużenia procesu, powtarzania czynności administracyjnych i wzrostu kosztów.

Na gruncie proponowanego przepisu inwestorzy, którzy zainicjowali procedurę przed dniem wejścia w życie ww. ustawy, zachowują możliwość zakończenia postępowania na dotychczasowych zasadach, z kolei organy administracji publicznej unikną konieczności powtarzania czynności i prowadzenia postępowań według zmienionych reguł.

Przedmiotowa zmiana pozytywnie wpłynie na stabilność i przewidywalność prawa, zwiększając zaufanie stron procesu inwestycyjnego do stanowionych regulacji. Pozwoli na uniknięcie poczucia niepewności prawnej i poczucia niesprawiedliwości u inwestorów, którzy podjęli działania w dobrej wierze na gruncie obowiązujących dotąd przepisów.

Planowane inwestycje mają możliwość zostać wykonane zgodnie z przedstawionym harmonogramem i spełnić oczekiwania społeczeństwa, co w przypadku inwestycji komunikacyjnych (metro) jest niezwykle istotne.

Projektowana zmiana nie generuje dodatkowych obciążeń finansowych dla budżetu państwa ani jednostek samorządu terytorialnego. Wręcz przeciwnie, wyłączenie konieczności ponownego prowadzenia postępowań oznacza racjonalizację kosztów funkcjonowania administracji publicznej.

Przepisy przejściowe i końcowe (art. 24–67 ustawy nowelizującej)

Krajowa Ocena Ryzyka zostanie sporządzona po raz pierwszy w terminie 6 miesięcy od dnia wejścia w życie ustawy nowelizującej.

Strategia Odporności Podmiotów Krytycznych zostanie sporządzona po raz pierwszy w terminie 6 miesięcy od dnia wejścia w życie ustawy nowelizującej.

Krajowy Plan Zarządzania Ryzykiem Rada Ministrów przyjmie po raz pierwszy w terminie 12 miesięcy od dnia wejścia w życie ustawy nowelizującej.

Plany zarządzania ryzykiem:

- ✓ ministra kierującego działem administracji rządowej,
- ✓ Szefa Agencji Bezpieczeństwa Wewnętrznego, Szefa Agencji Wywiadu oraz Szefa Centralnego Biura Antykorupcyjnego,
- ✓ kierownika urzędu centralnego wskazanego przez ministra kierującego działem administracji rządowej, któremu podlega lub jest przez tego ministra nadzorowany plan zarządzania ryzykiem kierownika urzędu centralnego,

- ✓ wojewody

– zostaną zatwierdzone po raz pierwszy w terminie 3 miesięcy od dnia przyjęcia Krajowego Planu Zarządzania Ryzykiem.

Plan zarządzania ryzykiem starosty jest zatwierdzany po raz pierwszy w terminie 3 miesięcy od dnia przyjęcia planu zarządzania ryzykiem właściwego wojewody.

Plan zarządzania ryzykiem wójta (burmistrza, prezydenta miasta) jest zatwierdzany po raz pierwszy w terminie 3 miesięcy od dnia przyjęcia planu zarządzania ryzykiem właściwego starosty.

W przypadku Krajowego Planu Reagowania Kryzysowego – Rada Ministrów przyjmuje po raz pierwszy ten plan w terminie 9 miesięcy od dnia przyjęcia Krajowego Planu Zarządzania Ryzykiem.

Plany reagowania kryzysowego:

- ✓ ministra kierującego działem administracji rządowej,
- ✓ Szefa Agencji Bezpieczeństwa Wewnętrznego, Szefa Agencji Wywiadu oraz Szefa Centralnego Biura Antykorupcyjnego,
- ✓ kierownika urzędu centralnego wskazanego przez ministra kierującego działem administracji rządowej, któremu podlega lub jest przez tego ministra nadzorowany plan zarządzania ryzykiem kierownika urzędu centralnego,
- ✓ wojewody

– zostaną zatwierdzone po raz pierwszy w terminie 3 miesięcy od dnia przyjęcia Krajowego Planu Reagowania Kryzysowego.

Plan reagowania kryzysowego starosty jest zatwierdzany po raz pierwszy w terminie 3 miesięcy od dnia przyjęcia planu reagowania kryzysowego właściwego wojewody.

Plan reagowania kryzysowego wójta (burmistrza, prezydenta miasta) jest zatwierdzany po raz pierwszy w terminie 3 miesięcy od dnia przyjęcia planu reagowania kryzysowego właściwego starosty.

Dotychczasowe plany zarządzania kryzysowego zatwierdzone na podstawie dotychczasowych przepisów pozostają w mocy do czasu nowych planów i mogą być w tym czasie aktualizowane.

Szczegółowe kryteria pozwalające wyodrębnić obiekty, instalacje, urządzenia i usługi, w brzmieniu dotychczasowym, pozostają w mocy do czasu sporządzenia nowych kryteriów. Kryteria identyfikacji infrastruktury krytycznej w brzmieniu nadanym projektowaną ustawą zostaną sporządzone po raz pierwszy w terminie 3 miesięcy od dnia wejścia w życie ustawy nowelizującej.

Jednolity wykaz obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej w brzmieniu dotychczasowym, pozostaje w mocy do czasu sporządzenia nowego wykazu i może być w tym czasie aktualizowany.

Właściciele, posiadacze samoistni i zależni obiektów instalacji, urządzeń i usług ujętych w jednolitym wykazie infrastruktury krytycznej w brzmieniu dotychczasowym, realizują zadania w zakresie ochrony infrastruktury krytycznej na podstawie dotychczasowych przepisów do czasu ujęcia w „nowym" wykazie infrastruktury krytycznej.

Organy do spraw podmiotów krytycznych, o których mowa w art. 6zk ust. 1 ustawy zmienianej w art. 1, w brzmieniu nadanym niniejszą ustawą, po raz pierwszy identyfikują podmioty krytyczne i wpisują je do wykazu podmiotów krytycznych w terminie 9 miesięcy od dnia wejścia w życie ustawy nowelizującej.

Pojedynczy Punkt Kontaktowy po raz pierwszy opracowuje i przekazuje Komisji Europejskiej oraz Grupie do spraw Odporności Podmiotów Krytycznych sprawozdanie dotyczące incydentów istotnych zgłaszanych przez podmioty krytyczne mających wpływ na ciągłość świadczonych przez nich usług kluczowych na terytorium Rzeczypospolitej Polskiej oraz ciągłość świadczonych usług kluczowych w państwach członkowskich Unii Europejskiej w terminie do dnia 17 lipca 2028 r.

Pojedynczy Punkt Kontaktowy po raz pierwszy przekazuje Komisji Europejskiej informacje o przepisach dotyczących kar pieniężnych nie później niż w ciągu 7 dni od dnia wejścia w życie ustawy.

Komendant Główny Straży Granicznej w terminie 7 dni od dnia wejścia w życie przepisów dotyczących Centrum Bezpieczeństwa Morskiego (wchodzą w życie po 6 miesiącach od dnia ogłoszenia projektu ustawy) wyznacza spośród oficerów Straży Granicznej Pełnomocnika Komendanta Głównego Straży Granicznej do spraw utworzenia Centrum Bezpieczeństwa Morskiego w celu podjęcia czynności przygotowawczych i organizacyjnych niezbędnych do rozpoczęcia funkcjonowania Centrum Bezpieczeństwa Morskiego, w szczególności wskazania lokalizacji i pomieszczeń, wyposażenia w niezbędny sprzęt, zapewnienia funkcjonalności i

komplementarności odpowiednich systemów teleinformatycznych i stanowisk pracy oraz wspierania procesu oddelegowania przedstawicieli innych podmiotów do Straży Granicznej do wykonywania zadań CBM. Pełnomocnik zakończy swoją działalność z dniem utworzenia Centrum Bezpieczeństwa Morskiego.

Załącznik do ustawy określa sektory, a w ich obrębie, podsektory. Wskazane w załączniku obszary, bazują na wskazanych w dyrektywie 2022/2557, jak również zostały w części skorelowane z sektorami, które muszą zostać zaimplementowane z dyrektywy 2022/2555.

Projektowana ustawa wejdzie w życie po upływie 14 dni od dnia jej ogłoszenia, z wyjątkiem przepisów dotyczących Centrum Bezpieczeństwa Morskiego, które wejdą w życie po upływie 6 miesięcy od dnia ogłoszenia projektowanej ustawy.

Pozostałe informacje

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, z późn. zm.) i w związku z tym nie podlega procedurze notyfikacji.

Projekt ustawy jest zgodny z przepisami prawa Unii Europejskiej i służy ich stosowaniu.

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.

Projekt ustawy stosownie do wymogów art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2025 r. poz. 677, z późn. zm.) 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 poz. 806, z późn. zm.) został zamieszczony w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji, w serwisie Rządowy Proces Legislacyjny oraz w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Bezpieczeństwa.

Nazwa projektu Ustawa o zmianie ustawy o zarządzaniu kryzysowym oraz niektórych innych ustaw **Ministerstwo wiodące i ministerstwa współpracujące** Rządowe Centrum Bezpieczeństwa **Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu** Pan Zbigniew Muszyński, Dyrektor Rządowego Centrum Bezpieczeństwa **Kontakt do opiekuna merytorycznego projektu** (pkt I rozwiązań zawartych w projekcie) Pan Karol Stec, Szef Wydziału Oceny Ryzyka i Planowania tel. kom 532-451-765, e-mail: karol.stec@rcb.gov.pl (pkt II rozwiązań zawartych w projekcie) Pan Witold Skomra, Doradca w Rządowym Centrum Bezpieczeństwa tel. kom. 785-700-176, e-mail: witold.skomra@rcb.gov.pl	**Data sporządzenia** 26.02.2026 r. **Źródło:** Upoważnienie Prezesa Rady Ministrów Decyzja Parlamentu Europejskiego i Rady nr 1313/2013/EU z dnia 17 grudnia 2013 r. w sprawie Unijnego Mechanizmu Ochrony Ludności (Dz. Urz. UE L 347 z 20.12.2013, str. 924, z późn. zm.) Dyrektywa 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 333 z 27.12.2022, str. 164) **Nr w Wykazie prac legislacyjnych i programowych Rady Ministrów:** UC47

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

I. Wdrożenie rozwiązań zapewniających podstawy zarządzania ryzykiem, z uwzględnieniem postanowień Decyzji Parlamentu Europejskiego i Rady nr 1313/2013/EU z dnia 17 grudnia 2013 r. w sprawie Unijnego Mechanizmu Ochrony Ludności (Dz. Urz. UE L 347 z 20.12.2013, str. 924, L 250 z 04.10.2018, str. 1 oraz L 77A z 20.03.2019, str. 1), zwanej dalej „UMOL".

Posiadanie planów zarządzania ryzykiem jest o tyle istotne, iż są one niezbędne do spełnienia tzw. warunkowości ex ante w perspektywie finansowej UE na lata 2021-2027, co ma przełożenie na możliwość pozyskiwania środków finansowych w ramach polityki spójności z Europejskiego Funduszu Rozwoju Regionalnego, Funduszu Spójności oraz Europejskiego Funduszu Morskiego i Rybackiego.

Opracowanie dokumentów planistycznych w obszarze zarządzania ryzykiem jest bowiem bezpośrednio powiązane z jednym z warunków podstawowych perspektywy finansowej, który mówi o „osiągnięciu skutecznych ram zarządzania ryzykiem". Wskazuje się wprost na konieczność opracowania planu zarządzania ryzykiem na szczeblu krajowym lub regionalnym, powiązanego ze strategiami adaptacji do zmian klimatu. Ponadto państwa członkowskie opracowują oceny ryzyka na szczeblu krajowym lub niższym oraz udostępniają Komisji Europejskiej tzw. Streszczenie istotnych elementów tych ocen.

Obowiązujące obecnie w tym obszarze regulacje ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym nie pozwalają w pełni odzwierciedlać w planach zarządzania kryzysowego kwestii dotyczących zarządzania ryzykiem. Istnieje zatem konieczność opracowywania planów zarządzania ryzykiem, na szczeblu krajowym lub odpowiednio niższym, wskazanie podmiotów odpowiedzialnych za ich opracowanie, zakresu merytorycznego takiego planu oraz określenie cyklu planowania.

Konieczna jest tym samym modyfikacja dotychczasowych rozwiązań w kierunku zapewnienia podstaw prawnych i organizacyjnych dotyczących kwestii zarządzania ryzykiem, co znajdzie odzwierciedlenie w projekcie w rozwiązaniach dotyczących dokumentów strategicznych w zakresie oceny ryzyka oraz treści planów zarządzania kryzysowego. Nowe regulacje pozwolą również na efektywne przekazywanie dokumentów o charakterze sprawozdawczym Komisji Europejskiej, m.in. „Streszczenia istotnych elementów krajowej oceny ryzyka" oraz „Streszczenia istotnych elementów krajowej oceny zdolności zarządzania ryzykiem".

II. Wdrożenie 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 333 z 27.12.2022 r. str. 164), zwaną dalej „dyrektywą 2022/2557".
Zapewnienie ciągłości świadczenia usług kluczowych realizowanych w sektorach lub podsektorach wskazanych w dyrektywie 2022/2557.
Identyfikacja usług kluczowych świadczonych przez operatorów infrastruktury krytycznej z uwzględnieniem potencjalnych skutków zakłócenia zarówno w odniesieniu do funkcjonowania państwa jak i społeczeństwa. Minimalizacja skutków zakłócenia poprzez wprowadzenie procesów oceny i zarządzania ryzykiem. Uwzględnienie zadań związanych z

ochroną usług kluczowych i infrastruktury krytycznej o szczególnym znaczeniu europejskim. Modyfikacja obecnych rozwiązań dotyczących infrastruktury krytycznej jako niezbędnych elementów świadczenia usług kluczowych.

III. Redefinicja regulacji dotyczących infrastruktury krytycznej, która jest m.in. niezbędna do świadczenia usług kluczowych przez podmioty krytyczne.

IV. Wdrożenie rozwiązań prawnych umożliwiających wzmocnienie ochrony najważniejszych dla państwa obszarów, obiektów i urządzeń, w szczególności infrastruktury morskiej. Mając na uwadze istniejący wysoki poziom zagrożenia szeroko rozumianymi atakami hybrydowymi ze strony Federacji Rosyjskiej oraz Białorusi, poważnym wyzwaniem dla bezpieczeństwa Polski staje się ochrona infrastruktury morskiej. Instalacje energetyczne, rurociągi i porty morskie wyspecjalizowane do przeładunku paliw płynnych są kluczowymi instrumentami dla zapewnienia nieprzerwanych dostaw ropy i gazu do Polski. Co więcej, w najbliższych latach realizowane będą nowe strategiczne inwestycje, mające na celu zwiększenie bezpieczeństwa energetycznego Polski, takie jak elektrownia jądrowa oraz morskie farmy wiatrowe. Planowana jest również rozbudowa terminalu regazyfikacyjnego skroplonego gazu ziemnego w Świnoujściu, portów morskich w Gdańsku, Gdyni i Szczecinie-Świnoujściu, a także budowa pływającego terminalu LNG (FSRU) w Zatoce Gdańskiej, które dzięki tym inwestycjom zwiększą przepustowość i zdolności logistyczne Polski dla transportu morskiego. W tym kontekście niezbędnym jest podjęcie działań mających na celu zwiększenie poziomu ochrony infrastruktury morskiej. Będzie to możliwe poprzez, po pierwsze, zapewnienie stałego monitoringu i bieżącej oceny sytuacji dla tej infrastruktury, po drugie, usprawnianie reakcji służb na potencjalne zdarzenia, w tym również specjalistycznych uzbrojonych formacji ochronnych (SUFO) odpowiedzialnych za bezpośrednią ochronę fizyczną tej infrastruktury, po trzecie, zapewnienie efektywnego zarządzania kryzysowego z użyciem nowoczesnej technologii informacyjnej.”.

2. Rekomendowane rozwiązanie, w tym planowane narzędzia interwencji, i oczekiwany efekt

I. W zakresie kwestii zarządzania ryzykiem, z uwzględnieniem postanowień UMOL przewiduje się wdrożenie zintegrowanego podejścia do zarządzania ryzykiem, obejmującego cały cykl zarządzania, od oceny ryzyka przez przygotowanie planów zarządzania nim oraz wdrażanie środków zapobiegawczych i zapewniających gotowość do ich użycia.
Przewiduje się opracowanie na szczeblu centralnym dokumentu rządowego, tzw. Krajowej Oceny Ryzyka, który zastąpi obecnie funkcjonujący Raport o zagrożeniach bezpieczeństwa narodowego. Dotychczasowe doświadczenia wykazują, że Raport o zagrożeniach bezpieczeństwa narodowego jest dokumentem nadmiernie obszernym, mającym charakter quasi cyklicznej oceny zidentyfikowanych zagrożeń, a jednocześnie nie przekładającym się na procesy planistyczne dotyczące zarządzania ryzykiem.

Krajowa Ocena Ryzyka będzie funkcjonalnym dokumentem zawierającym zidentyfikowane zagrożenia o różnym charakterze (naturalne, techniczne, związane z konfliktem zbrojnym w tym hybrydowe, o charakterze terrorystycznym, z obszaru cyberbezpieczeństwa, itp.) oraz ocenę ryzyk wynikających z tych zagrożeń, pozwalającą określić cele strategiczne i priorytety na rzecz ich ograniczania. Istotne jest bowiem zrozumienie, że dopiero prawidłowo przeprowadzona ocena ryzyka identyfikuje zagrożenia i obszary, w których konieczne jest podjęcie działań, w tym zwiększenie nakładów finansowych na realizację przedsięwzięć ograniczających.

Krajowa Ocena Ryzyka – w obszarze planowania cywilnego – wykorzystywana będzie wykorzystywana na potrzeby opracowywania planów zarządzania ryzykiem (działania w zakresie zapobiegania sytuacji kryzysowej oraz przygotowywania do jej wystąpienia) oraz planów reagowania kryzysowego (działania w zakresie reagowania w przypadku wystąpienia sytuacji kryzysowej oraz usuwaniu jej skutków) ministrów, kierowników urzędów centralnych, wojewodów, jak również planów zarządzania kryzysowego na szczeblu powiatowym oraz gminnym.

Planistyka na szczeblu krajowym (tj. opracowanie Krajowego Planu Zarządzania Ryzykiem oraz Krajowego Planu Reagowania Kryzysowego) będzie należała do obowiązków Dyrektora RCB.

Konieczne będzie dostosowanie terminologii do regulacji unijnych, co stworzy efektywne narzędzia do prowadzenia oceny ryzyka i zarządzania nim. Jednocześnie zostaną ujednolicone terminy cyklów planistycznych krajowych z unijnymi, gdyż obowiązujące przepisy krajowe przewidują cykl 2-letni, podczas gdy unijne regulacje wskazują na 3-letnie cykle planistyczne. Nowy cykl planistyczny będzie obejmował 3 lata.

Dodatkowo przewiduje się, że Krajowa Ocena Ryzyka oraz Krajowy Plan Zarządzania Ryzykiem będą punktami odniesienia do opracowania dokumentów udostępnianych Komisji Europejskiej w ramach realizacji postanowień UMOL, tj. odpowiednio:
1) streszczenia istotnych elementów krajowej oceny ryzyka;
2) streszczenia istotnych elementów krajowej oceny zdolności zarządzania ryzykiem.

II. Wdrożenie 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 333 z 27.12.2022, str. 164), zwaną dalej „dyrektywą 2022/2557”, obejmuje poniżej wskazane kwestie.

Usługi kluczowe

Rada Ministrów określi w drodze rozporządzenia wykaz usług kluczowych w poszczególnych sektorach lub podsektorach, wskazując jednocześnie kategorie podmiotów mogących świadczyć usługi oraz tzw. „progi istotności" skutku zakłócającego daną usługę.

Usługi kluczowe, co do zasady, będą realizowane przez operatorów infrastruktury krytycznej, za pomocą posiadanej przez nich infrastruktury. Niemniej jednak, aby operator infrastruktury krytycznej uzyskał status podmiotu krytycznego, konieczne jest przeprowadzenie jego identyfikacji w oparciu o ww. rozporządzenie Rady Ministrów.

Strategia Odporności Podmiotów Krytycznych

W celu jak najlepszego doboru działań zmierzających do identyfikacji podmiotów krytycznych, zbudowania ich odporności i zapewnienia niezakłóconego świadczenia usług kluczowych – opracowany zostanie, na szczeblu krajowym, dokument o charakterze strategicznym. Strategia określi cele i priorytety w zakresie zapewnienia niezakłóconego świadczenia usług kluczowych przez podmioty krytyczne i operatorów infrastruktury krytycznej jak również określi wszelkie niezbędne zakresy działań oraz formy działań służące osiąganiu tych celów. Strategia wskaże również podmioty właściwe do realizacji postanowień strategii oraz określi ich role.

Podmioty krytyczne

Wzorując się na dyrektywie 2022/2557 – przyjmuje się, że podmiotem krytycznym może być operator infrastruktury krytycznej, prowadzący działalność na terytorium RP, który świadczy co najmniej jedną usługę kluczową a incydent miałby istotny skutek zakłócający jej świadczenie.

Podmioty krytyczne będą identyfikowane przez wskazane ustawą organy do spraw podmiotów krytycznych i ujmowane w wykazach podmiotów krytycznych, prowadzonych przez te organy, zgodnie z ich właściwością.

Podmiot krytyczny będzie obowiązany do:

1) prowadzenia systematycznej oceny ryzyka świadczonej usługi kluczowej;
2) wdrożenia odpowiednich i proporcjonalnych do wyników oceny ryzyka rozwiązań organizacyjno-technicznych, dotyczących bezpieczeństwa świadczonej usługi (w tym infrastruktury krytycznej, za pomocą której świadczona jest usługa kluczowa), z uwzględnieniem polskich norm;
3) zapewnienia obsługi incydentów mających wpływ na świadczenie usługi kluczowej, w tym informowania o incydentach właściwych organów do spraw podmiotów krytycznych;
4) informowanie właściwych organów zarządzania kryzysowego o incydentach mających istotny wpływ na świadczenie usługi kluczowej, w przypadku gdy może to doprowadzić do sytuacji kryzysowej;
5) zapewnienia przeprowadzenia cyklicznych audytów wdrożonych rozwiązań, o których mowa w pkt 2;
6) zapewnienia udziału struktur organizacyjnych lub pracowników w szkoleniach i ćwiczeniach, w tym ćwiczeniach z zakresu obrony cywilnej, ochrony ludności, zarządzania kryzysowego oraz obronnych;
7) wyznaczenia tzw. osób odpowiedzialnych za utrzymanie kontaktów z właściwymi organami do spraw podmiotów krytycznych oraz zapewnienie im organizacyjnych warunków realizacji funkcji.

Zgodnie z dyrektywą CER projektowane przepisy określą również sposób identyfikacji i wyznaczania tzw. podmiotu krytycznego o szczególnym znaczeniu europejskim oraz wskażą obowiązki z tym związane.

Organy do spraw podmiotów krytycznych

Projektowana regulacja wskaże organy do spraw podmiotów krytycznych w poszczególnych sektorach i podsektorach.

Do podstawowych zadań organu należeć będzie:

1) prowadzenie bieżącej analizy podmiotów w danym sektorze lub podsektorze pod kątem uznania ich za podmiot krytyczny oraz ujmowania ich w wykazie;
2) prowadzenie bieżącej analizy podmiotów krytycznych w danym sektorze lub podsektorze pod kątem niespełniania warunków kwalifikujących dany podmiot jako podmiot krytyczny oraz wykreślanie ich z wykazu;
3) monitorowanie stosowania przepisów ustawy przez podmioty krytyczne;
4) prowadzanie kontroli podmiotów krytycznych;
5) nakładanie kar;
6) uczestniczenie w planowaniu, organizowaniu ćwiczeń podmiotów krytycznych oraz w razie potrzeby udział w tych ćwiczeniach;
7) prowadzenie działań informacyjnych dotyczących dobrych praktyk, działań edukacyjnych i kampanii na rzecz poszerzania wiedzy i budowania wiadomości w zakresie bezpieczeństwa usług kluczowych przez podmioty krytyczne.

Rządowe Centrum Bezpieczeństwa

Mając na względzie dotychczasowa praktykę w zakresie koordynacji zadań na szczeblu krajowym w zakresie ochrony infrastruktury krytycznej – przewiduje się, iż do zadań RCB należeć będzie:

1) monitorowanie wdrażania Strategii;

2) opracowywanie rocznych sprawozdań dotyczących tzw. incydentów istotnych zgłaszanych przez podmioty krytyczne, mających wpływ na ciągłość świadczonych przez nich usług kluczowych;
3) prowadzenie działań informacyjnych dotyczących dobrych praktyk, działań edukacyjnych i kampanii na rzecz poszerzania wiedzy i budowania świadomości w zakresie bezpieczeństwa świadczenia usług kluczowych przez podmioty krytyczne;
4) gromadzenie informacji o incydentach istotnych, które zostały przekazane przez inne państwa członkowskie Unii Europejskiej;
5) udostępnianie informacji i dobrych praktyk związanych ze zgłaszaniem incydentów istotnych przez podmioty krytyczne, uzyskane z tzw. Grupy do spraw Odporności Podmiotów Krytycznych;
6) prowadzenie tzw. Pojedynczego Punktu Kontaktowego (Pojedynczy Punkt Kontaktowy wykonuje funkcję łącznikową w celu zapewnienia współpracy transgranicznej z pojedynczymi punktami kontaktowymi innych państw członkowskich i z Grupą ds. Odporności Podmiotów Krytycznych. Ponadto Pojedynczy Punkt Kontaktowy będzie wykonywał również funkcję łącznikową z Komisją i zapewniał współpracę z państwami trzecimi), do którego zadań należeć m.in. będzie:
    a) odbieranie zgłoszeń incydentu istotnego dotyczącego dwóch lub większej liczby państw członkowskich Unii Europejskiej z pojedynczych punktów kontaktowych w innych państwach członkowskich Unii Europejskiej,
    b) przekazywanie zgłoszenia incydentu istotnego dotyczącego dwóch lub większej liczby państw członkowskich Unii Europejskiej do pojedynczych punktów kontaktowych w innych państwach członkowskich Unii Europejskiej,
    c) zapewnienie reprezentacji Rzeczypospolitej Polskiej w Grupie do spraw Podmiotów Krytycznych,
    d) zapewnienie współpracy z Komisją Europejską w obszarze bezpieczeństwa świadczenia usług kluczowych,
    e) koordynacja współpracy między organami do spraw podmiotów krytycznych i organami administracji publicznej w Rzeczypospolitej Polskiej z odpowiednimi organami w państwach członkowskich Unii Europejskiej,
    f) zapewnienie wymiany informacji na potrzeby Grupy do spraw Odporności Podmiotów Krytycznych oraz organami do spraw podmiotów krytycznych.

Nadzór i kontrola podmiotów krytycznych

Przewiduje się, iż nadzór w zakresie stosowania przepisów ustawy sprawują organy do spraw podmiotów krytycznych w zakresie:
1) spełniania przez podmioty krytyczne wymogów bezpieczeństwa dotyczących świadczenia usług kluczowych;
2) wykonywania przez podmioty krytyczne obowiązków dotyczących przeciwdziałania zagrożeniom dla świadczonych usług kluczowych i zgłaszania incydentów istotnych.

W ramach nadzoru organ do spraw podmiotów krytycznych:
1) prowadzi kontrole podmiotów krytycznych;
2) przeprowadza lub zleca audyt rozwiązań dotyczących bezpieczeństwa świadczenia usługi kluczowej;
3) nakłada kary pieniężne na podmioty krytyczne.

Projektowane rozwiązania przewidują, iż do kontroli realizowanej wobec podmiotów:
1) będących przedsiębiorcami stosuje się przepisy 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.

Przepisy o karach pieniężnych

Przepisy w tym zakresie wskażą – w zgodzie z dyrektywą 2022/2557 – zamknięty katalog kar nakładanych na podmioty krytyczne za niestosowanie się do przepisów ustawy oraz sposób zagospodarowania wpływów z tytułu tych kar.

III. Projekt zawiera zarówno regulacje w zakresie implementacji dyrektywy 2022/2557 jak również zawiera szereg regulacji wykraczających poza samą implementację, jednakże niezbędnych do jej prawidłowego wdrożenia, a przede wszystkim funkcjonowania tych rozwiązań w praktyce. Regulacje stricte wdrażające dyrektywę 2022/2557 zostały ujęte w tabeli zgodności, natomiast regulacje wykraczające poza implementację, w tym regulacje niezbędne do jej prawidłowego wdrożenia (identyfikacja i ochrona infrastruktury krytycznej), zostały wskazane w odwróconej tabeli zgodności.

Wdrożenie rozwiązań zawartych w dyrektywie 2022/2557 nie może odbyć się bez redefiniowania regulacji dotyczących infrastruktury krytycznej, która jest niezbędna do świadczenia usług kluczowych przez podmioty krytyczne, o których traktuje ta dyrektywa. W szczególności należy doprowadzić do niezakłóconego „przejścia" z dotychczasowych systemów infrastruktury krytycznej na sektory i podsektory, o których mówi dyrektywa. Ponadto, biorąc pod uwagę że dyrektywa stanowi jedynie minimum harmonizacyjne, projekt zakłada nie tylko utrzymanie dotychczasowego poziomu ochrony infrastruktury krytycznej, ale również wprowadzenie dodatkowych mechanizmów zapewniających jej ochronę, nawet już na etapie jej projektowania lub budowy.

Projektowane rozwiązania mają na celu wzmocnienie mechanizmów ochrony infrastruktury krytycznej, biorąc pod uwagę, iż stanowi ona rdzeń świadczenia usług niezbędnych dla funkcjonowania państwa oraz jego obywateli. Wynikają one również z analizy przebiegu wojny w Ukrainie i pojawiających się działań o charakterze sabotażowym i hybrydowym.

Infrastruktura krytyczna
Przewiduje się nowe kryteria umożliwiające identyfikację obiektów, instalacji oraz urządzeń jako infrastruktury krytycznej, a tym samym wyłaniania operatorów infrastruktury krytycznej (właściciel lub posiadacz takiej infrastruktury). Jednocześnie z kryteriami zostanie wskazany mechanizm identyfikacji infrastruktury krytycznej przez ministrów kierującymi działami administracji rządowej, wojewodów oraz przez inne podmioty, w zakresie ich właściwości. Ponadto zostaną wskazane ramy współpracy na linii administracja publiczna – przedsiębiorcy, będący operatorami infrastruktury krytycznej.

W celu zapewnienia właściwego poziomu ochrony infrastruktury krytycznej przewiduje się wprowadzenie minimalnych standardów w obszarach bezpieczeństwa fizycznego, technicznego, osobowego, teleinformatycznego, prawnego oraz zapewnienia planów ciągłości działania i odtwarzania.

Do obowiązków operatorów infrastruktury krytycznej będzie należało opracowanie i wdrożenie rozwiązań w zakresie infrastruktury krytycznej uwzględniającej minimalne standardy. Dodatkowo operator będzie zobowiązany do opracowania i prowadzenia dokumentacji odzwierciedlającej wdrożone rozwiązania, która to dokumentacja zastąpi obecne plany ochrony infrastruktury krytycznej.
Przewiduje się wprowadzenie instytucji koordynatora do spraw ochrony infrastruktury krytycznej u operatorów infrastruktury krytycznej. Operatorzy infrastruktury krytycznej będą obowiązani wyznaczać osoby koordynujące działania na linii operator – organy administracji publicznej, co jest analogią do obecnie wyznaczonych tzw. Osób kontaktowych, funkcjonujących u operatorów infrastruktury krytycznej.
Zmiana ta nie generuje dodatkowych kosztów dla operatorów IK, natomiast wprowadza efektywnie działające narzędzie systemowe w zakresie organizacji ochrony infrastruktury krytycznej. Dokonuje instytucjonalizacji osoby do utrzymywania kontaktów, zastępując ją funkcją „koordynatora ochrony infrastruktury krytycznej".
Koordynatorowi (oraz jego zastępcy) zostaną przyznane stosowne kompetencje – będzie on realizował działania przypisane ustawowo operatorowi i w jego imieniu.

Elementem „weryfikującym" poziom ochrony infrastruktury krytycznej oraz stopień wdrożenia rozwiązań w tym zakresie, będą raporty operatorów zawierające w szczególności informacje dotyczące funkcjonowania ochrony infrastruktury krytycznej w zakresie zapewnienia bezpieczeństwa fizycznego, technicznego, osobowego, teleinformatycznego, prawnego oraz zapewnienia planów ciągłości działania i odtwarzania. Raportowanie o stanie infrastruktury krytycznej w obowiązującym stanie prawnym dotyczy tylko systemu zaopatrzenia w energię, surowce energetyczne i paliwa. Dotychczas raporty te w powyżej wskazanym systemie sporządzane były z częstotliwością raz na kwartał. W odniesieniu do pozostałych systemów obowiązywało raportowanie doraźne.

Projektowane rozwiązania przewidują obowiązek okresowego raportowania przez wszystkich operatorów infrastruktury krytycznej, a cykl raportowania zostanie ujednolicony i będzie wynosił 12 miesięcy. W odniesieniu do przypadków wystąpienia incydentu naruszającego bezpieczeństwo infrastruktury krytycznej – operator zobowiązany będzie do doraźnego sporządzania raportów w tym zakresie.

Raport o stanie ochrony infrastruktury krytycznej sporządzany będzie m.in. z uwzględnieniem rozwiązań wdrożonych przez operatora, informacji zawartych w dokumentacji ochrony infrastruktury krytycznej, możliwości wystąpienia zidentyfikowanych ryzyk, incydentów oraz zdarzeń, które zakłóciły lub mogły zakłócić funkcjonowanie infrastruktury krytycznej, wyników przeprowadzonych kontroli i audytów odnoszących się do zabezpieczeń infrastruktury krytycznej.
Z tytułu jego sporządzania operatorzy nie będą ponosić dodatkowych kosztów.

IV. Projekt przewiduje wprowadzenie do porządku prawnego regulacji, które pozwolą na wzmocnienie ochrony najważniejszych dla państwa obszarów, obiektów i urządzeń, w tym morskiej infrastruktury krytycznej. W tym zakresie istotne pozostają zmiany proponowane do ustawy o ochronie osób i mienia oraz do ustawy o ochronie żeglugi i portów morskich.
W odniesieniu do pierwszej z wymienionych ustaw proponuje się wdrożenie przepisów, które m.in. umożliwią stosowanie określonych w tej ustawie środków ochrony fizycznej i zabezpieczenia technicznego od strony wody poza granicami obiektów podlegających obowiązkowej ochronie. Równolegle proponuje się rozszerzenie uprawnień pracowników ochrony o możliwość podejmowania dodatkowych działań względem infrastruktury portowej w celu zapewnienia jej większego poziomu zabezpieczenia. Jednocześnie projekt przewiduje zmiany przepisów, mające na celu usprawnienie przepływu informacji pomiędzy poszczególnymi podmiotami odpowiedzialnymi za zapewnienie ochrony tej infrastruktury.
Z kolei w ustawie o ochronie żeglugi i portów morskich proponuje się powołanie Centrum Bezpieczeństwa Morskiego (CBM), które będzie stanowiło wyraz międzysektorowego i wieloinstytucjonalnego podejścia w odniesieniu do ochrony szeroko rozumianej infrastruktury morskiej. Oczekiwanym efektem będzie zwiększenie odporności tej infrastruktury na wszelkiego rodzaju ataki, w tym o charakterze hybrydowym. Do zadań CBM będzie należało m.in. bieżące monitorowanie zagrożeń oraz wspieranie współpracy, w tym wymiany informacji, pomiędzy służbami i podmiotami realizującymi zadania w zakresie ochrony infrastruktury morskiej, statków, granicy państwa na morzu, a także ochrony życia lub zdrowia ludzi,

mienia i środowiska znajdujących się na polskich obszarach morskich w tym w wyłącznej strefie ekonomicznej. Funkcję CBM będzie pełniła komórka organizacyjna Straży Granicznej, do której oddelegowani będą również przedstawiciele innych służb oraz podmiotów właściwych do zapewnienia realizacji poszczególnych zadań CBM. Zadania te CBM będzie realizowało w sposób ciągły, tj. w systemie całodobowym.
Ponadto w ustawie o ochronie żeglugi i portów morskich wprowadza się przepisy umożliwiające zniszczenie, unieruchomienie lub przejmowanie kontroli nad bezzałogowym obiektem pływającym, w przypadkach gdy przebieg operacji lub działania takiego obiektu stanowiłoby lub mogłoby stanowić szeroko rozumiane zagrożenie dla bezpieczeństwa, w tym zagrożenie dla chronionych obiektów, urządzeń lub obszarów. Analogiczne rozwiązania proponuje się w ustawie o środkach przymusu bezpośredniego oraz broni palnej względem bezzałogowych obiektów lądowych.

3. Jak problem został rozwiązany w innych krajach, w szczególności krajach członkowskich OECD/UE?

Obowiązek opracowania planów zarządzania ryzykiem jest wdrażany w innych krajach UE, co wynika z postanowienia Decyzji Parlamentu Europejskiego i Rady nr 1313/2013/EU z dnia 17 grudnia 2013 r. w sprawie Unijnego Mechanizmu Ochrony Ludności. Brak jest danych dotyczących wdrożonych rozwiązań w innych państwach w tym obszarze.

W przypadku ochrony usług kluczowych – koncepcja zawarta w dyrektywie 2022/2557 jest rozwiązaniem odmiennym od stosowanego dotychczas w Unii Europejskiej tzw. „podejścia obiektowego". W efekcie wszystkie kraje UE stają przed problemem zaimplementowania rozwiązań, które dotychczas nie było stosowane. Brak tym samym rozwiązań, które mogłyby być przeanalizowane na potrzeby opracowania projektu ustawy.

4. Podmioty, na które oddziałuje projekt

Grupa	Wielkość	Źródło danych	Oddziaływanie
Planowanie cywilne – wdrożenie postanowień UMOL			
Ministrowie kierujący działami administracji rządowej	19		Opracowanie wkładów do Krajowej Oceny Ryzyka oraz Krajowego Planu Zarządzania Ryzykiem. Opracowanie planów zarządzania ryzykiem oraz planów reagowania kryzysowego.
Kierownicy urzędów centralnych	40		Opracowanie wkładów do Krajowej Oceny Ryzyka oraz Krajowego Planu Zarządzania Ryzykiem. Opracowanie planów zarządzania ryzykiem oraz planów reagowania kryzysowego.
Wojewodowie	16		Opracowanie wkładów do Krajowej Oceny Ryzyka oraz Krajowego Planu Zarządzania Ryzykiem. Opracowanie planów zarządzania ryzykiem oraz planów reagowania kryzysowego.
Rządowe Centrum Bezpieczeństwa	1		Opracowanie Krajowej Oceny Ryzyka, opracowanie Krajowego Planu Zarządzania Ryzykiem oraz Krajowego Planu Reagowania Kryzysowego.
Powiaty	314		Opracowanie planów zarządzania ryzykiem oraz planów reagowania kryzysowego.
Gminy	2 477		Opracowanie planów zarządzania ryzykiem oraz planów reagowania kryzysowego.

Implementacja dyrektywy 2022/2557			
Operatorzy infrastruktury krytycznej	135	Wykaz infrastruktury krytycznej prowadzony przez dyrektora RCB	Wyznaczenie osoby koordynującej działania na linii operator – organy administracji publicznej, tzw. Koordynatorów ochrony infrastruktury krytycznej. Wdrażanie rozwiązań w zakresie ochrony infrastruktury krytycznej.
Podmioty krytyczne świadczące usługi w sektorze energii	80	Szacunki RCB uwzględniające dotychczasową liczbę operatorów infrastruktury krytycznej oraz zmiany liczbowe jakie mogą nastąpić przy zastosowaniu kryteriów stosowanych obecnie w ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (dalej „ustawa k.s.c.") w odniesieniu do operatorów usług kluczowych.	Przeprowadzenie oceny ryzyka świadczonej usługi kluczowej. Wdrożenie odpowiednich i proporcjonalnych do wyników oceny ryzyka rozwiązań organizacyjno-technicznych, dotyczących bezpieczeństwa świadczonej usługi. Zapewnienie obsługi incydentów mających wpływ na świadczenie usługi kluczowej, w tym informowania o incydentach właściwych organów do spraw podmiotów krytycznych. Informowanie właściwych organów zarządzania kryzysowego o incydentach mających istotny wpływ na świadczenie usługi kluczowej, w przypadku gdy może to doprowadzić do sytuacji kryzysowej. Zapewnienie przeprowadzenia cyklicznych audytów wdrożonych rozwiązań organizacyjno-technicznych, dotyczących bezpieczeństwa świadczonej usługi. Zapewnienie udziału struktur organizacyjnych lub pracowników w szkoleniach i ćwiczeniach, w tym ćwiczeniach z zakresu obrony cywilnej, ochrony ludności, zarządzania kryzysowego oraz obronnych. Wyznaczenie tzw. osób odpowiedzialnych za utrzymanie kontaktów z właściwymi organami do spraw podmiotów krytycznych oraz zapewnienie im organizacyjnych warunków realizacji funkcji.
Podmioty krytyczne świadczące usługi w sektorze transportu	40	Szacunki RCB uwzględniające dotychczasową liczbę operatorów infrastruktury krytycznej oraz zmiany liczbowe jakie mogą nastąpić przy zastosowaniu kryteriów jakie są	j.w.

		stosowane w ustawie k.s.c. w odniesieniu do operatorów usług kluczowych.	
Podmioty krytyczne świadczące usługi w sektorze bankowości	10	Szacunki RCB uwzględniające dotychczasową liczbę operatorów infrastruktury krytycznej oraz zmiany liczbowe jakie mogą nastąpić przy zastosowaniu kryteriów jakie są stosowane w ustawie k.s.c. w odniesieniu do operatorów usług kluczowych.	Zgodnie z dyrektywą 2022/2557 podmioty w tym sektorze nie muszą podlegać niektórym obowiązkom dla podmiotów krytycznych. Podmioty krytyczne z sektora bankowości i infrastruktury rynków finansowych nie stosują niektórych przepisów 2022/2557 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).
Podmioty krytyczne świadczące usługi w sektorze infrastruktury rynków finansowych	10	Szacunki RCB uwzględniające dotychczasową liczbę operatorów infrastruktury krytycznej oraz zmiany liczbowe jakie mogą nastąpić przy zastosowaniu kryteriów jakie są stosowane w ustawie k.s.c. w odniesieniu do operatorów usług kluczowych.	j.w.
Podmioty krytyczne świadczące usługi w sektorze zdrowia	15	Szacunki RCB uwzględniające dotychczasową liczbę operatorów infrastruktury krytycznej oraz zmiany liczbowe jakie mogą nastąpić przy zastosowaniu kryteriów jakie są stosowane w ustawie k.s.c. w odniesieniu do operatorów usług kluczowych.	Przeprowadzenie oceny ryzyka świadczonej usługi kluczowej. Wdrożenie odpowiednich i proporcjonalnych do wyników oceny ryzyka rozwiązań organizacyjno-technicznych, dotyczących bezpieczeństwa świadczonej usługi. Zapewnienie obsługi incydentów mających wpływ na świadczenie usługi kluczowej, w tym informowania o incydentach właściwych organów do spraw podmiotów krytycznych. Informowanie właściwych organów zarządzania kryzysowego o incydentach mających istotny wpływ na świadczenie usługi kluczowej, w przypadku gdy może to doprowadzić do sytuacji kryzysowej. Zapewnienie przeprowadzenia cyklicznych audytów

			wdrożonych rozwiązań, o których mowa w pkt 2; Zapewnienie udziału struktur organizacyjnych lub pracowników w szkoleniach i ćwiczeniach, w tym ćwiczeniach z zakresu obrony cywilnej, ochrony ludności, zarządzania kryzysowego oraz obronnych. Wyznaczenie tzw. osób odpowiedzialnych za utrzymanie kontaktów z właściwymi organami do spraw podmiotów krytycznych oraz zapewnienie im organizacyjnych warunków realizacji funkcji.
Podmioty krytyczne świadczące usługi w sektorze zaopatrzenia w wodę pitną i jej dystrybucji	70	Szacunki RCB uwzględniające dotychczasową liczbę operatorów infrastruktury krytycznej oraz zmiany liczbowe jakie mogą nastąpić przy zastosowaniu kryteriów jakie są stosowane w ustawie k.s.c. w odniesieniu do operatorów usług kluczowych.	j.w.
Podmioty krytyczne świadczące usługi w sektorze zbiorowego odprowadzania ścieków	10	Szacunki RCB uwzględniające dotychczasową liczbę operatorów infrastruktury krytycznej oraz zmiany liczbowe jakie mogą nastąpić przy zastosowaniu kryteriów jakie są stosowane w ustawie k.s.c. w odniesieniu do operatorów usług kluczowych.	j.w.
Podmioty krytyczne świadczące usługi w sektorze infrastruktury cyfrowej	40		Zgodnie z dyrektywą 2022/2557 podmioty w tym sektorze nie muszą podlegać wszystkim obowiązkom przewidzianym dla podmiotów krytycznych (rozdz. III oraz IV dyrektywy 2022/2557).
Podmioty krytyczne świadczące usługi w sektorze administracji publicznej	60	Szacunki RCB oparte o wykaz jednostek sektora finansów publicznych zawarty w art. 9 pkt 1, 8, 9 i 14 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych.	Przeprowadzenie oceny ryzyka świadczonej usługi kluczowej. Wdrożenie odpowiednich i proporcjonalnych do wyników oceny ryzyka rozwiązań organizacyjno-technicznych, dotyczących bezpieczeństwa świadczonej usługi. Zapewnienie obsługi incydentów mających wpływ na świadczenie usługi kluczowej, w tym informowania o incydentach właściwych organów do spraw podmiotów krytycznych. Informowanie właściwych organów zarządzania kryzysowego o incydentach mających istotny wpływ na

			świadczenie usługi kluczowej, w przypadku gdy może to doprowadzić do sytuacji kryzysowej. Zapewnienie przeprowadzenia cyklicznych audytów wdrożonych rozwiązań, organizacyjno-technicznych dotyczących zapewniania bezpieczeństwa świadczonej usługi. Zapewnienie udziału struktur organizacyjnych lub pracowników w szkoleniach i ćwiczeniach, w tym ćwiczeniach z zakresu obrony cywilnej, ochrony ludności, zarządzania kryzysowego oraz obronnych. Wyznaczenie tzw. osób odpowiedzialnych za utrzymanie kontaktów z właściwymi organami do spraw podmiotów krytycznych oraz zapewnienie im organizacyjnych warunków realizacji funkcji.
Podmioty krytyczne świadczące usługi w sektorze przestrzeni kosmicznej	5	Szacunek RCB oparty o decyzję Rady (WPZiB) 2021/698 z dnia 30 kwietnia 2021 r. w sprawie bezpieczeństwa systemów i usług wdrażanych, udostępnianych i użytkowanych w ramach Unijnego programu kosmicznego, które mogą mieć wpływ na bezpieczeństwo Unii, oraz uchylenia decyzji 2014/496/WPZiB.	j.w.
Podmioty krytyczne świadczące usługi w sektorze produkcji, przetwarzania i dystrybucji żywności	30	Szacunki RCB uwzględniające kryteria jakie są stosowane w ustawie k.s.c. w odniesieniu do operatorów usług kluczowych.	j.w.
Podmioty krytyczne świadczące usługi w sektorze zarządzania usługami ICT	43	Szacunki RCB uwzględniające liczbę podmiotów kluczowych i podmiotów ważnych z sektora zarządzania ICT, wskazaną w projekcie ustawy nowelizującej ustawę k.s.c.	Sektor wprowadzony dla zapewnienia spójności z dyrektywą NIS2.
Podmioty krytyczne świadczące usługi w sektorze produkcji wytwarzania i dystrybucji chemikaliów i innych produktów przemysłowych	25	Szacunki RCB uwzględniające dotychczasową ilość operatorów infrastruktury krytycznej w systemie oraz zmiany liczbowe jakie mogą nastąpić przy zastosowaniu kryteriów jakie są stosowane w ustawie k.s.c. w odniesieniu do operatorów usług kluczowych.	Sektor wprowadzony dla zachowania spójności z dotychczasowym wykazem obiektów infrastruktury krytycznej w tym obszarze. Konieczność wprowadzenia takiego sektora wynika z analiz prowadzonych przez RCB w zakresie wykrywania zależności operatorów infrastruktury krytycznej od innych podmiotów (rozwiązania niezbędne dla wynikającej z

			dyrektywy 2022/2557 ochrony łańcuchów dostaw).
Podmioty krytyczne świadczące usługi w sektorze usług pocztowych	10	Szacunki RCB uwzględniające dotychczasową liczbę operatorów infrastruktury krytycznej w systemie oraz zmiany liczbowe jakie mogą nastąpić przy zastosowaniu kryteriów jakie są stosowane w ustawie k.s.c. w odniesieniu do operatorów usług kluczowych.	Sektor wprowadzony dla zachowania spójności z dotychczasowym wykazem obiektów infrastruktury krytycznej w tym obszarze.
Podmioty krytyczne świadczące usługi w sektorze gospodarowania odpadami	10	Szacunki RCB uwzględniające zmiany jakie mogą nastąpić przy zastosowaniu kryteriów jakie są stosowane w ustawie o KSC w odniesieniu do operatorów usług kluczowych.	Sektor wprowadzony dla zachowania spójności z dotychczasowym wykazem obiektów infrastruktury krytycznej w tym obszarze.
Podmioty krytyczne świadczące usługi w sektorze finansów publicznych	10		Identyfikowanie podmiotów krytycznych i ujmowanie w wykazie podmiotów krytycznych dla danego sektora lub podsektora. Współpraca z podmiotami krytycznym w zakresie obsługi incydentów istotnych. Zadania w zakresie nadzoru i kontroli podmiotów krytycznych w danym sektorze lub podsektorze. Nakładanie kar na podmioty krytyczne w danym sektorze lub podsektorze.
Organy do spraw podmiotów krytycznych	16	Maksymalna liczba organów do spraw podmiotów krytycznych, wynikająca z poszczególnych działów administracji rządowej. Liczba może być mniejsza w przypadku gdy kilka działów kierowanych będzie przez jednego ministra.	Identyfikowanie podmiotów krytycznych i ujmowanie w wykazie podmiotów krytycznych dla danego sektora lub podsektora. Współpraca z podmiotami krytycznym w zakresie obsługi incydentów istotnych. Zadania w zakresie nadzoru i kontroli podmiotów krytycznych w danym sektorze lub podsektorze. Nakładanie kar na podmioty krytyczne w danym sektorze lub podsektorze.
Ministrowie kierujący działami administracji rządowej	12		Identyfikowanie – zgodnie z kryteriami – obiektów, urządzeń lub instalacji jako infrastruktury krytycznej i przedkładanie wniosków o wpis do wykazu infrastruktury krytycznej prowadzonego przez RCB.
Wojewodowie	16		Identyfikowanie – zgodnie z kryteriami – obiektów, urządzeń lub instalacji jako infrastruktury krytycznej i ujmowanie ich w wykazach infrastruktury krytycznej na obszarze danego województwa. Współpraca z operatorami infrastruktury krytycznej ujętymi w danym

			wykazie infrastruktury krytycznej.
Rządowe Centrum Bezpieczeństwa	1		W obszarze infrastruktury krytycznej – opracowanie kryteriów identyfikacji infrastruktury krytycznej niezbędnej dla funkcjonowania państwa i zaspokojenia potrzeb obywateli oraz infrastruktury krytycznej niezbędnej dla zaspokojenie potrzeb lokalnych społeczności danego województwa. Prowadzenie wykazu infrastruktury krytycznej niezbędnej dla funkcjonowania państwa i zaspokojenia potrzeb obywateli, zgodnie z wnioskami zgłaszanymi przez ministrów wyznaczonych jako odpowiedzialnych za identyfikację infrastruktury krytycznej w poszczególnych sektorach lub podsektorach. Opracowanie minimalnych standardów w obszarach bezpieczeństwa fizycznego, technicznego, osobowego, teleinformatycznego, prawnego oraz zapewnienia planów ciągłości działania i odtwarzania. W sytuacjach niecierpiących zwłoki – identyfikowanie – zgodnie z kryteriami – obiektów, urządzeń lub instalacji jako infrastruktury krytycznej i ujmowanie w wykazie infrastruktury krytycznej.
Komisja Nadzoru Finansowego	1		Identyfikowanie – zgodnie z kryteriami – obiektów, urządzeń lub instalacji jako infrastruktury krytycznej i ujmowanie ich w wykazach infrastruktury krytycznej na obszarze danego województwa. Współpraca z operatorami infrastruktury krytycznej ujętymi w danym wykazie infrastruktury krytycznej. W obszarze podmiotów krytycznych – realizacja powierzonych obowiązków organu do spraw podmiotów krytycznych dla sektora bankowości i infrastruktury rynków finansowych.
Sądy administracyjne			Rozpatrywanie skarg na decyzje o nałożeniu kary

			pieniężnej na podmiot krytyczny.
Zmiany w innych ustawach			
Rządowa Agencja Rezerw Strategicznych	1		Usprawnienie działania RARS w sytuacjach kryzysowych, w działaniach związanych z ochroną ludności i obroną cywilną.
Komendant Główny Straży Granicznej			Realizacja zadań w ramach CBM.
Szef Krajowej Administracji Skarbowej			Realizacja zadań w ramach CBM.
Morska Służba Poszukiwania i Ratownictwa			Realizacja zadań w ramach CBM.
Urzędy Morskie			Realizacja Zadań w ramach CBM.

5. Informacje na temat zakresu, czasu trwania i podsumowanie wyników konsultacji

Stosownie do postanowień § 36 ust. 1 i 38 § 1 uchwały nr 190 Rady Ministrów z dnia 29 października 2013 r. – Regulamin pracy Rady w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji, w serwisie Rządowy Proces Legislacyjny, udostępniony został projekt ustawy o zmianie ustawy o zarządzaniu kryzysowym oraz niektórych innych ustaw a właściwe podmioty zostały bezpośrednio poinformowane o zamieszczeniu projektu.

W ramach konsultacji publicznych projekt został skierowany do następujących podmiotów Business Centre Club, Federacji Konsumentów, Fundacji Bezpieczna Cyberprzestrzeń, Fundacji ePaństwo, Fundacji im. Stefana Batorego, Fundacji Instytut Mikromakro, Fundacji My Pacjenci, Fundacji Nowoczesna Polska, Fundacji Panoptykon, Fundacji Projekt Polska, Fundacji Pułaskiego, Internet Society Poland Chapter, Internet Society Poland, Izby Gospodarki Elektronicznej, Konfederacji Lewiatan, Krajowego Związku Banków Spółdzielczych, Krajowej Izby Gospodarczej Elektroniki i Telekomunikacji, Krajowej Izby Gospodarczej, Krajowej Izby Gospodarki Cyfrowej, Krajowej Izby Gospodarki Morskiej, Krajowej Izby Komunikacji Ethernetowej, Krajowej Izby Rozliczeniowej, Krajowej Spółdzielczej Kasy Oszczędnościowo-Kredytowej, Naczelnej Organizacji Technicznej, Naczelnej Rady Zrzeszeń Handlu i Usług, Polskiego Centrum Badań i Certyfikacji S.A., Polskiego Towarzystwa Informatycznego, Polskiej Izby Brokerów Ubezpieczeniowych i Reasekuracyjnych, Polskiej Izby Handlu, Polskiej Izby Informatyki i Telekomunikacji, Polskiej Izby Komunikacji Elektronicznej, Polskiej Izby Producentów Urządzeń i Usług na rzecz Kolei, Polskiej Izby Radiodyfuzji Cyfrowej, Polskiej Izby Ubezpieczeń, Polskiej Organizacji Handlu i Dystrybucji, Polskiej Organizacji Niebankowych Instytucji Płatności, Polskiej Rady Biznesu, Polskiej Wytwórni Papierów Wartościowych, Sektorowej Rady ds. Kompetencji – Telekomunikacja i Cyberbezpieczeństwo, Stowarzyszenia Inżynierów Telekomunikacji, Stowarzyszenia Polskich Brokerów Ubezpieczeniowych i Reasekuracyjnych, Towarzystwa Gospodarczego Polskie Elektrownie, Związku Banków Polskich oraz operatorów infrastruktury krytycznej.

W ramach opiniowania projekt został udostępniony: Prokuratorii Generalnej Rzeczypospolitej Polskiej, Prezesowi Urzędu Ochrony Konkurencji i Konsumentów, Prezesowi Urzędu Komunikacji Elektronicznej, Prezesowi Urzędu Ochrony Danych Osobowych, Komisji Nadzoru Finansowego, Rzecznikowi Małych i Średnich Przedsiębiorców, Urzędowi Zamówień Publicznych, Polskiemu Komitetowi Normalizacyjnemu, Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Biuru Bezpieczeństwa Narodowego, Centralnemu Biuru Antykorupcyjnemu, Służbie Kontrwywiadu Wojskowego, Służbie Wywiadu Wojskowego oraz Służbie Ochrony Państwa.

Przeprowadzono konferencje uzgodnieniowe mające na celu dopracowanie przepisów w poszczególnych sektorach, o których mowa w projekcie ustawy oraz nowych zadań w zakresie identyfikacji i ochrony infrastruktury krytycznej.

Mając na względzie, iż identyfikacja podmiotów krytycznych będzie odbywała się spośród operatorów infrastruktury krytycznej - projekt był przedmiotem wielu spotkań z udziałem operatorów infrastruktury krytycznej, na których prezentowano i omawiano zawarte w nim rozwiązania, w tym na:

- ✓ seminarium „Podnoszenie Cyberodporności u operatorów IK” w dniach 13–14 maja 2024 r.,
- ✓ Ogólnopolskim Szczycie Energetycznym w dniu 18 czerwca 2024 r.,
- ✓ VII Międzynarodowym Kongresie Naukowo-Technicznym „Safe Place” w dniu 27 listopada 2024 r.,
- ✓ XI Krajowym Forum Ochrony Infrastruktury Krytycznej w dniach 3–4 grudnia 2024 r.

Podsumowanie wyników konsultacji zostało zamieszczone w raporcie z konsultacji.

Projekt ustawy był rozpatrywany na forum Komisji Wspólnej Rządu i Samorządu Terytorialnego i uzyskał akceptację projektowanych w niej rozwiązań.

Projekt ustawy nie podlegał konsultacjom z właściwymi organami i instytucjami Unii Europejskiej, w tym Europejskim Bankiem Centralnym. Na etapie konsultacji do projektu ustawy nie został zgłoszony żaden wniosek w trybie przepisów o działalności lobbingowej w procesie stanowienia prawa.

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	**7,19**	**7,98**	**8,24**	**8,43**	**8,64**	**8,88**	**9,12**	**9,36**	**9,61**	**9,84**	**10,11**	97,40
budżet państwa	0,19	0,21	0,23	0,23	0,23	0,23	0,25	0,26	0,26	0,27	0,27	2,63
JST	1,09	1,19	1,24	1,29	1,32	1,37	1,41	1,46	1,51	1,55	1,61	15,04
Fundusz Pracy	0,17	0,19	0,20	0,20	0,21	0,21	0,22	0,22	0,23	0,23	0,24	2,32
FS	0,25	0,28	0,29	0,29	0,30	0,31	0,32	0,32	0,33	0,34	0,35	3,38
FUS	5,36	5,97	6,13	6,27	6,43	6,59	6,75	6,92	7,10	7,27	7,45	72,24
NFZ	0,13	0,14	0,15	0,15	0,15	0,17	0,17	0,18	0,18	0,18	0,19	1,79
Wydatki ogółem	**27,56**	**24,02**	**24,61**	**25,20**	**25,83**	**27,90**	**27,10**	**27,78**	**28,46**	**29,17**	**31,34**	298,97
budżet państwa	27,56	24,02	24,61	25,20	25,83	27,90	27,10	27,78	28,46	29,17	31,34	298,97
JST												
pozostałe jednostki (oddzielnie)												
Saldo ogółem	**-20,37**	**-16,04**	**-16,37**	**-16,77**	**-17,19**	**-19,02**	**-17,98**	**-18,42**	**-18,85**	**-19,33**	**-21,23**	-201,57
budżet państwa	-27,37	-23,81	-24,38	-24,97	-25,60	-27,67	-26,85	-27,52	-28,20	-28,90	-31,07	-296,34
JST	1,09	1,19	1,24	1,29	1,32	1,37	1,41	1,46	1,51	1,55	1,61	15,04
Fundusz Pracy	0,17	0,19	0,20	0,20	0,21	0,21	0,22	0,22	0,23	0,23	0,24	2,32
FS	0,25	0,28	0,29	0,29	0,30	0,31	0,32	0,32	0,33	0,34	0,35	3,38
FUS	5,36	5,97	6,13	6,27	6,43	6,59	6,75	6,92	7,10	7,27	7,45	72,24
NFZ	0,13	0,14	0,15	0,15	0,15	0,17	0,17	0,18	0,18	0,18	0,19	1,79

Źródła finansowania	Wejście w życie ustawy wywoła skutki finansowe dla budżetu państwa w rozumieniu art. 50 ust. 1 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych. Środki finansowe na realizację zadań w 2026 r. powinny zostać sfinansowane z rezerwy celowej budżetu państwa z poz. 56 na koszty wskazane w następujących częściach budżetu państwa: – 20 – gospodarka; – 21 – gospodarka morska; – 22 – gospodarka wodna; – 27 – informatyzacja; – 32 – rolnictwo; – 37 – sprawiedliwość; – 39 – transport; – 42 – sprawy wewnętrzne; – 46 – zdrowie; – 47 – energia; – 48 – gospodarka surowcami energetycznymi; – 51 – klimat; – 69 – żegluga śródlądowa; – 76 – Urząd Komunikacji Elektronicznej; – 85/02 – województwo dolnośląskie; – 85/04 – województwo kujawsko-pomorskie;

	– 85/06 – województwo lubelskie; – 85/08 – województwo lubuskie; – 85/10 – województwo łódzkie; – 85/12 – województwo małopolskie; – 85/14 – województwo mazowieckie; – 85/16 – województwo opolskie; – 85/18 – województwo podkarpackie; – 85/20 – województwo podlaskie; – 85/22 – województwo pomorskie; – 85/24 – województwo śląskie; – 85/26 – województwo świętokrzyskie; – 85/28 – województwo warmińsko-mazurskie; – 85/30 – województwo wielkopolskie; – 85/32 – województwo zachodniopomorskie. W przypadku UKNF – źródłem finansowania wydatków będą środki finansowe pochodzące z opłat nadzorczych wnoszonych przez podmioty finansowe. Maksymalne limity wydatków w podziale na poszczególne części budżetu państwa zostały wskazane w projekcie ustawy, z wyłączeniem części 46 budżetu państwa – zdrowie. Maksymalny limit wydatków w części 46 budżetu państwa – zdrowie kształtuje się następująco: 1) w 2026 r. – 586 tys. zł; 2) w 2027 r. – 611 tys. zł; 3) w 2028 r. – 626 tys. zł; 4) w 2029 r. – 642 tys. zł; 5) w 2030 r. – 658 tys. zł; 6) w 2031 r. – 710 tys. zł; 7) w 2032 r. – 691 tys. zł; 8) w 2033 r. – 708 tys. zł; 9) w 2034 r. – 726 tys. zł; 10) w 2035 r. – 744 tys. zł. Skutki finansowe wynikające z wejścia w życie projektowanych przepisów w zakresie ochrony zdrowia będą mieścić się corocznie w ramach wysokości wydatków ustalanych wg art. 131c ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych bez konieczności ich zwiększania. Rozbicie kosztów na poszczególne resorty oraz wyszczególnienie wydatków na wynagrodzenia osobowe oraz pozostałe wydatki zamieszczono w załączniku nr 3.
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	**<u>Wydatki Budżetu Państwa</u>** W oszacowaniu skutków finansowych wykorzystano dostępne prognozy wskaźników makroekonomicznych Ministra Finansów w zakresie CPI – dynamiki średniorocznej, zawarte w „Wytycznych dotyczących stosowania jednolitych wskaźników makroekonomicznych będących podstawą oszacowania skutków finansowych projektowanych ustaw, Aktualizacja – lipiec 2025 r. ***<u>Organy do spraw podmiotów krytycznych</u>*** Projektowane zmiany mają zapewnić środki finansowe na działania związane z realizacją ustawowych zadań nałożonych na podmioty właściwe do ich realizacji. Jako rok 0 przyjmuje się rok 2026. W przypadku zadań z zakresu planowania cywilnego – rozwiązania zawarte w ustawie wprowadzają w głównej mierze dodatkowe formalno-prawne narzędzia realizacji ustawowych obowiązków organów zarządzania kryzysowego, w ramach posiadanych na te zadania środków finansowych. Natomiast w przypadku realizacji zadań nakładanych dyrektywą CER konieczne jest de facto zdefiniowanie ich od podstaw oraz zapewnienie finansowania na odpowiednim poziomie. Dyrektywa CER wprowadza jako novum zadania dla organów do spraw podmiotów krytycznych, które to zadania wymagają zatrudnienia dodatkowego personelu i poniesienia kosztów związanych z odpowiednimi wynagrodzeniami. Ponadto konieczne jest poniesienie wydatków związanych z zapewnieniem narzędzi niezbędnych do pracy (koszty utworzenia stanowisk pracy). Zadania w zakresie obowiązków związanych z wdrożeniem rozwiązań zawartych w dyrektywie CER z punktu widzenia organu do spraw podmiotów krytycznych będą obejmować m.in.

1) identyfikację podmiotu krytycznego oraz jego ujęcie we właściwym wykazie prowadzonym przez organ do spraw podmiotów krytycznych;
2) współpracę z podmiotami krytycznym w zakresie obsługi incydentów istotnych, w tym wydawanie rekomendacji przez ministra w tym zakresie;
3) czynności nadzorcze, w tym zadania związane z kontrolą podmiotów krytycznych;
4) czynności związane z nakładaniem kar.

Mając na względzie, iż tematyka zawarta w dyrektywie CER związana jest nierozerwalnie z tematyką ochrony infrastruktury krytycznej – należy przyjąć możliwość maksymalnie efektywnego wykorzystania obecnego potencjału kadrowego urzędów obsługujących przyszłe organy do spraw podmiotów krytycznych. Propozycje dodatkowych etatów na realizację nowych zadań uwzględniają konieczność ograniczania deficytu budżetowego, przy jednoczesnym inwestowaniu środków finansowych w szerokorozumiane kwestie bezpieczeństwa.

Dlatego przy zwiększonych obowiązkach podmiotów przyjęto założenie minimalne w postaci dodania 3 etatów w odniesieniu do każdego z podmiotów pełniących funkcję organu do spraw podmiotów krytycznych co daje liczbę **36 nowych etatów**.

Dodatkowo przyznano **1** etat dla Ministra Sprawiedliwości na realizacje zadań związanych z procesami „tzw. sprawdzania przeszłości".

Analiza pracochłonności stanowi załącznik nr 1 do Oceny Skutków Regulacji.

Wojewodowie
Propozycje dodatkowych etatów na realizację nowych zadań uwzględniają konieczność ograniczania deficytu budżetowego, przy jednoczesnym inwestowaniu środków finansowych w szerokorozumiane kwestie bezpieczeństwa.
Koszty związane będą z realizacją nowego zadania dla wojewodów dotyczącego identyfikacji obiektów, urządzeń oraz instalacji jako infrastruktury krytycznej jak również dalszych czynności w zakresie wsparcia operatorów w realizacji zadań związanych z ochrona infrastruktury krytycznej. Dlatego też wskazane jest dokonanie zwiększenia zatrudnienia w wszystkich urzędach wojewodów o 3 etaty, co daje łącznie **48 nowych etatów**.

Jednostkowe wyliczenie etatu – jako podstawę wyliczeń przyjęto stanowisko głównego specjalisty, z wynagrodzeniem 9 044zł brutto miesięcznie. Dodatkowo należy uwzględnić koszty pracodawcy, tj. składkę na ubezpieczenie społeczne oraz składkę na Fundusz Pracy i Fundusz Solidarnościowy.
W kolejnych latach koszt pracownika wzrośnie (zgodnie ze wskaźnikami makroekonomicznymi) oraz z uwzględnieniem dodatkowego wynagrodzenia rocznego.

Analiza pracochłonności stanowi załącznik nr 1 do Oceny Skutków Regulacji.

Koszty stanowiska pracy

Dodatkowo jednostkowy koszt wyposażenia stanowiska pracy określono na 12 000 zł (laptop, dodatkowy monitor, telefon komórkowy). Przy uwzględnieniu zużycia sprzętu i konieczności jego wymiany proponuje się analogiczną kwotę ująć w budżecie co 5 lat.

Rządowe Centrum Bezpieczeństwa
Projektowane zmiany mają zapewnić środki finansowe na działania związane z realizacją ustawowych zadań nakładanych na Rządowe Centrum Bezpieczeństwa.
Jako rok 0 przyjmuje się rok 2026.

UMOL (wskazanie czynności w ramach zadań)
W przypadku zadań z zakresu planowania cywilnego - rozwiązania implementujące decyzję Parlamentu Europejskiego i Rady nr 1313/2013/EU w sprawie Unijnego Mechanizmu Ochrony Ludności, wprowadzają nowe zadania w zakresie oceny ryzyka i kwestii zarządzania ryzykiem. Wymagają one wzmocnienia potencjału kadrowego RCB. W tym obszarze, obok „standardowych" prac planistycznych konieczne będzie znaczące rozbudowanie zadań o procesy gromadzenia i analizy informacji, które są niezbędne do skutecznego zarządzania ryzykiem.
Do nowych zadań RCB należeć będzie:
1) opracowanie od podstaw nowego dokumentu strategicznego – Krajowej Oceny Ryzyka;

2) opracowanie od podstaw dokumentów planistycznych na wszystkich szczeblach zarządzania kryzysowego – zarówno planów zarządzania ryzykiem jak również planów reagowania kryzysowego. W przypadku RCB będzie to konieczność opracowywania oraz bieżącej aktualizacji Krajowego Planu Zarządzania Ryzykiem oraz Krajowego Planu Reagowania Kryzysowego;
3) uzgadnianie planów ministrów kierujących działami administracji rządowej oraz kierowników urzędów centralnych w zakresie spójności ich planów z Krajowym Planem Zarządzania Ryzykiem albo Krajowym Planem Reagowania Kryzysowego;
4) prowadzenie rozbudowanej sprawozdawczości na rzecz Komisji Europejskiej dotyczącej zarządzania ryzykiem;
5) konieczność korelacji planów reagowania kryzysowego z planami ewakuacji ludności.

Dyrektywa 2022/2557

Natomiast w przypadku realizacji zadań nakładanych dyrektywą 2022/2557 konieczne jest zapewnienie finansowania na odpowiednim poziomie realizacji nowych zadań Rządowego Centrum Bezpieczeństwa. W celu realizacji nowych zadań konieczne jest zatrudnienie dodatkowego personelu i poniesienia dodatkowych kosztów związanych ze zwiększeniem zatrudnienia.

Do nowych zadań Rządowego Centrum Bezpieczeństwa – w ramach implementacji dyrektywy 2022/2557 – należeć będzie m.in.:
1) opracowanie, od podstaw, nowych dokumentów planistycznych o charakterze strategicznym, tj. Krajowej Oceny Ryzyka oraz Strategii Odporności Podmiotów Krytycznych, w tym dokonywanie ich regularnych aktualizacji, a w przypadku Strategii, jej monitorowania stopnia jej wdrażania i przedkładanie corocznych sprawozdań w tym zakresie;
2) prowadzenie – rozbudowanego w stosunku do obecnego – wykazu infrastruktury krytycznej obejmującego obiekty urządzenia, instalacje lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje oraz sieci, systemy lub usługi, identyfikowane przez uprawnionych do tego ministrów, wojewodów oraz Przewodniczącego Komisji Nadzoru Finansowego;
3) prowadzenie drugiego wykazu – tzw. potencjalnej infrastruktury krytycznej;
4) koordynacja międzynarodowej współpracy w zakresie realizacji postanowień dyrektywy CER, w tym prowadzenie Pojedynczego Punktu Kontaktowego oraz zapewniać reprezentację kraju na forum Grupy do spraw Odporności Podmiotów Krytycznych;
5) prowadzenie wykazu podmiotów krytycznych – identyfikowanych spośród operatorów infrastruktury krytycznej oraz współpraca w tym zakresie z tzw. organami ds. podmiotów krytycznych, wyznaczonych na podstawie projektowanej ustawy.

Do realizacji zadań w zakresie, o których mowa powyżej niezbędne będzie zapewnienie, poza obsługą merytoryczną, zapewnienie obsługi prawnej tych procesów, w tym ewentualne prowadzenie postępowań przed sądami administracyjnymi.

Powyższe zadania nie mogą odbywać się bez zapewnienia całodobowego, efektywnego, obiegu informacji oraz obsługi strony teleinformatycznej wszystkich procesów. Obecna sytuacja finansowa jak i stan kadrowy uniemożliwia efektywne wykonywanie obowiązków w tym zakresie.
Proponowane zmiany w zakresie zatrudnienia i kosztów z tym związanych dostosowano adekwatnie do przyszłych potrzeb. Planowane jest zwiększenie stanu osobowego RCB o **28 etatów**, co powinno zapewnić właściwą realizację przyszłych zadań.

Jednostkowe wyliczenie etatu – jako podstawę wyliczeń przyjęto stanowisko głównego specjalisty, przy maksymalnej stawce w tej kategorii zaszeregowania oraz 20% dodatek stażowy (wynagrodzenie 11 108,16 zł brutto miesięcznie). Dodatkowo należy uwzględnić koszty pracodawcy, tj. składkę na ubezpieczenie społeczne oraz składkę na Fundusz Pracy i Fundusz Solidarnościowy.

W kolejnych latach koszt pracownika wzrośnie (zgodnie ze wskaźnikami makroekonomicznymi) oraz z uwzględnieniem dodatkowego wynagrodzenia rocznego.
Dodatkowe zatrudnienie ma obejmować łącznie **28 etatów,** w tym:
1) 5 etatów w komórce planistycznej w związku z opracowaniem nowych dokumentów strategicznych i planistycznych dotyczących zarządzania kryzysowego oraz opracowanie nowej planistyki dotyczącej ewakuacji ludności;
2) 6 etatów w komórce, która będzie realizować zadania związane z identyfikacją infrastruktury krytycznej oraz potencjalnej infrastruktury krytycznej (w tym prowadzenie dokumentacji w zakresie wykazów) oraz współpracować z właściwymi podmiotami w zakresie zapewnienia ochrony infrastruktury krytycznej. Ponadto nowe zadania w zakresie komórki obejmą identyfikację podmiotów krytycznych, w tym obsługę wykazu podmiotów krytycznych, opracowywanie cyklicznych strategii odporności podmiotów

krytycznych oraz krajowych ocen ryzyka dla podmiotów krytycznych. Dodatkowo – w ramach współpracy z UE w zakresie ochrony infrastruktury krytycznej, podmiotów krytycznych i usług kluczowych – realizacja zadań w zakresie prowadzenia pojedynczego punktu kontaktowego czy też obsługa tzw. misji doradczych UE;

3) 2 etaty w komórce, zajmującej się ochroną informacji niejawnych w celu zapewnienia efektywnego funkcjonowania obiegu informacji niejawnych, w tym zapewniającego niezakłócone funkcjonowanie systemów teleinformatycznych służących do przekazywania informacji niejawnych (UE, NATO oraz krajowych);
4) 2 etaty w komórce zajmującej się sprawami związanymi z edukacją dla odporności;
5) 4 etaty w komórce zajmującej się całodobowym obiegiem na potrzeby zarządzania kryzysowego, ochrony ludności oraz obrony cywilnej oraz prowadzącej bieżące analizy pojawiających się zagrożeń;
6) 2 etaty w komórce zajmującej się współpracą międzynarodową, szczególności współpracą cywilno-wojskową wynikającą z zobowiązań sojuszniczych Organizacji Traktatu Północnoatlantyckiego (prowadzenie punktu kontaktowego NATO, budowanie odporności);
7) 3 etaty w komórce zajmującej się zapewnieniem bieżącego funkcjonowania systemów teleinformatycznych oraz cyberbezpieczeństwa procesów realizowanych przez pozostałe komórki;
8) 3 etaty na zapewnienie obsługi kadrowej, finansowej oraz logistycznej procesów realizowanych przez pozostałe komórki przy ich zwiększonym zakresie zadań;
9) 1 etat w zakresie zapewnienia obsługi prawnej pozwalające na obsługę prawną procesów prowadzonych przez komórki merytoryczne (w tym ewentualnych postępowań sądowych), opracowywanie bieżących analiz prawnych i analiz systemowych oraz opracowywania interpretacji stosowania przepisów.

Analiza pracochłonności stanowi załącznik nr 1 do Oceny Skutków Regulacji.

Dodatkowo należy wskazać koszty związane z wyjazdami osób odpowiedzialnych za współpracę międzynarodową szacowane na 444 400,00 zł rocznie (założenie 4 osoby, 44 wyjazdy na rok, po dwa dni). Obejmują one wyjazdy zagraniczne w ramach współpracy z właściwymi podmiotami UE w zakresie realizacji zadań UMOL, w ramach współpracy w zakresie realizacji postanowień CER oraz spraw związanych z sprawami odporności w NATO.

Koszty stanowiska pracy

Dodatkowo jednostkowy koszt wyposażenia stanowiska pracy określono na 12 000 zł (laptop, dodatkowy monitor, telefon komórkowy). Przy uwzględnieniu zużycia sprzętu i konieczności jego wymiany proponuje się analogiczną kwotę ująć w budżecie co 5 lat.

Wykaz podmiotów krytycznych – system S46

Wykaz podmiotów krytycznych będzie prowadzony w systemie S46. Jest to system prowadzony przez ministra właściwego do spraw informatyzacji w celu współpracy podmiotów krajowego systemu cyberbezpieczeństwa. W tym systemie będzie prowadzony wykaz podmiotów kluczowych i podmiotów ważnych w rozumieniu dyrektywy NIS 2. Z tego powodu zasadne jest, aby w tym systemie prowadzony był także wykaz podmiotów krytycznych.
Szacunek kosztów realizacji zadania – prowadzenia wykazu podmiotów krytycznych w systemie S46 przedstawia się one następująco:

1) rok 2026: 1 875 tys. zł
2) rok 2027: 482 tys. zł
3) rok 2028: 497 tys. zł
4) rok 2029: 511 tys. zł
5) rok 2030: 527 tys. zł
6) rok 2031: 543 tys. zł
7) rok 2032: 559 tys. zł
8) rok 2033: 576 tys. zł
9) rok 2034: 593 tys. zł
10) rok 2035: 611 tys. zł
11) rok 2036: 629 tys. zł

Powyższe wydatki planowane są wyłącznie w ramach kosztów bieżących (paragraf 283), ze względu na możliwość wykorzystania istniejącej i obecnie rozbudowywanej infrastruktury systemu S46.

Koszty prowadzenia wykazu do spraw podmiotów krytycznych w ramach systemu S46 określa załącznik nr 2 do Oceny Skutków Regulacji.

<u>Centrum Bezpieczeństwa Morskiego</u>

Funkcję CBM będzie pełnić komórka organizacyjna Straży Granicznej utworzona przez Komendanta Głównego Straży Granicznej w wybranym oddziale Straży Granicznej.
Koszty dostosowania do realizacji zadań tego centrum będą wynosić szacunkowo 3 000 tys. zł. i wynikają one z konieczności przeprowadzenia robót budowlano-remontowych celem przystosowania budynku Straży Granicznej, w którym planuje się funkcjonowanie tej komórki organizacyjnej SG. Koszty te uwzględniają wykonanie robót branż: budowlanej, sanitarnej, elektrycznej, teletechnicznej i teleinformatycznej, w tym serwerowni, a także koszty mediów.
W związku z utworzeniem CBM nie jest planowane zwiększenie etatowe w Straży Granicznej. Funkcjonowanie tej komórki będzie zapewnione w ramach istniejącej struktury etatowej Straży Granicznej i nie pociągnie za sobą konieczności zwiększenia wydatków budżetu państwa w tym zakresie. Planowane jest zwiększenie etatowe w Straży Granicznej dotyczące funkcjonowania CBM, które zostanie zabezpieczone w ramach Programu Modernizacji Policji, Straży Granicznej, Państwowej Straży Pożarnej i Służby Ochrony Państwa na lata 2026–2029.

Krajowa Administracja Skarbowa – w związku z utworzeniem CBM nie jest planowane zwiększenie etatowe KAS.

Z kolei mając na uwadze, że projektowane przepisy przewidują instytucję oddelegowania innych funkcjonariuszy, żołnierzy lub pracowników do służby lub pracy w CBM, koszty tych oddelegowań, w tym wypłaty uposażeń albo wynagrodzeń oraz innych należności pieniężnych dla oddelegowanych będą pokrywane w ramach posiadanych zasobów kadrowych oraz limitów wydatków będących w dyspozycji danej służby lub podmiotu (wyjątek od powyższego stanowią urzędy morskie oraz Morska Służba Poszukiwania i Ratownictwa (Służba SAR), które w związku z potrzebą oddelegowania pracowników do CBM wymagają zwiększenia etatowego o 4 etaty w odniesieniu do urzędów morskich oraz o 4 etaty – Służba SAR).

W ramach części 21 budżetu państwa – gospodarka morska ujęto **8** etatów na realizacje zadań w ramach Centrum Bezpieczeństwa Morskiego (4 etaty – urzędy morskie, 4 etaty – Morska Służba Poszukiwania i Ratownictwa).

Analiza pracochłonności stanowi załącznik nr 1 do Oceny Skutków Regulacji.

Jednostkowe wyliczenie etatu – jako podstawę wyliczeń przyjęto stanowisko głównego specjalisty z wynagrodzeniem 12 768zł brutto miesięcznie. Dodatkowo należy uwzględnić koszty pracodawcy, tj. składkę na ubezpieczenie społeczne oraz składkę na Fundusz Pracy i Fundusz Solidarnościowy.
W kolejnych latach koszt pracownika wzrośnie (zgodnie ze wskaźnikami makroekonomicznymi) oraz z uwzględnieniem dodatkowego wynagrodzenia rocznego.

<u>Koszty stanowiska pracy</u>

Dodatkowo jednostkowy koszt wyposażenia stanowiska pracy określono na 12 000 zł (laptop, dodatkowy monitor, telefon komórkowy). Przy uwzględnieniu zużycia sprzętu i konieczności jego wymiany proponuje się analogiczną kwotę ująć w budżecie co 5 lat.

Przyznanie nowego zadania funkcjonariuszom Policji, Straży Granicznej, Służbie Ochrony Państwa oraz w stosownym zakresie pracownikom ochrony, polegającego na zniszczeniu lub unieruchomieniu bezzałogowego obiektu pływającego albo przejęciu nad nim kontroli nie będzie wpływało na zwiększenie z tego tytułu wydatków tych formacji. Koszty powstałe w tym zakresie będą pokrywane w ramach limitu wydatków oraz zasobów kadrowych poszczególnych formacji.

<u>Rządowa Agencja Rezerw Strategicznych</u>
Wskazanie konieczności wzrostu zatrudnienia wynikającego z nałożenia nowych zadań na Rządową Agencję Rezerw Strategicznych (dalej „Agencja"), co będzie miało bezpośredni wpływ na zwiększenie wydatków Agencji w tym zakresie.
W związku z rozszerzeniem zakresu zadań wynikających ze zmian legislacyjnych Agencja przeprowadzi optymalizację struktury organizacyjnej. Celem działań jest dostosowanie obecnego modelu funkcjonowania do nowych potrzeb. Pozwoli to na zwiększenie efektywności procesów oraz zapewnienie

ciągłości działania. Proponowane zmiany stworzą podstawy do rozwinięcia nowych kompetencji Agencji w obszarach: tworzenia i utrzymywania nowych rodzajów rezerw strategicznych oraz w zakresie uczestnictwa Agencji w procedurach związanych z międzynarodowymi mechanizmami przewidzianymi na wypadek sytuacji kryzysowych oraz zwiększenia elastyczności i sprawności w działaniach Agencji, poprzez zmodyfikowanie instytucji zadań powierzonych w celu szybkiego i sprawnego reagowania w sytuacjach kryzysowych.

W wyniku analizy zasobów oraz zakresu kompetencji przewiduje się konieczność zwiększenia zatrudnienia o 10 etatów, w szczególności z przeznaczeniem na realizację zadań takich, jak:

1) stworzenie struktur zarzadzania kryzysowego i włączenia ich w cały system zarządzania kryzysowego kraju. Doświadczenia ostatniej klęski żywiołowej dobitnie pokazują, iż istnieje konieczność wzmocnienia działania w zakresie reakcji na sytuacje kryzysowe. Agencja podjęła działania związane z budową struktur zarzadzania kryzysowego, ale pełna realizacji zadań jakie będą przed nią stawiane, wymaga wsparcia merytorycznego i osobowego;
2) rozszerzenie zakresu tworzenia i zarządzania rezerwami – planowanie rezerw na potrzeby ochrony ludności. W ramach tego zadania wystąpi konieczność pozyskiwania i przechowywanie rezerw strategicznych o pożądanej strukturze i ilości, w tym sprzętów i środków służących ochronie ludności, które określone zostaną przez organy i podmioty ochrony ludności;
3) współpraca międzyresortowa – Agencja będzie występowała jako podmiot ochrony ludności, który będzie współpracował z innymi organami administracji rządowej oraz służbami, inspekcjami i innymi jednostkami realizującymi zadania w zakresie bezpieczeństwa i obronności państwa, obrony cywilnej, zarządzania kryzysowego i ochrony infrastruktury krytycznej oraz bezpieczeństwa, porządku i zdrowia publicznego;
4) wsparcie systemu obrony cywilnej – zgodnie z przepisami prawa międzynarodowego, Agencja powinna stać się ośrodkiem eksperckim w zakresie zadań humanitarnych i ochrony ludności w czasie wojny;
5) prowadzenie i aktualizacja ewidencji zasobów – Agencji jako podmiot z zakresu ochrony ludności podległy Ministrowi właściwemu do spraw wewnętrznych będzie współuczestniczyła w uaktualnianiu Centralnej Ewidencji Zasobów, który we właściwy sposób musi zapewniać ochronę przed nieuprawnionym dostępem i w odpowiedni sposób przetwarzać dane, a co się z tym wiąże odpowiednią realizację zdań z zakresu cyberbezpieczeństwa;
6) realizacja Programu Ochrony Ludności i Obrony Cywilnej na lata 2025–2026, który przewiduje się m.in. modernizację infrastruktury krytycznej, budowę lub modernizację obiektów użyteczności publicznej, uzupełnienie magazynów oraz zakup sprzętu do prowadzenia działań w warunkach zagrożeń hybrydowych, chemicznych, biologicznych, radiacyjnych i nuklearnych. Powyższe stanowi części składowe budowanych od podstaw systemów państwa Polskiego w zakresie ochrony ludności i obrony cywilnej, który wpisywał się będzie w system odporności całej UE;
7) uczestnictwo w mechanizmach pomocowych, m.in. organizacji międzynarodowych, jak np. Unijny Mechanizm Ochrony Ludności - udział w realizowaniu przedsięwzięć związanych z bezpieczeństwem państwa oraz udzielaniem pomocy humanitarnej także na szczeblu międzynarodowym;
8) tworzenie rezerw strategicznych w obszarze utrzymywania wirtualnego środowiska informatycznego, które mogłoby być wykorzystywane w sytuacjach kryzysowych związanych z niepożądanymi działaniami w cyberprzestrzeni państwa i jego instytucji.

W ramach części 42 budżetu państwa – sprawy wewnętrzne ujęto 10 etatów na realizacje nowych zadań Rządowej Agencji Rezerw Strategicznych. Środki finansowe, pochodzące z rezerwy celowej budżetu państwa (poz. 56), na utworzenie 10 dodatkowych etatów na realizację zadań RARS zostaną przekazane przez MSWiA w formie dotacji podmiotowej.

Analiza pracochłonności stanowi załącznik nr 1 do Oceny Skutków Regulacji.

Jednostkowe wyliczenie etatu – jako podstawę wyliczeń przyjęto stanowisko głównego specjalisty z wynagrodzeniem 12 768zł brutto miesięcznie. Dodatkowo należy uwzględnić koszty pracodawcy, tj. składkę na ubezpieczenie społeczne oraz składkę na Fundusz Pracy i Fundusz Solidarnościowy.

W kolejnych latach koszt pracownika wzrośnie (zgodnie ze wskaźnikami makroekonomicznymi) oraz z uwzględnieniem dodatkowego wynagrodzenia rocznego.

Natomiast w przypadku modyfikacji katalogu rezerw (projektowany art. 4 ustawy o RARS) nie będzie to miało wpływu na wzrost wydatków budżetowych przeznaczonych na tworzenie i utrzymanie rezerw strategicznych. Minister Spraw Wewnętrznych i Administracji przedkłada bowiem Radzie Ministrów propozycje asortymentu poszczególnych rodzajów rezerw strategicznych w ramach przyznanych środków

	finansowych (ostatecznie to Rada Ministrów podejmuje decyzje co do wielkości dotacji oraz asortymentu rezerw strategicznych). **<u>Dochody Budżetu Państwa</u>** Jako dochody budżetu państwa należy wskazać udział budżetu państwa w podatku dochodowym od osób fizycznych na stałym poziomie 15%. Jako dochody JST należy wskazać udział JST w podatku dochodowym od osób fizycznych na stałym poziomie 85%.

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	W celu wdrożenia projektowanych przepisów przedsiębiorstwa muszą wdrożyć środki techniczne i organizacyjne proporcjonalne do wielkości podmiotu oraz rodzaju prowadzonej działalności. Przedsiębiorcy powinni oszacować swoje posiadane zasoby tak aby zbudować system bezpieczeństwa świadczonej usługi z ich wykorzystaniem, bez generowania nadmiernych kosztów. Przy budowie bezpieczeństwa usługi kluczowej niezbędne jest systematyczne szacowanie ryzyka wystąpienia incydentu oraz odpowiednie zarządzanie ryzykiem. Takie działanie pozwoli na wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych. Istotne będzie również zbudowanie obiegu informacji o incydentach lub możliwościach ich wystąpienia, zarządzania incydentami oraz stosowania środków zapobiegawczych jak również ograniczających wpływ incydentów na świadczenie usługi kluczowej.
	sektor mikro-, małych i średnich przedsiębiorstw	Brak możliwości oszacowania wpływu nowych regulacji na przedsiębiorców. Projekt oddziałuje na podmioty o zróżnicowanej wielkości – od małych do dużych przedsiębiorstw. Jakiej wielkości przedsiębiorstwa zostaną objęte reżimem ustawy – będzie to uzależnione od uzgodnienia parametrów progów istotności skutku zakłócającego.
	rodzina, obywatele oraz gospodarstwa domowe	Projektowane regulacje przyczynią się do zwiększenia bezpieczeństwa świadczenia usług, z których korzystają obywatele.
	osoby starsze i niepełnosprawne	Projektowane regulacje przyczynią się do zwiększenia bezpieczeństwa świadczenia usług, z których korzystają obywatele.
Niemierzalne		
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	Oszacowanie kosztów przedsiębiorców w zakresie dostosowania się do nowych regulacji nie jest możliwe. Środki techniczne i organizacyjne wdrażane przez przedsiębiorców będą uzależnione od oceny ryzyka, która będzie przeprowadzana dopiero po ujęciu przedsiębiorcy w wykazie podmiotów krytycznych w danym sektorze. Obecnie wielu przedsiębiorców, będących właścicielami lub posiadaczami infrastruktury krytycznej wdraża systemy zarządzania bezpieczeństwem lub ciągłością działania zgodnie z obowiązującymi w tym zakresie normami lub posiada certyfikację zgodności z tymi normami. Nakładane obowiązki na przedsiębiorców są konieczne i niezbędne dla osiągnięcia celów ustawy – należy uznać, iż została tu zachowana zasada proporcjonalności.	

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).	X tak ☐ nie ☐ nie dotyczy

☐ zmniejszenie liczby dokumentów ☐ zmniejszenie liczby procedur ☐ skrócenie czasu na załatwienie sprawy ☐ inne:	x zwiększenie liczby dokumentów x zwiększenie liczby procedur ☐ wydłużenie czasu na załatwienie sprawy ☐ inne:
Wprowadzane obciążenia są przystosowane do ich elektronizacji.	☐ tak ☐ nie ☐ nie dotyczy

Komentarz:
Ustawa powoduje zmianę kształtu obecnie opracowywanych dokumentów planistycznych. Krajowa Ocena Ryzyka zastąpi Raport o zagrożeniach bezpieczeństwa narodowego.
Przewiduje się cykliczne sporządzanie streszczenia istotnych elementów krajowej oceny ryzyka oraz streszczenia istotnych elementów krajowej oceny zdolności zarządzania ryzykiem.
Sporządzone zostaną w nowej formule plany zarządzania kryzysowego na wszystkich szczeblach administracji publicznej.

W odniesieniu do infrastruktury krytycznej – opracowane zostaną kryteria wyłaniania infrastruktury krytycznej.
Operator infrastruktury krytycznej będzie sporządzał raport o stanie ochrony infrastruktury krytycznej. W celu realizacji zadań w zakresie ochrony infrastruktury krytycznej - operatorzy powołają koordynatorów. Do uprawnień koordynatora, któremu operator zapewnia warunki do wykonywania zadań, zalicza się m.in. możliwość przedkładania rekomendacji organowi zarządzającemu operatora w zakresie ochrony jego obiektów, instalacji urządzeń i usług.
Ponadto przewidziano, iż operator infrastruktury krytycznej w związku z realizacją przedsięwzięć w zakresie ochrony jego obiektów, instalacji, urządzeń i usług zapewnia zdolność do ochrony informacji niejawnych. Należy bowiem przyjąć, że informacje wrażliwe wytworzone w ramach opracowywania, uzgadniania oraz realizacji dokumentacji dotyczącej ochrony infrastruktury krytycznej oraz informacje wymieniane z właściwymi organami administracji publicznej o zidentyfikowanych zagrożeniach lub zakłóceniach infrastruktury krytycznej oraz podejmowanych działaniach w celu jej ochrony lub odtworzenia, powinny być klasyfikowane jako informacje niejawne. Regulacja, zgodnie z postanowieniami ustawy o ochronie informacji niejawnych, pozostawia operatorom infrastruktury krytycznej decyzję co do sposobów zapewnienia ochrony informacji niejawnych, w zależności od poziomu niejawności wytwarzanych informacji.

W odniesieniu do podmiotów krytycznych w poszczególnych sektorach lub podsektorach – ze strony organów do spraw podmiotów krytycznych konieczne będzie:
1) wdrożenie procesów ich identyfikacji oraz ujmowania w odpowiednich wykazach;
2) prowadzenie wykazów, w tym ich bieżąca aktualizacja;
3) wdrożenie procedur audytu i kontroli podmiotów krytycznych;
4) wdrożenie procedur dotyczących nakładania kar na podmioty krytyczne.

Ze strony podmiotów krytycznych konieczne będzie wdrażanie rozwiązań związanych z bezpieczeństwem świadczenia usługi kluczowej czy też przeprowadzenie cyklicznych audytów.

9. Wpływ na rynek pracy

Projektowane rozwiązania wpłyną pozytywnie na rynek pracy. Nowe regulacje przewidują obowiązek wyznaczania przez podmioty krytyczne tzw. osób odpowiedzialnych za utrzymanie kontaktów z właściwymi organami do spraw podmiotów krytycznych oraz zapewnienie im organizacyjnych warunków realizacji funkcji. W praktyce przełoży się to na zwiększone zapotrzebowanie na usługi specjalistów z zakresu kompleksowego zapewnienia bezpieczeństwa oraz ciągłości świadczenia usług. Wpłyną one również pozytywnie na firmy świadczące usługi z zakresu audytu.

10. Wpływ na pozostałe obszary

☐ środowisko naturalne ☐ sytuacja i rozwój regionalny x sądy powszechne, administracyjne lub wojskowe	☐ demografia ☐ mienie państwowe ☐ inne:	☐ informatyzacja ☐ zdrowie
Omówienie wpływu	Projekt ustawy przewiduje nakładanie kar pieniężnych. Skargi na decyzje administracyjne w sprawie nałożenia kary będą rozpatrywały sądy administracyjne.	

11.Planowane wykonanie przepisów aktu prawnego

Wykonanie przepisów ustawy nastąpi po dniu jej wejścia w życie.

12. W jaki sposób i kiedy nastąpi ewaluacja efektów projektu oraz jakie mierniki zostaną zastosowane?

W odniesieniu do rozwiązań w obszarze planowania cywilnego - ewaluacja będzie odbywać się w formie ćwiczeń z zakresu zarządzania kryzysowego, testujących rozwiązania zawarte w dokumentach planistycznych oraz kontrole realizacji zadań/przedsięwzięć przeprowadzane przez uprawnione do tego podmioty (np. kontrole prowadzone przez NIK).

W przypadku rozwiązań dotyczących podmiotów krytycznych świadczących usługi kluczowe, możliwe do zastosowania mierniki to m.in. liczba podmiotów wpisanych do wykazu podmiotów krytycznych, liczba zgłoszonych incydentów istotnych w danym roku kalendarzowym, liczba przeprowadzonych audytów przez podmioty krytyczne oraz liczba nałożonych administracyjnych kar pieniężnych.
Powyższe mierniki powinny dać odpowiedź na pytanie, czy i w jaki sposób przepisy ustawy są stosowane.

Po dwóch latach od wejścia w życie projektowanych przepisów zostanie dokonana ocena efektywności realizacji zadań organów do spraw podmiotów krytycznych, uwzględniająca m.in. obciążenie pracą tych organów oraz kosztów poniesionych w związku z podejmowanymi działaniami. Wyniki tej oceny mogą stanowić podstawę do podjęcia działań związanych ze zwiększeniem liczby etatów przewidzianych na realizację zadań podmiotów krytycznych oraz zapewnieniem odpowiedniego poziomu finansowania kosztów funkcjonowania tychże organów.

13. Załączniki (istotne dokumenty źródłowe, badania, analizy itp.)

Analiza pracochłonności – załącznik nr 1.
Koszty wykazu podmiotów krytycznych w ramach systemu S46 – załącznik nr 2.
Rozbicie kosztów na poszczególne resorty oraz wyszczególnienie wydatków na wynagrodzenia osobowe oraz pozostałe wydatki – załącznik nr 3.

Załącznik nr 1 do Oceny Skutków Regulacji projektu ustawy o zmianie ustawy o zarządzaniu kryzysowym oraz niektórych innych ustaw (UC47)

ANALIZA PRACOCHŁONNOŚCI

Wojewodowie:

Założenia analizy pracochłonności uzasadniające potrzebę pozyskania nowych etatów na realizację nowych zadań:

- ✓ nowe zadania nie mogą być realizowane w ramach posiadanych etatów oraz przez zwiększenie zakresu obowiązków dostępnych pracowników;
- ✓ mając na względzie realizację nowych zadań – wymagają one pozyskania nowych pracowników posiadających specjalistyczną wiedzę, charakteryzujących się kreatywnością oraz umiejętnościami analizowania i proponowania efektywnych rozwiązań pojawiających się zagadnień. Doświadczeni pracownicy mogą wykonać realizacje zadań szybciej niż pracownicy z mniejszym doświadczeniem. Takie rozwiązanie obniża koszty związane z przystosowaniem mniej doświadczonych pracowników do realizacji nowych zadań (koszty szkoleń oraz czas potrzebny na wdrożenie w realizację zadań na odpowiednim poziomie);
- ✓ mając na względzie stopień automatyzacji procesów – zadanie będą wykonywane „ręcznie", bez wspomagania zaawansowanymi technologiami teleinformatycznymi, które umożliwiałyby wykonywanie zadań mniejsza liczbą pracowników. Brak środków finansowych na nowe narzędzia umożliwiające automatyzacje procesów generuje konieczność zatrudnienia dodatkowego personelu. Koszty zatrudnienia nowego personelu co do zasady będą mniejsze niż koszty „budowania" nowych narzędzi służących automatyzacji procesów;
- ✓ brak możliwości outsourcingu realizacji zadań.

Zgodnie z ustaleniami – wojewoda otrzymuje 3 etaty na realizacje nowych zadań. Takie rozwiązania zapewnia niezbędne minimum do realizacji nowych zadań przy braku generowania kosztów zwiększających deficyt budżetowy.

Wyliczenia pracochłonności opierają się na następujących parametrach:

Założenia dotyczące rocznej dostępności pracownika:

- ✓ liczba dni roboczych w roku – 252,
- ✓ urlop wypoczynkowy – 26 dni,
- ✓ średnia absencja chorobowa – 10 dni,
- ✓ szkolenia – 7 dni,
- ✓ faktyczna liczba dni pracy – 209,
- ✓ roczna pracochłonność – 209 dni × 8 h = 1 672 h,
- ✓ po uwzględnieniu odejścia od monitora (40 min/dzień × 209 = 139 h) 1 533 h/rok.

Rozbicie czynności niezbędnych do realizacji zadań i szacowana ich pracochłonność:

Czynność	Pracochłonność
Identyfikowanie infrastruktury krytycznej, w tym: ✓ występowanie do właściciela lub posiadacza obiektu, urządzenia, instalacji, sieci, systemu oraz usługi lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji, sieci, systemów oraz usług o ocenę czy posiadane aktywa spełniają warunki ich uznania za infrastrukturę krytyczną; ✓ prowadzenie dokumentacji prowadzonych postępowań; ✓ wizyty studyjne; ✓ opracowywanie wniosków do Dyrektora RCB o ujęcie obiektu, urządzenia, instalacji, sieci, systemu oraz usługi lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji, sieci, systemów oraz usług w wykazie infrastruktury krytycznej; ✓ prowadzenie postępowań administracyjnych w przypadku odmowy właściciela lub posiadacza w kwestii jego ujęcia w wykazie infrastruktury krytycznej; ✓ prowadzenie bieżącej wymiany informacji z innymi podmiotami w zakresie realizacji czynności w zakresie identyfikacji obiektów, urządzeń, instalacji, sieci, systemów oraz usług lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji, sieci, systemów oraz usług, które mogą zostać wpisane do wykazu infrastruktury krytycznej.	1000 h
Identyfikowanie potencjalnej infrastruktury krytycznej, w tym: ✓ występowanie do inwestora prowadzącego prace projektowe lub budowlane dotyczące potencjalnej infrastruktury o ocenę czy inwestycja spełnia warunki uznania za potencjalną infrastrukturę krytyczną; ✓ prowadzenie dokumentacji prowadzonych postępowań; ✓ wizyty studyjne; ✓ opracowywanie wniosków do Dyrektora RCB o ujęcie inwestycji w wykazie potencjalnej infrastruktury krytycznej; ✓ prowadzenie postępowań administracyjnych w przypadku odmowy inwestora w kwestii jego ujęcia w wykazie potencjalnej infrastruktury krytycznej; ✓ prowadzenie bieżącej wymiany informacji z innymi podmiotami dotyczących realizacji czynności w zakresie identyfikacji inwestycji, które mogą zostać wpisane do wykazu potencjalnej infrastruktury krytycznej.	200 h
Bieżąca wymiana informacji na temat zagrożeń dla bezpieczeństwa ochrony infrastruktury krytycznej, w tym: ✓ prowadzenie analiz zagrożeń dla lokalnej infrastruktury krytycznej o zagrożeniach zakłócających lub mogących zakłócić funkcjonowanie infrastruktury krytycznej; ✓ spodziewanych przerwach lub zakłóceniach w funkcjonowaniu infrastruktury krytycznej.	400 h
Udzielanie bieżących odpowiedzi na zapytania operatorów infrastruktury krytycznej lub interpretacji stosowania przepisów.	100 h
Analiza oświadczeń operatorów infrastruktury krytycznej o opracowaniu dokumentacji ochrony infrastruktury krytycznej, weryfikacja wdrożenia rozwiązań zawartych w dokumentacji	250 h
Prowadzenie uzgodnień z operatorami w przypadku braku możliwości wdrożenia rozwiązań, o których mowa w ustawie z uwzględnieniem minimalnych standardów.	250 h

Analiza corocznych niejawnych raportów o stanie ochrony infrastruktury krytycznej przekazywanego do wojewody przez każdego operatora i opracowanie zbiorczych raportów.	200 h
Prowadzenie działań informacyjnych dotyczących dobrych praktyk, działań edukacyjnych na rzecz poszerzania wiedzy w zakresie bezpieczeństwa oraz zapewnienia funkcjonowania infrastruktury krytycznej, w tym organizowanie konferencji, seminariów lub forów wymiany wiedzy.	250 h
Całodobowe zapewnienie obiegu informacji o zagrożeniach dla infrastruktury krytycznej oraz odbieranie od operatorów infrastruktury krytycznej informacji, o zakłóceniu funkcjonowania tej infrastruktury, które może skutkować wystąpieniem na wskazanym obszarze sytuacji kryzysowej.	2000 h
Suma	**4650 h**

Szacunkowa, łączna liczba godzin wyniosła 4650 h rocznie co przy założeniu dostępności pracownika 1533 h rocznie daje następujące wyliczenie potrzeb 4650/1533= 3,03 etatu. Proponowana liczba etatów – 3.

Organy do spraw podmiotów krytycznych

Założenia analizy pracochłonności uzasadniające potrzebę pozyskania nowych etatów na realizację nowych zadań:

- ✓ nowe zadania nie mogą być realizowane w ramach posiadanych etatów oraz przez zwiększenie zakresu obowiązków dostępnych pracowników;
- ✓ mając na względzie realizację nowych zadań – wymagają one pozyskania nowych pracowników posiadających specjalistyczną wiedzę, charakteryzujących się kreatywnością oraz umiejętnościami analizowania i proponowania efektywnych rozwiązań pojawiających się zagadnień. Doświadczeni pracownicy mogą wykonać realizacje zadań szybciej niż pracownicy z mniejszym doświadczeniem. Takie rozwiązanie obniża koszty związane z przystosowaniem mniej doświadczonych pracowników do realizacji nowych zadań (koszty szkoleń oraz czas potrzebny na wdrożenie w realizację zadań na odpowiednim poziomie);
- ✓ mając na względzie stopień automatyzacji procesów – zadanie będą wykonywane „ręcznie”, bez wspomagania zaawansowanymi technologiami teleinformatycznymi, które umożliwiałyby wykonywanie zadań mniejsza liczbą pracowników. Brak środków finansowych na nowe narzędzia umożliwiające automatyzacje procesów generuje konieczność zatrudnienia dodatkowego personelu. Koszty zatrudnienia nowego personelu co do zasady będą mniejsze niż koszty „budowania” nowych narzędzi służących automatyzacji procesów;
- ✓ brak możliwości outsourcingu realizacji zadań.

Zgodnie z ustaleniami – organ do spraw podmiotów krytycznych otrzymuje 3 etaty na prowadzenie spraw w obrębie jednego sektora. Takie rozwiązania zapewnia niezbędne minimum do realizacji nowych zadań przy braku generowania kosztów zwiększających deficyt budżetowy.

Wyliczenia pracochłonności opierają się na następujących parametrach:

Założenia dotyczące rocznej dostępności pracownika:

- ✓ liczba dni roboczych w roku – 252,
- ✓ urlop wypoczynkowy – 26 dni,

- ✓ średnia absencja chorobowa – 10 dni,
- ✓ szkolenia – 7 dni,
- ✓ faktyczna liczba dni pracy – 209,
- ✓ roczna pracochłonność – 209 dni × 8 h = 1 672 h,
- ✓ po uwzględnieniu odejścia od monitora (40 min/dzień × 209 = 139 h) 1 533 h/rok.

Rozbicie czynności niezbędnych do realizacji zadań i szacowana ich pracochłonność:

Czynność	**Pracochłonność**
Identyfikowanie infrastruktury krytycznej, w tym: ✓ występowanie do właściciela lub posiadacza obiektu, urządzenia, instalacji, sieci, systemu oraz usługi lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji, sieci, systemów oraz usług o ocenę czy posiadane aktywa spełniają warunki ich uznania za infrastrukturę krytyczną; ✓ prowadzenie dokumentacji prowadzonych postępowań; ✓ wizyty studyjne; ✓ opracowywanie wniosków do Dyrektora RCB o ujęcie obiektu, urządzenia, instalacji, sieci, systemu oraz usługi lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji, sieci, systemów oraz usług w wykazie infrastruktury krytycznej; ✓ prowadzenie postępowań administracyjnych w przypadku odmowy właściciela lub posiadacza w kwestii jego ujęcia w wykazie infrastruktury krytycznej; ✓ prowadzenie bieżącej wymiany informacji z innymi podmiotami w zakresie realizacji czynności w zakresie identyfikacji obiektów, urządzeń, instalacji, sieci, systemów oraz usług lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji, sieci, systemów oraz usług, które mogą zostać wpisane do wykazu infrastruktury krytycznej; ✓ prowadzenie bieżącej analizy infrastruktury krytycznej ujętej wykazie pod kątem niespełniania warunków ujęcia w wykazie, w tym wnioskowanie o jej usunięcie z wykazu.	400 h
Identyfikowanie potencjalnej infrastruktury krytycznej, w tym: ✓ występowanie do inwestora prowadzącego prace projektowe lub budowlane dotyczące potencjalnej infrastruktury o ocenę czy inwestycja spełnia warunki uznania za potencjalną infrastrukturę krytyczną; ✓ prowadzenie dokumentacji prowadzonych postępowań; ✓ wizyty studyjne; ✓ opracowywanie wniosków do Dyrektora RCB o ujęcie inwestycji w wykazie potencjalnej infrastruktury krytycznej;	100 h

✓ prowadzenie postępowań administracyjnych w przypadku odmowy inwestora w kwestii jego ujęcia w wykazie potencjalnej infrastruktury krytycznej; ✓ prowadzenie bieżącej wymiany informacji z innymi podmiotami dotyczących realizacji czynności w zakresie identyfikacji inwestycji, które mogą zostać wpisane do wykazu potencjalnej infrastruktury krytycznej; ✓ prowadzenie bieżącej analizy infrastruktury krytycznej ujętej wykazie pod kątem niespełniania warunków ujęcia w wykazie, w tym wnioskowanie o jej usunięcie z wykazu.	
Bieżąca wymiana informacji na temat zagrożeń dla bezpieczeństwa ochrony infrastruktury krytycznej, w tym: ✓ prowadzenie analiz zagrożeń dla lokalnej infrastruktury krytycznej o zagrożeniach zakłócających lub mogących zakłócić funkcjonowanie infrastruktury krytycznej; ✓ spodziewanych przerwach lub zakłóceniach w funkcjonowaniu infrastruktury krytycznej.	300 h
Udzielanie bieżących odpowiedzi na zapytania operatorów infrastruktury krytycznej lub interpretacji stosowania przepisów.	100 h
Analiza oświadczeń operatorów infrastruktury krytycznej o opracowaniu dokumentacji ochrony infrastruktury krytycznej, weryfikacja wdrożenia rozwiązań zawartych w dokumentacji.	100 h
Prowadzenie uzgodnień z operatorami w przypadku braku możliwości wdrożenia rozwiązań, o których mowa w ustawie z uwzględnieniem minimalnych standardów.	200 h
Analiza corocznych raportów o stanie ochrony infrastruktury krytycznej przekazywanego do wojewody przez każdego operatora i opracowanie zbiorczych raportów.	100 h
Prowadzenie działań informacyjnych dotyczących dobrych praktyk, działań edukacyjnych na rzecz poszerzania wiedzy w zakresie bezpieczeństwa oraz zapewnienia funkcjonowania infrastruktury krytycznej, w tym organizowanie konferencji, seminariów lub forów wymiany wiedzy.	150 h
Zapewnienie obiegu informacji o zagrożeniach dla infrastruktury krytycznej oraz odbieranie od operatorów infrastruktury krytycznej informacji, o zakłóceniu funkcjonowania tej infrastruktury, które może skutkować wystąpieniem na wskazanym obszarze sytuacji kryzysowej.	400 h
Prowadzenie bieżącej analizy operatorów infrastruktury krytycznej pod kątem uznania ich za podmiot krytyczny w danym sektorze lub podsektorze, w tym: ✓ występowanie do operatora infrastruktury krytycznej o udzielenie informacji, które umożliwią wstępną ocenę, czy spełnia warunki do uznania za podmiot krytyczny; ✓ prowadzenie dokumentacji prowadzonych postępowań; ✓ wizyty studyjne; ✓ opracowywanie wniosków do o ujęcie operatora infrastruktury krytycznej w wykazie podmiotów krytycznych;	400 h

✓ prowadzenie postępowań administracyjnych w przypadku odmowy inwestora w kwestii jego ujęcia w wykazie potencjalnej infrastruktury krytycznej; ✓ prowadzenie bieżącą analizę podmiotów krytycznych w danym sektorze lub podsektorze pod kątem niespełniania warunków kwalifikujących dany podmiot jako podmiot krytyczny; ✓ składanie wniosków o dokonanie wpisu do wykazu podmiotów krytycznych oraz wykreślenia z tego wykazu (w tym prowadzenie niezbędnej dokumentacji).	
Monitorowanie stosowania przepisów ustawy – udzielanie bieżących odpowiedzi na zapytania operatorów infrastruktury krytycznej lub interpretacji stosowania przepisów.	150 h
Prowadzenie bieżącej wymianę informacji z podmiotami krytycznymi oraz wprowadzanie mechanizmów ułatwiających dobrowolną wymianę informacji między podmiotami krytycznymi w danym sektorze lub podsektorze.	150 h
Wspieranie podmiotów krytycznych w zakresie wdrażania rozwiązań organizacyjno-technicznych zintegrowanego systemu zarządzania bezpieczeństwem świadczenia usługi kluczowej. Analiza sposobu wdrażania rozwiązań zawartych w zintegrowanym systemie bezpieczeństwa usługi kluczowej.	350 h
Ustalanie rodzajów certyfikatów oraz klauzul tajności niezbędnych do wdrażania rozwiązań w zakresie bezpieczeństwa usługi kluczowej oraz wytwarzania niezbędnej dokumentacji.	120 h
Analiza informacji o incydentach podmiotów krytycznych oraz incydentach mających wpływ na świadczenie usługi kluczowej oraz monitorowanie postępowania z incydentami.	300 h
Prowadzenie kontroli podmiotów krytycznych, w tym przygotowanie planów i programów kontroli, upoważnień oraz zawiadomień dotyczących kontroli.	2200 h
Prowadzenie działań informacyjnych dotyczących dobrych praktyk, działań edukacyjnych i kampanii na rzecz poszerzania wiedzy i budowania odporności podmiotów krytycznych.	150 h
Planowanie i organizowanie ćwiczeń podmiotów krytycznych oraz w udział w tych ćwiczeniach.	150 h
Opracowywanie stanowisk organu dla Pojedynczego Punktu Kontaktowego w celu zapewnienia współpracy z odpowiednimi organami państw członkowskich	120 h
Udział w procesach identyfikacji podmiotu krytycznego o szczególnym znaczeniu europejskim oraz obsługa tzw. misji doradczych.	150 h
Analiza audytów przeprowadzanych przez podmioty krytyczne oraz zlecenie audytów.	220 h
Prowadzenie postępowań w zakresie nakładania kar pieniężnych na podmiot krytyczny.	120 h
Suma	**6430 h**

Szacunkowa, łączna liczba godzin wyniosła 6430 h rocznie co przy założeniu dostępności pracownika 1533 h rocznie daje następujące wyliczenie 6430/1533= 4,2 etatu. Proponowana liczba etatów – 3.

Rządowe Centrum Bezpieczeństwa

Założenia analizy pracochłonności uzasadniające potrzebę pozyskania nowych etatów na realizację nowych zadań:

- ✓ nowe zadania nie mogą być realizowane w ramach posiadanych etatów oraz przez zwiększenie zakresu obowiązków dostępnych pracowników;
- ✓ mając na względzie realizację nowych zadań – wymagają one pozyskania nowych pracowników posiadających specjalistyczną wiedzę, charakteryzujących się kreatywnością oraz umiejętnościami analizowania i proponowania efektywnych rozwiązań pojawiających się zagadnień. Doświadczeni pracownicy mogą wykonać realizacje zadań szybciej niż pracownicy z mniejszym doświadczeniem. Takie rozwiązanie obniża koszty związane z przystosowaniem mniej doświadczonych pracowników do realizacji nowych zadań (koszty szkoleń oraz czas potrzebny na wdrożenie w realizację zadań na odpowiednim poziomie);
- ✓ mając na względzie stopień automatyzacji procesów – zadanie będą wykonywane „ręcznie", bez wspomagania zaawansowanymi technologiami teleinformatycznymi, które umożliwiałyby wykonywanie zadań mniejsza liczbą pracowników. Brak środków finansowych na nowe narzędzia umożliwiające automatyzacje procesów generuje konieczność zatrudnienia dodatkowego personelu. Koszty zatrudnienia nowego personelu co do zasady będą mniejsze niż koszty „budowania" nowych narzędzi służących automatyzacji procesów;
- ✓ brak możliwości outsourcingu realizacji zadań.

Wyliczenia pracochłonności opierają się na następujących parametrach:

Założenia dotyczące rocznej dostępności pracownika:

- ✓ liczba dni roboczych w roku – 252,
- ✓ urlop wypoczynkowy – 26 dni,
- ✓ średnia absencja chorobowa – 10 dni,
- ✓ szkolenia – 7 dni,
- ✓ faktyczna liczba dni pracy – 209,
- ✓ roczna pracochłonność – 209 dni × 8 h = 1 672 h,
- ✓ po uwzględnieniu odejścia od monitora (40 min/dzień × 209 = 139 h) 1 533 h/rok.

Rozbicie czynności niezbędnych do realizacji zadań i szacowana ich pracochłonność:

Wydział Oceny Ryzyka i Planowania

Czynność	**Pracochłonność**
Przygotowywanie, uzgadnianie oraz aktualizowanie Krajowej Oceny Ryzyka oraz dokonywanie analiz w zakresie jej wykorzystywania w planach zarządzania ryzykiem, planach reagowania kryzysowego oraz innych dokumentach opracowywanych przez organy administracji publicznej w zakresie zarządzania kryzysowego.	1100 h
Opracowanie i aktualizacja wytycznych do opracowywania Krajowej oceny Ryzyka.	600 h

Przygotowanie, uzgadnianie oraz aktualizacja Krajowego Planu Zarządzania Ryzykiem.	1200 h
Opracowanie i aktualizacja wytycznych do opracowywania Krajowego Planu Zarządzania Ryzykiem.	600 h
Uzgadnianie projektów planów zarządzania ryzykiem ministrów, kierowników urzędów centralnych pod względem spójności z Krajowym Planem Zarządzania Ryzykiem.	3200
Przygotowywanie, uzgadnianie oraz aktualizacja Krajowego Planu Reagowania Kryzysowego.	1200 h
Opracowanie i aktualizacja wytycznych do opracowywania Krajowego Planu Reagowania Kryzysowego.	600 h
Uzgadnianie projektów planów reagowania kryzysowego ministrów, kierowników urzędów centralnych pod względem spójności z Krajowym Planem Reagowania Kryzysowego.	3200 h
Cykliczne przedkładanie Komisji Europejskiej sprawozdań z realizacji zadań w zakresie zarządzania ryzykiem, w tym przekazywanie cyklicznych streszczeń istotnych elementów oceny ryzyka oraz istotnych elementów krajowej oceny zdolności zarządzania ryzykiem, wynikających z Krajowej Oceny Ryzyka oraz Krajowego Planu Zarządzania Ryzykiem.	480 h
Agregacja danych o stratach i szkodach spowodowanych przez zagrożenia wskazane w Krajowej Ocenie Ryzyka.	790 h
Zapewnienie spójności rozwiązań zawartych planach reagowania kryzysowego z planami ewakuacji ludności.	400 h
Suma	**13 370**

Szacunkowa, łączna liczba godzin wyniosła 13 370 h rocznie co przy założeniu dostępności pracownika 1533 h rocznie daje następujące wyliczenie 13 370/1533= 8,7 etatu. Proponowana liczba etatów – 5.

Wydział Ochrony Infrastruktury Krytycznej

Czynność	**Pracochłonność**
Opracowywanie Krajowej Oceny Ryzyka w zakresie podmiotów krytycznych	400 h
Opracowywanie kryteriów identyfikacji infrastruktury krytycznej (dokumenty niejawne) i ich aktualizacja.	300 h
Współpraca z ministrami kierującymi działami administracji rządowej, wojewodami oraz Komisją Nadzoru Finansowego w zakresie identyfikacji infrastruktury krytycznej, w tym prowadzenie bieżącą wymiany informacji dotyczących realizacji czynności w zakresie identyfikacji.	1200 h
Obsługa i weryfikacja wniosków o ujęcie zidentyfikowanej infrastruktury krytycznej w wykazie infrastruktury krytycznej.	300 h
Informowanie właścicieli lub posiadaczy o ujęciu ich infrastruktury w wykazie infrastruktury krytycznej.	150 h
Merytoryczne wsparcie w zakresie postępowań administracyjnych w przypadku odmowy właściciela lub posiadacza w kwestii jego ujęcia w wykazie infrastruktury krytycznej.	100 h
Prowadzenie wykazu infrastruktury krytycznej, w tym bieżąca aktualizacja wykazu (dokument niejawny).	500 h

Sporządzanie wyciągów z wykazu infrastruktury krytycznej oraz ich dystrybucja (dokumenty niejawne)	400 h
Współpraca z ministrami kierującymi działami administracji rządowej, wojewodami oraz Komisją Nadzoru Finansowego w zakresie identyfikacji potencjalnej infrastruktury krytycznej, tym prowadzenie bieżącą wymiany informacji dotyczących realizacji czynności w zakresie identyfikacji.	500 h
Obsługa i weryfikacja wniosków o ujęcie zidentyfikowanej potencjalnej infrastruktury krytycznej w wykazie infrastruktury krytycznej.	100 h
Informowanie inwestorów o ujęciu ich infrastruktury w wykazie potencjalnej infrastruktury krytycznej.	50 h
Merytoryczne wsparcie w zakresie postępowań administracyjnych w przypadku odmowy inwestora w kwestii jego ujęcia w wykazie potencjalnej infrastruktury krytycznej.	50 h
Prowadzenie wykazu potencjalnej infrastruktury krytycznej, w tym bieżąca aktualizacja wykazu (dokument niejawny).	50 h
Sporządzanie wyciągów z wykazu potencjalnej infrastruktury krytycznej oraz ich dystrybucja (dokumenty niejawne).	50 h
Ustalanie klauzul tajności oraz szczegółowych wymagań dotyczące ochrony informacji niejawnych związanych z realizacją przez operatora infrastruktury krytycznej przedsięwzięć związanych z ochroną tej infrastruktury.	100 h
Analiza oświadczeń operatorów infrastruktury krytycznej o opracowaniu dokumentacji ochrony infrastruktury krytycznej, weryfikacja wdrożenia rozwiązań zawartych w dokumentacji 250 h	400 h
Analiza raportów o stanie ochrony infrastruktury krytycznej	300 h
Wymiana informacji z koordynatorami ochrony infrastruktury krytycznej na temat zagrożeń dla bezpieczeństwa ochrony infrastruktury krytycznej, w tym prowadzenie analiz zagrożeń dla infrastruktury krytycznej o zagrożeniach zakłócających lub mogących zakłócić funkcjonowanie infrastruktury krytycznej lub spodziewanych przerwach lub zakłóceniach w funkcjonowaniu infrastruktury krytycznej, które mogą doprowadzić do sytuacji kryzysowej.	300 h
Udzielanie bieżących odpowiedzi na zapytania operatorów infrastruktury krytycznej lub interpretacji stosowania przepisów.	300 h
Prowadzenie działań informacyjnych dotyczących dobrych praktyk, działań edukacyjnych na rzecz poszerzania wiedzy w zakresie bezpieczeństwa oraz zapewnienia funkcjonowania infrastruktury krytycznej, w tym organizowanie konferencji, seminariów lub forów wymiany wiedzy.	400 h
Ustalanie klauzul tajności oraz szczegółowych wymagań dotyczących ochrony informacji niejawnych związanych z realizacją przez podmiot krytyczny przedsięwzięć związanych z zapewnieniem bezpieczeństwa świadczenia usługi kluczowej.	100 h
Zapewnienie funkcjonowania wykazu pomiotów krytycznych, w tym weryfikacja wniosków przedkładanych do tego wykazu.	300 h
Analizy incydentów zgłaszanych przez podmioty krytyczne.	200 h
Współdziałanie w zakresie obsługi incydentów.	300 h
Współpraca przy planowaniu i organizowaniu szkoleń i ćwiczeń podmiotów krytycznych.	100 h
Bieżąca współpraca z pełnomocnikami bezpieczeństwa usług kluczowych	150 h
Zapewnienie reprezentacji Rzeczypospolitej Polskiej w grupie PROCIV CER oraz w grupie CERG, w tym: ✓ analiza dokumentów;	250 h

✓ przygotowywanie stanowisk oraz uzgadnianie stanowisk krajowych z właściwymi podmiotami; ✓ udział w posiedzeniach.	
Zapewnienie reprezentacji Rzeczypospolitej Polskiej w Grupie do spraw Odporności Podmiotów Krytycznych, w tym: ✓ analiza dokumentów; ✓ przygotowywanie stanowisk oraz uzgadnianie stanowisk krajowych z właściwymi podmiotami; ✓ udział w posiedzeniach.	500 h
Zapewnienie wymiany informacji nt. incydentów istotnych przekazywanych za pośrednictwem z pojedynczych punktów kontaktowych w innych państwach członkowskich Unii Europejskiej; ✓ weryfikacja incydentów krajowych w kontekście oddziaływań międzynarodowych; ✓ ustalanie podmiotów zagranicznych, na które incydent może oddziaływać; ✓ wymiana informacji z partnerami zagranicznymi; ✓ udział w spotkaniach wielostronnych.	200 h
Cykliczne opracowywanie i przekazywanie Komisji Europejskiej oraz Grupie do spraw Odporności Podmiotów Krytycznych sprawozdań dotyczących incydentów istotnych zgłaszanych przez podmioty krytyczne mających wpływ na ciągłość świadczonych przez nich usług kluczowych na terytorium Rzeczypospolitej Polskiej oraz ciągłość świadczonych usług kluczowych w państwach członkowskich Unii Europejskiej (weryfikacja danych, ustalenie zakresu oddziałania, ustalenie interesariuszy, prowadzenie sprawozdawczości).	500 h
Przekazywanie zgłoszeń incydentów istotnych dotyczących innych państw członkowskich Unii Europejskiej do pojedynczych punktów kontaktowych tych państw (weryfikacja danych, ustalenie zakresu oddziałania, ustalenie interesariuszy, sprawozdawczość).	350 h
Zapewnienie współpracy z Komisją Europejską w obszarze zapewnienia bezpieczeństwa świadczenia usług kluczowych, w tym: ✓ analiza spójności usług kluczowych w relacjach bilateralnych ✓ identyfikacja infrastruktury niezbędnej do świadczenia usług kluczowych ✓ przygotowanie raportu.	200 h
Identyfikacja podmiotów krytycznych o szczególnym znaczeniu europejskim ✓ analiza raportów sporządzanych przed podmioty krytyczne pod kątem świadczenia usług w innych krajach ✓ identyfikacja usług o znaczeniu ponadkrajowym ✓ identyfikacja podmiotów o potencjalnym oddziaływaniu europejskim.	300 h
Obsługa misji doradczych Komisji Europejskiej	400 h
Koordynacja współpracy między organami do spraw podmiotów krytycznych i organami administracji publicznej w Rzeczypospolitej Polskiej z odpowiednimi organami w państwach członkowskich Unii Europejskiej;	300 h
Suma	**10 100 h**

Szacunkowa, łączna liczba godzin wyniosła 10 100 h rocznie co przy założeniu dostępności pracownika 1533 h rocznie daje następujące wyliczenie 10 100/1533= 6,6 etatu. Proponowana liczba etatów – 6.

Samodzielny Wydział Ochrony i Kontroli

Czynność	**Pracochłonność**
Wspólnie z Organem do spraw podmiotów krytycznych ustalenie właściwej klauzuli tajności oraz opracowanie szczegółowych wymagań dotyczących ochrony informacji niejawnych związanych z realizacją przez podmiot krytyczny (operatora IK) przedsięwzięć związanych z zapewnieniem bezpieczeństwa świadczenia usługi kluczowej.	300 h
Wykonywanie czynności związanych z nadzorem, kontrolą i doradztwem w zakresie ochrony informacji niejawnych w związku z wykonywaniem wykonywania zadań ochrony infrastruktury krytycznej.	500 h
Przygotowanie i utrzymanie systemu teleinformatycznego służącego do przetwarzania informacji niejawnych, na którym będzie prowadzony „Wykaz infrastruktury krytycznej", o którym mowa u Ustawie.	400 h
Przygotowanie i utrzymanie niejawnego systemu teleinformatycznego do prowadzenia przez dyrektora Centrum, Pojedynczego Punktu Kontaktowego w zakresie zadań związanych z: ✓ odbieraniem zgłoszeń incydentów istotnych z pojedynczych punktów kontaktowych w innych państwach członkowskich Unii Europejskiej; ✓ przekazywanie zgłoszeń incydentów istotnych dotyczących innych państw członkowskich Unii Europejskiej do pojedynczych punktów kontaktowych tych państw; ✓ zapewnienie wymiany informacji na potrzeby Grupy Współpracy, o której mowa w dyrektywie (UE) 2022/2555 oraz organów właściwych do spraw cyberbezpieczeństwa; ✓ współpraca z pojedynczym punktem kontaktowym, o którym mowa w ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.	1100 h
Utrzymanie i rozbudowa systemu teleinformatycznego służącego do wymiany informacji niejawnych pomiędzy podmiotami zarządzania kryzysowego a Operatorami Infrastruktury Krytycznej i Podmiotami Krytycznymi.	1100 h
Obsługa kancelaryjna dokumentacji niejawnej z korespondencji pomiędzy podmiotami zarządzania kryzysowego a operatorami infrastruktury krytycznej i podmiotami krytycznymi.	100 h
Suma	**3500 h**

Szacunkowa, łączna liczba godzin wyniosła 3500 h rocznie co przy założeniu dostępności pracownika 1533 h rocznie daje następujące wyliczenie 3500/1533= 2,3 etatu. Proponowana liczba etatów – 2.

Wydział Polityki Informacyjnej

Czynność	**Pracochłonność**
Przygotowanie i prowadzenie programów edukacyjnych oraz materiałów informacyjnych, w tym promowanie działań zwiększających świadomość na	1320 h

temat zagrożeń zidentyfikowanych w Krajowej Ocenie Ryzyka oraz sposobów reagowania na incydenty.	
Współpraca z partnerami instytucjonalnymi i organizacjami pozarządowymi.	424 h
Opracowywanie i aktualizowanie scenariuszy ćwiczeń i materiałów szkoleniowych dla personelu operatorów infrastruktury krytycznej lub podmiotów krytycznych odpowiedzialnego za bezpieczeństwo i ciągłość działania oraz organów zarządzania kryzysowego.	1032 h
Analizy skuteczności działań edukacyjnych i rekomendacje.	652 h
Zapewnienie koordynacji polityki informacyjnej w przypadkach incydentów związanych z bezpieczeństwem infrastruktury krytycznej oraz zakłóceniach świadczenia usług kluczowych realizowanych przez podmioty krytyczne.	440 h
Suma	**3868 h**

Szacunkowa, łączna liczba godzin wyniosła 3868 h rocznie co przy założeniu dostępności pracownika 1533 h rocznie daje następujące wyliczenie 3868/1533=2,5 etatu. Proponowana liczba etatów – 2.

Centrum Operacyjno-Analityczne

Czynność	**Pracochłonność**
Monitorowanie potencjalnych zagrożeń zidentyfikowanych w Krajowej Ocenie Ryzyka we współpracy z organami zarządzania kryzysowego, właściwymi służbami, operatorami infrastruktury krytycznej oraz podmiotami krytycznymi wraz z samodzielną weryfikacją pozyskiwanych danych na podstawie monitorowania dostępnej przestrzeni informacyjnej.	3180 h
Utrzymywanie całodobowej wymiany informacji z organami zarządzania kryzysowego, właściwymi służbami, operatorami infrastruktury krytycznej oraz podmiotami krytycznymi (poprzez bezpieczną łączność telefoniczną oraz teleinformatyczne systemy niejawne) w zakresie monitorowania zagrożeń zidentyfikowanych w Krajowej Ocenie Ryzyka, w szczególność tych, które skutkują lub mogą skutkować wystąpieniem sytuacji kryzysowej. Bieżąca wymiana informacji na temat zagrożeń dla bezpieczeństwa ochrony infrastruktury krytycznej, w tym: ✓ prowadzenie analiz zagrożeń dla lokalnej infrastruktury krytycznej o zagrożeniach zakłócających lub mogących zakłócić funkcjonowanie infrastruktury krytycznej; ✓ spodziewanych przerwach lub zakłóceniach w funkcjonowaniu infrastruktury krytycznej. Prowadzenie stałej kontroli poprawności działania kanałów łączności służących do wymiany informacji z krajowymi organami i strukturami zarządzania kryzysowego oraz operatorami infrastruktury krytycznej i podmiotami krytycznymi, w tym systematyczna weryfikacja danych kontaktowych.	1140 h
Uruchamianie procedur wskazanych w Krajowym Planie Reagowania Kryzysowego.	720 h

Analiza informacji o incydentach podmiotów krytycznych oraz incydentach mających wpływ na świadczenie usługi kluczowej mogących skutkować wystąpieniem sytuacji kryzysowej.	340 h
Natychmiastowe informowanie Kierownictwa KPRM, MSWiA oraz innych organów wchodzących w skład struktury zarządzania kryzysowego na szczeblu krajowym, a także służb dyżurnych resortów i służb o zagrożeniach, w szczególności zidentyfikowanych w Krajowej Ocenie Ryzyka, mogących skutkować potencjalną sytuacją kryzysową lub wystąpieniem takiej sytuacji.	690 h
Planowanie i wdrażanie szkoleń i ćwiczeń w celu prawidłowego stosowania i weryfikacji procedur zawartych w Krajowym Planie Reagowania Kryzysowego. Bezpośredni udział szkoleniach i ćwiczeniach z udziałem organów zarządzania kryzysowego, właściwych służb oraz operatorów infrastruktury krytycznej i podmiotów krytycznych.	1340 h
Opracowywanie dobrych praktyk (i ich aktualizowanie) dla operatorów infrastruktury krytycznej i podmiotów krytycznych w zakresie raportowania o zagrożeniach mogących skutkować potencjalną sytuacją kryzysową lub w przypadku jej wystąpienia.	360 h
Rezerwa operacyjna na zdarzenia nieprzewidziane, w tym reagowanie w sytuacjach kryzysowych.	1 040 h
Suma	**8810 h**

Szacunkowa, łączna liczba godzin wyniosła 8810 h rocznie co przy założeniu dostępności pracownika 1533 h rocznie daje następujące wyliczenie 8810/1533= 5,7 etatu. Proponowana liczba etatów – 4.

Wydział Współpracy Międzynarodowej

Czynność	**Pracochłonność**
Koordynacja udziału przedstawicieli Rzeczypospolitej Polskiej w pracach Komitetu do spraw Odporności Organizacji Traktatu Północnoatlantyckiego oraz zapewnienie wsparcie merytoryczne prowadzonych prac, w tym opracowywanie analiz, opinii i rekomendacji. Koordynacja terminów i uczestników spotkań z partnerami z krajów członkowskich NATO.	520 h
Koordynacja opracowywania oraz przedstawianie Komitetowi Odporności NATO stanowisk narodowe w sprawach będących przedmiotem prac tego Komitetu. Uzgadnianie stanowisk narodowych z właściwymi organami administracji rządowej.	500 h
Uczestnictwo w posiedzeniach plenarnych Komitetu Odporności Organizacji Traktatu Północnoatlantyckiego.	180 h
Udział w pracach grup roboczych Komitetu Odporności Organizacji Traktatu Północnoatlantyckiego.	320 h
Bieżąca wymiana informacji ze Stałym Przedstawicielstwem Rzeczypospolitej Polskiej przy NATO, w zakresie prac Komitetu Odporności NATO;	300 h

Zapewnienia funkcjonowanie punktu kontaktowego do przekazywania zadań oraz uruchamiania procedur wynikających z członkostwa Rzeczypospolitej Polskiej w Organizacji Traktatu Północnoatlantyckiego, w tym: ✓ implementacja środków reagowania kryzysowego (wymiana informacji Polska – NATO oraz uzgadnianie stanowisk z właściwymi organami administracji rządowej); ✓ opracowywanie nowych i aktualizacja obowiązujących procedur we współpracy z właściwymi organami NATO oraz uzgadnianie stanowisk w tym zakresie z właściwymi organami administracji rządowej)	1250 h
Suma	**3070 h**

Szacunkowa, łączna liczba godzin wyniosła 3070 h rocznie co przy założeniu dostępności pracownika 1533 h rocznie daje wyliczenie 3070/1533= 2,0 etatu. Proponowana liczba etatów – 2.

Wydział Informatyki i Łączności

Czynność	**Pracochłonność**
Monitorowanie systemów zapewniających całodobową wymianę informacji na potrzeby organów administracji rządowej, operatorów infrastruktury krytycznej oraz podmiotów krytycznych, w tym: ✓ monitoring logów i zdarzeń z systemów bezpieczeństwa; ✓ wykrywanie nietypowych aktywności i potencjalnych zagrożeń.	560 h
Analiza incydentów, w tym: ✓ identyfikacja i klasyfikacja incydentów bezpieczeństwa; ✓ ocena wpływu incydentu na organizację; ✓ korelacja danych z różnych źródeł w celu ustalenia przyczyny i zakresu naruszenia.	380 h
Reagowanie na incydenty: ✓ podejmowanie działań mających na celu ograniczenie skutków incydentu; ✓ dokumentowanie przebiegu incydentu i działań naprawczych.	285 h
Raportowanie, w tym: ✓ tworzenie raportów z incydentów; ✓ udział w tworzeniu statystyk i analiz trendów zagrożeń.	195 h
Utrzymywanie i rozwój narzędzi niezbędnych do zarządzania informacjami i zdarzeniami dotyczącymi bezpieczeństwa - konfiguracja i optymalizacja systemów, w tym wdrażanie nowych reguł i alertów oraz testowanie i aktualizacja narzędzi wykrywających zagrożenia.	290 h
Edukacja, w tym udział w szkoleniach i ćwiczeniach z zakresu reagowania na incydenty oraz edukowanie użytkowników w zakresie cyberbezpieczeństwa.	190 h
Zarządzanie infrastrukturą sieciową, w tym: ✓ konfiguracja i utrzymanie urządzeń sieciowych: routerów, switchy, firewalli, itp. ✓ monitorowanie wydajności sieci i optymalizacja jej działania; ✓ zarządzanie adresacją IP, VLAN-ami, DNS, itp.	580 h
Zapewnienie bezpieczeństwa sieci służących realizacji wymiany informacji z operatorami infrastruktury krytycznej oraz podmiotów krytycznych, w tym: ✓ wdrażanie polityk bezpieczeństwa (np. segmentacja sieci, kontrola dostępu);	385 h

✓ aktualizacja oprogramowania i firmware'u urządzeń sieciowych; ✓ wykrywanie i reagowanie na zagrożenia (np. ataki DDoS, nieautoryzowany dostęp).	
Rozwiązywanie bieżących problemów, w tym: ✓ diagnozowanie i usuwanie awarii sieciowych; ✓ wsparcie techniczne dla użytkowników i zespołów IT; ✓ analiza logów i raportów z systemów monitorujących.	280 h
Zarządzanie dostępem, w tym: ✓ konfiguracja VPN, sieci Wi-Fi, połączeń zdalnych; ✓ utrzymywanie kontroli nad dostępem do zasobów sieciowych; ✓ obsługa systemów uwierzytelniania.	195 h
Dokumentowanie działań i raportowanie: ✓ tworzenie i aktualizacja dokumentacji technicznej sieci; ✓ raportowanie stanu sieci, incydentów i zmian w infrastrukturze.	190 h
Planowanie i rozwój, w tym: ✓ projektowanie nowych segmentów sieci; ✓ wdrażanie nowych technologii i rozwiązań; ✓ udział w planowaniu budżetu IT i zakupie sprzętu sieciowego.	295 h
Wsparcie użytkowników, w tym: ✓ odbieranie zgłoszeń (telefonicznie, mailowo, przez system ticketowy); ✓ pomoc w rozwiązywaniu problemów z oprogramowaniem, sprzętem, dostępem do systemów; ✓ udzielanie instrukcji i porad technicznych.	670 h
Rejestrowanie i klasyfikacja zgłoszeń, w tym: ✓ tworzenie zgłoszeń w systemie zarządzania incydentami; ✓ kategoryzowanie problemów według priorytetu i rodzaju; ✓ przekazywanie bardziej złożonych zgłoszeń do drugiej lub trzeciej linii wsparcia.	290 h
Rozwiązywanie bieżących problemów, w tym: ✓ resetowanie haseł, konfiguracja poczty, instalacja podstawowego oprogramowania; ✓ rozwiązywanie problemów z drukarkami, siecią, dostępem do zasobów; ✓ pomoc przy aktualizacjach systemów i aplikacji.	385 h
Zarządzanie sprzętem i oprogramowaniem, w tym: ✓ przygotowanie i konfiguracja komputerów dla nowych pracowników; ✓ inwentaryzacja sprzętu IT; ✓ udzielanie wsparcia przy wdrażaniu nowych narzędzi i systemów	190 h
Edukacja użytkowników, w tym: ✓ informowanie o dobrych praktykach bezpieczeństwa (np. phishing, silne hasła); ✓ pomoc w korzystaniu z systemów firmowych (np. CRM, ERP, Teams);	190 h
Monitorowanie i raportowanie, w tym: ✓ śledzenie statusu zgłoszeń i czasu ich realizacji; ✓ raportowanie najczęstszych problemów i sugestii usprawnień; ✓ współpraca z zespołami IT w celu poprawy jakości usług.	190 h
Suma	**5740 h**

Szacunkowa, łączna liczba godzin wyniosła 5740 h rocznie co przy założeniu dostępności pracownika 1533 h rocznie daje następujące wyliczenie 5740/1533= 3,7 etatu. Proponowana liczba etatów – 3.

Wydział Administracyjno-Finansowy

Czynność	**Pracochłonność**
Zapewnienie obsługi kadrowej, w tym: ✓ sporządzanie listy płac; ✓ obsługa ZUS (Płatnik, zgłoszenia, deklaracje); ✓ obsługa PPK; ✓ obsługa urlopów i zwolnień lekarskich; ✓ wystawianie zaświadczeń i dokumentów; ✓ aktualizacja danych pracowników; ✓ prowadzenie rekrutacji nowych pracowników; ✓ sporządzanie raportów kadrowo-płacowych; ✓ szkolenia BHP i medycyna pracy; ✓ archiwizacja dokumentów, porządkowanie akt osobowych; ✓ obsługa systemu kadrowo-płacowego.	1764 h
Obsługa finansowa, w tym: ✓ rozliczanie podróży służbowych (krajowe i zagraniczne); ✓ rozliczanie faktur zakupowych; ✓ obsługa wniosków zakupowych; ✓ realizacja przelewów płatności; ✓ przelewy wynagrodzeń; ✓ prowadzenie sprawozdawczości budżetowej; ✓ ewidencja księgowa dokumentów; ✓ uzgadnianie kont księgowych; ✓ obsługa systemu finansowo-księgowego; ✓ rezerwa operacyjna (audyt, kontrole); ✓ przygotowanie danych do Planu Rzeczowo-Finansowego.	1580 h
Zabezpieczenie logistyczne, w tym: ✓ realizacja zakupów/ obsługa zamówień publicznych; ✓ magazynowanie zasobów oraz monitorowanie potrzeb; ✓ organizowanie serwisów i napraw; ✓ zapewnienie funkcjonowania kolumny transportowej;	1790 h

✓ zabezpieczenie logistyczne organizacji spotkań, konferencji, forów, wizyt.	
Suma	**5134 h**

Szacunkowa, łączna liczba godzin wyniosła 5134 h rocznie co przy założeniu dostępności pracownika 1533 h rocznie daje następujące wyliczenie 5134/1533= 3,3 etatu. Proponowana liczba etatów – 3.

Obsługa prawna

Czynność	**Pracochłonność**
Prowadzenie postępowań administracyjnych, w tym: ✓ przygotowywanie dokumentacji formalnej (wnioski, decyzje, zawiadomienia); ✓ reprezentowanie jednostki przed sądami administracyjnymi; ✓ udział w rozprawach i czynnościach procesowych; ✓ monitorowanie terminów i procedur zgodnie z KPA; ✓ współpraca z komórkami merytorycznymi w zakresie ustaleń stanu faktycznego i materiałów dowodowych.	650 h
Interpretacja przepisów prawnych, w tym: ✓ analizy obowiązujących aktów prawnych (ustawy, rozporządzenia, dyrektywy UE); ✓ wydawanie opinii prawnych na potrzeby operatorów infrastruktury krytycznej oraz podmiotów krytycznych; ✓ monitoring zmian w przepisach oraz informowanie o ich ewentualnych skutkach; ✓ opracowywanie analiz i rekomendacji dotyczących funkcjonowania infrastruktury krytycznej w Polsce oraz Unii Europejskiej w tym rozwiązań prawnych oraz organizacyjnych.	570 h
Opracowywanie oraz opiniowanie aktów normatywnych w zakresie ochrony infrastruktury krytycznej oraz podmiotów krytycznych, w tym: ✓ zapewnienie zgodności projektów aktów prawnych przygotowywanych w RCB z obowiązującym w Rzeczypospolitej Polskiej systemem prawnym oraz zasadami techniki prawodawczej, a także koordynowanie procesu ich uzgadniania; ✓ koordynacja opracowywania projektów stanowisk: ▪ rządu wobec przekazanych dyrektorowi RCB innych niż rządowe projektów ustaw, ▪ dyrektora RCB wobec przekazanych dyrektorowi RCB do uzgodnienia projektów aktów prawnych przygotowywanych przez naczelne i centralne organy administracji rządowej; ✓ przygotowywanie dla kierownictwa RCB materiałów analitycznych dotyczących projektów aktów prawnych rozpatrywanych przez Stały Komitet Rady Ministrów, Radę Ministrów oraz komisje sejmowe i senackie.	400 h
Suma	**1620 h**

Szacunkowa, łączna liczba godzin wyniosła 1620 h rocznie co przy założeniu dostępności pracownika 1533 h rocznie daje następujące wyliczenie 1620/1533= 1,0 etatu. Proponowana liczba etatów – 1.

Centrum Bezpieczeństwa Morskiego

Założenia analizy pracochłonności uzasadniające potrzebę pozyskania nowych etatów na realizację nowych zadań:

- ✓ nowe zadania nie mogą być realizowane w ramach posiadanych etatów oraz przez zwiększenie zakresu obowiązków dostępnych pracowników;
- ✓ mając na względzie realizację nowych zadań – wymagają one pozyskania nowych pracowników posiadających specjalistyczną wiedzę, charakteryzujących się kreatywnością oraz umiejętnościami analizowania i proponowania efektywnych rozwiązań pojawiających się zagadnień. Doświadczeni pracownicy mogą wykonać realizacje zadań szybciej niż pracownicy z mniejszym doświadczeniem. Takie rozwiązanie obniża koszty związane z przystosowaniem mniej doświadczonych pracowników do realizacji nowych zadań (koszty szkoleń oraz czas potrzebny na wdrożenie w realizację zadań na odpowiednim poziomie);
- ✓ mając na względzie stopień automatyzacji procesów – zadanie będą wykonywane „ręcznie", bez wspomagania zaawansowanymi technologiami teleinformatycznymi, które umożliwiałyby wykonywanie zadań mniejsza liczbą pracowników. Brak środków finansowych na nowe narzędzia umożliwiające automatyzacje procesów generuje konieczność zatrudnienia dodatkowego personelu. Koszty zatrudnienia nowego personelu co do zasady będą mniejsze niż koszty „budowania" nowych narzędzi służących automatyzacji procesów;
- ✓ brak możliwości outsourcingu realizacji zadań.

Wyliczenia pracochłonności opierają się na następujących parametrach:

Założenia dotyczące rocznej dostępności pracownika:

- ✓ liczba dni roboczych w roku – 252,
- ✓ urlop wypoczynkowy – 26 dni,
- ✓ średnia absencja chorobowa – 10 dni,
- ✓ szkolenia – 7 dni,
- ✓ faktyczna liczba dni pracy – 209,
- ✓ roczna pracochłonność – 209 dni × 8 h = 1 672 h,
- ✓ po uwzględnieniu odejścia od monitora (40 min/dzień × 209 = 139 h) 1 533 h/rok.

Rozbicie czynności niezbędnych do realizacji zadań i szacowana ich pracochłonność:

Czynność	**Pracochłonność**
Monitoring zagrożeń na podstawie dostępnych systemów monitorowania oraz śledzenie zewnętrznych źródeł informacji o zagrożeniach.	2000 h
Zapewnienie całodobowego obiegu informacji m.in. związanych z przyjmowaniem zgłoszeń o incydentów od operatorów infrastruktury krytycznej. oraz ich klasyfikowanie. Dokumentowanie przebiegu incydentów zgłaszanych przez operatorów infrastruktury krytycznej oraz prowadzonych działań naprawczych. Przekazywanie informacji do właściwych organów oraz służb, w tym Ministra Obrony Narodowej, Szefa Służby Kontrwywiadu Wojskowego, Szefa Agencji Bezpieczeństwa Wewnętrznego, Szefa Agencji Wywiadu, Komendanta	3200 h

Głównego Policji, Komendanta Głównego Państwowej Straży Pożarnej, Dyrektora Morskiej Służby Poszukiwania i Ratownictwa (Służby SAR), dyrektorów urzędów morskich oraz właściwych terytorialnie wojewodów i operatorów infrastruktury krytycznej.	
Analiza zagrożeń lub zdarzeń, w tym tworzenie cyklicznych raportów oraz raportów ad hoc.	3100 h
Formułowanie rekomendacji w zakresie bezpieczeństwa infrastruktury krytycznej z uwzględnieniem analizy incydentów, w odniesieniu do identyfikacji przyczyn wystąpienia (ustalenie stanu faktycznego, przede wszystkim źródła zagrożenia) oraz wskazanie rozwiązań technicznych i proceduralnych ograniczających możliwość wystąpienia incydentów w przyszłości.	2 300 h
Współpracy z właściwymi organami (punktami kontaktowymi) innych państw, ustalanie sposobów wspólnego przeciwdziałania zagrożeniom oraz korelacja wspólnych działań.	2000 h
Suma	**12 600 h**

Szacunkowa, łączna liczba godzin wyniosła 12 600 h rocznie co przy założeniu dostępności pracownika 1533 h rocznie daje następujące wyliczenie 12 600/1533= 8,2 etatu. Proponowana liczba etatów – 8.

Rządowa Agencja Rezerw Strategicznych

Założenia analizy pracochłonności uzasadniające potrzebę pozyskania nowych etatów na realizację nowych zadań:

- ✓ nowe zadania nie mogą być realizowane w ramach posiadanych etatów oraz przez zwiększenie zakresu obowiązków dostępnych pracowników;
- ✓ mając na względzie realizację nowych zadań – wymagają one pozyskania nowych pracowników posiadających specjalistyczną wiedzę, charakteryzujących się kreatywnością oraz umiejętnościami analizowania i proponowania efektywnych rozwiązań pojawiających się zagadnień. Doświadczeni pracownicy mogą wykonać realizacje zadań szybciej niż pracownicy z mniejszym doświadczeniem. Takie rozwiązanie obniża koszty związane z przystosowaniem mniej doświadczonych pracowników do realizacji nowych zadań (koszty szkoleń oraz czas potrzebny na wdrożenie w realizację zadań na odpowiednim poziomie);
- ✓ mając na względzie stopień automatyzacji procesów – zadanie będą wykonywane „ręcznie", bez wspomagania zaawansowanymi technologiami teleinformatycznymi, które umożliwiałyby wykonywanie zadań mniejsza liczbą pracowników. Brak środków finansowych na nowe narzędzia umożliwiające automatyzacje procesów generuje konieczność zatrudnienia dodatkowego personelu. Koszty zatrudnienia nowego personelu co do zasady będą mniejsze niż koszty „budowania" nowych narzędzi służących automatyzacji procesów;
- ✓ brak możliwości outsourcingu realizacji zadań.

Zgodnie z ustaleniami – RARS otrzymuje 10 etatów na realizację nowych zadań. Takie rozwiązania zapewnia niezbędne minimum do realizacji nowych zadań przy braku generowania kosztów zwiększających deficyt budżetowy.

Wyliczenia pracochłonności opierają się na następujących parametrach:

Założenia dotyczące rocznej dostępności pracownika:

- ✓ liczba dni roboczych w roku – 252,
- ✓ urlop wypoczynkowy – 26 dni,
- ✓ średnia absencja chorobowa – 10 dni,
- ✓ szkolenia – 7 dni,
- ✓ faktyczna liczba dni pracy – 209,
- ✓ roczna pracochłonność – 209 dni × 8 h = 1 672 h,
- ✓ po uwzględnieniu odejścia od monitora (40 min/dzień × 209 = 139 h) 1 533 h/rok.

Rozbicie czynności niezbędnych do realizacji zadań i szacowana ich pracochłonność:

Czynność	**Pracochłonność**
Stworzenie struktur zarządzania kryzysowego - integracja z system zarządzania kryzysowego kraju, w szczególności włączenie RARS w system wymiany bieżącej informacji z RCB i centrami zarządzania kryzysowego wojewodów o sytuacji kryzysowej i posiadanych zasobach oraz możliwościach ich wykorzystania w sytuacjach kryzysowych i nadzwyczajnych Stała współpraca z MSWiA, MON i RCB w zakresie monitorowania oceny zagrożeń występujących w otoczeniu krajowym i zagranicznym, gromadzenie danych i przygotowywanie cyklicznych analiz o dostępnych zasobach strategicznych i prognozowanym zapotrzebowaniu, uwzględnianie oceny ryzyka i Strategii Oporności Podmiotów Krytycznych w planowaniu rezerw, aktualizacja procedur działania zgodnie z wytycznym.	1560 h
Zarządzanie nowymi kategoriami rezerw (wirtualne środowisko informatyczne, fizyczne i wirtualne zasoby teleinformatyczne) – pozyskiwanie, ewidencja, zabezpieczenie cyfrowych zasobów, współpraca z dostawcami usług chmurowych i operatorami infrastruktury krytycznej. Zadanie ustawowe rozszerzające katalog rezerw strategicznych, działania długofalowe, wymagane są specjalistyczne kompetencje IT/cyberbezpieczeństwa oraz procedury ochrony informacji niejawnych.	3130 h
Udostępnianie wirtualnego środowiska informatycznego i zasobów teleinformatycznych – obsługa umów, monitorowanie wykorzystania i zwrotu zasobów cyfrowych. Zadanie ustawowe rozszerzające katalog rezerw strategicznych, działania długofalowe, wymagana jest umiejętność zarzadzania zasobami teleinformatycznymi, rozliczeń finansowych, prowadzenia dokumentacji technicznej.	1565 h
Obsługa powierzonych zadań przez inne organy oraz realizacja zadań humanitarnych oraz działań mających na celu przeciwdziałanie wystąpieniu zagrożenia bezpieczeństwa i obronności państwa, porządku i zdrowia publicznego, klęski żywiołowej lub sytuacji kryzysowej; – realizacja zadań	3125 h

związanych z przeciwdziałaniem zagrożeniom ich neutralizacją i pomocą humanitarną na podstawie prawa międzynarodowego. Wymaga koordynacji z wieloma instytucjami m.in.: donatorami, KE, obdarowanymi, brokerami logistycznymi, przedstawicielstwami krajów pośredniczących ect., zarządzania projektami i obsługi finansowej w ramach środków powierzonych, znajomości prawa międzynarodowego i pracy w trybie zadaniowym.	
Realizacja zadań powierzonych: Minister właściwy do spraw wewnętrznych może powierzyć Agencji, w drodze decyzji, realizację innych zadań niż określone w art. 31 w związku z tworzeniem, utrzymywaniem, udostępnianiem i likwidacją rezerw strategicznych. Agencja jest uprawniona w szczególności do: ✓ nabywania, zbywania, transportowania, przechowywania, wydawania oraz do wywozu poza terytorium Rzeczypospolitej Polskiej i przywozu z terytorium innego państwa określonego asortymentu; ✓ nabywania oraz świadczenia usług, w szczególności usług o charakterze logistycznym, transportowym i magazynowym, na terytorium Rzeczypospolitej Polskiej lub poza jej granicami; ✓ zlecania wykonania robót budowlanych oraz usług związanych z ich wykonaniem; ✓ przyjmowania i przekazywania darowizn. Realizacja zadań w warunkach dynamicznie zmieniającego się otoczenia, wymaga utrzymania stałej gotowości operacyjnej, elastycznego podejścia, sprawnie funkcjonującej logistyki oraz skutecznej obsługi zamówień. Konieczne jest posiadanie wiedzy specjalistycznej w zakresie szerokiego katalogu asortymentu, umiejętność koordynacji działań między jednostkami organizacyjnymi, znajomość przepisów krajowych i międzynarodowych, prowadzenie dokumentacji formalno-prawnej, nadzór nad realizacją umów oraz bieżące monitorowanie wykorzystania zasobów.	6250 h
Suma	**15 630 h**

Szacunkowa, łączna liczba godzin wyniosła 15 630 h rocznie co przy założeniu dostępności pracownika 1533 h rocznie daje następujące wyliczenie 15 630/1533= 10,2 etatu. Proponowana liczba etatów – 10.

Załącznik nr 2 do Oceny Skutków Regulacji projektu ustawy o zmianie ustawy o zarządzaniu kryzysowym oraz niektórych innych ustaw (UC47)

Koszty prowadzenia wykazu podmiotów krytycznych w systemie S46											
	2025	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035
Bieżące	1 775 000,00	457 062,50	470 774,38	484 897,61	499 444,53	514 427,87	529 860,71	545 756,53	562 129,22	578 993,10	596 362,89
Inwestycje	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
Usługi wsparcia	100 000,00	25 000,00	25 750,00	26 522,50	27 318,18	28 137,72	28 981,85	29 851,31	30 746,85	31 669,25	32 619,33
Suma	1 875 000,00	482 000,00	497 000,00	511 000,00	527 000,00	543 000,00	559 000,00	576 000,00	593 000,00	611 000,00	629 000,00
Zaokrąglenie	1 875,00	482,00	497,00	511,00	527,00	543,00	559,00	576,00	593,00	611,00	629,00
podział na kategorie											
Wynagrodzenia	1 420 000,00	366 000,00	377 000,00	388 000,00	400 000,00	412 000,00	424 000,00	437 000,00	450 000,00	464 000,00	478 000,00
Usługi obce	100 000,00	25 000,00	25 750,00	26 522,50	27 318,18	28 137,72	28 981,85	29 851,31	30 746,85	31 669,25	32 619,33
Koszty ogólne	355 000,00	91 062,50	93 774,38	96 897,61	99 444,53	102 427,87	105 860,71	108 756,53	112 129,22	114 993,10	118 362,89
Suma	1 875 000,00	482 062,50	496 524,38	511 420,11	526 762,71	542 565,59	558 842,56	575 607,84	592 876,07	610 662,35	628 982,22
Suma zaokrąglenie	1 875 000,00	482 000,00	497 000,00	511 000,00	527 000,00	543 000,00	559 000,00	576 000,00	593 000,00	611 000,00	629 000,00
Koszt osobomiesiące + inflacja	23 081,54	23 773,99	24 487,21	25 221,82	25 978,48	26 757,83	27 560,57	28 387,38	29 239,00	30 116,17	31 019,66
obliczanie kosztów osobowych											
FTE zaokrąglenie	61,50	15,38	15,38	15,38	15,38	15,38	15,38	15,38	15,38	15,38	15,38
koszty osobowe	1 419 514,71	365 643,91	376 613,22	387 911,62	399 548,97	411 535,44	423 881,50	436 597,95	449 695,89	463 186,76	477 082,37
koszty osobowe zaokrąglenie	1 420 000,00	366 000,00	377 000,00	388 000,00	400 000,00	412 000,00	424 000,00	437 000,00	450 000,00	464 000,00	478 000,00

Załącznik nr 3 do OSR ustawy o zmianie ustawy o zarządzaniu kryzysowym oraz niektórych innych ustaw (UC47) - podsumowanie wydatków dla poszczególnych części budżetowych w tys. zł.

Numer części budżetowej	Nazwa/Rok	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035	2036
część 20												
	Wynagrodzenie roczne	459,7	471,6	483,3	495	507,4	520	533	546,1	560,1	574,1	588,4
	Dodatkowe wynagrodzenie roczne	0	39	40	41	42,1	43,1	44	45,4	46,5	47,6	49
	Składki na ubezpieczenie społeczne	79	87,9	90	93	95	97,1	100	102	104,5	107,1	110
	Składki na Fundusz Pracy	4,6	5,1	5,2	5,3	5,5	5,6	5,7	5,9	6,1	6,2	6,4
	Składki na Fundusz Solidarnościowy	6,7	7,4	7,5	7,7	8	8,2	8,3	8,6	8,8	9	9,2
	Wyposażenie stanowiska pracy	36	0	0	0	0	36	0	0	0	0	36
	SUMA	**586**	**611**	**626**	**642**	**658**	**710**	**691**	**708**	**726**	**744**	**799**
część 21												
	Wynagrodzenie roczne	1685,4	1729,2	1772,4	1814,8	1860,3	1906,8	1954,5	2003,2	2053,4	2104,9	2157,4
	Dodatkowe wynagrodzenie roczne	0	143,3	147	150,6	154,3	158	162,1	166,1	170,2	174,5	178,9
	Składki na ubezpieczenie społeczne	290,4	322,7	330,7	338,5	347,1	355,7	364,6	373,7	383	392,7	402,5
	Składki na Fundusz Pracy	16,8	18,7	19,1	19,6	20,1	20,6	21,1	21,6	22,2	22,8	23,3
	Składki na Fundusz Solidarnościowy	24,4	27,1	27,8	28,5	29,2	29,9	30,7	31,4	32,2	33,1	33,9
	Wyposażenie stanowiska pracy	132	0	0	0	0	132	0	0	0	0	132
	SUMA	**2149**	**2241**	**2297**	**2352**	**2411**	**2603**	**2533**	**2596**	**2661**	**2728**	**2928**
część 22												
	Wynagrodzenie roczne	459,7	471,6	483,3	495	507,4	520	533	546,1	560,1	574,1	588,4
	Dodatkowe wynagrodzenie roczne	0	39	40	41	42,1	43,1	44	45,4	46,5	47,6	49

	Składki na ubezpieczenie społeczne	79	87,9	90	93	95	97,1	100	102	104,5	107,1	110
	Składki na Fundusz Pracy	4,6	5,1	5,2	5,3	5,5	5,6	5,7	5,9	6,1	6,2	6,4
	Składki na Fundusz Solidarnościowy	6,7	7,4	7,5	7,7	8	8,2	8,3	8,6	8,8	9	9,2
	Wyposażenie stanowiska pracy	36	0	0	0	0	36	0	0	0	0	36
	SUMA	**586**	**611**	**626**	**642**	**658**	**710**	**691**	**708**	**726**	**744**	**799**
część 27												
	Wynagrodzenie roczne	459,7	471,6	483,3	495	507,4	520	533	546,1	560,1	574,1	588,4
	Dodatkowe wynagrodzenie roczne	0	39	40	41	42,1	43,1	44	45,4	46,5	47,6	49
	Składki na ubezpieczenie społeczne	79	87,9	90	93	95	97,1	100	102	104,5	107,1	110
	Składki na Fundusz Pracy	4,6	5,1	5,2	5,3	5,5	5,6	5,7	5,9	6,1	6,2	6,4
	Składki na Fundusz Solidarnościowy	6,7	7,4	7,5	7,7	8	8,2	8,3	8,6	8,8	9	9,2
	Wyposażenie stanowiska pracy	36	0	0	0	0	36	0	0	0	0	36
	Koszty prowadzenia wykazu podmiotów krytycznych w systemie S46 (koszty bieżące i usługi wsparcia)	1875	482	497	511	527	543	559	576	593	611	629
	SUMA	**2461**	**1093**	**1123**	**1153**	**1185**	**1253**	**1250**	**1284**	**1319**	**1355**	**1428**
część 32												
	Wynagrodzenie roczne	459,7	471,6	483,3	495	507,4	520	533	546,1	560,1	574,1	588,4
	Dodatkowe wynagrodzenie roczne	0	39	40	41	42,1	43,1	44	45,4	46,5	47,6	49
	Składki na ubezpieczenie społeczne	79	87,9	90	93	95	97,1	100	102	104,5	107,1	110
	Składki na Fundusz Pracy	4,6	5,1	5,2	5,3	5,5	5,6	5,7	5,9	6,1	6,2	6,4
	Składki na Fundusz Solidarnościowy	6,7	7,4	7,5	7,7	8	8,2	8,3	8,6	8,8	9	9,2

	Wyposażenie stanowiska pracy	36	0	0	0	0	36	0	0	0	0	36
	SUMA	**586**	**611**	**626**	**642**	**658**	**710**	**691**	**708**	**726**	**744**	**799**
część 37												
	Wynagrodzenie roczne	153	157,3	161,2	165,1	169,1	173,6	177,6	182,1	186,8	191,3	196,1
	Dodatkowe wynagrodzenie roczne	0	13,1	13,4	13,7	14	14,4	14,7	15,1	15,5	15,9	16,3
	Składki na ubezpieczenie społeczne	26,3	29,4	30,1	30,8	31,5	32,4	33,1	34	34,8	35,7	36,5
	Składki na Fundusz Pracy	1,5	1,7	1,8	1,8	1,8	1,9	1,9	2	2	2,1	2,1
	Składki na Fundusz Solidarnościowy	2,2	2,5	2,5	2,6	2,6	2,7	2,7	2,8	2,9	3	3
	Wyposażenie stanowiska pracy	12	0	0	0	0	12	0	0	0	0	12
	SUMA	**195**	**204**	**209**	**214**	**219**	**237**	**230**	**236**	**242**	**248**	**266**
część 39												
	Wynagrodzenie roczne	459,7	471,6	483,3	495	507,4	520	533	546,1	560,1	574,1	588,4
	Dodatkowe wynagrodzenie roczne	0	39	40	41	42,1	43,1	44	45,4	46,5	47,6	49
	Składki na ubezpieczenie społeczne	79	87,9	90	93	95	97,1	100	102	104,5	107,1	110
	Składki na Fundusz Pracy	4,6	5,1	5,2	5,3	5,5	5,6	5,7	5,9	6,1	6,2	6,4
	Składki na Fundusz Solidarnościowy	6,7	7,4	7,5	7,7	8	8,2	8,3	8,6	8,8	9	9,2
	Wyposażenie stanowiska pracy	36	0	0	0	0	36	0	0	0	0	36
	SUMA	**586**	**611**	**626**	**642**	**658**	**710**	**691**	**708**	**726**	**744**	**799**
część 42												
	Wynagrodzenie roczne	3733	3829,4	3925,1	4019,3	4119,8	4222,9	4329	4436,5	4547,4	4661,2	4777,7
	Dodatkowe wynagrodzenie roczne	0	317,3	325,5	333,6	341,6	350,2	358,9	367,9	377,1	386,5	396,2
	Składki na ubezpieczenie społeczne	643,1	714,5	732,4	750,1	768,7	788	807,6	827,8	848,5	869,7	891,5

RCB	Składki na Fundusz Pracy	37,3	41,5	42,5	43,5	44,6	45,7	46,9	48	49,2	50,4	51,7
	Składki na Fundusz Solidarnościowy	54,1	60,1	61,6	63,1	64,6	66,3	67,9	69,6	71,4	73,2	75
	Wyposażenie stanowiska pracy	336	0	0	0	0	336	0	0	0	0	336
	Delegacje	444	444	444	444	444	444	444	444	444	444	444
	Wynagrodzenie roczne	1532,1	1572	1611	1650	1691,2	1733,6	1776,8	1821,2	1866,8	1913,5	1961,3
	Dodatkowe wynagrodzenie roczne	0	130,2	133,6	136,9	140,2	143,8	147,3	151	154,8	158,7	162,6
RARS	Składki na ubezpieczenie społeczne	263,9	293,3	300,6	307,8	315,5	323,5	331,5	339,8	348,3	357,1	366
	Składki na Fundusz Pracy	15,3	17	17,4	17,8	18,3	18,8	19,2	19,7	20,2	20,7	21,2
	Składki na Fundusz Solidarnościowy	22,2	24,7	25,3	25,9	26,5	27,2	27,9	28,5	29,3	30	30,8
	Koszt przystosowania pomieszczeń (roboty budowlane-przebudowa ścian działowych, przygotowanie pomieszczeń pod instalacje elektryczne, sanitarne i teletechniczne, wykonanie robót wykończeniowych, wykonanie wentylacji, klimatyzacji, instalacji wo.-kan., systemów ppoż, zasilenie stanowisk, oświetlenie specjalistyczne, UPS, zabezpieczenie elektryczne).	2250										
	Media- wzrost zapotrzebowania na energię elektryczną, chłodzenia, łączość.	100										
CBM	Zakup wyposażenia do remontowanych pomieszczeń.	100										

	Instalacje teletechniczne i teleinformatyczne (w tym serwerownia). Zakres obejmuje um.in.: instalację okablowania strukturalnego, uzupełnienie systemu kontroli dostępu, uzupełnienie systemu monitoringu, uzupełnienie systemu alarmowego, uzupełnienie struktury sieci, remont serwerowni, w tym klimatyzacji precyzyjnej, systemów ppoż i zabudowy serwerowej.	550										
	SUMA-część 42	**10081**	**7444**	**7619**	**7792**	**7975**	**8500**	**8357**	**8554**	**8757**	**8965**	**9514**
część 47												
	Wynagrodzenie roczne	459,7	471,6	483,3	495	507,4	520	533	546,1	560,1	574,1	588,4
	Dodatkowe wynagrodzenie roczne	0	39	40	41	42,1	43,1	44	45,4	46,5	47,6	49
	Składki na ubezpieczenie społeczne	79	87,9	90	93	95	97,1	100	102	104,5	107,1	110
	Składki na Fundusz Pracy	4,6	5,1	5,2	5,3	5,5	5,6	5,7	5,9	6,1	6,2	6,4
	Składki na Fundusz Solidarnościowy	6,7	7,4	7,5	7,7	8	8,2	8,3	8,6	8,8	9	9,2
	Wyposażenie stanowiska pracy	36	0	0	0	0	36	0	0	0	0	36
	SUMA	**586**	**611**	**626**	**642**	**658**	**710**	**691**	**708**	**726**	**744**	**799**
część 48												
	Wynagrodzenie roczne	459,7	471,6	483,3	495	507,4	520	533	546,1	560,1	574,1	588,4
	Dodatkowe wynagrodzenie roczne	0	39	40	41	42,1	43,1	44	45,4	46,5	47,6	49
	Składki na ubezpieczenie społeczne	79	87,9	90	93	95	97,1	100	102	104,5	107,1	110

	Składki na Fundusz Pracy	4,6	5,1	5,2	5,3	5,5	5,6	5,7	5,9	6,1	6,2	6,4
	Składki na Fundusz Solidarnościowy	6,7	7,4	7,5	7,7	8	8,2	8,3	8,6	8,8	9	9,2
	Wyposażenie stanowiska pracy	36	0	0	0	0	36	0	0	0	0	36
	SUMA	**586**	**611**	**626**	**642**	**658**	**710**	**691**	**708**	**726**	**744**	**799**
część 51												
	Wynagrodzenie roczne	459,7	471,6	483,3	495	507,4	520	533	546,1	560,1	574,1	588,4
	Dodatkowe wynagrodzenie roczne	0	39	40	41	42,1	43,1	44	45,4	46,5	47,6	49
	Składki na ubezpieczenie społeczne	79	87,9	90	93	95	97,1	100	102	104,5	107,1	110
	Składki na Fundusz Pracy	4,6	5,1	5,2	5,3	5,5	5,6	5,7	5,9	6,1	6,2	6,4
	Składki na Fundusz Solidarnościowy	6,7	7,4	7,5	7,7	8	8,2	8,3	8,6	8,8	9	9,2
	Wyposażenie stanowiska pracy	36	0	0	0	0	36	0	0	0	0	36
	SUMA	**586**	**611**	**626**	**642**	**658**	**710**	**691**	**708**	**726**	**744**	**799**
część 69												
	Wynagrodzenie roczne	459,7	471,6	483,3	495	507,4	520	533	546,1	560,1	574,1	588,4
	Dodatkowe wynagrodzenie roczne	0	39	40	41	42,1	43,1	44	45,4	46,5	47,6	49
	Składki na ubezpieczenie społeczne	79	87,9	90	93	95	97,1	100	102	104,5	107,1	110
	Składki na Fundusz Pracy	4,6	5,1	5,2	5,3	5,5	5,6	5,7	5,9	6,1	6,2	6,4
	Składki na Fundusz Solidarnościowy	6,7	7,4	7,5	7,7	8	8,2	8,3	8,6	8,8	9	9,2
	Wyposażenie stanowiska pracy	36	0	0	0	0	36	0	0	0	0	36
	SUMA	**586**	**611**	**626**	**642**	**658**	**710**	**691**	**708**	**726**	**744**	**799**
część 76												
	Wynagrodzenie roczne	459,7	471,6	483,3	495	507,4	520	533	546,1	560,1	574,1	588,4

	Dodatkowe wynagrodzenie roczne	0	39	40	41	42,1	43,1	44	45,4	46,5	47,6	49
	Składki na ubezpieczenie społeczne	79	87,9	90	93	95	97,1	100	102	104,5	107,1	110
	Składki na Fundusz Pracy	4,6	5,1	5,2	5,3	5,5	5,6	5,7	5,9	6,1	6,2	6,4
	Składki na Fundusz Solidarnościowy	6,7	7,4	7,5	7,7	8	8,2	8,3	8,6	8,8	9	9,2
	Wyposażenie stanowiska pracy	36	0	0	0	0	36	0	0	0	0	36
	SUMA	**586**	**611**	**626**	**642**	**658**	**710**	**691**	**708**	**726**	**744**	**799**
część 85/02												
	Wynagrodzenie roczne	326	334,2	342,5	350,6	359,5	368,3	377,5	387,2	396,7	406,6	416,8
	Dodatkowe wynagrodzenie roczne	0	27,7	28,5	29,1	29,9	30,5	31,3	32,2	32,8	33,7	34,5
	Składki na ubezpieczenie społeczne	56,1	62,3	64	65,3	67,2	68,6	70,3	72,3	74	75,9	77,7
	Składki na Fundusz Pracy	3,2	3,6	3,7	3,7	3,9	3,9	4	4,2	4,3	4,4	4,5
	Składki na Fundusz Solidarnościowy	4,7	5,2	5,3	5,3	5,5	5,7	5,9	6,1	6,2	6,4	6,5
	Wyposażenie stanowiska pracy	36	0	0	0	0	36	0	0	0	0	36
	SUMA	**426**	**433**	**444**	**454**	**466**	**513**	**489**	**502**	**514**	**527**	**576**
część 85/04												
	Wynagrodzenie roczne	326	334,2	342,5	350,6	359,5	368,3	377,5	387,2	396,7	406,6	416,8
	Dodatkowe wynagrodzenie roczne	0	27,7	28,5	29,1	29,9	30,5	31,3	32,2	32,8	33,7	34,5
	Składki na ubezpieczenie społeczne	56,1	62,3	64	65,3	67,2	68,6	70,3	72,3	74	75,9	77,7
	Składki na Fundusz Pracy	3,2	3,6	3,7	3,7	3,9	3,9	4	4,2	4,3	4,4	4,5
	Składki na Fundusz Solidarnościowy	4,7	5,2	5,3	5,3	5,5	5,7	5,9	6,1	6,2	6,4	6,5
	Wyposażenie stanowiska pracy	36	0	0	0	0	36	0	0	0	0	36

	SUMA	426	433	444	454	466	513	489	502	514	527	576
część 85/06												
	Wynagrodzenie roczne	326	334,2	342,5	350,6	359,5	368,3	377,5	387,2	396,7	406,6	416,8
	Dodatkowe wynagrodzenie roczne	0	27,7	28,5	29,1	29,9	30,5	31,3	32,2	32,8	33,7	34,5
	Składki na ubezpieczenie społeczne	56,1	62,3	64	65,3	67,2	68,6	70,3	72,3	74	75,9	77,7
	Składki na Fundusz Pracy	3,2	3,6	3,7	3,7	3,9	3,9	4	4,2	4,3	4,4	4,5
	Składki na Fundusz Solidarnościowy	4,7	5,2	5,3	5,3	5,5	5,7	5,9	6,1	6,2	6,4	6,5
	Wyposażenie stanowiska pracy	36	0	0	0	0	36	0	0	0	0	36
	SUMA	**426**	**433**	**444**	**454**	**466**	**513**	**489**	**502**	**514**	**527**	**576**
część 85/08												
	Wynagrodzenie roczne	326	334,2	342,5	350,6	359,5	368,3	377,5	387,2	396,7	406,6	416,8
	Dodatkowe wynagrodzenie roczne	0	27,7	28,5	29,1	29,9	30,5	31,3	32,2	32,8	33,7	34,5
	Składki na ubezpieczenie społeczne	56,1	62,3	64	65,3	67,2	68,6	70,3	72,3	74	75,9	77,7
	Składki na Fundusz Pracy	3,2	3,6	3,7	3,7	3,9	3,9	4	4,2	4,3	4,4	4,5
	Składki na Fundusz Solidarnościowy	4,7	5,2	5,3	5,3	5,5	5,7	5,9	6,1	6,2	6,4	6,5
	Wyposażenie stanowiska pracy	36	0	0	0	0	36	0	0	0	0	36
	SUMA	**426**	**433**	**444**	**454**	**466**	**513**	**489**	**502**	**514**	**527**	**576**
część 85/10												
	Wynagrodzenie roczne	326	334,2	342,5	350,6	359,5	368,3	377,5	387,2	396,7	406,6	416,8
	Dodatkowe wynagrodzenie roczne	0	27,7	28,5	29,1	29,9	30,5	31,3	32,2	32,8	33,7	34,5
	Składki na ubezpieczenie społeczne	56,1	62,3	64	65,3	67,2	68,6	70,3	72,3	74	75,9	77,7
	Składki na Fundusz Pracy	3,2	3,6	3,7	3,7	3,9	3,9	4	4,2	4,3	4,4	4,5

	Składki na Fundusz Solidarnościowy	4,7	5,2	5,3	5,3	5,5	5,7	5,9	6,1	6,2	6,4	6,5
	Wyposażenie stanowiska pracy	36	0	0	0	0	36	0	0	0	0	36
	SUMA	**426**	**433**	**444**	**454**	**466**	**513**	**489**	**502**	**514**	**527**	**576**
część 85/12												
	Wynagrodzenie roczne	326	334,2	342,5	350,6	359,5	368,3	377,5	387,2	396,7	406,6	416,8
	Dodatkowe wynagrodzenie roczne	0	27,7	28,5	29,1	29,9	30,5	31,3	32,2	32,8	33,7	34,5
	Składki na ubezpieczenie społeczne	56,1	62,3	64	65,3	67,2	68,6	70,3	72,3	74	75,9	77,7
	Składki na Fundusz Pracy	3,2	3,6	3,7	3,7	3,9	3,9	4	4,2	4,3	4,4	4,5
	Składki na Fundusz Solidarnościowy	4,7	5,2	5,3	5,3	5,5	5,7	5,9	6,1	6,2	6,4	6,5
	Wyposażenie stanowiska pracy	36	0	0	0	0	36	0	0	0	0	36
	SUMA	**426**	**433**	**444**	**454**	**466**	**513**	**489**	**502**	**514**	**527**	**576**
część 85/14												
	Wynagrodzenie roczne	326	334,2	342,5	350,6	359,5	368,3	377,5	387,2	396,7	406,6	416,8
	Dodatkowe wynagrodzenie roczne	0	27,7	28,5	29,1	29,9	30,5	31,3	32,2	32,8	33,7	34,5
	Składki na ubezpieczenie społeczne	56,1	62,3	64	65,3	67,2	68,6	70,3	72,3	74	75,9	77,7
	Składki na Fundusz Pracy	3,2	3,6	3,7	3,7	3,9	3,9	4	4,2	4,3	4,4	4,5
	Składki na Fundusz Solidarnościowy	4,7	5,2	5,3	5,3	5,5	5,7	5,9	6,1	6,2	6,4	6,5
	Wyposażenie stanowiska pracy	36	0	0	0	0	36	0	0	0	0	36
	SUMA	**426**	**433**	**444**	**454**	**466**	**513**	**489**	**502**	**514**	**527**	**576**
część 85/16												
	Wynagrodzenie roczne	326	334,2	342,5	350,6	359,5	368,3	377,5	387,2	396,7	406,6	416,8
	Dodatkowe wynagrodzenie roczne	0	27,7	28,5	29,1	29,9	30,5	31,3	32,2	32,8	33,7	34,5

	Składki na ubezpieczenie społeczne	56,1	62,3	64	65,3	67,2	68,6	70,3	72,3	74	75,9	77,7
	Składki na Fundusz Pracy	3,2	3,6	3,7	3,7	3,9	3,9	4	4,2	4,3	4,4	4,5
	Składki na Fundusz Solidarnościowy	4,7	5,2	5,3	5,3	5,5	5,7	5,9	6,1	6,2	6,4	6,5
	Wyposażenie stanowiska pracy	36	0	0	0	0	36	0	0	0	0	36
	SUMA	**426**	**433**	**444**	**454**	**466**	**513**	**489**	**502**	**514**	**527**	**576**
część 85/18												
	Wynagrodzenie roczne	326	334,2	342,5	350,6	359,5	368,3	377,5	387,2	396,7	406,6	416,8
	Dodatkowe wynagrodzenie roczne	0	27,7	28,5	29,1	29,9	30,5	31,3	32,2	32,8	33,7	34,5
	Składki na ubezpieczenie społeczne	56,1	62,3	64	65,3	67,2	68,6	70,3	72,3	74	75,9	77,7
	Składki na Fundusz Pracy	3,2	3,6	3,7	3,7	3,9	3,9	4	4,2	4,3	4,4	4,5
	Składki na Fundusz Solidarnościowy	4,7	5,2	5,3	5,3	5,5	5,7	5,9	6,1	6,2	6,4	6,5
	Wyposażenie stanowiska pracy	36	0	0	0	0	36	0	0	0	0	36
	SUMA	**426**	**433**	**444**	**454**	**466**	**513**	**489**	**502**	**514**	**527**	**576**
część 85/20												
	Wynagrodzenie roczne	326	334,2	342,5	350,6	359,5	368,3	377,5	387,2	396,7	406,6	416,8
	Dodatkowe wynagrodzenie roczne	0	27,7	28,5	29,1	29,9	30,5	31,3	32,2	32,8	33,7	34,5
	Składki na ubezpieczenie społeczne	56,1	62,3	64	65,3	67,2	68,6	70,3	72,3	74	75,9	77,7
	Składki na Fundusz Pracy	3,2	3,6	3,7	3,7	3,9	3,9	4	4,2	4,3	4,4	4,5
	Składki na Fundusz Solidarnościowy	4,7	5,2	5,3	5,3	5,5	5,7	5,9	6,1	6,2	6,4	6,5
	Wyposażenie stanowiska pracy	36	0	0	0	0	36	0	0	0	0	36
	SUMA	**426**	**433**	**444**	**454**	**466**	**513**	**489**	**502**	**514**	**527**	**576**
część 85/22												

	Wynagrodzenie roczne	326	334,2	342,5	350,6	359,5	368,3	377,5	387,2	396,7	406,6	416,8
	Dodatkowe wynagrodzenie roczne	0	27,7	28,5	29,1	29,9	30,5	31,3	32,2	32,8	33,7	34,5
	Składki na ubezpieczenie społeczne	56,1	62,3	64	65,3	67,2	68,6	70,3	72,3	74	75,9	77,7
	Składki na Fundusz Pracy	3,2	3,6	3,7	3,7	3,9	3,9	4	4,2	4,3	4,4	4,5
	Składki na Fundusz Solidarnościowy	4,7	5,2	5,3	5,3	5,5	5,7	5,9	6,1	6,2	6,4	6,5
	Wyposażenie stanowiska pracy	36	0	0	0	0	36	0	0	0	0	36
	SUMA	**426**	**433**	**444**	**454**	**466**	**513**	**489**	**502**	**514**	**527**	**576**
część 85/24												
	Wynagrodzenie roczne	326	334,2	342,5	350,6	359,5	368,3	377,5	387,2	396,7	406,6	416,8
	Dodatkowe wynagrodzenie roczne	0	27,7	28,5	29,1	29,9	30,5	31,3	32,2	32,8	33,7	34,5
	Składki na ubezpieczenie społeczne	56,1	62,3	64	65,3	67,2	68,6	70,3	72,3	74	75,9	77,7
	Składki na Fundusz Pracy	3,2	3,6	3,7	3,7	3,9	3,9	4	4,2	4,3	4,4	4,5
	Składki na Fundusz Solidarnościowy	4,7	5,2	5,3	5,3	5,5	5,7	5,9	6,1	6,2	6,4	6,5
	Wyposażenie stanowiska pracy	36	0	0	0	0	36	0	0	0	0	36
	SUMA	**426**	**433**	**444**	**454**	**466**	**513**	**489**	**502**	**514**	**527**	**576**
część 85/26												
	Wynagrodzenie roczne	326	334,2	342,5	350,6	359,5	368,3	377,5	387,2	396,7	406,6	416,8
	Dodatkowe wynagrodzenie roczne	0	27,7	28,5	29,1	29,9	30,5	31,3	32,2	32,8	33,7	34,5
	Składki na ubezpieczenie społeczne	56,1	62,3	64	65,3	67,2	68,6	70,3	72,3	74	75,9	77,7
	Składki na Fundusz Pracy	3,2	3,6	3,7	3,7	3,9	3,9	4	4,2	4,3	4,4	4,5
	Składki na Fundusz Solidarnościowy	4,7	5,2	5,3	5,3	5,5	5,7	5,9	6,1	6,2	6,4	6,5

	Wyposażenie stanowiska pracy	36	0	0	0	0	36	0	0	0	0	36
	SUMA	**426**	**433**	**444**	**454**	**466**	**513**	**489**	**502**	**514**	**527**	**576**
część 85/28												
	Wynagrodzenie roczne	326	334,2	342,5	350,6	359,5	368,3	377,5	387,2	396,7	406,6	416,8
	Dodatkowe wynagrodzenie roczne	0	27,7	28,5	29,1	29,9	30,5	31,3	32,2	32,8	33,7	34,5
	Składki na ubezpieczenie społeczne	56,1	62,3	64	65,3	67,2	68,6	70,3	72,3	74	75,9	77,7
	Składki na Fundusz Pracy	3,2	3,6	3,7	3,7	3,9	3,9	4	4,2	4,3	4,4	4,5
	Składki na Fundusz Solidarnościowy	4,7	5,2	5,3	5,3	5,5	5,7	5,9	6,1	6,2	6,4	6,5
	Wyposażenie stanowiska pracy	36	0	0	0	0	36	0	0	0	0	36
	SUMA	**426**	**433**	**444**	**454**	**466**	**513**	**489**	**502**	**514**	**527**	**576**
część 85/30												
	Wynagrodzenie roczne	326	334,2	342,5	350,6	359,5	368,3	377,5	387,2	396,7	406,6	416,8
	Dodatkowe wynagrodzenie roczne	0	27,7	28,5	29,1	29,9	30,5	31,3	32,2	32,8	33,7	34,5
	Składki na ubezpieczenie społeczne	56,1	62,3	64	65,3	67,2	68,6	70,3	72,3	74	75,9	77,7
	Składki na Fundusz Pracy	3,2	3,6	3,7	3,7	3,9	3,9	4	4,2	4,3	4,4	4,5
	Składki na Fundusz Solidarnościowy	4,7	5,2	5,3	5,3	5,5	5,7	5,9	6,1	6,2	6,4	6,5
	Wyposażenie stanowiska pracy	36	0	0	0	0	36	0	0	0	0	36
	SUMA	**426**	**433**	**444**	**454**	**466**	**513**	**489**	**502**	**514**	**527**	**576**
część 85/32												
	Wynagrodzenie roczne	326	334,2	342,5	350,6	359,5	368,3	377,5	387,2	396,7	406,6	416,8
	Dodatkowe wynagrodzenie roczne	0	27,7	28,5	29,1	29,9	30,5	31,3	32,2	32,8	33,7	34,5
	Składki na ubezpieczenie społeczne	56,1	62,3	64	65,3	67,2	68,6	70,3	72,3	74	75,9	77,7

	Składki na Fundusz Pracy	3,2	3,6	3,7	3,7	3,9	3,9	4	4,2	4,3	4,4	4,5
	Składki na Fundusz Solidarnościowy	4,7	5,2	5,3	5,3	5,5	5,7	5,9	6,1	6,2	6,4	6,5
	Wyposażenie stanowiska pracy	36	0	0	0	0	36	0	0	0	0	36
	SUMA	**426**	**433**	**444**	**454**	**466**	**513**	**489**	**502**	**514**	**527**	**576**
zdrowie												
	Wynagrodzenie roczne	459,7	471,6	483,3	495	507,4	520	533	546,1	560,1	574,1	588,4
	Dodatkowe wynagrodzenie roczne	0	39	40	41	42,1	43,1	44	45,4	46,5	47,6	49
	Składki na ubezpieczenie społeczne	79	87,9	90	93	95	97,1	100	102	104,5	107,1	110
	Składki na Fundusz Pracy	4,6	5,1	5,2	5,3	5,5	5,6	5,7	5,9	6,1	6,2	6,4
	Składki na Fundusz Solidarnościowy	6,7	7,4	7,5	7,7	8	8,2	8,3	8,6	8,8	9	9,2
	Wyposażenie stanowiska pracy	36	0	0	0	0	36	0	0	0	0	36
	SUMA	**586**	**611**	**626**	**642**	**658**	**710**	**691**	**708**	**726**	**744**	**799**

RAPORT Z KONSULTACJI

projektu ustawy o zmianie ustawy o zarządzaniu kryzysowym oraz niektórych innych ustaw

Omówienie wyników przeprowadzanych konsultacji publicznych i opiniowania.

W ramach konsultacji publicznych projekt został skierowany do następujących podmiotów Business Centre Club, Federacji Konsumentów, Fundacji Bezpieczna Cyberprzestrzeń, Fundacji ePaństwo, Fundacji im. Stefana Batorego, Fundacji Instytut Mikromakro, Fundacji My Pacjenci, Fundacji Nowoczesna Polska, Fundacji Panoptykon, Fundacji Projekt Polska, Fundacji Pułaskiego, Internet Society Poland Chapter, Internet Society Poland, Izby Gospodarki Elektronicznej, Konfederacji Lewiatan, Krajowego Związku Banków Spółdzielczych, Krajowej Izby Gospodarczej Elektroniki i Telekomunikacji, Krajowej Izby Gospodarczej, Krajowej Izby Gospodarki Cyfrowej, Krajowej Izby Gospodarki Morskiej, Krajowej Izby Komunikacji Ethernetowej, Krajowej Izby Rozliczeniowej, Krajowej Spółdzielczej Kasy Oszczędnościowo-Kredytowej, Naczelnej Organizacji Technicznej, Naczelnej Rady Zrzeszeń Handlu i Usług, Polskiego Centrum Badań i Certyfikacji S.A., Polskiego Towarzystwa Informatycznego, Polskiej Izby Brokerów Ubezpieczeniowych i Reasekuracyjnych, Polskiej Izby Handlu, Polskiej Izby Informatyki i Telekomunikacji, Polskiej Izby Komunikacji Elektronicznej, Polskiej Izby Producentów Urządzeń i Usług na rzecz Kolei, Polskiej Izby Radiodyfuzji Cyfrowej, Polskiej Izby Ubezpieczeń, Polskiej Organizacji Handlu i Dystrybucji, Polskiej Organizacji Niebankowych Instytucji Płatności, Polskiej Rady Biznesu, Polskiej Wytwórni Papierów Wartościowych, Sektorowej Rady ds. Kompetencji – Telekomunikacja i Cyberbezpieczeństwo, Stowarzyszenia Inżynierów Telekomunikacji, Stowarzyszenia Polskich Brokerów Ubezpieczeniowych i Reasekuracyjnych, Towarzystwa Gospodarczego Polskie Elektrownie, Związku Banków Polskich oraz operatorów infrastruktury krytycznej.

W ramach opiniowania projekt został udostępniony: Prokuratorii Generalnej Rzeczypospolitej Polskiej, Prezesowi Urzędu Ochrony Konkurencji i Konsumentów, Prezesowi Urzędu Komunikacji Elektronicznej, Prezesowi Urzędu Ochrony Danych Osobowych, Komisji Nadzoru Finansowego, Rzecznikowi Małych i Średnich Przedsiębiorców, Urzędowi Zamówień Publicznych, Polskiemu Komitetowi Normalizacyjnemu, Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Biuru Bezpieczeństwa Narodowego, Centralnemu Biuru

Antykorupcyjnemu, Służbie Kontrwywiadu Wojskowego, Służbie Wywiadu Wojskowego, Służbie Ochrony Państwa oraz wojewodom.

Mając na względzie, iż wyłanianie podmiotów krytycznych będzie odbywało się spośród operatorów infrastruktury krytycznej – projekt był dodatkowo przedmiotem wielu spotkań z udziałem operatorów infrastruktury krytycznej, na których prezentowano i omawiano zawarte w nim rozwiązania, w tym m.in.

- ✓ seminarium „Podnoszenie Cyberodporności u operatorów IK" w dniach 13–14 maja 2024 r.,
- ✓ Ogólnopolskiego Szczytu Energetycznego w dniu 18 czerwca 2024 r.,
- ✓ VII Międzynarodowego Kongresu Naukowo-Technicznego „Safe Place" w dniu 27 listopada 2024 r.
- ✓ XI Krajowego Forum Ochrony Infrastruktury Krytycznej w dniach 3–4 grudnia 2024 r.

Zgłoszone w trakcie konsultacji i opiniowania uwagi dotyczyły treści rozwiązań zawartych w projekcie ustawy. Część uwag powielała się. Dokonano weryfikacji oraz analizy tych uwag i propozycji, które w części były wzajemnie wykluczającymi się z uwagi na sprzeczność interesów w danych branżach. Niektóre uwagi były poza zakresem treści projektowanych regulacji. Część zgłoszonych uwag i propozycji zostało przyjętych w całości i wychodząc naprzeciw oczekiwaniom w głównej mierze operatorów infrastruktury krytycznej.

Na podstawie uwag wojewodów doprecyzowano kwestie związane z dokumentami strategicznymi, m.in. Krajową Ocena Ryzyka, planami zarządzania ryzykiem oraz planami reagowania kryzysowego, jak również doprecyzowano rolę i zadania wojewodów w zakresie identyfikacji infrastruktury krytycznej oraz wsparcia operatorów w zakresie jej ochrony.

Uwzględnione uwagi operatorów infrastruktury krytycznej dotyczyły m.in. doprecyzowania definicji ustawowych zawartych w projekcie. W siatce pojęciowej doprecyzowano m.in. definicje „infrastruktury krytycznej" oraz „incydentu". Doprecyzowano również definicje „operatora infrastruktury krytycznej" oraz „podmiotu krytycznego" tak aby wykazać korelacje między tymi pojęciami. Uwzględniono również w definicji podmiotu krytycznego aspekt obszarów morskich, co jest niezbędne w związku z inwestycjami na morzu bałtyckim.

Aby uczynić bardziej czytelnym projektowane rozwiązania zmieniono układ rozdziałów wskazując najpierw przepisy konstytuujące organy do spraw podmiotów krytycznych a dopiero

potem przepisy materialne wskazujące na udział tychże organów w poszczególnych rozwiązaniach przewidzianych ustawą.

Na bazie uwag zmodyfikowano (wydłużono) terminy dotyczące wdrażania rozwiązań w zakresie ochrony infrastruktury krytycznej po wejściu w życie i zastosowaniu nowych rozwiązań dla infrastruktury krytycznej.

W regulacjach dodano służby, inspekcje i straże jako współpracującymi z operatorami infrastruktury krytycznej przy zdarzeniach zakłócających lub mogących zakłócić funkcjonowanie infrastruktury krytycznej oraz sposobu postępowania w przypadku takiego zdarzenia.

Zrezygnowano z tworzenia wykazów podmiotów krytycznych przez organy do spraw podmiotów krytycznych na rzecz jednego centralnego wykazu prowadzonego przez dyrektora RCB.

Doprecyzowano przepisy w zakresie stosowania norm technicznych, które mogą być uwzględniane stosowne do wdrażania rozwiązań w zakresie bezpieczeństwa świadczeni usług kluczowych przez podmioty krytyczne przyjęto argumentację, iż Polskie Normy nie są dokumentami obligatoryjnymi do stosowania, lecz mają być uwzględniane we wdrażaniu rozwiązań niezbędnych dla bezpieczeństwa świadczenia usług kluczowych. Dodatkowo wskazano, iż poziom zabezpieczeń ma być adekwatny do prowadzonej przez podmioty krytyczne analizy ryzyka.

W trakcie konferencji uzgodnieniowych rozpatrzono uwagi UODO w zakresie ochrony danych osobowych czy też uwagi UZP w zakresie zamówień publicznych. Ustalenia w tym zakresie zaowocowały tym, iż brak jest kolizji projektowanych przepisów z przepisami w zakresie ochrony danych osobowych – wyjaśniano zakres przetwarzania danych oraz ich czas przetwarzania i przechowywania. Podobny efekt osiągnięto w przypadku kwestii zamówień publicznych – projektowane regulacje nie zawierają norm kolizyjnych z przepisami ustawy – Prawo zamówień publicznych.

Uwzględniono postulaty NBP tak aby nie nakładać w ramach projektowanych regulacji nadmiernych obciążeń na ten bank, mając na względzie status centralnego banku Rzeczypospolitej Polskiej.

Poprawiono przepisy przejściowe w zakresie niezakłóconego przejścia z obecnego wykazu infrastruktury krytycznej do wykazu, który będzie opracowany na podstawie projektowanych przepisów.

Nie zostały uwzględnione postulaty w zakresie zmian przepisów dotyczących wydawania poleceń w sytuacji kryzysowej (art. 7a i następne ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym), postulowanych przez Prokuratorię Generalną Rzeczypospolitej Polskiej (PG RP wnioskowało o jej wyłączenie z procesu opiniowania poleceń na podstawie przepisów ustawy o zarządzaniu kryzysowym, wskazując jednocześnie taką możliwość w oparciu o przepisy ustawy o Prokuratorii Generalnej Rzeczypospolitej Polskiej). Nieuwzględnienie propozycji związane jest z nowelizacją przepisów ustawy o zarządzaniu kryzysowym w zakresie wydawania poleceń, która to nowelizacja została dokonana jako jeden z elementów rozwiązań związanych z przeciwdziałaniem skutkom powodzi (*vide* ustawa z dnia 1 października 2024 r. o zmianie ustawy o szczególnych rozwiązaniach związanych z usuwaniem skutków powodzi oraz niektórych innych ustaw).

Projekt ustawy nie podlegał konsultacjom z właściwymi organami i instytucjami Unii Europejskiej, w tym Europejskim Bankiem Centralnym. Na etapie konsultacji do projektu ustawy nie został zgłoszony żaden wniosek w trybie przepisów o działalności lobbingowej w procesie stanowienia prawa.

TYTUŁ WDRAŻAJĄCEGO AKTU PRAWNEGO		**Ustawa o zmianie ustawy o zarządzaniu kryzysowym oraz niektórych innych ustaw Rozporządzenie Rady Ministrów w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego**			
TYTUŁ WDRAŻANEGO AKTU PRAWNEGO / WDRAŻANYCH AKTÓW PRAWNYCH		**Dyrektywa 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 333 z 27.12.2022 r. str. 164).**			
WYJAŚNIENIE TERMINU WEJŚCIA W ŻYCIE PROJEKTU / PROJEKTÓW		Ustawa wchodzi w życie po upływie 14 dni od dnia ogłoszenia			
JEDN. RED.	**TREŚĆ PRZEPISU UE**	**KONIECZNOŚĆ WDROŻENIA TAK / NIE***	**JEDN. RED.**	**TREŚĆ PRZEPISU / PRZEPISÓW PROJEKTU**	**UZASADNIENIE**
Art. 1	Rozdział I Przepisy ogólne Artykuł 1 Przedmiot i zakres stosowania 1. W niniejszej dyrektywie ustanawia się: a) obowiązki państw członkowskich polegające na przyjmowaniu konkretnych środków mających na celu zapewnienie niezakłóconego świadczenia na rynku wewnętrznym usług kluczowych dla utrzymania niezbędnych funkcji społecznych lub niezbędnej działalności gospodarczej, w ramach zakresu stosowania art. 114 TFUE, w szczególności obowiązki polegające na identyfikowaniu podmiotów krytycznych oraz wspieraniu podmiotów krytycznych w wypełnianiu przez nie nałożonych na nie obowiązków; b) obowiązki podmiotów krytycznych mające na celu zwiększenie ich odporności i zdolności do świadczenia usług, o których mowa w lit. a), na rynku wewnętrznym; c) przepisy: (i) dotyczące nadzoru nad podmiotami krytycznymi; (ii)dotyczące egzekwowania przepisów; (iii) w zakresie identyfikacji podmiotów krytycznych o szczególnym znaczeniu europejskim oraz w zakresie misji doradczych w celu oceny środków, które takie podmioty	**T**	Art. 1 pkt 3 projektu (art. 1 ust. 1 ustawy o zarządzaniu kryzysowym)	Art. 1. 1. Ustawa określa: 3) zadania i obowiązki operatorów infrastruktury krytycznej; 4) usługi kluczowe oraz zadania i obowiązki podmiotów krytycznych;	

	wdrożyły, aby wypełniać swoje obowiązki wynikające z Rozdziału III; d) wspólne procedury dotyczące współpracy i sprawozdawczości w zakresie stosowania niniejszej dyrektywy; e) środki mające na celu osiągnięcie wysokiego poziomu odporności podmiotów krytycznych, aby zapewnić świadczenie usług kluczowych w Unii oraz usprawnić funkcjonowanie rynku wewnętrznego.				
Art. 1	2. Niniejszej dyrektywy nie stosuje się do kwestii objętych dyrektywą (UE) 2022/2555, bez uszczerbku dla art. 8 niniejszej dyrektywy. Z uwagi na powiązanie między fizycznym bezpieczeństwem a cyberbezpieczeństwem podmiotów krytycznych państwa członkowskie zapewniają skoordynowane wdrażanie niniejszej dyrektywy i dyrektywy (UE) 2022/2555.	N			
Art. 1	3. Nie stosuje się odpowiednich przepisów niniejszej dyrektywy, w tym przepisów dotyczących nadzoru i egzekwowania przepisów przewidzianych w rozdziale VI, jeżeli w przepisach sektorowych aktów prawa Unii nałożono na podmioty krytyczne obowiązek zastosowania środków zwiększających ich odporność i jeżeli wymogi te są uznawane przez państwa członkowskie za co najmniej równoważne odpowiadającym im obowiązkom przewidzianym w niniejszej dyrektywie.	N			
Art. 1	4. 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	T			Wymiana informacji na potrzeby realizacji zadań w obszarze podmiotów krytycznych odbywa się z zachowaniem bezpieczeństwa i poufności tychże

	wymianie ograniczają się do tego, co jest istotne dla celów takiej wymiany i proporcjonalne do jej celów. Przy wymianie informacji należy chronić poufność oraz bezpieczeństwo i interesy handlowe podmiotów krytycznych, przy jednoczesnym poszanowaniu bezpieczeństwa państw członkowskich.				informacji, na podstawie obowiązujących przepisów, w tym przepisów ustawy o ochronie informacji niejawnych oraz ustawy o zwalczaniu nieuczciwej konkurencji.
Art. 1	5. Niniejsza dyrektywa pozostaje bez uszczerbku dla obowiązku państw członkowskich w zakresie gwarantowania bezpieczeństwa narodowego i obronności i ich uprawnień do gwarantowania innych podstawowych funkcji państwa, w tym zapewniania integralności terytorialnej państwa i utrzymywania porządku publicznego.	N			
Art. 1	6. Niniejszej dyrektywy nie stosuje się do podmiotów administracji publicznej, które prowadzą swoją działalność w obszarach bezpieczeństwa narodowego, bezpieczeństwa publicznego, obronności lub egzekwowania prawa, w tym w zakresie prowadzenia postępowań przygotowawczych oraz wykrywania i ścigania przestępstw. L 333/176 PL Dziennik Urzędowy Unii Europejskiej 27.12.2022 .	T	Art. 1 pkt 3 projektu (art. 1 ust. 2 ustawy o zarządzaniu kryzysowym)	2. Ustawy w zakresie, o którym mowa w: 1) ust. 1 pkt 3 i 4, nie stosuje się do organów oraz jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych; 2) ust. 1 pkt 4 nie stosuje się do podmiotów, które w zakresie swojej działalności prowadzą postępowania przygotowawcze, o których mowa w art. 297 ustawy z dnia 6 czerwca 1997 r. - Kodeks postępowania karnego (Dz. U. z 2024 r. poz. 37, 1222 i 1248).”;	
Art. 1	7. Państwa członkowskie mogą zdecydować, że art. 11 i rozdziałów III, IV i VI, w całości lub w części, nie stosuje się do konkretnych podmiotów krytycznych, które prowadzą działalność w obszarach bezpieczeństwa narodowego, bezpieczeństwa publicznego, obronności lub egzekwowania prawa, w tym w zakresie prowadzenia postępowań przygotowawczych oraz wykrywania i ścigania przestępstw, lub które świadczą usługi wyłącznie na rzecz podmiotów	T	Art. 1 pkt 3 projektu (art. 1 ust. 2 ustawy o zarządzaniu kryzysowym)	2. Ustawy w zakresie, o którym mowa w: 1) ust. 1 pkt 3 i 4, nie stosuje się do organów oraz jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych; 2) ust. 1 pkt 4 nie stosuje się do podmiotów, które w zakresie swojej działalności prowadzą postępowania przygotowawcze, o których mowa w art. 297 ustawy z dnia 6 czerwca 1997 r. - Kodeks	

	administracji publicznej, o których mowa w ust. 6 niniejszego artykułu.			postępowania karnego (Dz. U. z 2024 r. poz. 37, 1222 i 1248).”;	
Art. 1	8. Obowiązki ustanowione w niniejszej dyrektywie nie wiążą się z dostarczaniem informacji, których ujawnienie byłoby sprzeczne z podstawowymi interesami bezpieczeństwa narodowego, bezpieczeństwa publicznego lub obronności państw członkowskich.	N			
Art. 1	9. Niniejsza dyrektywa pozostaje bez uszczerbku dla prawa Unii w sprawie ochrony danych osobowych, w szczególności rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679. i dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady.	N			
Art. 2	Artykuł 2 Definicje Do celów niniejszej dyrektywy stosuje się następujące definicje: 1) „podmiot krytyczny” oznacza podmiot publiczny lub prywatny zidentyfikowany przez państwo członkowskie zgodnie z art. 6 jako należący do jednej z kategorii wymienionych w trzeciej kolumnie tabeli w załączniku; 2) „odporność” oznacza zdolność podmiotu krytycznego do zapobiegania incydentowi,	T	Art. 1 pkt 4 lit. b, c, j projektu (art. 3 ustawy o zarządzaniu kryzysowym – pkt 1a, pkt 1 c, pkt 1d, pkt 1e, pkt 1f, pkt 2, pkt 13, pkt 24, pkt 25) Art. 1 pkt 7 projektu (art. 6e ust. 4 pkt 3 ustawy o zarządzaniu kryzysowym)	1a) podmiocie krytycznym - należy przez to rozumieć operatora infrastruktury krytycznej wpisanego do wykazu podmiotów krytycznych, realizującego co najmniej jedną usługę kluczową, prowadzącego działalność w sektorze lub podsektorze wymienionym w załączniku do ustawy oraz posiadającego infrastrukturę krytyczną na terytorium Rzeczypospolitej Polskiej lub na obszarach morskich Rzeczypospolitej Polskiej, o których mowa 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); 1d) odporności podmiotu krytycznego - należy przez to rozumieć zdolność do zapobiegania	

	ochrony przed nim, odpowiedzi na niego, stawiania mu oporu, łagodzenia i absorbowania incydentu oraz adaptacji i odtworzenia po incydencie;			incydentowi, ochrony przed incydentem realizowanej w drodze zaplanowanych działań, z wykorzystaniem posiadanych zasobów, reagowania w przypadku wystąpienia incydentu i jego absorbowania oraz adaptacji i usuwania skutków incydentu, w tym odtwarzania infrastruktury krytycznej niezbędnej do świadczenia usługi kluczowej;	
	3) „incydent” oznacza każde zdarzenie, które może znacząco zakłócić lub które zakłóca świadczenie usługi kluczowej, w tym gdy wpływa ono na krajowe systemy chroniące praworządność;			1f) incydencie – należy przez to rozumieć każde zdarzenie mające lub mogące mieć niekorzystny wpływ na świadczenie usługi kluczowej;	
	4) „infrastruktura krytyczna” oznacza składnik, obiekt, sprzęt, sieć lub system lub część składnika, obiektu, sprzętu, sieci lub systemu, niezbędne do świadczenia usługi kluczowej;			„2) infrastrukturze krytycznej - należy przez to rozumieć obiekt, urządzenie, instalację, sieć, system oraz usługę lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje, sieci, systemy oraz usługi niezbędne do: a) realizacji ważnych interesów państwa, w tym zapewnienia funkcjonowania organów administracji publicznej, b) zapewnienia funkcjonowania przedsiębiorstw, c) zaspokajania oraz utrzymania potrzeb obywateli, w tym potrzeb o charakterze lokalnym, d) zapewnienia świadczenia usług kluczowych;",	
	5) „usługa kluczowa” oznacza usługę, która ma decydujące znaczenie dla utrzymania niezbędnych funkcji społecznych, niezbędnej działalności gospodarczej, zdrowia i bezpieczeństwa publicznego lub środowiska;			1e) usłudze kluczowej - należy przez to rozumieć usługę, która ma decydujące znaczenie dla utrzymania niezbędnych funkcji społecznych, niezbędnej działalności gospodarczej, zdrowia i bezpieczeństwa publicznego lub środowiska, wskazaną w przepisach wydanych na podstawie art. 6zp ust. 3 pkt 1;	
	6) „ryzyko” oznacza potencjalną stratę lub potencjalne zakłócenie spowodowane incydentem i ma być wyrażone jako wypadkowa skali takiej straty lub takiego zakłócenia oraz prawdopodobieństwa wystąpienia takiego incydentu;			Art. 6e (…) 4. Ocena ryzyka w odniesieniu do podmiotów krytycznych uwzględnia dodatkowo: „3) ryzyka określane jako potencjalne straty lub potencjalne zakłócenia spowodowane incydentami, wyrażane jako wypadkowe skali tych strat lub	

	7) „ocena ryzyka ” oznacza ogólny proces mający na celu określenie charakteru i zakresu ryzyka poprzez identyfikację i analizę potencjalnych odpowiednich zagrożeń, podatności na zagrożenia i niebezpieczeństw, które mogłyby prowadzić do incydentu, oraz poprzez ocenę potencjalnej straty lub potencjalnego zakłócenia świadczenia usługi kluczowej spowodowanych tym incydentem;			zakłóceń oraz prawdopodobieństwa wystąpienia takich incydentów;” 13) ocenie ryzyka - należy przez to rozumieć proces identyfikacji zagrożenia, podatności na zagrożenie, prawdopodobieństwa wystąpienia zagrożenia oraz skutków wystąpienia zagrożenia, który określa wartość ryzyka;	
	8) „norma” oznacza normę zdefiniowaną w art. 2 pkt 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1025/2012;			24) normie – należy przez to rozumieć normę, o której mowa w art. 2 pkt 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1025/2012 z dnia 25 października 2012 r. w sprawie normalizacji europejskiej, zmieniające dyrektywy Rady 89/686/EWG i 93/15/EWG oraz dyrektywy Parlamentu Europejskiego i Rady 94/9/WE, 94/25/WE, 95/16/WE, 97/23/WE, 98/34/WE, 2004/22/WE, 2007/23/WE, 2009/23/WE i 2009/105/WE oraz uchylające decyzję Rady 87/95/EWG i decyzję Parlamentu Europejskiego i Rady nr 1673/2006/WE (Dz.U. L 316 z 14.11.2012, s. 12);	
	9) „specyfikacja techniczna” oznacza specyfikację techniczną zdefiniowaną w art. 2 pkt 4 rozporządzenia (UE) nr 1025/2012;			25) specyfikacji technicznej – należy przez to rozumieć specyfikację techniczną, o której mowa w art. 2 pkt 4 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1025/2012 z dnia 25 października 2012 r. w sprawie normalizacji europejskiej, zmieniające dyrektywy Rady 89/686/EWG i 93/15/EWG oraz dyrektywy Parlamentu Europejskiego i Rady 94/9/WE, 94/25/WE, 95/16/WE, 97/23/WE, 98/34/WE, 2004/22/WE, 2007/23/WE, 2009/23/WE i 2009/105/WE oraz uchylające decyzję Rady 87/95/EWG i decyzję Parlamentu Europejskiego i Rady nr 1673/2006/WE (Dz.U. L 316 z 14.11.2012, s. 12);	

	10) „podmiot administracji publicznej” oznacza podmiot uznany za taki w danym państwie członkowskim zgodnie z prawem krajowym, z wyłączeniem sądownictwa, parlamentów lub banków centralnych, który spełnia następujące kryteria: a) został utworzony w celu zaspokajania potrzeb leżących w interesie ogólnym i nie ma charakteru przemysłowego ani handlowego; b) posiada osobowość prawną lub zgodnie z prawem jest uprawniony do działania w imieniu innego podmiotu posiadającego osobowość prawną; c) jest finansowany w przeważającej części przez organy państwa lub inne podmioty prawa publicznego ze szczebla centralnego, jego zarząd podlega nadzorowi ze strony tych organów lub podmiotów lub ponad połowa członków jego organu administrującego, zarządzającego lub nadzorczego została wyznaczona przez organy państwa lub inne podmioty prawa publicznego ze szczebla centralnego; 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 kapitału.			1c) podmiot publiczny - podmiot wskazany w załączniku do ustawy w sektorze administracji publicznej;	
Art. 3	Artykuł 3 Minimalna harmonizacja Niniejsza dyrektywa nie uniemożliwia państwom członkowskim przyjmowania lub utrzymywania przepisów prawa krajowego w celu osiągnięcia wyższego poziomu odporności podmiotów krytycznych, pod warunkiem że takie przepisy są zgodne z obowiązkami państw członkowskich ustanowionymi w prawie Unii.	N			

Art. 4	Rozdział II Krajowe ramy dotyczące odporności podmiotów krytycznych Artykuł 4 Strategia w zakresie odporności podmiotów krytycznych 1. Po przeprowadzeniu konsultacji otwartych – w zakresie, w jakim jest to praktycznie możliwe – dla odpowiednich zainteresowanych stron każde państwo członkowskie przyjmuje w terminie do dnia 17 stycznia 2026 r. strategię mającą na celu zwiększenie odporności podmiotów krytycznych (zwaną dalej „strategią”). W strategii określa się, w oparciu o odpowiednie istniejące strategie krajowe i sektorowe, plany lub podobne dokumenty, cele strategiczne i środki polityczne służące osiągnięciu i utrzymaniu wysokiego poziomu odporności po stronie podmiotów krytycznych oraz obejmujące co najmniej sektory określone w załączniku.	T	Art. 1 pkt 7 projektu (art. 6f ust. 1, 10-12 ustawy o zarządzaniu kryzysowym) oraz art. 24 ust. 2 projektu	Art. 6f. 1. W celu zwiększenia odporności podmiotów krytycznych opracowuje się Strategię Odporności Podmiotów Krytycznych, zwaną dalej „Strategią”. Rada Ministrów przyjmuje Strategię, w drodze uchwały. (…) 10.Dyrektor Centrum może udostępnić opracowany projekt Strategii na stronie podmiotowej Biuletynu Informacji Publicznej Centrum. 11. Dyrektor Centrum kieruje projekt Strategii do 30-dniowych konsultacji publicznych, z przeprowadzenia których sporządza raport, wskazując główne tezy zawarte w stanowiskach zgłoszonych do projektu Strategii oraz odniesienie się do nich. 12. Dyrektor Centrum udostępnia raport, o którym mowa w ust. 11, na stronie podmiotowej Biuletynu Informacji Publicznej Centrum. Art. 24. (…) 2. Strategię odporności podmiotów krytycznych, o której mowa w art. 6f ust. 1 ustawy zmienianej w art. 1, w brzmieniu nadanym niniejszą ustawą, Rada Ministrów przyjmuje po raz pierwszy w terminie 6 miesięcy od dnia wejścia w życie niniejszej ustawy.	
Art. 4	2. Każda strategia zawiera co najmniej następujące elementy: a) cele strategiczne i priorytety służące zwiększeniu ogólnej odporności podmiotów krytycznych, biorąc pod uwagę trans graniczne i międzysektorowe zależności i współzależności; b) ramy zarządzania służące osiągnięciu celów strategicznych i priorytetów, w tym opis ról i obowiązków poszczególnych organów,	T	Art. 1 pkt 7 projektu (art. 6f ust. 1 i 2, 10 ustawy o zarzadzaniu kryzysowym)	Art. 6f. 1.W celu zwiększenia odporności podmiotów krytycznych opracowuje się Strategię Odporności Podmiotów Krytycznych, zwaną dalej „KSOPK”. Rada Ministrów przyjmuje Strategię w drodze uchwały. 2. KSOPK: 1) określa cele strategiczne i priorytety w zakresie zapewnienia niezakłóconego świadczenia usług kluczowych przez podmioty krytyczne oraz niezakłóconego funkcjonowania infrastruktury krytycznej, z uwzględnieniem powiązań między	

	podmiotów krytycznych i innych stron zaangażowanych we wdrażanie strategii; c) opis środków niezbędnych do zwiększenia ogólnej odporności podmiotów krytycznych, w tym opis oceny ryzyka, o której mowa w art. 5; d) opis procesu, w ramach którego identyfikuje się podmioty krytyczne; e) opis procesu wspierania podmiotów krytycznych zgodnie z niniejszym rozdziałem, w tym środków służących zacieśnieniu współpracy między sektorem publicznym, z jednej strony, a sektorem prywatnym oraz podmiotami publicznymi i prywatnymi, z drugiej strony; f) wykaz głównych organów i odpowiednich zainteresowanych stron, innych niż podmioty krytyczne, zaangażowanych we wdrażanie strategii; g) ramy polityczne umożliwiające koordynację między właściwymi organami na podstawie niniejszej dyrektywy (zwanymi dalej „właściwymi organami") oraz właściwymi organami na podstawie dyrektywy (UE) 2022/2555 na potrzeby wymiany informacji na temat ryzyk w cyberprzestrzeni, cyberzagrożeń i cyberincydentów oraz ryzyk, zagrożeń i incydentów poza cyberprzestrzenią oraz wykonywania zadań nadzorczych; h) opis już wprowadzonych środków mających na celu ułatwienie wypełniania obowiązków wynikających z rozdziału III niniejszej dyrektywy przez małe i średnie przedsiębiorstwa w rozumieniu załącznika do zalecenia Komisji 2003/361/WE, które to przedsiębiorstwa dane państwo członkowskie zidentyfikowało jako podmioty krytyczne. Po przeprowadzeniu konsultacji otwartych – w zakresie w jakim jest to praktycznie możliwe – dla			zagrożeniami wynikającymi z oddziaływań transgranicznych oraz zależności międzysektorowych; 2) określa zakresy działań oraz formy działań służące osiąganiu celów strategicznych i priorytetów przez: a) organy właściwe w sprawach podmiotów krytycznych, b) ministrów kierujących działami administracji rządowej, którzy identyfikują infrastrukturę krytyczną, c) Komisję Nadzoru Finansowego identyfikującego, w zakresie swojej właściwości infrastrukturę krytyczną, d) wojewodów, którzy identyfikują infrastrukturę krytyczną, e) podmioty niewymienione w lit. a-d, zaangażowane we wdrażanie i realizację KSOPK; 3) zawiera opisy: a) procesów identyfikujących podmioty krytyczne, b) środków niezbędnych do zwiększenia ogólnej odporności podmiotów krytycznych, w tym opis oceny ryzyka, o której mowa w KOR, c) procesów wspierania podmiotów krytycznych przez podmioty, o których mowa w pkt 2 lit. a-d, d) środków mających na celu ułatwienie wypełniania obowiązków wynikających z rozdziału III dyrektywy 2022/2557 przez małe i średnie przedsiębiorstwa, w rozumieniu załącznika do zalecenia Komisji 2003/361/W, które zostały zidentyfikowane jako podmioty krytyczne; 4) określa zakres koordynacji działań organów do spraw podmiotów krytycznych i organów właściwych do spraw cyberbezpieczeństwa, o których mowa 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). 10. Szef Centrum przedkłada Radzie Ministrów projekt KSOPK nie rzadziej niż raz na trzy lata.	

	odpowiednich zainteresowanych stron państwa członkowskie aktualizują swoje strategie co najmniej raz na cztery lata.				
Art. 4	3. Państwa członkowskie przekazują Komisji swoje strategie i istotne aktualizacje tych strategii w terminie trzech miesięcy od ich przyjęcia.	T	Art. 1 pkt 7 projektu (art. 6f ust. 15 ustawy o zarzadzaniu kryzysowym)	14. Dyrektor Centrum udostępnia Komisji Europejskiej KSOPK nie później niż w terminie trzech miesięcy od dnia jej przyjęcia przez Radę Ministrów. 15. Przepisy ust. 3-15 stosuje się do aktualizacji KSOPK.	
Art. 5	Artykuł 5 Ocena ryzyka przeprowadzana przez państwa członkowskie 1. Komisja jest uprawniona do przyjęcia aktu delegowanego zgodnie z art. 23 do dnia 17 listopada 2023 r. w celu uzupełnienia niniejszej dyrektywy przez ustanowienie niewyczerpującego wykazu usług kluczowych w sektorach i podsektorach, określonych w załączniku. Właściwe organy wykorzystują ten wykaz usług kluczowych do celu przeprowadzenia oceny ryzyka (zwanej dalej „oceną ryzyka państwa członkowskiego") do dnia 17 stycznia 2026 r., a następnie w razie potrzeby, co najmniej raz na cztery lata. Właściwe organy wykorzystują oceny ryzyka państw członkowskich do celów identyfikacji podmiotów krytycznych zgodnie z art. 6 i udzielania pomocy tym podmiotom krytycznym we wprowadzaniu środków zgodnie z art. 13. Oceny ryzyka państw członkowskich muszą uwzględniać istotne czynniki ryzyka, naturalne i spowodowane przez człowieka, w tym zagrożenia mające charakter międzysektorowy i transgraniczny, wypadki, klęski żywiołowe, stany zagrożenia zdrowia publicznego i zagrożenia hybrydowe lub inne zagrożenia związane z konfliktem, w tym przestępstwa terrorystyczne	T	Art. 1 pkt 7 projektu ustawy (art. 6e ust. 1, ust. 13, ust. 14 pkt 2 i 3, ust. 2 ustawy o zarządzaniu kryzysowym) oraz art. 24 ust. 1 projektu ustawy	Art. 6e. 1. W celu dokonania oceny ryzyka zidentyfikowanych zagrożeń opracowuje się Krajową Ocenę Ryzyka, zwaną dalej „KOR". Rada Ministrów przyjmuje KOR w drodze uchwały. 13. Dyrektor Centrum przedkłada Radzie Ministrów projekt KOR nie rzadziej niż raz na trzy lata. **Art. 24.** 1. Krajową Ocenę Ryzyka, o której mowa w art. 6e ust. 1 ustawy zmienianej w art. 1, w brzmieniu nadanym niniejszą ustawą, Rada Ministrów przyjmuje po raz pierwszy w terminie 6 miesięcy od dnia wejścia w życie niniejszej ustawy. Art. 6e. ust. 14 pkt 2 i 3 14. KOR uwzględnia się w: 2) procesach identyfikacji podmiotów krytycznych; 3) opracowywaniu ocen ryzyka podmiotów krytycznych oraz wdrażaniu przez podmioty krytyczne środków w zakresie zwiększenia ich odporności; (Art. 6e) 2. KOR zawiera: 1) zidentyfikowane istotne zagrożenia:	

	przewidziane w dyrektywie Parlamentu Europejskiego i Rady (UE) 2017/541 (32).			a) stanowiące katastrofę naturalną lub awarię techniczną w rozumieniu przepisów ustawy z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej (Dz. U. z 2017 r. poz. 1897), b) hybrydowe, c) cyberbezpieczeństwa, d) o charakterze terrorystycznym, e) mogące spowodować niedostępność usług kluczowych, f) inne mogące spowodować znaczące negatywne skutki dla ludności, gospodarki lub dóbr kultury; 2) zagrożenia niezidentyfikowane jednoznacznie, które mogą wystąpić w przyszłości; 3) ocenę ryzyka wystąpienia zidentyfikowanych istotnych zagrożeń.	
Art. 5	2. Przeprowadzając oceny ryzyka państw członkowskich, państwa członkowskie biorą pod uwagę co najmniej: a) ogólną ocenę ryzyka przeprowadzoną na podstawie art. 6 ust. 1 decyzji nr 1313/2013/UE; b) inne istotne oceny ryzyka przeprowadzone zgodnie z wymogami właściwych sektorowych aktów prawnych Unii, w tym rozporządzeń Parlamentu Europejskiego i Rady (UE) 2017/1938 i (UE) 2019/941 oraz dyrektywy Parlamentu Europejskiego i Rady 2007/60/WE (35 (31) i 2012/18/UE; c) istotne ryzyka wynikające ze stopnia wzajemnej zależności między sektorami określonymi w załączniku, w tym od stopnia ich zależności od podmiotów znajdujących się w innych państwach członkowskich i państwach trzecich, oraz wpływ, jaki znaczące zakłócenie w jednym sektorze może mieć na inne sektory, w tym wszelkie istotne czynniki ryzyka dla obywateli i rynku wewnętrznego; d) wszelkie informacje na temat incydentów zgłoszonych zgodnie z art. 15. Do celów akapitu pierwszego lit. c) państwa członkowskie współpracują w stosownych przypadkach z	T	Art. 1 pkt 7 projektu (art. 6f ust. 3 i 4 ustawy o zarządzaniu kryzysowym)	3. Przy opracowaniu oceny ryzyka uwzględnia się w szczególności: 3) ogólną ocenę ryzyka przeprowadzoną na podstawie art. 6 ust. 1 decyzji nr 1313/2013/UE; 5) inne istotne oceny ryzyka przeprowadzone zgodnie z wymogami właściwych sektorowych aktów Unii Europejskiej. 4. Ocena ryzyka w odniesieniu do podmiotów krytycznych uwzględnia dodatkowo: 3) istotne ryzyka wynikające ze stopnia wzajemnej zależności między sektorami określonymi w załączniku do ustawy; 4) zależność ciągłości działania usług kluczowych od funkcjonowania podmiotów znajdujących się w innych państwach członkowskich i państwach trzecich; 5) wpływ znaczącego zakłócenia w jednym sektorze na inne sektory, w tym wszelkie istotne czynniki ryzyka dla obywateli i rynku wewnętrznego;	

	właściwymi organami innych państw członkowskich i właściwymi organami państw trzecich.			6) wpływ, jaki znaczące zakłócenie w jednym sektorze może mieć wpływ na inne sektory, w tym wszelkie istotne czynniki ryzyka dla obywateli i rynku wewnętrznego; 7) informacje dotyczące incydentów zgłaszanych przez podmioty krytyczne świadczące usługi kluczowe.	
Art. 5	3. Państwa członkowskie udostępniają, w stosownych przypadkach za pośrednictwem swoich pojedynczych punktów kontaktowych, odpowiednie elementy ocen ryzyka państw członkowskich podmiotom krytycznym, które zostały przez nie zidentyfikowane zgodnie z art. 6. Państwa członkowskie zapewniają, aby informacje przekazane podmiotom krytycznym pomagały im w przeprowadzaniu ich własnych ocen ryzyka, zgodnie z art. 12, oraz we wprowadzaniu środków służących zapewnieniu ich odporności, zgodnie z art. 13.	T	Art. 1 pkt 7 projektu (art. 6f ust. 1 ustawy o zarządzaniu kryzysowym)	1. W celu dokonania oceny ryzyka zidentyfikowanych zagrożeń opracowuje się Krajową Ocenę Ryzyka, zwaną dalej „KOR”. Rada Ministrów przyjmuje KOR w drodze uchwały.	
Art. 5	4. W terminie trzech miesięcy od przeprowadzenia oceny ryzyka państwa członkowskiego dane państwo członkowskie przekazuje Komisji odpowiednie informacje dotyczące rodzajów ryzyka stwierdzonych na podstawie oceny ryzyka państwa członkowskiego oraz wyników tej oceny w odniesieniu do poszczególnych sektorów i podsektorów określonych w załączniku.	T	Art. 1 pkt 7 projektu (art. 6f ust. 16 oraz art. 6zm ust. 5 ustawy o zarządzaniu kryzysowym)	16. Dyrektor Centrum, na podstawie KOR, opracowuje i udostępnia Komisji Europejskiej informacje dotyczące rodzajów ryzyka oraz wyników oceny ryzyka w odniesieniu do sektorów i podsektorów, o których mowa w załączniku do ustawy, w terminie trzech miesięcy od przyjęcia KOR. (Art. 6zm) 5. Pojedynczy Punkt Kontaktowy przekazuje Komisji Europejskiej: 1) niezwłocznie informacje o: a) wyznaczonych organach do spraw podmiotów krytycznych, Pojedynczym Punkcie Kontaktowym, ich zadaniach oraz późniejszych zmianach w tym zakresie,	

				b) przepisach dotyczących kar pieniężnych; 2) raz na dwa lata informacje umożliwiające ocenę wdrażania dyrektywy 2022/2557, obejmujące w szczególności: a) środki umożliwiające identyfikację podmiotów krytycznych, b) wykaz usług kluczowych, c) liczbę zidentyfikowanych podmiotów krytycznych w każdym sektorze lub podsektorze, o którym mowa w załączniku do ustawy, oraz wskazanie ich znaczenia w odniesieniu do tego sektora lub podsektora, d) progi istotności skutku zakłócającego dla świadczonej usługi kluczowej brane pod uwagę przy kwalifikowaniu podmiotów jako podmiotów krytycznych, przedstawiane wprost lub w formie zagregowanej; 3) informacje o środkach mających na celu zwiększenie odporności podmiotów krytycznych.	
Art. 5	5. Komisja – we współpracy z państwami członkowskimi – opracowuje dobrowolny wspólny formularz sprawozdawczy do celów wykonania ust. 4.	N			
Art. 6	1. Do dnia 17 lipca 2026 r. każde państwo członkowskie identyfikuje podmioty krytyczne dla sektorów i podsektorów określonych w załączniku.	T	Art. 29 projektu	**Art. 29.** Organy do spraw podmiotów krytycznych, o których mowa w art. 6zk ust. 1 ustawy zmienianej w art. 1, w brzmieniu nadanym niniejszą ustawą, po raz pierwszy identyfikują podmioty krytyczne i wpisują je do wykazu podmiotów krytycznych w terminie 9 miesięcy od dnia wejścia w życie niniejszej ustawy.	
Art. 6	2. Identyfikując podmioty krytyczne zgodnie z ust. 1, państwo członkowskie bierze pod uwagę wyniki swojej oceny ryzyka państwa członkowskiego i strategię oraz stosuje wszystkie następujące kryteria:	T	Art. 1 pkt 7 projektu (art. 6zp ustawy o zarządzaniu kryzysowym) Rozporządzenie Rady Ministrów w sprawie wykazu usług	Art. 6zp. 1. Operator infrastruktury krytycznej zostaje wpisany do wykazu podmiotów krytycznych w przypadku gdy: 1) świadczy co najmniej jedną usługę kluczową; 2) incydent miałby istotny skutek zakłócający dla świadczenia usługi kluczowej.	W załączniku do rozporządzenia Rady Ministrów wskazany zostanie wykaz usług kluczowych w podziale na sektory/podsektory, przypisanych do

	a) podmiot świadczy co najmniej jedną usługę kluczową; b) podmiot prowadzi działalność na terytorium tego państwa członkowskiego i jego infrastruktura krytyczna znajduje się na terytorium tego państwa członkowskiego; oraz c) ustalono, zgodnie z art. 7 ust. 1, że incydent miałby istotne skutki zakłócające dla świadczenia przez podmiot co naj mniej jednej usługi kluczowej lub dla świadczenia innych usług kluczowych w sektorach określonych w załączniku, które zależą od tej usługi kluczowej lub tych usług kluczowych.		kluczowych oraz progów istotności skutku zakłócającego	2. Istotność skutku zakłócającego incydentu dla świadczenia usługi kluczowej, o którym mowa w ust. 1 pkt 2, jest określana na podstawie progów istotności skutku zakłócającego określonych w przepisach wydanych na podstawie ust. 3. 3. Rada Ministrów określi, w drodze rozporządzenia wykaz usług kluczowych w podziale na sektory, podsektory i kategorie podmiotów wymienionych w załączniku do ustawy oraz progi istotności skutku zakłócającego dla świadczenia usług kluczowych, w zależności od: 1) liczby użytkowników zależnych od usługi kluczowej świadczonej przez dany podmiot, 2) stopnia, w jakim inne sektory lub podsektory, o których mowa w załączniku do ustawy, s5ą zależne od usługi świadczonej przez ten podmiot, 3) wpływu, jaki incydent - jeżeli chodzi o jego skalę i czas trwania - mógłby mieć na działalność gospodarczą i społeczną, środowisko, bezpieczeństwo publicznej lub na zdrowie ludności, 4) udziału podmiotu krytycznego w rynku w odniesieniu do świadczonej usługi kluczowej, 5) obszaru geograficznego , którego mógłby dotyczyć incydent, biorąc pod uwagę wpływ transgraniczny oraz stopień odizolowania geograficznego, 6) znaczenia podmiotu w utrzymywaniu wystarczającego poziomu świadczenia usługi kluczowej przy uwzględnieniu dostępności alternatywnych sposobów jej świadczenia, 7) innych czynników charakterystycznych dla danego sektora lub podsektora jeżeli występują. Wydając rozporządzenie należy określić co najmniej jeden próg istotności skutku zakłócającego dla świadczenia danej usługi kluczowej uwzględniając znaczenie danej usługi dla utrzymania niezbędnych funkcji społecznych, niezbędnej działalności gospodarczej, zdrowia i bezpieczeństwa publicznego lub środowiska	poszczególnych kategorii podmiotów wymienionych w załączniku do ustawy. Dodatkowo rozporządzenie określa progi istotności skutku zakłócającego dla poszczególnych usług kluczowych – oparte na kategoriach progów wskazanych w ustawie.

				naturalnego oraz obniżenia jakości świadczonej usługi kluczowej. Rozporządzenie Rady Ministrów w sprawie wykazu usług kluczowych (…) **§ 1.** Określa się wykaz usług kluczowych oraz progi istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych, stanowiące załącznik do rozporządzenia.	
Art. 6	3. Każde państwo członkowskie sporządza wykaz zidentyfikowanych podmiotów krytycznych zgodnie z ust. 2 i zapewnia, aby te podmioty krytyczne były powiadamiane o tym zidentyfikowaniu w terminie jednego miesiąca od jego dokonania. Państwa członkowskie informują te podmioty krytyczne o ich obowiązkach przewidzianych w rozdziałach III i IV oraz o dacie, począwszy od której obowiązki te mają do nich zastosowanie, bez uszczerbku dla art. 8. Państwa członkowskie informują podmioty krytyczne w sektorach określonych w pkt 3, 4 i 8 tabeli w załączniku, że nie spoczywają na nich obowiązki przewidziane w rozdziałach III i IV, chyba że środki krajowe stanowią inaczej. W przypadku odnośnych podmiotów krytycznych rozdział III stosuje się po 10 miesiącach od daty powiadomienia, o którym mowa w akapicie pierwszym niniejszego ustępu.	T	Art. 1 pkt 7 projektu (art. 6zo, art. 6zr, art. 6zs, art. 6zt ust. 3 i 4, art. 6zze, art. 6zzt, art. 6zzu ustawy o zarządzaniu kryzysowym)	Art. 6zo. 1. Dyrektor Centrum w celu zapewnienia: 1) identyfikacji podmiotów krytycznych, 2) prowadzenia czynności nadzorczych nad podmiotami krytycznymi - prowadzi wykaz podmiotów krytycznych. 2. Wykaz podmiotów krytycznych zawiera: 1) nazwę (firmę) podmiotu krytycznego; 2) siedzibę i adres oraz adres do doręczeń elektronicznych; 3) numer identyfikacji podatkowej (NIP), jeżeli został nadany; 4) nazwę usługi kluczowej, zgodną z wykazem usług kluczowych; 5) wskazanie sektora, podsektora i kategorii podmiotu; 6) datę rozpoczęcia świadczenia usługi kluczowej; 7) informację, w których państwach członkowskich Unii Europejskiej podmiot został uznany za podmiot świadczący usługę kluczową; 8) datę zakończenia świadczenia usługi kluczowej; 9) datę wykreślenia z wykazu podmiotów krytycznych. Art. 6zr. 1. Organ do spraw podmiotów krytycznych składa wniosek o wpis do wykazu podmiotów krytycznych zawierający dane, o których mowa w art. 6zo ust. 2 pkt 1-7. 2. Wpis operatora infrastruktury krytycznej do wykazu podmiotów krytycznych dokonuje	

				automatycznie się z chwilą złożenia wniosku w systemie teleinformatycznym, o którym mowa w art. 46 ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. 3. Organ do spraw podmiotów krytycznych niezwłocznie, nie później jednak niż w ciągu miesiąca, informuje operatora infrastruktury krytycznej o dokonania wpisu do wykazu podmiotów krytycznych oraz obowiązkach z tym związanych. 4. Informację, o której mowa w ust. 3, organ do spraw podmiotów krytycznych niezwłocznie przekazuje: 1) dyrektorowi Centrum; 2) odpowiedniemu organowi właściwemu do spraw cyberbezpieczeństwa. 5. Dyrektor Centrum może weryfikować dane zawarte we wpisie do wykazu podmiotów krytycznych ze stanem faktycznym. 6. Dyrektor Centrum poprawia, z urzędu, oczywiste omyki i błędy pisarskie zawarte we wpisie do wykazu podmiotów krytycznych. Art. 6zs. 1. Podmiot krytyczny w przypadku zakończenia świadczenia usługi kluczowej niezwłocznie informuje właściwy organ do spraw podmiotów krytycznych o tym fakcie. 2. W przypadku zakończenia świadczenia usługi kluczowej przez podmiot krytyczny, organ do spraw podmiotów krytycznych składa wniosek o wykreślenie podmiotu krytycznego z wykazu podmiotów krytycznych, zawierający dane, o których mowa w art. 6zo ust. 2 pkt 1-8. 3. Wykreślenie podmiotu krytycznego z wykazu dokonuje się automatycznie z chwilą złożenia wniosku w systemie teleinformatycznym, o którym mowa w art. 46 ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. 4. Organ do spraw podmiotów krytycznych niezwłocznie, nie później jednak niż w ciągu miesiąca, informuje podmiot krytyczny o	

				wykreśleniu z wykazu podmiotów krytycznych i dacie wykreślenia. 5. Informację, o której mowa w ust. 4, organ do spraw podmiotów krytycznych przekazuje niezwłocznie: 1) dyrektorowi Centrum; 2) odpowiedniemu organowi właściwemu do spraw cyberbezpieczeństwa. 6. Dyrektor Centrum może weryfikować dane zawarte we wniosku o wykreślenie podmiotu krytycznego z wykazu podmiotów krytycznych ze stanem faktycznym. 7. Dyrektor Centrum poprawia, z urzędu, oczywiste omyki i błędy pisarskie zawarte we wniosku o wykreślenie podmiotu krytycznego z wykazu. Art. 6zze. Podmioty krytyczne sektora bankowości i infrastruktury rynków finansowych przeprowadzają po raz pierwszy ocenę ryzyka, o której mowa w art. 6zt ust. 1 pkt 1, w terminie 10 miesięcy od otrzymania informacji o ujęciu w wykazie podmiotów krytycznych. Art. 6zzt. Do podmiotów krytycznych z sektora bankowości i infrastruktury rynków finansowych nie stosuje się przepisów rozdziałów 11–14, z wyjątkiem art. 6zt ust. 1 pkt 1, art. 6zt ust. 1 pkt 2 lit. b–d, f, h, oraz i, art. 6zt pkt 3, art. 6zt ust. 2–11, art. 6zu ust. 1 i ust. 2 pkt 3, 4 i 6, art. 6zu ust. 3–6, art. 6zx, art. 6zy, art. 6zzb i art. 6zzd. Art. 6zzu. Do podmiotów krytycznych z sektora infrastruktury cyfrowej nie stosuje się przepisów rozdziałów 11–14.	
Art. 6	4. Państwa członkowskie zapewniają, aby ich właściwe organy na podstawie niniejszej dyrektywy przekazywały właściwym organom na podstawie dyrektywy (UE) 2022/2555 dane	T	Art. 1 pkt 7 projektu (art. 6zr ust. 1, 3, 4, art. 6zs ust. 1, 2, 4, 5	Art. 6zr. 1. Organ do spraw podmiotów krytycznych składa wniosek o wpis do wykazu podmiotów krytycznych zawierający dane, o których mowa w art. 6zo ust. 2 pkt 1-7.	

	identyfikacyjne podmiotów krytycznych, które państwa te zidentyfikowały na podstawie niniejszego artykułu, w terminie jednego miesiąca od takiego zidentyfikowania. W stosownych przypadkach powiadomienie to zawiera informację, że odnośne podmioty krytyczne to podmioty z sektorów określonych w pkt 3, 4 i 8 tabeli w załączniku do niniejszej dyrektywy i że nie spoczywają na nich obowiązki przewidziane w rozdziałach III i IV niniejszej dyrektywy.		ustawy o zarządzaniu kryzysowym)	3. Organ do spraw podmiotów krytycznych niezwłocznie, nie później jednak niż w ciągu miesiąca, informuje operatora infrastruktury krytycznej o dokonania wpisu do wykazu podmiotów krytycznych oraz obowiązkach z tym związanych. 4. Informację, o której mowa w ust. 3, organ do spraw podmiotów krytycznych niezwłocznie przekazuje: 1) dyrektorowi Centrum; 2) odpowiedniemu organowi właściwemu do spraw cyberbezpieczeństwa. Art. 6zs. 1. Podmiot krytyczny w przypadku zakończenia świadczenia usługi kluczowej niezwłocznie informuje właściwy organ do spraw podmiotów krytycznych o tym fakcie. 2. W przypadku zakończenia świadczenia usługi kluczowej przez podmiot krytyczny, organ do spraw podmiotów krytycznych składa wniosek o wykreślenie podmiotu krytycznego z wykazu podmiotów krytycznych, zawierający dane, o których mowa w art. 6zo ust. 2 pkt 1-8. 4. Organ do spraw podmiotów krytycznych niezwłocznie, nie później jednak niż w ciągu miesiąca, informuje podmiot krytyczny o wykreśleniu z wykazu podmiotów krytycznych i dacie wykreślenia. 5. Informację, o której mowa w ust. 4, organ do spraw podmiotów krytycznych przekazuje niezwłocznie: 1) dyrektorowi Centrum; 2) odpowiedniemu organowi właściwemu do spraw cyberbezpieczeństwa.	
Art. 6	5. W razie potrzeby, a w każdym przypadku co najmniej co cztery lata państwa członkowskie dokonują przeglądu wykazu zidentyfikowanych podmiotów krytycznych, o którym mowa w ust. 3, oraz, w stosownych przypadkach, aktualizują go.	T			Zgodnie z projektowanymi przepisami art. 6zr i art. 6zs ustawy o zarządzaniu

	Jeżeli takie aktualizacje prowadzą do zidentyfikowania dodatkowych podmiotów krytycznych, w odniesieniu do tych dodatkowych podmiotów krytycznych stosuje się ust. 3 i 4. Ponadto państwa członkowskie zapewniają, aby podmioty, które wskutek takiej aktualizacji nie są już zidentyfikowane jako podmioty krytyczne, zostały w odpowiednim terminie powiadomione o tym fakcie oraz o facie, że od dnia otrzymania takiego powiadomienia nie podlegają już obowiązkom określonym w rozdziale III.				kryzysowym zarówno wpis jak i wykreślenie z wykazu podmiotów krytycznych realizowane jest na bieżąco, a informacje w tym zakresie organy do spraw podmiotów krytycznych przekazują podmiotom krytycznym w czasie jednego miesiąca od momentu wpisania lub wykreślenia z wykazu.
Art. 6	6. Komisja we współpracy z państwami członkowskimi opracowuje zalecenia i niewiążące wytyczne, aby wesprzeć państwa członkowskie w identyfikowaniu podmiotów krytycznych.	N			
Art. 7	Artykuł 7 Istotny skutek zakłócający 1. Przy określaniu istotności skutku zakłócającego, o którym mowa w art. 6 ust. 2 lit. c), państwa członkowskie uwzględniają następujące kryteria: a) liczbę użytkowników zależnych od usługi kluczowej świadczonej przez odnośny podmiot; b) stopień, w jakim inne sektory i podsektory określone w załączniku zależą od danej usługi kluczowej; c) wpływ, jaki incydenty – jeżeli chodzi o ich skalę i czas trwania – mogłyby mieć na działalność gospodarczą i społeczną, środowisko, bezpieczeństwo publiczne lub na zdrowie ludności; d) udział podmiotu w rynku odnośnej usługi kluczowej lub odnośnych usług kluczowych; e) obszar geograficzny, którego mógłby dotyczyć incydent, z uwzględnieniem wszelkiego wpływu	T	Art. 1 pkt 7 projektu (art. 6zp ust. 2 i 3)	(Art. 6zp.) 2. Istotność skutku zakłócającego incydentu dla świadczenia usługi kluczowej, o którym mowa w ust. 1 pkt 2, jest określana na podstawie progów istotności skutku zakłócającego określonych w przepisach w przepisach wydanych na podstawie ust. 3. 3. Rada Ministrów określi, w drodze rozporządzenia wykaz usług kluczowych w podziale na sektory, podsektory i kategorie podmiotów wymienionych w załączniku do ustawy oraz progi istotności skutku zakłócającego dla świadczenia usług kluczowych, wymienionych w wykazie usług kluczowych, w zależności od: 1) liczby użytkowników zależnych od usługi kluczowej świadczonej przez dany podmiot, 2) stopnia, w jakim inne sektory lub podsektory, o których mowa w załączniku do ustawy, są zależne od usługi świadczonej przez ten podmiot,	

	transgranicznego, przy uwzględnieniu podatności na zagrożenia związanej ze stopniem odizolowania niektórych rodzajów obszarów geograficznych, takich jak regiony wyspiarskie, regiony oddalone lub obszary górskie; f) znaczenie podmiotu w utrzymywaniu wystarczającego poziomu usługi kluczowej przy uwzględnieniu dostępności alternatywnych sposobów świadczenia tej usługi kluczowej.			3) wpływu, jaki incydent - jeżeli chodzi o jego skalę i czas trwania - mógłby mieć na działalność gospodarczą i społeczną, środowisko, bezpieczeństwo publicznej lub na zdrowie ludności, 4) udziału podmiotu krytycznego w rynku w odniesieniu do świadczonej usługi kluczowej, 5) obszaru geograficznego , którego mógłby dotyczyć incydent, biorąc pod uwagę wpływ transgraniczny oraz stopień odizolowania geograficznego, 6) znaczenia podmiotu w utrzymywaniu wystarczającego poziomu świadczenia usługi kluczowej przy uwzględnieniu dostępności alternatywnych sposobów jej świadczenia, 7) innych czynników charakterystycznych dla danego sektora lub podsektora jeżeli występują. Wydając rozporządzenie należy określić co najmniej jeden próg istotności skutku zakłócającego dla świadczenia danej usługi kluczowej uwzględniając znaczenie danej usługi dla utrzymania niezbędnych funkcji społecznych, niezbędnej działalności gospodarczej, zdrowia i bezpieczeństwa publicznego lub środowiska naturalnego oraz obniżenia jakości świadczonej usługi kluczowej.	
Art. 7	2. Po zidentyfikowaniu podmiotów krytycznych na podstawie art. 6 ust. 1, każde państwo członkowskie bez zbędnej zwłoki przekazuje Komisji następujące informacje: a) wykaz usług kluczowych w danym państwie członkowskim, jeżeli istnieją dodatkowe usługi kluczowe w porównaniu do wykazu usług kluczowych, o którym mowa w art. 5 ust. 1; b) liczbę podmiotów krytycznych zidentyfikowanych w każdym sektorze i podsektorze, określonych w załączniku, oraz zidentyfikowanych w odniesieniu do każdej z usług kluczowych;	T	Art. 1 pkt 7 projektu (Art. 6zm ust. 5 ustawy o zarządzaniu kryzysowym)	(Art. 6zm) 5. Pojedynczy Punkt Kontaktowy przekazuje Komisji Europejskiej: 1) niezwłocznie informacje o: a) wyznaczonych organach do spraw podmiotów krytycznych, Pojedynczym Punkcie Kontaktowym, ich zadaniach oraz późniejszych zmianach w tym zakresie, b) przepisach dotyczących kar pieniężnych; 2) raz na dwa lata informacje umożliwiające ocenę wdrażania dyrektywy 2022/2557, obejmujące w szczególności: a) środki umożliwiające identyfikację podmiotów krytycznych,	

	c) wszelkie progi zastosowane w celu określenia co najmniej jednego spośród kryteriów określonych w ust. 1. Progi, o których mowa w akapicie pierwszym lit. c), można przedstawić wprost lub w formie zagregowanej. Następnie państwa członkowskie przekazują informacje, o których mowa w akapicie pierwszym, w razie potrzeby i co najmniej raz na cztery lata.			b) wykaz usług kluczowych, c) liczbę zidentyfikowanych podmiotów krytycznych w każdym sektorze lub podsektorze, o którym mowa w załączniku do ustawy, oraz wskazanie ich znaczenia w odniesieniu do tego sektora lub podsektora, d) progi istotności skutku zakłócającego dla świadczonej usługi kluczowej brane pod uwagę przy kwalifikowaniu podmiotów jako podmiotów krytycznych, przedstawiane wprost lub w formie zagregowanej; 3) informacje o środkach mających na celu zwiększenie odporności podmiotów krytycznych.	
Art. 7 Art. 8	3. Komisja – po skonsultowaniu się z Grupą ds. Odporności Podmiotów Krytycznych, o której mowa w art. 19 – przyjmuje niewiążące wytyczne mające na celu ułatwienie stosowania kryteriów, o których mowa w ust. 1 niniejszego artykułu, biorąc pod uwagę informacje, o których mowa w ust. 2 niniejszego artykułu. Państwa członkowskie zapewniają, aby art. 11 i rozdziały III, IV i VI nie miały zastosowania w odniesieniu do podmiotów krytycznych, które zostały przez nie zidentyfikowane w sektorach określonych w pkt 3, 4 i 8 tabeli w załączniku. Państwa członkowskie mogą przyjąć lub utrzymać przepisy prawa krajowego w celu osiągnięcia wyższego poziomu odporności tych podmiotów krytycznych, pod warunkiem że przepisy te są zgodne z mającym zastosowanie prawem Unii.	N T	Art. 1 pkt 7 projektu (art. 6zze ust. 1 i 2 ustawy o zarządzaniu kryzysowym)	Art. 6zze. 1. Do podmiotów krytycznych z sektora bankowego i infrastruktury rynków finansowych nie stosuje się przepisów rozdziału 11-14 ustawy, z wyjątkiem art. 6zt ust. 1 pkt 1, art. 6zt ust. 1 pkt 2 lit. b-d, f, h, i i, art. 6zt pkt 3, art. 6zt ust. 2-11, art. 6zu ust. 1 i ust. 2 pkt 3, 4, i 6, art. 6zu ust. 3-6, art. 6zx, art. 6zy, art. 6zzb, art. 6zzd. 2. Do podmiotów krytycznych z sektora infrastruktury cyfrowej nie stosuje się przepisów rozdziału 11-14 ustawy.	
Art. 9	Artykuł 9 Właściwe orany i pojedynczy punkt kontaktowy 1. Każde państwo członkowskie wyznacza lub ustanawia co najmniej jeden właściwy organ odpowiedzialny za prawidłowe stosowanie i – w stosownych przypadkach – egzekwowanie	T	Art. 1 pkt 7 projektu (art. 6zk ustawy o zarządzaniu kryzysowym)	Art. 6zk.1. Organami do spraw podmiotów krytycznych są: 1) dla sektora energii: a) minister właściwy do spraw energii w podsektorach: - energii elektrycznej, - ciepła,	

	przepisów określonych w niniejszej dyrektywie na poziomie krajowym. W odniesieniu do podmiotów krytycznych w sektorach określonych w pkt 3 i 4 tabeli w załączniku do niniejszej dyrektywy, właściwymi organami są co do zasady właściwe organy, o których mowa w art. 46 rozporządzenia (UE) 2022/2554. W odniesieniu do podmiotów krytycznych w sektorze określonym w pkt 8 tabeli w załączniku do niniejszej dyrektywy, właściwymi organami są co do zasady właściwe organy na podstawie dyrektywy (UE) 2022/2555. Państwa członkowskie mogą wyznaczyć inny właściwy organ dla sektorów określonych w pkt 3, 4 i 8 tabeli w załączniku do niniejszej dyrektywy zgodnie z istniejącymi ramami krajowymi. Jeżeli państwa członkowskie wyznaczą lub ustanowią więcej niż jeden właściwy organ, wyraźnie określają odpowiednie zadania każdego z przedmiotowych organów oraz zapewniają ich skuteczną współpracę w wypełnianiu ich zadań na mocy niniejszej dyrektywy, w tym w odniesieniu do wyznaczenia i działań pojedynczego punktu kontaktowego, o którym mowa w ust. 2.			b) minister właściwy do spraw gospodarki surowcami energetycznymi w podsektorach: - wydobywania kopalin, - ropy i paliw, - gazu, - energetyki jądrowej, - wodoru; 2) dla sektora transportu: a) minister właściwy do spraw transportu w podsektorach: - transport lotniczy, - transport kolejowy, - transport publiczny, - transport drogowy, b) minister właściwy do spraw gospodarki morskiej oraz minister właściwy do spraw żeglugi śródlądowej w podsektorze transportu wodnego; 3) dla sektora bankowości oraz infrastruktury rynków finansowych - Komisja Nadzoru Finansowego; 4) dla sektora ochrony zdrowia - minister właściwy do spraw zdrowia; 5) dla sektora zaopatrzenia w wodę pitną i jej dystrybucji oraz sektora zbiorowego odprowadzania ścieków - minister właściwy do spraw gospodarki wodnej; 6) dla sektora infrastruktury cyfrowej: a) minister właściwy do spraw informatyzacji w podsektorze infrastruktury cyfrowej z wyłączeniem komunikacji elektronicznej, b) Prezes Urzędu Komunikacji Elektronicznej w podsektorze komunikacji elektronicznej; 7) dla sektora administracji publicznej: a) minister właściwy do spraw administracji publicznej w podsektorze podmiotów publicznych, b) minister właściwy do spraw finansów publicznych w podsektorze finansów publicznych; 8) dla sektora przestrzeni kosmicznej - minister właściwy do spraw gospodarki;	

				9) dla sektora produkcji, przetwarzania i dystrybucji żywności - minister właściwy do spraw rolnictwa; 10) dla sektora zarządzania usługami ICT - minister właściwy do spraw informatyzacji; 11) dla sektora produkcji, wytwarzania i dystrybucji chemikaliów – minister właściwy do spraw gospodarki; 12) dla sektora usług pocztowych - Prezes Urzędu Komunikacji Elektronicznej; 13) dla sektora gospodarowania odpadami – minister właściwy do spraw klimatu. 2. Dla podmiotu publicznego, który jest wymieniony w innym sektorze niż sektor administracji publicznej, organem do spraw podmiotów krytycznych jest organ właściwy dla danego sektora.	
Art. 9	2. Każde państwo członkowskie wyznacza lub ustanawia jeden pojedynczy punkt kontaktowy, który wykonuje funkcję łącznikową w celu zapewnienia współpracy transgranicznej z pojedynczymi punktami kontaktowymi innych państw członkowskich i z Grupą ds. Odporności Podmiotów Krytycznych, o której mowa w art. 19 (zwany dalej „pojedynczym punktem kontaktowym"). W stosownych przypadkach państwo członkowskie wyznacza swój pojedynczy punkt kontaktowy w ramach właściwego organu. W stosownych przypadkach państwo członkowskie może postanowić, że jego pojedynczy punkt kontaktowy będzie wykonywał również funkcję łącznikową z Komisją i zapewniał współpracę z państwami trzecimi.	T	Art. 1 pkt 7 projektu (art. 6zm ust. 1 ustawy o zarządzaniu kryzysowym)	Art. 6zm. 1. Dyrektor Centrum prowadzi Pojedynczy Punkt Kontaktowy do którego zadań należy: 1) odbieranie zgłoszeń incydentów istotnych z pojedynczych punktów kontaktowych w innych państwach członkowskich Unii Europejskiej; 2) przekazywanie zgłoszeń incydentów istotnych dotyczących innych państw członkowskich Unii Europejskiej do pojedynczych punktów kontaktowych tych państw; 3) opracowywanie i przekazywanie raz na dwa lata Komisji Europejskiej oraz Grupie do spraw Odporności Podmiotów Krytycznych sprawozdań dotyczących incydentów istotnych zgłaszanych przez podmioty krytyczne mających wpływ na ciągłość świadczonych przez nich usług kluczowych na terytorium Rzeczypospolitej Polskiej oraz ciągłość świadczonych usług kluczowych w państwach członkowskich Unii Europejskiej; 4) zapewnienie reprezentacji Rzeczypospolitej Polskiej w Grupie do spraw Odporności Podmiotów Krytycznych;	

				5) zapewnienie współpracy z Komisją Europejską w obszarze zapewnienia bezpieczeństwa świadczenia usług kluczowych; 6) koordynacja współpracy między organami do spraw podmiotów krytycznych i organami administracji publicznej w Rzeczypospolitej Polskiej z odpowiednimi organami w państwach członkowskich Unii Europejskiej; 7) zapewnienie wymiany informacji na potrzeby Grupy Współpracy, o której mowa w dyrektywie (UE) 2022/2555 oraz organów właściwych do spraw cyberbezpieczeństwa; 8) współpraca z pojedynczym punktem kontaktowym, o którym mowa w ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.	
Art. 9	3. W terminie do dnia 17 lipca 2028 r., a następnie co dwa lata, pojedyncze punkty kontaktowe przekazują Komisji oraz Grupie ds. Odporności Podmiotów Krytycznych, o której mowa w art. 19, sprawozdanie podsumowujące na temat otrzymanych zgłoszeń, w tym liczby zgłoszeń, charakteru zgłoszonych incydentów oraz działań podjętych zgodnie z art. 15 ust. 3. Komisja, we współpracy z Grupą ds. Odporności Podmiotów Krytycznych, opracowuje wspólny formularz sprawozdawczy. Właściwe organy mogą dobrowolnie korzystać z tego wspólnego formularza sprawozdawczego do celów przedkładania sprawozdań podsumowujących, o których mowa w akapicie pierwszym.	T	Art. 1 pkt 7 projektu (art. 6zm ust. 1 pkt 2 i 3 oraz ust. 2 ustawy o zarządzaniu kryzysowym) Art. 26 projektu ustawy	Art. 6zm. 1. Dyrektor Centrum prowadzi Pojedynczy Punkt Kontaktowy do którego zadań należy: przekazywanie zgłoszeń incydentów istotnych dotyczących innych państw członkowskich Unii Europejskiej do pojedynczych punktów kontaktowych tych państw; 3) opracowywanie i przekazywanie raz na dwa lata Komisji Europejskiej oraz Grupie do spraw Odporności Podmiotów Krytycznych sprawozdań dotyczących incydentów istotnych zgłaszanych przez podmioty krytyczne mających wpływ na ciągłość świadczonych przez nich usług kluczowych na terytorium Rzeczypospolitej Polskiej oraz ciągłość świadczonych usług kluczowych w państwach członkowskich Unii Europejskiej; 2. Pojedynczy Punkt Kontaktowy przekazuje Grupie do spraw Odporności Podmiotów Krytycznych: 2) dobre praktyki związane ze zgłaszaniem i obsługą incydentów istotnych;	

				3) propozycje do programu prac Grupy do spraw Odporności Podmiotów Krytycznych; **Art. 26.** 1. Pojedynczy Punkt Kontaktowy, o którym mowa w art. 6zm ust. 1 ustawy zmienianej w art. 1 po raz pierwszy opracowuje i przekazuje Komisji Europejskiej oraz Grupie do spraw Odporności Podmiotów Krytycznych sprawozdanie dotyczące incydentów istotnych zgłaszanych przez podmioty krytyczne mających wpływ na ciągłość świadczonych przez nich usług kluczowych na terytorium Rzeczypospolitej Polskiej oraz ciągłość świadczonych usług kluczowych w państwach członkowskich Unii Europejskiej w terminie do dnia 17 lipca 2028 r.	
Art. 9	4. Każde państwo członkowskie zapewnia, aby jego właściwy organ i pojedynczy punkt kontaktowy posiadały uprawnienia oraz odpowiednie zasoby finansowe, ludzkie i techniczne, by w sposób skuteczny i wydajny wykonywać przydzielone im zadania.	N			Organy do spraw podmiotów krytycznych jako instytucje państwowe na szczeblu centralnym, będące jednostkami budżetowymi w rozumieniu przepisów ustawy o finansach publicznych, będą miały zapewnione finansowanie ze środków publicznych.
Art. 9	5. Każde państwo członkowskie zapewnia, aby jego właściwy organ – w stosownych przypadkach oraz zgodnie z prawem Unii i prawem krajowym – konsultował się oraz współpracował z innymi odpowiednimi organami krajowymi, w tym z organami, które zajmują się ochroną ludności, egzekwowaniem prawa i ochroną danych osobowych, oraz z podmiotami krytycznymi i odpowiednimi zainteresowanymi stronami.	T	Art. 1 pkt 7 projektu (art. 6zm ust. 5 pkt 2 i 3 ustawy o zarządzaniu kryzysowym)	Art. 6zl. Organ do spraw podmiotów krytycznych: 5) współpracuje z podmiotami krytycznymi w danym sektorze lub podsektorze w zakresie obsługi incydentów; 6) monitoruje stosowanie przepisów ustawy przez podmioty krytyczne; 7) prowadzi kontrole podmiotów krytycznych; 8) prowadzi działania informacyjne dotyczące dobrych praktyk, działań edukacyjnych i kampanii	Organy do spraw podmiotów krytycznych jako instytucje rządowe oprócz wskazanych bezpośrednio przepisów nakazujących współpracę w ramach realizacji zadań

				na rzecz poszerzania wiedzy i budowania odporności podmiotów krytycznych; 9) uczestniczy w planowaniu i organizowaniu ćwiczeń podmiotów krytycznych oraz w razie potrzeby bierze w nich udział; 10) współpracuje z innymi organami do spraw podmiotów krytycznych oraz organami właściwymi do spraw cyberbezpieczeństwa, o których mowa w ustawie o ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa; 11) współpracuje, za pośrednictwem Pojedynczego Punktu Kontaktowego z odpowiednimi organami państw członkowskich;	organu, mogą prowadzić na podstawie innych przepisów prawa bieżącą współpracę z organami krajowymi, które zajmują się m.in. ochroną ludności, egzekwowaniem prawa czy też ochroną danych osobowych.
Art. 9	6. Każde państwo członkowskie zapewnia, aby jego właściwy organ na podstawie niniejszej dyrektywy współpracował i wymieniał się informacjami z właściwymi organami na podstawie dyrektywy (UE) 2022/2555 w zakresie ryzyk w cyberprzestrzeni, cyberzagrożeń i cyberincydentów oraz ryzyk, zagrożeń i incydentów poza cyberprzestrzenią wpływających na podmioty krytyczne, w tym w odniesieniu do odpowiednich środków podjętych przez jego właściwy organ i właściwe organy na podstawie dyrektywy (UE) 2022/2555.	T	Art. 1 pkt 7 projektu (art. 6zl pkt 10 ustawy o zarządzaniu kryzysowym)	Art. 6zl. Organ do spraw podmiotów krytycznych: 10) współpracuje z innymi organami do spraw podmiotów krytycznych oraz organami właściwymi do spraw cyberbezpieczeństwa, o których mowa w ustawie o ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;	
Art. 9	7. W terminie trzech miesięcy od wyznaczenia lub ustanowienia właściwego organu i pojedynczego punktu kontaktowego każde państwo członkowskie powiadamia Komisję o ich danych identyfikacyjnych i o ich zadaniach i obowiązkach wynikających z niniejszej dyrektywy, o ich danych kontaktowych oraz o wszelkich późniejszych zmianach w tym zakresie. Państwa członkowskie informują Komisję, w przypadku gdy postanowiły wyznaczyć organ inny niż organy właściwe, o których mowa w ust. 1 akapit drugi, jako właściwe organy w odniesieniu do	T	Art. 1 pkt 7 projektu ustawy (art. 6zm ust. 5 pkt 1 lit. a) Art. 26 ust. 3 projektu ustawy	(Art. 6zm) 5. Pojedynczy Punkt Kontaktowy przekazuje Komisji Europejskiej: 1) niezwłocznie informacje o: a) wyznaczonych organach do spraw podmiotów krytycznych, Pojedynczym Punkcie Kontaktowym, ich zadaniach oraz późniejszych zmianach w tym zakresie, Art. 26 3. Pojedynczy Punkt Kontaktowy, o którym mowa w art. 6zm ust. 1 ustawy zmienianej w art. 1 przekazuje Komisji Europejskiej dane kontaktowe	

	podmiotów krytycznych w sektorach określonych w pkt 3, 4 i 8 tabeli w załączniku. Każde państwo członkowskie podaje do publicznej wiadomości informację o danych identyfikacyjnych właściwego organu i pojedynczego punktu kontaktowego.			wyznaczonych organów do spraw podmiotów krytycznych, Pojedynczego Punktu Kontaktowego oraz wskazuje zakres realizowanych zadań, w terminie trzech miesięcy od dnia wejścia w życie ustawy.	
Art. 9	8. Komisja podaje do wiadomości publicznej wykaz pojedynczych punktów kontaktowych.	N			
Art. 10	Artykuł 10 Wsparcie państw członkowskich na rzecz podmiotów krytycznych 1. Państwa członkowskie wspierają podmioty krytyczne w zwiększaniu ich odporności. Wsparcie to może obejmować opracowywanie materiałów zawierających wytyczne oraz metodyk, pomoc w organizacji ćwiczeń mających na celu sprawdzenie odporności tych podmiotów oraz zapewnianie doradztwa i szkoleń dla personelu podmiotów krytycznych. Bez uszczerbku dla mających zastosowanie przepisów dotyczących pomocy państwa, jeżeli jest to konieczne i uzasadnione celami interesu publicznego, państwa członkowskie mogą przekazywać zasoby finansowe podmiotom krytycznym.	T	Art. 1 pkt 7 projektu (art. 6zl pkt 4,5,8,9 ustawy o zarządzaniu kryzysowym)	Art. 6zl. Organ do spraw podmiotów krytycznych: 4) prowadzi bieżącą wymianę informacji z podmiotami krytycznymi oraz ułatwia dobrowolną wymianę informacji między podmiotami krytycznymi w danym sektorze lub podsektorze 5) współpracuje z podmiotami krytycznymi w danym sektorze lub podsektorze w zakresie obsługi incydentów; 8) prowadzi działania informacyjne dotyczące dobrych praktyk, działań edukacyjnych i kampanii na rzecz poszerzania wiedzy i budowania odporności podmiotów krytycznych; 9) uczestniczy w planowaniu i organizowaniu ćwiczeń podmiotów krytycznych oraz w razie potrzeby bierze w nich udział;	
Art. 10	2. Każde państwo członkowskie zapewnia, aby jego właściwy organ współpracował z podmiotami krytycznymi z sektorów określonych w załączniku oraz aby prowadził z nimi wymianę informacji i dobrych praktyk.	T	Art. 1 pkt 7 projektu (art. 6zl pkt 4,5,8,9 ustawy o zarządzaniu kryzysowym)	Art. 6zl. Organ do spraw podmiotów krytycznych: 4) prowadzi bieżącą wymianę informacji z podmiotami krytycznymi oraz zapewnia ułatwia dobrowolną wymianę informacji między podmiotami krytycznymi w danym sektorze lub podsektorze 5) współpracuje z podmiotami krytycznymi w danym sektorze lub podsektorze w zakresie obsługi incydentów; 8) prowadzi działania informacyjne dotyczące dobrych praktyk, działań edukacyjnych i kampanii na rzecz poszerzania wiedzy i budowania odporności podmiotów krytycznych;	

				9) uczestniczy w planowaniu i organizowaniu ćwiczeń podmiotów krytycznych oraz w razie potrzeby bierze w nich udział;	
Art. 10	3. Państwa członkowskie ułatwiają dobrowolną wymianę informacji między podmiotami krytycznymi w odniesieniu do kwestii objętych niniejszą dyrektywą zgodnie z prawem Unii i prawem krajowym, w szczególności z przepisami dotyczącymi informacji niejawnych i szczególnie chronionych, konkurencji i ochrony danych osobowych.	T	Art. 1 pkt 7 projektu (art. 6zl pkt 4 i 8 ustawy o zarzadzaniu kryzysowym)	Art. 6zl. Organ do spraw podmiotów krytycznych: 4) prowadzi bieżącą wymianę informacji z podmiotami krytycznymi oraz ułatwia dobrowolną wymianę informacji między podmiotami krytycznymi w danym sektorze lub podsektorze; 8) współpracuje z innymi organami do spraw podmiotów krytycznych oraz organami właściwymi do spraw cyberbezpieczeństwa, o których mowa w ustawie o ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;	Wymiana informacji na potrzeby realizacji zadań w obszarze podmiotów krytycznych będzie odbywać się z zachowaniem bezpieczeństwa i poufności tychże informacji, na podstawie obowiązujących przepisów, w tym przepisów ustawy o ochronie informacji niejawnych, ustawy o zwalczaniu nieuczciwej konkurencji oraz ustawy o ochronie danych osobowych.
Art. 11	Artykuł 11 Współpraca między państwami członkowskimi 1. W stosownych przypadkach państwa członkowskie prowadzą wzajemne konsultacje dotyczące podmiotów krytycznych w celu zapewnienia spójnego stosowania niniejszej dyrektywy. Konsultacje takie odbywają się w szczególności w odniesieniu do podmiotów krytycznych, które: a) korzystają z infrastruktury krytycznej, która jest fizycznie połączona na terytorium co najmniej dwóch państw członkowskich;	T	Art. 1 pkt 7 projektu (art. 6zn ust. 1 ustawy o zarządzaniu kryzysowym)	Art. 6zn. 1. Na potrzeby realizacji zadań, o których mowa w art. 6zl, organy do spraw podmiotów krytycznych, za pośrednictwem Pojedynczego Punktu Kontaktowego, prowadzą konsultacje z właściwymi organami państw członkowskich w przypadku gdy podmioty krytyczne: 1) korzystają z infrastruktury krytycznej, która jest fizycznie połączona na terytorium co najmniej dwóch państw członkowskich; 2) są częścią struktur przedsiębiorstw połączonych lub powiązanych z podmiotami krytycznymi w innych państwach członkowskich; 3) zostały zidentyfikowane jako podmioty krytyczne w jednym państwie członkowskim i świadczą usługi kluczowe na rzecz innych państw	

	b) są częścią struktur przedsiębiorstw połączonych lub powiązanych z podmiotami krytycznymi w innych państwach członkowskich; c) zostały zidentyfikowane jako podmioty krytyczne w jednym państwie członkowskim i świadczą usługi kluczowe na rzecz innych państw członkowskich lub w innych państwach członkowskich.			członkowskich lub w innych państwach członkowskich.	
Art. 11	2. Konsultacje, o których mowa w ust. 1, mają na celu zwiększenie odporności podmiotów krytycznych oraz, w miarę możliwości, zmniejszenie ich obciążenia administracyjnego.	T	Art. 1 pkt 7 projektu (art. 6zn ust. 1 i 2 ustawy o zarządzaniu kryzysowym)	Art. 6zn. 1. Na potrzeby realizacji zadań, o których mowa w art. 6zl, organy do spraw podmiotów krytycznych (…) prowadzą konsultacje (…) 2. W konsultacjach, o których mowa w ust. 1, organy do spraw podmiotów krytycznych wypracowują, w zależności od potrzeb, rozwiązania w zakresie zwiększania odporności lub redukcji obciążeń administracyjnych podmiotów krytycznych.	
Art. 12	ROZDZIAŁ III ODPORNOŚĆ PODMIOTÓW KRYTYCZNYCH Artykuł 12 Ocena ryzyka przeprowadzana przez podmioty krytyczne 1. Niezależnie od terminu określonego w art. 6 ust. 3 akapit drugi państwa członkowskie zapewniają przeprowadzenie oceny ryzyka przez podmioty krytyczne w terminie dziewięciu miesięcy po otrzymaniu powiadomienia, o którym mowa w art. 6 ust. 3, a następnie w razie potrzeby, co najmniej co cztery lata, na podstawie ocen ryzyka państw członkowskich i innych istotnych źródeł informacji, aby ocenić wszystkie istotne czynniki ryzyka, które mogłyby zakłócać świadczenie ich usług kluczowych zwanej dalej „oceną ryzyka podmiotu krytycznego”	T	Art. 1 pkt 7 projektu ustawy (art. 6zt ust.1 pkt 1 ustawy o zarządzaniu kryzysowym)	Art. 6zt. 1. Podmiot krytyczny wdraża zintegrowany system zarządzania bezpieczeństwem świadczenia usługi kluczowej obejmujący: 1) przeprowadzenie nie rzadziej niż raz na 2 lata oceny ryzyka z uwzględnieniem: a) zagrożeń i związanych z tym ryzyk wymienionych w Krajowej Ocenie Ryzyka oraz innych zagrożeń charakterystycznych dla świadczonej usługi kluczowej, w tym zagrożeń antagonistycznych, b) stopnia zależności innych sektorów lub podsektorów określonych w załączniku do ustawy od usługi kluczowej świadczonej przez podmiot krytyczny oraz stopnia zależności tego podmiotu krytycznego od usług kluczowych świadczonych przez inne podmioty w innych sektorach, w tym w stosownych przypadkach w sąsiadujących państwach członkowskich Unii Europejskiej i w państwach trzecich,	

				c) identyfikacji alternatywnych łańcuchów dostaw w celu przywrócenia świadczenia usługi kluczowej, d) ocen ryzyka prowadzonych na podstawie odrębnych przepisów;	
Art. 12	2. Oceny ryzyka podmiotów krytycznych obejmują wszystkie istotne naturalne i spowodowane przez człowieka czynniki ryzyka mogące prowadzić do incydentu, w tym czynniki ryzyka o charakterze międzysektorowym lub transgranicznym, wypadki, klęski żywiołowe, stany zagrożenia zdrowia publicznego i zagrożenia hybrydowe oraz inne zagrożenia związane z konfliktem, w tym przestępstwa terrorystyczne przewidziane w dyrektywie (UE) 2017/541. Ocena ryzyka podmiotu krytycznego musi uwzględniać stopień zależności innych sektorów określonych w załączniku od usługi kluczowej świadczonej przez podmiot krytyczny oraz stopień zależności tego podmiotu krytycznego od usług kluczowych świadczonych przez inne podmioty w takich innych sektorach, w tym w stosownych przypadkach w sąsiadujących państwach członkowskich i w państwach trzecich. W przypadku gdy podmiot krytyczny przeprowadził inne oceny ryzyka lub sporządził	T	Art. 1 pkt 7 projektu ustawy (art. 6zt ust.1 pkt 1, ust. 3, ust. 11 ustawy o zarządzaniu kryzysowym)	Art. 6zt. 1.Podmiot krytyczny wdraża zintegrowany system zarządzania bezpieczeństwem świadczenia usługi kluczowej obejmujący: 1) przeprowadzenie nie rzadziej niż raz na 2 lata oceny ryzyka z uwzględnieniem: a) zagrożeń i związanych z tym ryzyk wymienionych w Krajowej Ocenie Ryzyka oraz innych zagrożeń charakterystycznych dla świadczonej usługi kluczowej, w tym zagrożeń antagonistycznych, b) stopnia zależności innych sektorów lub podsektorów określonych w załączniku do ustawy od usługi kluczowej świadczonej przez podmiot krytyczny oraz stopnia zależności tego podmiotu krytycznego od usług kluczowych świadczonych przez inne podmioty w innych sektorach, w tym w stosownych przypadkach w sąsiadujących państwach członkowskich Unii Europejskiej i w państwach trzecich, c) identyfikacji alternatywnych łańcuchów dostaw w celu przywrócenia świadczenia usługi kluczowej, d) ocen ryzyka prowadzonych na podstawie odrębnych przepisów; 3. Podmiot krytyczny przeprowadza po raz pierwszy ocenę ryzyka, o której mowa w ust. 1 pkt 1, w terminie 9 miesięcy od otrzymania informacji o ujęciu w wykazie podmiotów krytycznych. Art. 6zt. 1. Podmiot krytyczny wdraża zintegrowany system zarządzania	

	dokumenty zgodnie z obowiązkami określonymi w innych aktach prawnych, które to oceny ryzyka lub dokumenty są istotne dla jego oceny ryzyka podmiotu krytycznego, podmiot ten może wykorzystać te oceny i dokumenty do spełnienia wymogów określonych w niniejszym artykule. Wykonując swoje funkcje nadzorcze, właściwy organ może uznać istniejącą ocenę ryzyka przeprowadzoną przez podmiot krytyczny, która odnosi się do czynników ryzyka i stopnia zależności, o których mowa w akapicie pierwszym niniejszego ustępu, za spełniającą –w całości lub w części – wymogi niniejszego artykułu.			bezpieczeństwem świadczenia usługi kluczowej obejmujący: 1) przeprowadzenie nie rzadziej niż raz na 2 lata oceny ryzyka z uwzględnieniem: d) ocen ryzyka prowadzonych na podstawie odrębnych przepisów; 11. W przypadku gdy podmiot krytyczny prowadzi ocenę ryzyka oraz opracowuje dokumentację dotyczącą oceny ryzyka na podstawie odrębnych przepisów, odpowiadającą przepisom rozdziału 11 ustawy, uznaje się wymóg prowadzenia oceny ryzyka za spełniony w całości lub w części.	
Art. 13	Artykuł 13 Środki w zakresie odporności wprowadzane przez podmioty krytyczne 1. Państwa członkowskie zapewniają, aby podmioty krytyczne wprowadzały odpowiednie i proporcjonalne środki techniczne, środki bezpieczeństwa i środki organizacyjne służące zapewnieniu ich odporności, w oparciu o odpowiednie informacje dostarczone przez państwa członkowskie dotyczące oceny ryzyka państwa członkowskiego oraz wyników oceny ryzyka podmiotu krytycznego, w tym środki niezbędne w celu: a) zapobiegania incydentom, z należytym uwzględnieniem środków zmniejszania ryzyka związanego z katastrofami i przystosowania się do zmiany klimatu; b) zapewnienia odpowiedniej fizycznej ochrony ich budynków i terenów oraz infrastruktury krytycznej, z należytym uwzględnieniem na przykład zainstalowania ogrodzeń, budowy barier, narzędzi i procedur monitorowania terenu podlegającego ochronie, sprzętu do wykrywania i kontroli dostępu;	T	Art. 1 pkt 7 projektu ustawy (art. 6zt ust.1-ust. 4, ust. 8 ustawy o zarządzaniu kryzysowym)	Art. 6zt. 1. Podmiot krytyczny wdraża zintegrowany system zarządzania bezpieczeństwem świadczenia usługi kluczowej obejmujący: 2) wdrożenie odpowiednich i proporcjonalnych do wyników oceny ryzyka rozwiązań organizacyjno-technicznych, w szczególności: a) polityk zarządzania ryzykiem, b) bezpieczeństwa fizycznego, w tym ochrony fizycznej budynków i terenów należących do podmiotu krytycznego oraz zabezpieczeń technicznych, uwzględniających kontrolę dostępu, c) ochrony infrastruktury krytycznej niezbędnej do świadczenia usługi kluczowej, zgodnie z wymogami ochrony infrastruktury krytycznej, o których mowa w przepisach rozdziału 7 ustawy, d) bezpieczeństwa osobowego dotyczącego pracowników i dostawców zewnętrznych, e) cyberbezpieczeństwa, zgodnie z wymogami dotyczącymi podmiotów kluczowych, o których mowa w przepisach ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, f) bezpieczeństwa prawnego świadczenia usługi kluczowej, g) ciągłości działania i odtwarzania, w tym utrzymywania własnych systemów rezerwowych zapewniających bezpieczeństwo i	

	c) odpowiedzi na incydenty, stawiania im oporu i łagodzenia ich skutków, z należytym uwzględnieniem wdrażania procedur i protokołów zarządzania ryzykiem i zarządzania kryzysowego, a także procedur ostrzegawczych; d) odtworzenia po incydentach, z należytym uwzględnieniem środków na rzecz ciągłości działania oraz identyfikacji alter natywnych łańcuchów dostaw w celu przywrócenia świadczenia usługi kluczowej; e) zapewnienia odpowiedniego zarządzania bezpieczeństwem pracowników, z należytym uwzględnieniem środków takich jak ustanowienie kategorii personelu wykonującego funkcje krytyczne, ustanowienie praw dostępu do budynków i terenów, infrastruktury krytycznej i informacji szczególnie chronionych, ustanowienie procedur sprawdzenia przeszłości zgodnie z art. 14, wyznaczenie kategorii osób podlegających takim procedurom sprawdzenia przeszłości oraz określenie odpowiednich wymogów szkoleniowych i kwalifikacji; f) zwiększania świadomości odpowiedniego personelu na temat środków, o których mowa w lit. a)–e), z należytym uwzględnieniem szkoleń, materiałów informacyjnych i ćwiczeń. Do celów akapitu pierwszego lit. e) państwa członkowskie zapewniają, aby podmioty krytyczne uwzględniały personel zewnętrznych dostawców usług przy określaniu kategorii personelu, który wykonuje funkcje krytyczne.			podtrzymujących funkcjonowanie świadczenia usługi kluczowej do czasu jej pełnego odtworzenia, h) zdolności do ochrony informacji niejawnych w niezbędnym zakresie do zapewnienia świadczenia usługi kluczowej, i) szkoleń i ćwiczeń personelu w celu jego przygotowania na różnego rodzaju zagrożenia i incydenty, j) realizacji okresowych audytów i certyfikacji; 2. Rozwiązania organizacyjno-techniczne, o których mowa w ust. 1 pkt 2, uwzględniają wymagania określone w normach oraz wytycznych do ich stosowania, wskazanych w przepisach wydanych na podstawie ust. 5. 4. Podmiot krytyczny wdraża rozwiązania organizacyjno-techniczne, o których mowa w ust. 1 pkt 2, w terminie 3 miesięcy od dnia przeprowadzenia po raz pierwszy oceny ryzyka, a następnie stosownie do potrzeb, w zależności od wyników przeprowadzonej oceny ryzyka. 8. Podmiot krytyczny, przy opracowywaniu i zawieraniu umów zapewniających wdrożenie rozwiązań, o których mowa w ust. 1 pkt 2, żąda od usługodawców: 1) certyfikatów, uwzględniając dokumenty równoważne, zgodnie z zasadami wzajemnego uznawania w Unii Europejskiej lub w przypadku ich braku innych dokumentów właściwych dla poszczególnych rozwiązań, potwierdzających posiadanie odpowiednich kompetencji i uprawnień niezbędnych do ich realizacji; 2) potwierdzenia zdolności do ochrony informacji niejawnych oraz stosowania przepisów o ochronie informacji niejawnych, jeżeli opracowanie, przygotowanie i wykonanie umowy wiążą się dostępem do informacji niejawnych.	
Art. 13	2. Państwa członkowskie zapewniają, aby podmioty krytyczne posiadały i stosowały plan zwiększania odporności lub równoważny	T	Art. 1 pkt 7 projektu ustawy (art. 6zu ust.1, ust. 2 ustawy o	Art. 6zu.1. Podmiot krytyczny opracowuje, stosuje i aktualizuje dokumentację zintegrowanego	

	dokument lub równoważne dokumenty opisujące środki zastosowane na podstawie ust. 1. W przypadku gdy podmioty krytyczne sporządziły dokumenty lub zastosowały środki zgodnie z ustanowionymi w innych aktach prawnych obowiązkami, które są istotne dla środków określonych w ust. 1, podmioty te mogą skorzystać z tych dokumentów i środków do spełnienia wymogów określonych w niniejszym artykule. Wykonując swoje funkcje nadzorcze, właściwy organ może uznać istniejące środki w zakresie zwiększania odporności zastosowane przez podmiot krytyczny, które w odpowiedni i proporcjonalny sposób obejmują środki techniczne, środki bezpieczeństwa i środki organizacyjne, o których mowa w ust. 1, za spełniające – w całości lub w części – obowiązki wynikające z niniejszego artykułu.		zarządzaniu kryzysowym)	systemu zarządzania bezpieczeństwem świadczenia usługi kluczowej. 2. Dokumentację zintegrowanego systemu zarządzania bezpieczeństwem świadczenia usługi kluczowej stanowią: 1) dokumentacja systemu zarządzania bezpieczeństwem informacji; 2) dokumentacja systemu zarządzania ciągłością działania usługi kluczowej; 3) dokumentacja ochrony fizycznej oraz zabezpieczeń technicznych, o których mowa w art. 6zt ust. 1 pkt 2 lit. b oraz bezpieczeństwa osobowego, o którym mowa w art. 6zt ust. 1 pkt 2 lit. d; 4) dokumentacja ochrony infrastruktury krytycznej, o której mowa w art. 6zf ust. 1; 5) dokumentacja cyberbezpieczeństwa, opracowywana zgodnie z wymogami dla podmiotów kluczowych, o których mowa w przepisach ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa; 6) inna dokumentacja niż wskazana w pkt 1-5, biorąc pod uwagę rodzaj świadczonej usługi kluczowej.	
Art. 13	3. Państwa członkowskie zapewniają, aby każdy podmiot krytyczny wyznaczył urzędnika łącznikowego lub jego odpowiednika jako punkt kontaktowy z właściwymi organami.	T	Art. 1 pkt 7 projektu ustawy (art. 6zzd ustawy o zarządzaniu kryzysowym)	Art. 6zzd. 1. W celu realizacji zadań, o których mowa w art. 6zt ust. 1, art. 6zu ust. 1, art. 6zv ust. 1, art. 6zzb ust. 1 oraz art. 6zzc ust. 1, podmiot krytyczny wyznacza pełnomocnika bezpieczeństwa usługi kluczowej oraz zastępcę pełnomocnika bezpieczeństwa usługi kluczowej. 2. Podmiot krytyczny wyznacza pełnomocnika bezpieczeństwa usługi kluczowej oraz zastępcę pełnomocnika bezpieczeństwa usługi kluczowej w terminie 30 dni od dnia otrzymania informacji o ujęciu w wykazie podmiotów krytycznych. 3. Zastępca pełnomocnika bezpieczeństwa usługi kluczowej zastępuje pełnomocnika w czasie jego nieobecności lub czasowej niemożności wykonywania przez niego obowiązków.	

				4. Pełnomocnikiem bezpieczeństwa usługi kluczowej może być osoba, która: 1) jest pracownikiem podmiotu krytycznego albo żołnierzem lub funkcjonariuszem pełniącym służbę w jednostce organizacyjnej będącej podmiotem krytycznym; 2) korzysta z pełni praw publicznych; 3) posiada wiedzę, umiejętności i doświadczenie w zakresie zarządzania bezpieczeństwem, z uwzględnieniem przedmiotu działalności podmiotu świadczące usługę kluczową; 4) nie była skazana prawomocnym wyrokiem za umyślne przestępstwo lub umyślne przestępstwo skarbowe; 5) spełnia wymagania bezpieczeństwa osobowego w zakresie dostępu do informacji niejawnych o klauzuli „poufne”. 5. Pełnomocnik bezpieczeństwa usługi kluczowej podlega bezpośrednio organowi zarządzającemu podmiotu krytycznego. 6. O wyznaczeniu pełnomocnika bezpieczeństwa usługi kluczowej podmiot krytyczny informuje niezwłocznie właściwy organ do spraw podmiotów krytycznych oraz dyrektora Centrum, przekazując dane tej osoby obejmujące imię i nazwisko, numer telefonu oraz adres poczty elektronicznej. 7. Podmiot krytyczny zapewnia pełnomocnikowi bezpieczeństwa usługi kluczowej organizacyjne i techniczne warunki realizacji zadań, w tym dostęp do niezbędnych dokumentów i informacji. 8. Przepisy, o których mowa w ust. 4-7, stosuje się do zastępcy pełnomocnika bezpieczeństwa usługi kluczowej.	
Art. 13	4. Na wniosek państwa członkowskiego, które zidentyfikowało podmiot krytyczny, oraz za zgodą zainteresowanego podmiotu krytycznego Komisja organizuje misje doradcze – zgodnie z ustaleniami określonymi w art. 18 ust. 6, 8 i 9 – w celu zapewnienia zainteresowanemu podmiotowi krytycznemu doradztwa w zakresie wypełniania	T		Art. 6zzh. 4. Przepisy ust. 2 i 3 stosuje się odpowiednio do misji doradczej organizowanej dla podmiotu krytycznego niebędącego podmiotem krytycznym o szczególnym znaczeniu europejskim za zgodą tego podmiotu, na wniosek organu do spraw	Regulacje w ramach obsługi misji doradczej zostały określone w projektowanych przepisach dotyczących kwestii podmiotów

	przez niego obowiązków na podstawie rozdziału III. Misja doradcza zgłasza swoje ustalenia Komisji, danemu państwu członkowskiemu oraz zainteresowanemu podmiotowi krytycznemu.			podmiotów krytycznych, który zidentyfikował podmiot krytyczny.	krytycznych no szczególnym znaczeniu europejskim (projektowany przepis art. 6zzh ustawy o zarządzaniu kryzysowym).
Art. 13	5. Po konsultacji z Grupą ds. Odporności Podmiotów Krytycznych, o której mowa w art. 19, Komisja przyjmuje niewiążące wytyczne w celu doprecyzowania środków technicznych, środków bezpieczeństwa i środków organizacyjnych, które można wprowadzić na podstawie ust. 1 niniejszego artykułu.	N			
Art. 13	6. Komisja przyjmuje akty wykonawcze w celu określenia niezbędnych specyfikacji technicznych i metodycznych związanych ze stosowaniem środków, o których mowa w ust. 1 niniejszego artykułu. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 24 ust. 2.	N			
Art. 14	Artykuł 14 Sprawdzenie przeszłości 1. Państwa członkowskie określają warunki, na podstawie których podmiot krytyczny może – w należycie uzasadnionych przypadkach i z uwzględnieniem oceny ryzyka państwa członkowskiego – składać wnioski o sprawdzenie przeszłości osób, które: a) pełnią newralgiczne role w podmiocie krytycznym lub na jego rzecz, w szczególności w odniesieniu do odporności podmiotu krytycznego; b) są upoważnione do posiadania bezpośredniego lub zdalnego dostępu do budynków i terenów podmiotu krytycznego, jego informacji lub	T	Art. 1 pkt 7 projektu ustawy (art. 6zzc ust.1 ustawy o zarządzaniu kryzysowym)	Art. 6zzc. 1. Podmiot krytyczny, w celu zapewnienia ochrony ciągłości świadczenia usługi kluczowej, może prowadzić sprawdzenie przeszłości w odniesieniu do: 1) pracownika podmiotu krytycznego lub kandydata na pracownika: a) pełniącego newralgiczną rolę bezpośrednio w strukturze organizacyjnej podmiotu krytycznego lub działając na jego rzecz, w tym: - reprezentującego podmiot krytyczny samodzielnie lub łącznie z innymi osobami na podstawie statutu, umowy lub innego aktu założycielskiego, - pełniącego funkcje kierownicze lub koordynacyjne, b) posiadającego bezpośredni lub zdalny dostęp do budynków i terenów podmiotu krytycznego,	

	systemów kontroli, w tym w związku z bezpieczeństwem podmiotu krytycznego; c) są brane pod uwagę przy rekrutacji na stanowiska objęte kryteriami, określonymi w lit. a) lub b).			obiegu informacji lub systemów kontroli, w szczególności związanych z bezpieczeństwem podmiotu krytycznego, c) realizującego audyt, o którym mowa w art. 6zz ust. 1; 2) osoby świadczącej usługę na rzecz podmiotu krytycznego, niebędącej pracownikiem podmiotu krytycznego, posiadającej bezpośredni lub zdalny dostęp do budynków i terenów podmiotu krytycznego, obiegu informacji lub systemów kontroli, w szczególności związanych z bezpieczeństwem podmiotu krytycznego.	
Art. 14	2. Wnioski, o których mowa w ust. 1 niniejszego artykułu, są rozpatrywane w rozsądnym terminie i przetwarzane zgodnie z krajowymi przepisami i procedurami oraz z odpowiednim i mającym zastosowanie prawem Unii, w tym z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 i dyrektywą Parlamentu Europejskiego i Rady (UE) 2016/680 ( ). Sprawdzanie przeszłości musi być proporcjonalne i ściśle ograniczone do tego, co jest konieczne. Przeprowadza się je wyłącznie w celu oceny potencjalnego ryzyka dla bezpieczeństwa odnośnego podmiotu krytycznego.	T	Art. 1 pkt 7 projektu ustawy (art. 6zzc ust. 3, ust. 4 ustawy o zarządzaniu kryzysowym)	Art. 6zzc. 1. Podmiot krytyczny, w celu zapewnienia ochrony ciągłości świadczenia usługi kluczowej, może prowadzić sprawdzenie przeszłości w odniesieniu do: 3. Podmiot krytyczny, w odniesieniu do osoby, o której mowa w ust. 1 pkt 1, w celu: 1) potwierdzenia tożsamości: a) żąda przedłożenia ważnego dowodu osobistego lub ważnego dokumentu paszportowego tej osoby oraz podania nazwiska rodowego i poprzednio noszonego nazwiska, jeżeli było zmieniane, oraz nazwisk, imion, dat i miejsc urodzenia rodziców, b) wnioskuje do organu dowolnej gminy o udostępnienie danych jednostkowych zawartych w rejestrze PESEL oraz o udostępnienie danych w trybie jednostkowym z Rejestru Dowodów Osobistych; 2) dokonania oceny informacji pozyskanych z rejestrów karnych: a) pozyskuje informację z Krajowego Rejestru Karnego w zakresie skazań za przestępstwa umyślne ścigane z oskarżenia publicznego oraz umyślne przestępstwa skarbowe, b) występuje do Biura Informacyjnego Krajowego Rejestru Karnego z wnioskiem o wystąpienie do organów centralnych państw członkowskich Unii Europejskiej państwa obywatelstwa osoby	Terminy rozpatrywania i przetwarzania wniosków realizowane są na podstawie odrębnych przepisów, m.in. ustawy o Krajowym Rejestrze Karnym.

				podlegającej sprawdzeniu przeszłości z zapytaniem o udzielenie informacji o osobie, w przypadku gdy osoba podlegająca sprawdzeniu ma obywatelstwo państwa członkowskiego innego niż Rzeczpospolita Polska. 4. Podmiot krytyczny, w odniesieniu do osoby, o której mowa w ust. 1 pkt 2, ma prawo żądać: 1) przedłożenia przez tę osobę ważnego dowodu osobistego lub ważnego dokumentu paszportowego tej osoby oraz podania nazwiska rodowego i poprzednio noszonego nazwiska, jeżeli było zmieniane, oraz nazwisk, imion, dat i miejsc urodzenia rodziców; 2) przedłożenia przez tę osobę informacji z Krajowego Rejestru Karnego w zakresie skazań za przestępstwa umyślne ścigane z oskarżenia publicznego oraz umyślne przestępstwa skarbowe.	
Art. 14	3. W ramach sprawdzenia przeszłości, o którym mowa w ust. 1, dokonuje się co najmniej: a) potwierdzenia tożsamość osoby, która podlega sprawdzeniu przeszłości; b) sprawdzenia rejestrów karnych tej osoby pod kątem przestępstw, które miałyby znaczenie dla danego stanowiska; Podczas przeprowadzania sprawdzenia przeszłości państwa członkowskie wykorzystują europejski system przekazywania informacji z rejestrów karnych zgodnie z procedurami określonymi w decyzji ramowej 2009/315/WSiSW oraz, w razie potrzeby i w stosownych przypadkach, w rozporządzeniu (UE) 2019/816 w celu uzyskania informacji z rejestrów karnych prowadzonych przez inne państwa członkowskie. Organy centralne, o których mowa w art. 3 ust. 1 decyzji ramowej 2009/315/WSiSW oraz w art. 3 pkt 5 rozporządzenia (UE) 2019/816, udzielają odpowiedzi na wnioski o przekazanie takich informacji w terminie 10 dni roboczych od	T	Art. 1 pkt 7 projektu ustawy (art. 6zzc ust.2, ust. 3, ust. 4, ust. 8 ustawy o zarządzaniu kryzysowym)	(Art. 6zzc) 2. Sprawdzenie przeszłości osób, o których mowa w ust. 1, obejmuje: 1) potwierdzenie tożsamości; 2) ocenę informacji pozyskanych z rejestrów karnych pod kątem przestępstw, które mogą mieć znaczenie dla zajmowanego stanowiska, ubiegania się o to stanowisko lub świadczenia usług na rzecz podmiotu krytycznego. 3. Podmiot krytyczny, w odniesieniu do osoby, o której mowa w ust. 1 pkt 1, w celu: 1) potwierdzenia tożsamości: a) żąda przedłożenia ważnego dowodu osobistego lub ważnego dokumentu paszportowego tej osoby oraz podania nazwiska rodowego i poprzednio noszonego nazwiska, jeżeli było zmieniane, oraz nazwisk, imion, dat i miejsc urodzenia rodziców, b) wnioskuje do organu dowolnej gminy o udostępnienie danych jednostkowych zawartych w rejestrze PESEL oraz o udostępnienie danych w trybie jednostkowym z Rejestru Dowodów Osobistych;	

	dnia otrzymania wniosku zgodnie z art. 8 ust. 1 decyzji ramowej 2009/315/WSiSW.			2) dokonania oceny informacji pozyskanych z rejestrów karnych: a) pozyskuje informację z Krajowego Rejestru Karnego w zakresie skazań za przestępstwa umyślne ścigane z oskarżenia publicznego oraz umyślne przestępstwa skarbowe, b) występuje do Biura Informacyjnego Krajowego Rejestru Karnego z wnioskiem o wystąpienie do organów centralnych państw członkowskich Unii Europejskiej państwa obywatelstwa osoby podlegającej sprawdzeniu przeszłości z zapytaniem o udzielenie informacji o osobie, w przypadku gdy osoba podlegająca sprawdzeniu ma obywatelstwo państwa członkowskiego innego niż Rzeczpospolita Polska. 4. Podmiot krytyczny, w odniesieniu do osoby, o której mowa w ust. 1 pkt 2, ma prawo żądać: 1) przedłożenia przez tę osobę ważnego dowodu osobistego lub ważnego dokumentu paszportowego tej osoby oraz podania nazwiska rodowego i poprzednio noszonego nazwiska, jeżeli było zmieniane, oraz nazwisk, imion, dat i miejsc urodzenia rodziców; 2) przedłożenia przez tę osobę informacji z Krajowego Rejestru Karnego w zakresie skazań za przestępstwa umyślne ścigane z oskarżenia publicznego oraz umyślne przestępstwa skarbowe. (…) 8. Sprawdzenia przeszłości nie prowadzi się w odniesieniu do osoby wskazanej w ust. 1 pkt 1, która samodzielnie przedłożyła wymagane dokumenty albo posiada co najmniej poświadczenie bezpieczeństwa o klauzuli "poufne".	
Art. 15	Artykuł 15 Zgłaszanie incydentów 1. Państwa członkowskie zapewniają, aby podmioty krytyczne bez zbędnej zwłoki zgłaszały właściwemu organowi incydenty, które istotnie zakłócają lub mogą istotnie zakłócać świadczenie usług kluczowych. Państwa członkowskie	T	Art. 1 pkt 7 projektu ustawy (art. 6zv, art. 6zw ust. 4, art. 6zm ust. 1 pkt 3 ustawy o zarządzaniu kryzysowym)	Art. 6zv. 1. Podmiot krytyczny jest obowiązany do zarządzania incydentem, w tym: 1) zapewnienia obsługi incydentu; 2) zapewnienia dostępu do informacji o zarejestrowanym incydencie organowi do spraw podmiotów krytycznych oraz dyrektorowi Centrum;	

	zapewniają, aby podmioty krytyczne dokonały, chyba że jest to niemożliwe z operacyjnego punktu widzenia, zgłoszenia wstępnego –nie później niż 24 godziny od chwili uzyskania wiedzy o zaistnieniu incydentu, a następnie, w stosownych przypadkach, przedłożyły szczegółowe sprawozdanie w terminie nie dłuższym niż jeden miesiąc od zaistnienia incydentu. W celu określenia wagi zakłócenia uwzględnia się w szczególności następujące parametry: a) liczba i odsetek użytkowników dotkniętych zakłóceniem; b) czas trwania zakłócenia; c) obszar geograficzny, którego dotyczy zakłócenie, z uwzględnieniem tego, czy obszar jest geograficznie odizolowany.			3) klasyfikowania incydentu jako istotnego, na podstawie progów uznawania incydentu za istotny, określonych w przepisach wykonawczych wydanych na podstawie ust. 4; 4) zgłaszania incydentu istotnego niezwłocznie, nie później niż w terminie 24 godzin od momentu jego wystąpienia lub wykrycia: a) właściwemu organowi do spraw podmiotów krytycznych oraz dyrektorowi Centrum, b) Szefowi Agencji Bezpieczeństwa Wewnętrznego, c) podmiotowi, w ramach którego funkcjonuje Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT) poziomu krajowego; 5) współdziałania podczas obsługi incydentu istotnego z właściwym organem do spraw podmiotów krytycznych lub dyrektorem Centrum; 6) informowania właściwego organu do spraw podmiotów krytycznych oraz dyrektora Centrum o usunięciu incydentu istotnego; 7) w szczególnie uzasadnionych przypadkach przekazywania sprawozdania z czynności, o których mowa w pkt 1-6 organowi do spraw podmiotów krytycznych oraz dyrektorowi Centrum w terminie nie dłuższym niż miesiąc, licząc od dnia wystąpienia incydentu istotnego. 2. Zgłoszenie, o którym mowa w ust. 1 pkt 4, dokonuje się za pomocą systemu, o którym mowa w art. 46 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. 3. W przypadku braku możliwości dokonania zgłoszenia w systemie, o którym mowa w art. 46 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, zgłoszenie przekazywane jest na piśmie utrwalonym w postaci elektronicznej, opatrzonym kwalifikowanym podpisem elektronicznym, podpisem osobistym, podpisem zaufanym albo kwalifikowaną pieczęcią elektroniczną. 4. Rada Ministrów określi, w drodze rozporządzenia, progi uznania incydentu	

	W przypadku gdy incydent ma lub może mieć znaczący wpływ na ciągłość świadczenia usług kluczowych na rzecz co naj mniej sześciu państw członkowskich lub w co najmniej sześciu państwach członkowskich, właściwe organy państw członkowskich, których incydent ten dotyczy, powiadamiają o tym incydencie Komisję.			za incydent istotny według zdarzenia w poszczególnych sektorach i podsektorach określonych w załączniku do ustawy, w zależności od: 1) liczby użytkowników dotkniętych zakłóceniem, 2) czasu trwania zakłócenia usługi kluczowej, 3) obszaru geograficznego, którego dotyczy zakłócenie z uwzględnieniem jego odizolowania geograficznego, 4) innych czynników charakterystycznych dla danego sektora lub podsektora, jeżeli występują. Wydając rozporządzenie należy określić co najmniej jeden próg uznania incydentu za incydent istotny dla każdego zdarzenia kierując się potrzebą zapewnienia ochrony przed zagrożeniami życia lub zdrowia ludzi, znacznymi stratami majątkowymi oraz zagrożeniem obniżenia jakości świadczonej usługi kluczowej. (Art. 6zw) 4. Organ do spraw podmiotów krytycznych, za pośrednictwem Pojedynczego Punktu Kontaktowego, informuje Komisję Europejską o incydencie istotnym, który ma lub może mieć wpływ na ciągłość świadczenia usługi kluczowej na rzecz co najmniej sześciu państw członkowskich Unii Europejskiej lub w co najmniej sześciu państwach członkowskich Unii Europejskiej. Art. 6zm. 1. Dyrektor Centrum prowadzi Pojedynczy Punkt Kontaktowy do którego zadań należy: 3) opracowywanie i przekazywanie raz na dwa lata Komisji Europejskiej oraz Grupie do spraw Odporności Podmiotów Krytycznych sprawozdań dotyczących incydentów istotnych zgłaszanych przez podmioty krytyczne mających wpływ na ciągłość świadczonych przez nich usług kluczowych na terytorium Rzeczypospolitej Polskiej oraz ciągłość świadczonych usług	

				kluczowych w państwach członkowskich Unii Europejskiej;	
Art. 15	2. Zgłoszenia, o których mowa w ust. 1 akapit pierwszy, muszą zawierać wszelkie dostępne informacje, których właściwy organ potrzebuje, aby zrozumieć charakter, przyczynę i ewentualne konsekwencje incydentu, w tym wszelkie dostępne informacje niezbędne do ustalenia, czy dany incydent ma wpływ transgraniczny. Zgłoszenia takie nie mogą narażać podmiotów krytycznych na zwiększoną odpowiedzialność.	T	Art. 1 pkt 7 projektu ustawy (art. 6zw ust. 1, ust. 2 ustawy o zarządzaniu kryzysowym)	Art. 6zw. 1. Zgłoszenie, o którym mowa w art. 6zv ust. 1 pkt 4, zawiera: 1) dane podmiotu zgłaszającego, w tym firmę przedsiębiorcy, numer we właściwym rejestrze, siedzibę i adres; 2) imię i nazwisko, numer telefonu oraz adres poczty elektronicznej osoby dokonującej zgłoszenia; 3) imię i nazwisko, numer telefonu oraz adres poczty elektronicznej osoby uprawnionej do składania wyjaśnień dotyczących zgłaszanych informacji; 4) opis wpływu incydentu istotnego na świadczenie usługi kluczowej, w tym: a) usługi kluczowej zgłaszającego, na którą incydent miał wpływ, b) liczbę użytkowników usługi kluczowej, na których incydent miał wpływ, c) moment wystąpienia i wykrycia incydentu istotnego oraz czas jego trwania, d) obszar geograficzny, którego dotyczy incydent istotny, e) wpływ incydentu istotnego na świadczenie usług kluczowych przez inne podmioty krytyczne, f) przyczynę zaistnienia incydentu istotnego i sposób jego przebiegu oraz skutki jego oddziaływania na świadczoną usługę kluczową; 5) informacje umożliwiające właściwemu organowi do spraw podmiotów krytycznych oraz dyrektorowi Centrum określenie, czy incydent istotny dotyczy innych państw członkowskich Unii Europejskiej; 6) informacje o podjętych działaniach zapobiegawczych; 7) informacje o podjętych działaniach naprawczych; 8) inne istotne informacje.	

				2. Podmiot krytyczny przekazuje informacje znane mu w chwili dokonywania zgłoszenia, które uzupełnia w trakcie obsługi incydentu istotnego.	
Art. 15	3. Na podstawie informacji przekazanych przez podmiot krytyczny w zgłoszeniu, o którym mowa w ust. 1, odpowiedni właściwy organ – za pośrednictwem pojedynczego punktu kontaktowego – informuje o tym incydencie pojedynczy punkt kontaktowy innego państwa członkowskiego, którego dotyczy incydent, jeżeli incydent ma lub może mieć istotny wpływ na podmioty krytyczne oraz na ciągłość świadczenia usług kluczowych na rzecz co najmniej jednego innego państwa członkowskiego lub w co najmniej jednym innym państwie członkowskim. Pojedyncze punkty kontaktowe wysyłając i otrzymując informacje zgodnie z akapitem pierwszym traktują te informacje w sposób zapewniający zachowanie ich poufności zgodnie z prawem Unii lub prawem krajowym, chroniąc tym samym bezpieczeństwo i interesy handlowe danego podmiotu krytycznego.	T	Art. 1 pkt 7 projektu ustawy (art. 6zm ust.1 pkt 1 i 2 ustawy o zarządzaniu kryzysowym)	Art. 6zm. 1. Dyrektor Centrum prowadzi Pojedynczy Punkt Kontaktowy do którego zadań należy: 1) odbieranie zgłoszeń incydentów istotnych z pojedynczych punktów kontaktowych w innych państwach członkowskich Unii Europejskiej; 2) przekazywanie zgłoszeń incydentów istotnych dotyczących innych państw członkowskich Unii Europejskiej do pojedynczych punktów kontaktowych tych państw;	Wymiana informacji na potrzeby realizacji zadań w obszarze podmiotów krytycznych będzie odbywać się z zachowaniem bezpieczeństwa i poufności tychże informacji, na podstawie obowiązujących przepisów, w tym przepisów ustawy o ochronie informacji niejawnych, ustawy o zwalczaniu nieuczciwej konkurencji oraz ustawy o ochronie danych osobowych.
Art. 15	4. Jak najszybciej po otrzymaniu zgłoszenia, o którym mowa w ust. 1, zainteresowany właściwy organ przekazuje zainteresowanemu podmiotowi krytycznemu odpowiednie informacje zwrotne, w tym informacje, które mogą pomóc podmiotowi krytycznemu w skutecznej odpowiedzi na dany incydent. Państwa członkowskie informują opinię	T	Art. 1 pkt 7 projektu ustawy (art. 6zl pkt 5, art. 6zw ust.5 ustawy o zarządzaniu kryzysowym)	Art. 6zl. Organ do spraw podmiotów krytycznych: 5) współpracuje z podmiotami krytycznymi w danym sektorze lub podsektorze w zakresie obsługi incydentów;	

	publiczną, jeżeli stwierdzą, że leży to w interesie publicznym.			(Art. 6zw) 5. Organ do spraw podmiotów krytycznych informuje opinię publiczną o incydencie istotnym, jeżeli uzna, że leży to w interesie publicznym.	
Art. 16	Artykuł 16 Normy Aby wspierać spójne wdrażanie niniejszej dyrektywy, państwa członkowskie zachęcają, w przypadkach gdy może to być przydatne i nie narzucając ani nie faworyzując stosowania określonego rodzaju technologii, do stosowania europejskich i międzynarodowych norm i specyfikacji technicznych istotnych dla środków w zakresie bezpieczeństwa i w zakresie odporności mających zastosowanie do podmiotów krytycznych.	T	Art. 1 pkt 7 projektu ustawy (art. 6zt ust.1 ust. 5, ust. 6, ust. 7 ustawy o zarządzaniu kryzysowym)	Art. 6zt. 1. Podmiot krytyczny wdraża zintegrowany system zarządzania bezpieczeństwem świadczenia usługi kluczowej obejmujący: 2) wdrożenie odpowiednich i proporcjonalnych do wyników oceny ryzyka rozwiązań organizacyjno-technicznych, w szczególności: 2. Rozwiązania organizacyjno-techniczne, o których mowa w ust. 1 pkt 2, powinny spełniać wymagania określone w normach, wskazanych w akcie wykonawczym wydanym na podstawie ust. 5. 5. Rada Ministrów określi w drodze rozporządzenia wykaz norm oraz wytycznych do ich stosowania, które podmiot krytyczny uwzględnia przy wdrażaniu rozwiązań organizacyjno-technicznych, w zakresie: 1) zarządzania bezpieczeństwem informacji, 2) zarządzania ciągłością działania usługi kluczowej, 3) zapewnienia bezpieczeństwa fizycznego, w tym ochrony fizycznej infrastruktury służącej do świadczenia usługi kluczowej oraz zabezpieczeń technicznych, uwzględniających kontrolę dostępu - mając na względzie zapewnienie właściwego poziomu bezpieczeństwa świadczenia usług kluczowych. 6. Organ do spraw podmiotów krytycznych może opracować, odrębnie dla nadzorowanego sektora lub podsektora i udostępnić 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), które podmiot krytyczny uwzględnia przy wdrażaniu rozwiązań	

				organizacyjno-technicznych wskazanych w ust. 1 pkt 2. 7. W celu wdrożenia rozwiązań organizacyjno-technicznych, o których mowa w ust. 1 pkt 2, podmiot krytyczny uwzględnia specyfikacje techniczne określone w aktach wykonawczych Komisji Europejskiej, wydanych na podstawie art. 13 ust. 6 dyrektywy 2022/2557.	
Art. 17	ROZDZIAŁ IV PODMIOTY KRYTYCZNE O SZCZEGÓLNYM ZNACZENIU EUROPEJSKIM Artykuł 17 Identyfikowanie podmiotów krytycznych o szczególnym znaczeniu europejskim 1. Podmiot uznaje się za podmiot krytyczny o szczególnym znaczeniu europejskim, w przypadku gdy: a) zidentyfikowano go jako podmiot krytyczny na podstawie art. 6 ust. 1; b) świadczy on te same lub podobne usługi kluczowe na rzecz co najmniej sześciu państw członkowskich lub w co naj mniej sześciu państwach członkowskich; oraz c) powiadomiono go o tym fakcie na podstawie ust. 3 niniejszego artykułu.	T	Art. 1 pkt 7 projektu ustawy (art. 6zw ust.5 ustawy o zarządzaniu kryzysowym)	(Art. 3) 1b) podmiocie krytycznym o szczególnym znaczeniu europejskim - należy przez to rozumieć podmiot krytyczny świadczący co najmniej jedną usługę kluczową lub świadczący te same lub podobne usługi kluczowe, na rzecz co najmniej sześciu państw członkowskich Unii Europejskiej lub w co najmniej sześciu państwach członkowskich Unii Europejskiej, uznany za taki podmiot przez Komisję Europejską;	
Art. 17	2. Państwa członkowskie zapewniają, aby po powiadomieniu, o którym mowa w art. 6 ust. 3, podmiot krytyczny poinformował swój właściwy organ o tym, czy świadczy usługi kluczowe na rzecz co najmniej sześciu państw członkowskich lub w co najmniej sześciu państwach członkowskich. W takim przypadku państwa członkowskie zapewniają, aby podmiot krytyczny informował swój właściwy organ o usługach kluczowych, które świadczy na rzecz tych państw członkowskich lub w tych państwach członkowskich, a także o państwach	T	Art. 1 pkt 7 projektu ustawy (art. 6zzf ust.1, ust. 2, art. 6zzg ust. 1 ustawy o zarządzaniu kryzysowym)	Art. 6zzf. 1. Podmiot krytyczny informuje właściwy organ do spraw podmiotów krytycznych oraz Pojedynczy Punkt Kontaktowy o fakcie świadczenia co najmniej jednej usługi kluczowej spośród usług kluczowych wskazanych w przepisach rozporządzenia delegowanego wydanego na podstawie art. 5 ust. 1 dyrektywy 2022/2557, lub świadczenia tych samych lub podobnych usług kluczowych, na rzecz co najmniej sześciu państw członkowskich Unii Europejskiej lub w co najmniej sześciu państwach członkowskich Unii Europejskiej.	

	członkowskich, na rzecz których lub w których świadczy takie usługi kluczowe. Państwa członkowskie bez zbędnej zwłoki przekazują Komisji dane identyfikacyjne takich podmiotów krytycznych oraz informacje, które podmioty krytyczne przekazują na podstawie niniejszego ustępu. Komisja prowadzi konsultacje z właściwym organem państwa członkowskiego, które zidentyfikowało podmiot krytyczny, o którym mowa w akapicie pierwszym, właściwym organem innych zainteresowanych państw członkowskich oraz z odnośnym podmiotem krytycznym. W trakcie tych konsultacji każde państwo członkowskie informuje Komisję o tym, czy uważa, że usługi świadczone na jego rzecz przez podmiot krytyczny stanowią usługi kluczowe.			2. W przypadku, o którym mowa w ust. 1, właściwy organ do spraw podmiotów krytycznych, za pośrednictwem Pojedynczego Punktu Kontaktowego informuje Komisję Europejską o potencjalnym podmiocie krytycznym o szczególnym znaczeniu europejskim, przekazując dane, o których mowa w art. 6zo ust. 2 pkt 1-7. Art. 6zzg. 1. Organ do spraw podmiotów krytycznych, za pośrednictwem Pojedynczego Punktu Kontaktowego, inicjuje i prowadzi konsultacje z Komisją Europejską oraz właściwymi organami państw członkowskich Unii Europejskiej w celu ustalenia, czy podmiot krytyczny świadczący usługę kluczową na terytorium Rzeczypospolitej Polskiej, świadczy ją na rzecz co najmniej sześciu państw członkowskich Unii Europejskiej lub w co najmniej sześciu państwach członkowskich Unii Europejskiej.	
	3. Jeżeli na podstawie konsultacji, o których mowa w ust. 2 niniejszego artykułu, Komisja stwierdzi, że zainteresowany podmiot krytyczny świadczy usługi kluczowe na rzecz co najmniej sześciu państw członkowskich lub w co najmniej sześciu państwach członkowskich, Komisja powiadamia ten podmiot krytyczny za pośrednictwem jego właściwego organu, że uznaje się go za podmiot krytyczny o szczególnym znaczeniu europejskim i informuje ten podmiot krytyczny o obowiązkach spoczywających na nim na podstawie niniejszego rozdziału oraz o dniu, od którego obowiązki te mają wobec niego zastosowanie. Po tym jak Komisja poinformuje właściwy organ o swojej decyzji o uznaniu danego podmiotu krytycznego za podmiot krytyczny o szczególnym znaczeniu europejskim, właściwy organ bez zbędnej zwłoki powiadamia o tym fakcie ten podmiot krytyczny.	T	Art. 1 pkt 7 projektu ustawy (art. 6zzg ust.2, art. 6zzh ust. 1 ustawy o zarządzaniu kryzysowym)	(Art. 6zzg) 2. W przypadku uznania przez Komisję Europejska podmiotu krytycznego, o którym mowa w art. 6zzf ust. 1, za podmiot krytyczny o szczególnym znaczeniu europejskim, organ do spraw podmiotów krytycznych informuje niezwłocznie podmiot krytyczny, o tym fakcie oraz obowiązkach z tym związanych. Art. 6zzh. 1. Organ do spraw podmiotów krytycznych, za pośrednictwem Pojedynczego Punktu Kontaktowego, zapewnia współpracę z Komisją Europejską oraz właściwymi organami państwa członkowskiego, na rzecz którego lub w którym jest świadczona usługa kluczowa lub w przypadku gdy podmiot krytyczny o szczególnym znaczeniu europejskim zidentyfikowany przez państwo członkowskie świadczy usługę kluczową na rzecz Rzeczypospolitej Polskiej lub na jej terytorium, w tym prowadzi wymianę informacji w zakresie:	

				1) oceny ryzyka podmiotu krytycznego o szczególnym znaczeniu europejskim; 2) wdrażania odpowiednich i proporcjonalnych do wyników oceny ryzyka rozwiązań organizacyjno-technicznych służących zapewnieniu odporności tego podmiotu; 3) działań z zakresu nadzoru oraz egzekwowania przepisów ustawy przez właściwy organ do spraw podmiotów krytycznych.	
Art. 17	4. Niniejszy rozdział stosuje się do odnośnego podmiotu krytycznego o szczególnym znaczeniu europejskim, począwszy od dnia otrzymania powiadomienia, o którym mowa w ust. 3 niniejszego artykułu.	T	Art. 1 pkt 7 projektu ustawy (art. 6zzg ust.2 ustawy o zarządzaniu kryzysowym)	(art. 6zzg) 2. W przypadku uznania przez Komisję Europejska podmiotu krytycznego, o którym mowa w art. 6zzf ust. 1, za podmiot krytyczny o szczególnym znaczeniu europejskim, organ do spraw podmiotów krytycznych informuje niezwłocznie podmiot krytyczny, o tym fakcie oraz obowiązkach, o których mowa w przepisach rozdziału 11 ustawy.	
Art. 18	Artykuł 18 Misje doradcze 1. Na wniosek państwa członkowskiego, które zidentyfikowało podmiot krytyczny o szczególnym znaczeniu europejskim jako podmiot krytyczny zgodnie z art. 6 ust. 1, Komisja organizuje misję doradczą w celu oceny środków wprowadzonych przez ten podmiot krytyczny z myślą o wypełnianiu obowiązków spoczywających na nim na podstawie rozdziału III.	T	Art. 1 pkt 7 projektu ustawy (art. 6zzh ust.2 ustawy o zarządzaniu kryzysowym)	(Art. 6zzh) 2. Właściwy organ do spraw podmiotów krytycznych, za pośrednictwem Pojedynczego Punktu Kontaktowego, współpracuje z Komisją Europejską w zakresie organizowania i zapewnienia obsługi misji doradczej, w tym: 1) przedkłada wniosek o zorganizowanie misji doradczej; 2) konsultuje program misji doradczej, w tym proponuje kandydatów do uczestnictwa w misji doradczej; 3) koordynuje realizację czynności związanych z dostępem przedstawicieli misji doradczej do informacji oraz budynków, terenów i infrastruktury krytycznej podmiotu krytycznego o szczególnym znaczeniu europejskim;	

				4) przeprowadza analizę sprawozdania z ustaleń misji doradczej;	
Art. 18	2. Z własnej inicjatywy lub na wniosek co najmniej jednego państwa członkowskiego, na rzecz którego lub w którym świadczona jest usługa kluczowa, Komisja organizuje misję doradczą, o której mowa w ust. 1 niniejszego artykułu, pod warunkiem że zgodzi się na to państwo członkowskie, które zidentyfikowało podmiot krytyczny o szczególnym znaczeniu europejskim jako podmiot krytyczny zgodnie z art. 6 ust. 1.	T	Art. 1 pkt 7 projektu ustawy (art. 6zzh ust. 2 i ust. 5 ustawy o zarządzaniu kryzysowym)	(Art. 6zzh) 2. Właściwy organ do spraw podmiotów krytycznych, za pośrednictwem Pojedynczego Punktu Kontaktowego, współpracuje z Komisją Europejską w zakresie organizowania i zapewnienia obsługi misji doradczej, w tym: 1) przedkłada wniosek o zorganizowanie misji doradczej; 2) konsultuje program misji doradczej, w tym proponuje kandydatów do uczestnictwa w misji doradczej; 3) koordynuje realizację czynności związanych z dostępem przedstawicieli misji doradczej do informacji oraz budynków, terenów i infrastruktury krytycznej podmiotu krytycznego o szczególnym znaczeniu europejskim; 4) przeprowadza analizę sprawozdania z ustaleń misji doradczej; 5. Przepis ust. 2 stosuje się odpowiednio do wniosku o organizację misji doradczej, w przypadku gdy podmiot krytyczny o szczególnym znaczeniu europejskim zidentyfikowany przez państwo członkowskie świadczy usługę kluczową na rzecz Rzeczypospolitej Polskiej lub na jej terytorium.	
Art. 18	3. Na uzasadniony wniosek Komisji lub co najmniej jednego państwa członkowskiego, na rzecz którego lub w którym świadczona jest usługa kluczowa, państwo członkowskie, które zidentyfikowało podmiot krytyczny o szczególnym znaczeniu europejskim jako podmiot krytyczny zgodnie z art. 6 ust. 1, dostarcza Komisji: a) odpowiednie części oceny ryzyka podmiotu krytycznego;	T	Art. 1 pkt 7 projektu ustawy (art. 6zzh ust.1 ustawy o zarządzaniu kryzysowym)	Art. 6zzh. 1. Organ do spraw podmiotów krytycznych, za pośrednictwem Pojedynczego Punktu Kontaktowego, zapewnia współpracę z Komisją Europejską oraz właściwymi organami państwa członkowskiego, na rzecz którego lub w którym jest świadczona usługa kluczowa lub w przypadku gdy podmiot krytyczny o szczególnym znaczeniu europejskim zidentyfikowany przez państwo członkowskie świadczy usługę kluczową na rzecz Rzeczypospolitej Polskiej lub na jej	

	b) wykaz odnośnych środków wprowadzonych zgodnie z art. 13; c) informacje o działaniach z zakresu nadzoru lub egzekwowania przepisów, które zgodnie z art. 21 i 22 podjął wobec tego podmiotu krytycznego jego właściwy organ, w tym na temat przeprowadzonych ocen zgodności lub wydanych nakazów.			terytorium, w tym prowadzi wymianę informacji w zakresie: 1) oceny ryzyka podmiotu krytycznego o szczególnym znaczeniu europejskim; 2) wdrażania odpowiednich i proporcjonalnych do wyników oceny ryzyka rozwiązań organizacyjno-technicznych służących zapewnieniu odporności tego podmiotu; 3) działań z zakresu nadzoru oraz egzekwowania przepisów ustawy przez właściwy organ do spraw podmiotów krytycznych.	
Art. 18	4. Misja doradcza przedkłada sprawozdanie ze swoich ustaleń Komisji, państwu członkowskiemu, które zidentyfikowało podmiot krytyczny o szczególnym znaczeniu europejskim jako podmiot krytyczny zgodnie z art. 6 ust. 1, państwom członkowskim, na rzecz których lub w których świadczona jest usługa kluczowa, oraz podmiotowi krytycznemu, którego dotyczy misja, w terminie trzech miesięcy od zakończenia misji doradczej. Państwa członkowskie, na rzecz których lub w których świadczona jest usługa kluczowa, analizują sprawozdanie, o którym mowa w akapicie pierwszym, i w stosownych przypadkach doradzają Komisji w kwestii tego, czy dany podmiot krytyczny o szczególnym znaczeniu europejskim wywiązuje się z obowiązków spoczywających na nim na podstawie rozdziału III, oraz – w stosownych przypadkach – w kwestii tego, jakie środki można wprowadzić, aby zwiększyć odporność tego podmiotu krytycznego. Na podstawie porad, o których mowa w akapicie drugim niniejszego ustępu, Komisja przekazuje państwu członkowskiemu, które zidentyfikowało podmiot krytyczny o szczególnym znaczeniu europejskim jako podmiot krytyczny zgodnie z art. 6 ust. 1, państwom członkowskim, na rzecz	T	Art. 1 pkt 7 projektu ustawy (art. 6zzh ust. 3 ustawy o zarządzaniu kryzysowym)	(Art. 6zzh) 3. Właściwy organ do spraw podmiotów krytycznych za pośrednictwem Pojedynczego Punktu Kontaktowego: 1) po dokonaniu analizy sprawozdania z ustaleń misji doradczej, przedkłada Komisji Europejskiej informację o stopniu wdrożenia rozwiązań organizacyjno-technicznych służących zapewnieniu odporności podmiotu krytycznego o szczególnym znaczeniu europejskim lub przedkłada rekomendacje w zakresie zwiększenia odporności tego podmiotu, w celu wydania przez Komisję Europejską opinii dotyczącej wywiązywania się z nałożonych obowiązków przez ten podmiot lub wskazującej środki, które można wprowadzić, aby zwiększyć odporność tego podmiotu; 2) przekazuje opinię, o której mowa w pkt 1, podmiotowi krytycznemu o szczególnym znaczeniu europejskim oraz zapewnia wsparcie w przypadku konieczności wdrożenia dodatkowych środków zwiększających odporność; 3) informuje Komisję Europejską oraz właściwe organy państwa członkowskiego, na rzecz którego lub w którym jest świadczona usługa kluczowa, o środkach zwiększających odporność, wprowadzonych z uwzględnieniem opinii, o której mowa w pkt 1, albo informację o braku konieczności wprowadzania tych środków.	

	których lub w których świadczona jest usługa kluczowa, oraz temu pod miotowi krytycznemu swoją opinię na temat tego, czy ten podmiot krytyczny wywiązuje się z obowiązków spoczywających na nim na podstawie rozdziału III, oraz – w stosownych przypadkach – jakie środki można wprowadzić, aby zwiększyć odporność tego podmiotu krytycznego. Państwo członkowskie, które zidentyfikowało podmiot krytyczny o szczególnym znaczeniu europejskim jako podmiot krytyczny zgodnie z art. 6 ust. 1, zapewnia, by jego właściwy organ i odnośny podmiot krytyczny uwzględniły opinię, o której mowa w akapicie trzecim niniejszego ustępu, i przekazuje Komisji oraz państwom członkowskim, na rzecz których lub w których świadczona jest usługa kluczowa, informacje na temat środków, jakie podjęło na podstawie tej opinii.				
Art. 18	5. Każda misja doradcza składa się z ekspertów z państwa członkowskiego, w którym znajduje się podmiot krytyczny o szczególnym znaczeniu europejskim, ekspertów z państw członkowskich, na rzecz których lub w których świadczona jest usługa kluczowa, oraz z przedstawicieli Komisji. Te państwa członkowskie mogą proponować kandydatów do uczestnictwa w misji doradczej. Komisja, po konsultacji z państwem członkowskim, które zidentyfikowało podmiot krytyczny o szczególnym znaczeniu europejskim jako podmiot krytyczny zgodnie z art. 6 ust. 1, wybiera i powołuje członków każdej misji doradczej zgodnie z ich kwalifikacjami zawodowymi, zapewniając, w miarę możliwości, aby reprezentowali wszystkie te państwa członkowskie w sposób zrównoważony pod względem geograficznym. W razie potrzeby członkowie misji doradczej muszą posiadać ważne i odpowiednie poświadczenie bezpieczeństwa osobowego. Komisja ponosi	T	Art. 1 pkt 7 projektu ustawy (art. 6zzh ust.2 pkt 2 i 3 ustawy o zarządzaniu kryzysowym)	(Art. 6zzh) 2. Właściwy organ do spraw podmiotów krytycznych, za pośrednictwem Pojedynczego Punktu Kontaktowego, współpracuje z Komisją Europejską w zakresie organizowania i zapewnienia obsługi misji doradczej, w tym: 2) konsultuje program misji doradczej, w tym proponuje kandydatów do uczestnictwa w misji doradczej; 3) koordynuje realizację czynności związanych z dostępem przedstawicieli misji doradczej do informacji oraz budynków, terenów i infrastruktury krytycznej podmiotu krytycznego o szczególnym znaczeniu europejskim;	

	koszty związane z uczestnictwem w misjach doradczych. Komisja organizuje program każdej misji doradczej po konsultacji z członkami danej misji doradczej oraz w porozumieniu z państwem członkowskim, które zidentyfikowało podmiot krytyczny o szczególnym znaczeniu europejskim jako pod miot krytyczny zgodnie z art. 6 ust. 1.				
Art. 18	6. Komisja przyjmuje akt wykonawczy, w którym ustanawia przepisy dotyczące rozwiązań proceduralnych w zakresie wniosków o organizację misji doradczych, rozpatrywania takich wniosków, prowadzenia misji doradczych i opracowywania sprawozdań z tych misji oraz postępowania w zakresie przekazywania opinii Komisji, o której to opinii mowa w ust. 4 akapit trzeci niniejszego artykułu, i informowania o podjętych środkach, z należytym uwzględnieniem poufności i ochrony tajemnicy handlowej w zakresie odnośnych informacji. Ten akt wykonawczy przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 24 ust. 2.	N			
Art. 18	7. Państwa członkowskie zapewniają, aby podmioty krytyczne o szczególnym znaczeniu europejskim zapewniały misjom doradczym dostęp do informacji, systemów i obiektów związanych ze świadczeniem ich usług kluczowych, które są niezbędne do prowadzenia danej misji doradczej.	T	Art. 1 pkt 7 projektu ustawy (art. 6zzh ust.2 pkt 3 ustawy o zarządzaniu kryzysowym)	(Art. 6zzh) 2. Właściwy organ do spraw podmiotów krytycznych, za pośrednictwem Pojedynczego Punktu Kontaktowego, współpracuje z Komisją Europejską w zakresie organizowania i zapewnienia obsługi misji doradczej, w tym: 3) koordynuje realizację czynności związanych z dostępem przedstawicieli misji doradczej do informacji oraz budynków, terenów i infrastruktury krytycznej podmiotu krytycznego o szczególnym znaczeniu europejskim;	
Art. 18	8. Misje doradcze realizowane są zgodnie z obowiązującym prawem krajowym państwa członkowskiego, na terytorium którego się odbywają, z poszanowaniem odpowiedzialności tego państwa członkowskiego za bezpieczeństwo	N			

	narodowe i ochronę jego interesów w zakresie bezpieczeństwa.				
Art. 18	9. Organizując misje doradcze, Komisja bierze pod uwagę sprawozdania z inspekcji przeprowadzonych przez Komisję na podstawie rozporządzeń (WE) nr 725/2004 i (WE) nr 300/2008 oraz sprawozdania z monitorowania przeprowadzonego przez Komisję na podstawie dyrektywy 2005/65/WE w odniesieniu do odnośnego podmiotu krytycznego.	N			
Art. 18	10. Komisja informuje Grupę ds. Odporności Podmiotów Krytycznych, o której mowa w art. 19, o każdym przypadku zorganizowania misji doradczej. Państwo członkowskie, na terenie którego odbyła się misja doradcza, oraz Komisja informują również Grupę ds. Odporności Podmiotów Krytycznych o głównych wnioskach misji doradczej i zebranych doświadczeniach w celu promowania wzajemnego uczenia się.	T	Art. 1 pkt 7 projektu ustawy (art. 6zm ust.2 pkt 2-5 ustawy o zarządzaniu kryzysowym)	(Art. 6zm) 2. Pojedynczy Punkt Kontaktowy przekazuje Grupie do spraw Odporności Podmiotów Krytycznych: 2) dobre praktyki związane ze zgłaszaniem i obsługą incydentów istotnych; 3) propozycje do programu prac Grupy do spraw Odporności Podmiotów Krytycznych; 4) dobre praktyki krajowe dotyczące podnoszenia świadomości, szkoleń, badań i rozwoju w obszarze zapewnienia ciągłości świadczenia usług kluczowych; 5) dobre praktyki w odniesieniu do identyfikowania podmiotów krytycznych, w tym w odniesieniu do występujących w dwóch lub większej liczbie państw członkowskich Unii Europejskiej zależności dotyczących ryzyka i incydentów.	
Art. 19	Rozdział V WSPÓŁPRACA I SPRAWOZDAWCZOŚĆ Artykuł 19 Grupa ds. Odporności Podmiotów Krytycznych 1. Niniejszym ustanawia się Grupę ds. Odporności Podmiotów Krytycznych. Grupa ds. Odporności Podmiotów Kry tycznych wspiera Komisję i ułatwia współpracę między państwami	N			Dotyczy kompetencji Grupy ds. Odporności Podmiotów Krytycznych

	członkowskimi oraz wymianę informacji na temat kwestii związanych z niniejszą dyrektywą.				
Art. 19	2. Grupa ds. Odporności Podmiotów Krytycznych składa się z przedstawicieli państw członkowskich i Komisji posiadających, w stosownych przypadkach, poświadczenie bezpieczeństwa osobowego. Jeżeli jest to istotne dla wykonywania powierzonych jej zadań, Grupa ds. Odporności Podmiotów Krytycznych może zaprosić do udziału w swoich pracach odpowiednie zainteresowane strony. Na wniosek Parlamentu Europejskiego Komisja może zaprosić ekspertów z Parlamentu Europejskiego do udziału w posiedzeniach Grupy ds. Odporności Podmiotów Krytycznych. Grupie ds. Odporności Podmiotów Krytycznych przewodniczy przedstawiciel Komisji.	N			
Art. 19	3. Zadania Grupy ds. Odporności Podmiotów Krytycznych są następujące: a) wspieranie Komisji w pomocy państwom członkowskim w zwiększaniu ich zdolności do zapewniania odporności pod miotów krytycznych zgodnie z niniejszą dyrektywą; b) analizowanie strategii w celu określenia najlepszych praktyk w odniesieniu do tych strategii; c) ułatwianie wymiany najlepszych praktyk w odniesieniu do identyfikacji podmiotów krytycznych przez państwa członkowskie zgodnie z art. 6 ust. 1, w tym w odniesieniu do transgranicznych i międzysektorowych zależności oraz czynników ryzyka i incydentów; d) w stosownych przypadkach wnoszenie wkładu w przygotowywanie dokumentów dotyczących	N			

	odporności na poziomie Unii odnośnie do kwestii związanych z niniejszą dyrektywą; e) wnoszenie wkładu w przygotowywanie wytycznych, o których mowa w art. 7 ust. 3 i art. 13 ust. 5, oraz, na wniosek, wszelkich aktów delegowanych lub wykonawczych przyjętych zgodnie z niniejszą dyrektywą; f) analizowanie sprawozdań podsumowujących, o których mowa w art. 9 ust. 3 z myślą o promowaniu wymiany najlepszych praktyk co do działań podejmowanych zgodnie z art. 15 ust. 3; g) wymiana najlepszych praktyk dotyczących zgłaszania incydentów, o którym mowa w art. 15; h) omawianie sprawozdań podsumowujących misji doradczych i zebranych doświadczeń zgodnie z art. 18 ust. 10; i) wymiana informacji i najlepszych praktyk dotyczących innowacji, badań i rozwoju w zakresie odporności podmiotów krytycznych zgodnie z niniejszą dyrektywą; j) w stosownych przypadkach, wymiana informacji w sprawach dotyczących odporności podmiotów krytycznych z odpowiednimi instytucjami, organami i jednostkami organizacyjnymi Unii.				
Art. 19	4. W terminie do dnia 17 stycznia 2025 r., a następnie co dwa lata, Grupa ds. Odporności Podmiotów Krytycznych opracowuje program prac w odniesieniu do działań, jakie mają zostać podjęte na rzecz realizacji jej celów i zadań. Ten pro gram prac musi być spójny z wymogami i celami niniejszej dyrektywy.	N			

Art. 19	5. Grupa ds. Odporności Podmiotów Krytycznych spotyka się regularnie, w każdym razie co najmniej raz w roku, z Grupą Współpracy ustanowioną na podstawie dyrektywy (UE) 2022/2555 w celu propagowania i ułatwiania współpracy i wymiany informacji.	N			
Art. 19	6. Komisja może przyjmować akty wykonawcze określające rozwiązania proceduralne niezbędne do funkcjonowania Grupy ds. Odporności Podmiotów Krytycznych, z poszanowaniem art. 1 ust. 4. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 24 ust. 2.	N			
Art. 19	7. Komisja przekazuje Grupie ds. Odporności Podmiotów Krytycznych sprawozdanie podsumowujące dotyczące informacji przekazanych przez państwa członkowskie zgodnie z art. 4 ust. 3 i art. 5 ust. 4 w terminie do dnia 17 stycznia 2027 r., a następnie w razie potrzeby i co najmniej raz na cztery lata.	N			
Art. 20	Artykuł 20 Wsparcie Komisji na rzecz właściwych organów i podmiotów krytycznych 1. Komisja wspiera w stosownych przypadkach państwa członkowskie i podmioty krytyczne w wypełnianiu ich obowiązków przewidzianych w niniejszej dyrektywie. Komisja przygotowuje ogólnounijny przegląd transgranicznych i między sektorowych czynników ryzyka związanych ze świadczeniem usług kluczowych, organizuje misje doradcze, o których mowa w art. 13 ust. 4 i art. 18, oraz ułatwia wymianę informacji między państwami członkowskimi i ekspertami w całej Unii.	N			Dotyczy kompetencji Komisji
Art. 20	2. Komisja uzupełnia działania państw członkowskich, o których mowa w art. 10, opracowując najlepsze praktyki, materiały	N			

	zawierające wytyczne i metodyki oraz organizując transgraniczne działania szkoleniowe i ćwiczenia w celu sprawdzania odporności podmiotów krytycznych.				
Art. 20	3. Komisja informuje państwa członkowskie o dostępnych dla nich na poziomie Unii zasobach finansowych przeznaczonych na zwiększanie odporności podmiotów krytycznych.	N			
Art. 21	ROZDZIAŁ VI NADZÓR I EGZEKWOWANIE PRZEPISÓW Artykuł 21 Nadzór i egzekwowanie przepisów 1. W celu ocenienia, czy podmioty zidentyfikowane przez państwa członkowskie, zgodnie z art. 6 ust. 1, jako podmioty krytyczne wypełniają obowiązki ustanowione w niniejszej dyrektywie, państwa członkowskie zapewniają właściwym organom uprawnienia i środki do: a) przeprowadzania kontroli na miejscu w zakresie infrastruktury krytycznej oraz budynków i terenów wykorzystywanych przez podmiot krytyczny do świadczenia usług kluczowych, oraz prowadzenia zdalnego nadzoru nad środkami stosowanymi przez podmioty krytyczne zgodnie z art. 13; b) przeprowadzania lub zlecania audytów dotyczących podmiotów krytycznych.	T	Art. 1 pkt 7 projektu ustawy (art. 6zl pkt 6 i 7, art. 6zzi ust. 1 i ust. 2 , art. 6zz ust. 1 i ust. 3 ustawy o zarządzaniu kryzysowym)	Art. 6zl. Organ do spraw podmiotów krytycznych: 6) monitoruje stosowanie przepisów ustawy przez podmioty krytyczne; 7) prowadzi kontrole podmiotów krytycznych; Art. 6zzi. 1. Nadzór w zakresie stosowania przepisów ustawy sprawują organy do spraw podmiotów krytycznych w zakresie: 1) spełniania przez podmioty krytyczne wymogów bezpieczeństwa dotyczących świadczenia usług kluczowych; 2) wykonywania przez podmioty krytyczne obowiązków wynikających z ustawy dotyczących przeciwdziałania zagrożeniom dla świadczonych usług kluczowych i zgłaszania incydentów istotnych. 2. W ramach nadzoru, o którym mowa w ust. 1, organ do spraw podmiotów krytycznych: 1) prowadzi kontrole podmiotów krytycznych, w siedzibie podmiotu, miejscu wykonywania działalności gospodarczej lub zdalnie; 2) zleca audyt zintegrowanego systemu zarządzania bezpieczeństwem świadczenia usługi kluczowej na koszt podmiotu krytycznego, w przypadku, o którym mowa w art. 6zz ust. 3; Art. 6zz. 1. Podmiot krytyczny przeprowadza, co najmniej raz na 3 lata, na własny koszt, audyt zintegrowanego systemu zarządzania bezpieczeństwem świadczenia usługi kluczowej, zwanego dalej "audytem" w zakresie:	

				1) zarządzania bezpieczeństwem informacji; 2) zarządzania ciągłością działania usługi kluczowej; 3) zapewnienia bezpieczeństwa fizycznego, w tym ochrony fizycznej budynków i terenów należących do podmiotu krytycznego oraz zabezpieczeń technicznych, uwzględniających kontrolę dostępu. 3. W przypadku wystąpienia incydentu istotnego, organ do spraw podmiotów krytycznych może nakazać podmiotowi krytycznemu, w drodze decyzji, przeprowadzenie zewnętrznego audytu, wraz z określeniem terminu przekazania kopii raportu z przeprowadzonego audytu i wskazaniem kategorii podmiotów do przeprowadzenia audytu. Organ do spraw podmiotów krytycznych może również określić zakres audytu. Decyzja nakazująca przeprowadzenie zewnętrznego audytu podlega natychmiastowemu wykonaniu.	
Art. 21	2. Państwa członkowskie zapewniają właściwym organom uprawnienia i środki, gdy jest to konieczne w celu wykonywania przez nie ich zadań określonych w niniejszej dyrektywie, umożliwiające zobowiązanie podmiotów na podstawie dyrektywy (UE) 2022/2555 zidentyfikowanych przez państwa członkowskie, na podstawie niniejszej dyrektywy, jako podmioty krytyczne, do przekazania w rozsądnym terminie ustalonym przez te organy: a) informacji koniecznych do oceny, czy działania podjęte przez te podmioty w celu zapewniania ich odporności spełniają wymogi określone w art. 13; b) dowodów potwierdzających skuteczne wdrożenie tych środków, w tym wyników audytu przeprowadzonego na koszt tego podmiotu przez wybranego przez niego niezależnego i wykwalifikowanego audytora.	T	Art. 1 pkt 7 projektu ustawy (art. 6zu ust.1 i ust. 2, art. 6zzi ust. 3 i ust. 4 ustawy o zarządzaniu kryzysowym)	Art. 6zu.1. Podmiot krytyczny opracowuje, stosuje i aktualizuje dokumentację zintegrowanego systemu zarządzania bezpieczeństwem świadczenia usługi kluczowej. 2. Dokumentację zintegrowanego systemu zarządzania bezpieczeństwem świadczenia usługi kluczowej stanowią: 5) dokumentacja cyberbezpieczeństwa, opracowywana zgodnie z wymogami dla podmiotów kluczowych, o których mowa w przepisach ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa; (Art. 6zzi) 3. Organ do spraw podmiotów krytycznych może żądać od podmiotu krytycznego informacji w zakresie wdrożenia rozwiązań zawartych w dokumentacji cyberbezpieczeństwa, o której mowa w art. 6zu ust. 3 pkt 5, obejmujących:	

	Zwracając się o przekazanie tych informacji, właściwe organy podają cel tego żądania i określają, jakie informacje są wymagane.			1) wpływ wdrożonych rozwiązań na bezpieczeństwo świadczenia usługi kluczowej, 2) dowodów potwierdzających wdrożone rozwiązania, w tym wyniki audytów przeprowadzonych przez podmiot krytyczny. 4. Organ do spraw podmiotów krytycznych wskazuje cel i uzasadnienie żądania, o którym mowa w ust. 3.	
Art. 21	3. Bez uszczerbku dla możliwości nakładania sankcji zgodnie z art. 22 właściwe organy mogą, po przeprowadzeniu działań nadzorczych, o których mowa w ust. 1 niniejszego artykułu, lub oceny informacji, o których mowa w ust. 2 niniejszego artykułu, nakazać odnośnym podmiotom krytycznym podjęcie koniecznych i proporcjonalnych działań w celu wyeliminowania wszelkiego stwierdzonego naruszenia niniejszej dyrektywy w rozsądnym terminie ustalonym przez te organy oraz poinformowanie tych organów o podjętych działaniach. Nakazy te musza uwzględniać w szczególności wagę naruszenia.	T	Art. 1 pkt 7 projektu ustawy (art. 6zzn ust. 1-3 ustawy o zarządzaniu kryzysowym)	Art. 6zzn. 1. Jeżeli na podstawie informacji zgromadzonych w protokole kontroli organ do spraw podmiotów krytycznych uzna, że mogło dojść do naruszenia przepisów ustawy przez podmiot kontrolowany, przekazuje zalecenia pokontrolne dotyczące usunięcia nieprawidłowości, wskazując jednocześnie termin ich usunięcia. Przy określaniu terminu usunięcia nieprawidłowości, organ do spraw podmiotów krytycznych bierze pod uwagę zakres i rodzaj stwierdzonych naruszeń. 2. Od zaleceń pokontrolnych nie przysługują środki odwoławcze. 3. Podmiot kontrolowany, w wyznaczonym terminie, informuje organ do spraw podmiotów krytycznych o sposobie wykonania zaleceń.	Brak wykonania zaleceń pokontrolnych nie jest zagrożony sankcją (karą pieniężną). Stąd od zaleceń tych nie przewidziano środków odwoławczych. W przypadku nałożenia kary pieniężnej na podstawie dodawanego do ustawy o zarządzaniu kryzysowym art. 6zzo, stronie przysługują wszystkie środki zaskarżenia przewidziane przepisami ustawy – Kodeks postępowania administracyjnego.
Art. 21	4. Państwo członkowskie zapewnia, aby uprawnienia określone w ust. 1, 2 i 3 mogły być wykonywane wyłącznie z zastrzeżeniem odpowiednich gwarancji prawnych. Takie gwarancje muszą zapewniać w szczególności wykonywanie tych uprawnień w sposób obiektywny, przejrzysty i proporcjonalny oraz należyte zabezpieczenie praw i prawnie uzasadnionych interesów, takich jak ochrona tajemnicy przedsiębiorstwa i tajemnicy handlowej, podmiotów krytycznych, których to	T	Art. 1 pkt 7 projektu ustawy (Art. 6zzn. ust. 1, art. 6zzj , art. 6zzm ust.2 -11 ustawy o zarządzaniu kryzysowym)	Art. 6zzj. Do kontroli realizowanej wobec podmiotów: 1) będących przedsiębiorcami stosuje się przepisy rozdziału 5 ustawy z dnia 6 marca 2018 r. - Prawo przedsiębiorców (Dz. U. z 2024 r. poz. 236, z późn. zm); 2) niebędących przedsiębiorcami stosuje się przepisy ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (Dz. U. z 2020 r. poz. 224 oraz z 2025 r. poz. 1158) określające zasady i tryb przeprowadzania kontroli.	Wymiana informacji na potrzeby realizacji zadań w nadzoru nad podmiotami krytycznych odbywa się z zachowaniem bezpieczeństwa i poufności tychże informacji, na podstawie obowiązujących

	dotyczy, w tym prawa do bycia wysłuchanym, prawa do obrony oraz prawa do skutecznego środka odwoławczego przed niezależnym sądem.			Art. 6zzn. 1. Jeżeli na podstawie informacji zgromadzonych w protokole kontroli organ do spraw podmiotów krytycznych uzna, że mogło dojść do naruszenia przepisów ustawy przez podmiot kontrolowany, przekazuje zalecenia pokontrolne dotyczące usunięcia nieprawidłowości, wskazując jednocześnie termin ich usunięcia. Przy określaniu terminu usunięcia nieprawidłowości, organ do spraw podmiotów krytycznych bierze pod uwagę zakres i rodzaj stwierdzonych naruszeń. (Art. 6zzm) 2. Osoba prowadząca czynności kontrolne wobec podmiotów krytycznych będących przedsiębiorcami przedstawia przebieg przeprowadzonej kontroli w protokole kontroli. 3. Protokół kontroli zawiera: 1) wskazanie nazwy oraz adresu podmiotu kontrolowanego; 2) imię i nazwisko osoby reprezentującej podmiot kontrolowany lub nazwę organu reprezentującego ten podmiot; 3) imię i nazwisko oraz stanowisko służbowe osoby prowadzącej czynności kontrolne; 4) datę rozpoczęcia i zakończenia czynności kontrolnych; 5) określenie przedmiotu, zakresu oraz okresu kontroli; 6) opis stanu faktycznego ustalonego w toku kontroli; 7) ocenę kontrolowanej działalności, w tym zakres, przyczyny i skutki stwierdzonych nieprawidłowości; 8) wyszczególnienie załączników. 4. Protokół kontroli podpisują osoba prowadząca czynności kontrolne oraz osoba reprezentująca podmiot kontrolowany. 5. W przypadku zastrzeżeń dotyczących ustaleń zawartych w protokole kontroli podmiot krytyczny ma prawo odmówić podpisania protokołu kontroli	przepisów, w tym przepisów ustawy o ochronie informacji niejawnych, ustawy o zwalczaniu nieuczciwej konkurencji oraz ustawy o ochronie danych osobowych. W przypadku stwierdzenia nieprawidłowości - sankcje z tego tytułu mogą być nakładane na podmioty krytyczne w transparentnej procedurze przewidzianej projektowanymi przepisami ustawy oraz przepisami ustawy – Kodeks postępowania administracyjnego, gwarantującymi prawo do obrony i prawo do skutecznego środka odwoławczego przed niezależnym sądem.

				oraz złożyć umotywowane pisemne zastrzeżenia do tego protokołu w terminie 7 dni od dnia przedstawienia mu protokołu do podpisu. 6. Odmowę podpisania protokołu kontroli osoba prowadząca czynności kontrolne odnotowuje w protokole wraz ze wskazaniem daty tej odmowy. 7. W razie złożenia zastrzeżeń do protokołu kontroli kierownik komórki organizacyjnej prowadzącej czynności kontrolne dokonuje ich analizy. 8. Kierownik komórki organizacyjnej prowadzącej czynności kontrolne: 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. 9. W razie potrzeby, osoba prowadząca czynności kontrolne podejmuje dodatkowe czynności kontrolne, a w przypadku stwierdzenia przez kierownika komórki organizacyjnej prowadzącej czynności kontrolne zasadności zastrzeżeń do protokołu kontroli zmienia lub uzupełnia odpowiednią część protokołu kontroli w formie aneksu do protokołu. 10. Kierownik komórki organizacyjnej prowadzącej czynności kontrolne, po rozpatrzeniu zastrzeżeń do protokołu kontroli, sporządza stanowisko wobec tych zastrzeżeń. 11. W przypadku nieuwzględnienia zastrzeżeń do protokołu kontroli w całości albo w części kierownik komórki organizacyjnej prowadzącej czynności kontrolne informuje kontrolowany podmiot krytyczny na piśmie.	
Art. 21	5. Państwa członkowskie zapewniają, aby w przypadku, gdy właściwy organ na podstawie niniejszej dyrektywy prze prowadza, zgodnie z niniejszym artykułem, ocenę spełniania przez	T	Art. 1 pkt 7 projektu ustawy (art. 6zl pkt 10 ustawy o zarządzaniu kryzysowym)	Art. 6zl. Organ do spraw podmiotów krytycznych: 10) współpracuje z innymi organami do spraw podmiotów krytycznych oraz organami właściwymi do spraw cyberbezpieczeństwa, o	

	podmiot krytyczny jego obowiązków, ten właściwy organ informował właściwe organy odnośnych państw członkowskich na podstawie dyrektywy (UE) 2022/2555 W tym celu państwa członkowskie zapewniają, aby właściwe organy na podstawie niniejszej dyrektywy mogły zwracać się do właściwych organów na podstawie dyrektywy (UE) 2022/2555 o skorzystanie przez nie z ich uprawnień w zakresie nadzoru i egzekwowania przepisów w odniesieniu do podmiotu na podstawie tej dyrektywy, który to podmiot został zidentyfikowany jako podmiot krytyczny na podstawie niniejszej dyrektywy. W tym celu państwa członkowskie zapewniają, by właściwe organy na podstawie niniejszej dyrektywy współpracowały i prowadziły wymianę informacji z właściwymi organami na podstawie dyrektywy (UE) 2022/2555.			których mowa w ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;	
Art. 22	Artykuł 22 Sankcje Państwa członkowskie ustanawiają przepisy dotyczące sankcji mających zastosowanie w przypadku naruszeń przepisów krajowych przyjętych na podstawie niniejszej dyrektywy i podejmują wszelkie niezbędne środki w celu zapewnienia ich wykonywania. Przewidziane sankcje muszą być skuteczne, proporcjonalne i odstraszające. Państwa członkowskie powiadamiają Komisję o tych przepisach i środkach do dnia 17 października 2024 r., a także powiadamiają ją niezwłocznie o wszelkich późniejszych zmianach, które ich dotyczą.	T	Art. 1 pkt 7 projektu ustawy (art. 6zl pkt 12, art. 6zzi ust.2 pkt 3, art. 6zzo, art. 6zzp, art. 6zzq, art. 6zzr, art. 6zzs, art. 6zzm ust. 5 pkt 1 lit. b ustawy o zarządzaniu kryzysowym oraz art. 25 ust. 2 projektu ustawy).	Art. 6zl. Organ do spraw podmiotów krytycznych: 12) nakłada kary pieniężne na podmiot krytyczny. (Art. 6zzi) 2. W ramach nadzoru, o którym mowa w ust. 1, organ do spraw podmiotów krytycznych: 3) nakłada kary pieniężne na podmioty krytyczne. Art. 6zzo. 1. Karze pieniężnej podlega podmiot krytyczny, który: 1) nie przeprowadza systematycznej oceny ryzyka, o której mowa w art. 6zt ust. 1 pkt 1; 2) nie wdraża rozwiązań organizacyjno-technicznych, o których mowa w art. 6zt ust. 1 pkt 2; 3) nie prowadzi dokumentacji, o której mowa w art. 6zu ust. 1; 4) nie wykonuje obowiązku, o których mowa w art. 6zv ust. 1 pkt 1, w zakresie obsługi incydentu istotnego; 5) nie wykonuje obowiązku, o których mowa w art. 6zv ust. 1 pkt 4;	

				6) nie przeprowadza audytu, o którym mowa w art. 6zz ust. 1; 7) nie wyznacza pełnomocnika bezpieczeństwa usługi kluczowej lub zastępcy pełnomocnika bezpieczeństwa usługi kluczowej, o których mowa w art. 6zzd ust. 1; 8) uniemożliwia lub utrudnia wykonywanie kontroli, o której mowa w art. 6zzi ust. 2 pkt 1; 9) nie wykonał w wyznaczonym terminie zaleceń pokontrolnych, o których mowa w art. 6zzn ust. 1; 10) nie wdrożył rozwiązań dotyczących ochrony infrastruktury krytycznej, o których mowa w art. 6ze ust. 1 pkt 2, w odniesieniu do infrastruktury krytycznej niezbędnej do świadczenia usługi kluczowej; 11) nie opracował dokumentacji ochrony infrastruktury krytycznej, o której mowa w art. 6zf ust. 1, w odniesieniu do infrastruktury krytycznej niezbędnej do świadczenia usługi kluczowej. 2. Wysokość kary pieniężnej, o której mowa w: 1) ust. 1 pkt 1, wynosi do 100 000 zł; 2) ust. 1 pkt 2, wynosi do 150 000 zł; 3) ust. 1 pkt 3, wynosi do 50 000 zł; 4) ust. 1 pkt 4, wynosi do 20 000 zł za każdy stwierdzony przypadek zaniechania obsługi incydentu istotnego; 5) ust. 1 pkt 5, wynosi do 25 000 zł za każdy stwierdzony przypadek niezgłoszenia incydentu istotnego; 6) ust. 1 pkt 6, wynosi do 200 000 zł; 7) ust. 1 pkt 7, wynosi do 15 000 zł: 8) ust. 1 pkt 8, wynosi do 50 000 zł; 9) ust. 1 pkt 9, wynosi do 200 000 zł; 10) ust. 1 pkt 10, wynosi do 150 000 zł; 11) ust. 1 pkt 11, wynosi do 50 000 zł. 3. Kara, o której mowa w: 1) ust. 1 pkt 4,5 i 7, nie może być niższa niż 2000 zł; 2) ust. 1 pkt 3, 8 i 11, nie może być niższa niż 5000 zł;	

				3) ust. 1 pkt 1, 2, 6, 9 i 10, nie może być niższa niż 15 000 zł. Art. 6zzp. 1. Karę pieniężną, o której mowa w art. 6zzo, nakłada w drodze decyzji, organ do spraw podmiotów krytycznych. 2. Organ do spraw podmiotów krytycznych może decyzji, o której mowa w ust. 1, nadać rygor natychmiastowej wykonalności w całości albo w części, jeżeli wymaga tego ochrona bezpieczeństwa lub porządku publicznego oraz zagrożenie wywołania poważnych utrudnień w świadczeniu usług. 3. Wpływy z tytułu kar pieniężnych, o których mowa w art. 6zzo, stanowią: 1) w 70% dochód budżetu państwa; 2) w 30 % 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). Art. 6zzq. 1. W przypadku naruszenia przepisów ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa przez podmiot krytyczny będący jednocześnie podmiotem kluczowym w rozumieniu przepisów tej ustawy, karę pieniężną na ten podmiot nakłada organ właściwy do spraw cyberbezpieczeństwa. 2. Do ustalenia wysokości kary pieniężnej w przypadku, o którym mowa w ust. 1, stosuje się przepisy ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. 3. Organ właściwy do spraw cyberbezpieczeństwa niezwłocznie informuje organ do spraw podmiotów krytycznych, sprawujący nadzór nad podmiotem, o którym mowa w ust.1, o: 1) wszczęciu wobec tego podmiotu postępowania w sprawie nałożenia kary pieniężnej	

				2) naruszeniu dokonanym przez podmiot wraz z kwalifikacją prawną, 3) wysokości nałożonej na ten podmiot kary lub odstąpieniu od jej nałożenia. 4. Organ do spraw podmiotów krytycznych nie wszczyna postępowania w sprawie nałożenia kary pieniężnej w przypadku, o którym mowa w ust. 1, jeżeli postępowanie w przedmiocie tego naruszenia prowadzi organ właściwy do spraw cyberbezpieczeństwa. Art. 6zzr. 1. Organ do spraw podmiotów krytycznych, podejmując decyzję o nałożeniu kary pieniężnej i ustalając jej wysokość bierze pod uwagę: 1) wagę naruszenie i znaczenie naruszonych przepisów ustawy; 2) czasu trwania naruszenia; 3) wcześniejszych naruszeń ze strony danego podmiotu krytycznego; 4) spowodowane szkody majątkowe i niemajątkowe, w tym wpływ na użytkowników usługi oraz na inne usługi kluczowe; 5) środki zastosowane przez podmiot w celu ograniczenia szkód, o których mowa w pkt 4; 6) umyślny lub nieumyślny charakter czynu ze strony sprawcy naruszenia; 7) stopień współpracy podmiotu krytycznego z organem do spraw podmiotów krytycznych. 2. Podejmując decyzję organ uwzględnia również wysokość przychodu uzyskanego z działalności gospodarczej w roku obrotowym poprzedzającym wymierzenie kary pieniężnej lub możliwości finansowe podmiotu krytycznego będącego podmiotem publicznym. 3. W związku z toczącym się postępowaniem w sprawie nałożenia kary pieniężnej, organ do spraw podmiotów krytycznych może żądać od podmiotu krytycznego przekazania we wskazanym terminie, nie dłuższym niż 14 dni od dnia otrzymania	

				żądania, informacji niezbędnych do określenia wymiaru kary pieniężnej. 4. W przypadku nieprzekazania informacji, o których mowa w ust. 2, lub przekazania informacji uniemożliwiających ustalenie podstawy wymiaru kary pieniężnej, organ do spraw podmiotów krytycznych ustala podstawę wymiaru kary pieniężnej w sposób szacunkowy uwzględniając wielkość podmiotu krytycznego, specyfikę działalności tego podmiotu oraz 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 odrębny rachunek bankowy wskazany przez organ właściwy do spraw podmiotów krytycznych w decyzji o wymierzeniu kary pieniężnej. 6. Kara pieniężna nieuiszczona w terminie wraz z odsetkami podlega ściągnięciu w trybie określonym w przepisach o postępowaniu egzekucyjnym w administracji. 7. Organ właściwy do spraw podmiotów krytycznych może odstąpić od nałożenia kary pieniężnej, jeżeli waga naruszenia i znaczenie naruszonych przepisów jest znikome, a podmiot krytyczny zaprzestał naruszania prawa lub naprawił wyrządzoną szkodę. Art. 6zzs. W zakresie nieuregulowanym w niniejszym rozdziale stosuje się odpowiednio przepisy działu IVa ustawy z dnia 14 czerwca 1960 r. - Kodeks postępowania administracyjnego. (Art. 6zm) 5. Pojedynczy Punkt Kontaktowy przekazuje Komisji Europejskiej: 1) niezwłocznie informacje o: b) przepisach dotyczących kar pieniężnych; (Art. 25 projektu)	

				2.Pojedynczy Punkt Kontaktowy, o którym mowa w art. 6zm ust. 1 ustawy zmienianej w art. 1 po raz pierwszy przekazuje Komisji Europejskiej informacje o przepisach dotyczących kar pieniężnych nie później niż w ciągu 7 dni od dnia wejścia w życie ustawy.	
Art. 23	ROZDZIAŁ VII AKTY DELEGOWANE I AKTY WYKONAWCZE Artykuł 23 Wykonywanie przekazanych uprawnień 1. Powierzenie Komisji uprawnień do przyjmowania aktów delegowanych podlega warunkom określonym w niniejszym artykule.	N			W zakresie kompetencji Komisji
Art. 23	2. Uprawnienia do przyjmowania aktów delegowanych, o których mowa w art. 5 ust. 1, powierza się Komisji na okres pięciu lat od dnia 16 stycznia 2023 r.	N			
Art. 23	3. Przekazanie uprawnień, o którym mowa w art. 5 ust. 1, może zostać w dowolnym momencie odwołane 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.	N			
Art. 23	4. Przed przyjęciem aktu delegowanego Komisja konsultuje się z ekspertami wyznaczonymi przez każde państwo członkowskie zgodnie z zasadami określonymi w Porozumieniu międzyinstytucjonalnym z dnia 13 kwietnia 2016 r. w sprawie lepszego stanowienia prawa.	N			

Art. 23	5. Niezwłocznie po przyjęciu aktu delegowanego Komisja przekazuje go równocześnie Parlamentowi Europejskiemu i Radzie.	N			
Art. 23	6. Akt delegowany przyjęty na podstawie art. 5 ust. 1 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.	N			
Art. 24	Artykuł 24 Procedura komitetowa 1. Komisję wspomaga komitet. Komitet ten jest komitetem w rozumieniu rozporządzenia (UE) nr 182/2011.	N			
Art. 24	2. W przypadku odesłania do niniejszego ustępu stosuje się art. 5 rozporządzenia (UE) nr 182/2011.	N			
Art. 25	ROZDZIAŁ VIII PRZEPISY KOŃCOWE Artykuł 25 Sprawozdawczość i przegląd Do dnia 17 lipca 2027 r. Komisja składa Parlamentowi Europejskiemu i Radzie sprawozdanie, w którym ocenia, w jakim zakresie każde państwo członkowskie przyjęło środki niezbędne do wykonania niniejszej dyrektywy. Komisja dokonuje okresowego przeglądu funkcjonowania niniejszej dyrektywy i składa Parlamentowi Europejskiemu i Radzie				

	sprawozdanie na ten temat. Sprawozdanie to zawiera w szczególności ocenę wartości dodanej niniejszej dyrektywy, jej wpływ na zapewnienie odporności podmiotów krytycznych, oraz ocenę konieczności zmiany załącznika do niniejszej dyrektywy. Komisja składa pierwsze takie sprawozdanie do dnia 17 czerwca 2029 r. W celu składania sprawozdań na podstawie niniejszego artykułu Komisja uwzględnia odpowiednie dokumenty Grupy ds. Odporności Podmiotów Krytycznych.				
Art. 26 Art. 26	Artykuł 26 Transpozycja 1. Państwa członkowskie przyjmują i publikują do dnia 17 października 2024 r. przepisy niezbędne do wykonania niniejszej dyrektywy. Niezwłocznie powiadamiają o tym Komisję. Państwa członkowskie stosują te przepisy od dnia 18 października 2024 r. 2. Przyjęte przez państwa członkowskie przepisy, o których mowa w ust. 1, zawierają odniesienie do niniejszej dyrektywy lub odniesienie takie towarzyszy ich urzędowej publikacji. Sposób dokonywania takiego odniesienia określany jest przez państwa członkowskie.	T N			Ustawa wchodzi w życie po upływie 14 dni od dnia ogłoszenia.
Art. 27	Artykuł 27 Uchylenie dyrektywy Dyrektywa 2008/114/WE traci moc ze skutkiem od dnia 18 października 2024 r. Odesłania do uchylonej dyrektywy odczytuje się jako odesłania do niniejszej dyrektywy. 2008/114/WE	T	Art. 1 pkt 5 projektu ustawy	„d) uchyla się pkt 2a”	
Art. 28	Artykuł 28	N			

	Wejście w życie Niniejsza dyrektywa wchodzi w życie dwudziestego dnia po jej opublikowaniu w Dzienniku Urzędowym Unii Europejskiej.				
Art. 29	Artykuł 29 Adresaci Niniejsza dyrektywa skierowana jest do państw członkowskich.	N			Przepis nie ma charakteru normatywnego, określa adresatów dyrektywy

ZAŁĄCZNIK **SEKTORY, PODSEKTORY I KATEGORIE PODMIOTÓW** **Energia**		**T**	Załącznik do projektu ustawy			
a)Energia elektryczna	— Przedsiębiorstwa energetyczne zdefiniowane w art. 2 pkt 57 dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/944 (1), które wykonują funkcję „dostawy” zdefiniowaną w art. 2 pkt 12 tej dyrektywy	T		a)Energia elektryczna	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.	
	—Operatorzy systemów dystrybucyjnych zdefiniowani w art. 2 pkt 29 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.	
	—Operatorzy systemów przesyłowych zdefiniowani w art. 2 pkt 35 dyrektywy (UE) 2019/944					
	— Wytwórcy zdefiniowani w art. 2 pkt 38 dyrektywy (UE) 2019/944				Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 25 ustawy z dnia 10 kwietnia 1997	
	— Wyznaczeni operatorzy rynku energii elektrycznej zdefiniowani w					

	art. 2 pkt 8 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/943				r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie dystrybucji energii elektrycznej.	
	Uczestnicy rynku zdefiniowani w art. 2 pkt 25 rozporządzenia (UE) 2019/943, świadczący usługi w zakresie agregacji, odpowiedzi odbioru lub magazynowania energii zdefiniowane w art. 2 pkt 18, 20 i 59 dyrektywy (UE) 2019/944				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 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, świadczący usługę, o której mowa w art. 3 pkt 6e tej ustawy.	

					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.	
					Uczestnicy rynku świadczący usługę, o której mowa w art. 3 pkt 59 i 59a ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne.	
b) System ciepłowniczy i chłodniczy	Operatorzy systemów ciepłowniczych lub systemów chłodniczych zdefiniowanych w art. 2 pkt 19 dyrektywy Parlamentu Europejskiego i Rady (UE) 2018/2001	T		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..
c) Ropa naftowa	— Operatorzy ropociągów	T		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.
	— Operatorzy instalacji służących do produkcji, rafinacji, przetwarzania ropy naftowej, magazynowania i przesyłu				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.
	— Krajowe centrale zapasów zdefiniowane w art. 2 lit. f) dyrektywy Rady 2009/119/WE				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.
d) Gaz	— Przedsiębiorstwa dostarczające gaz zdefiniowane w art. 2 pkt 8 dyrektywy Parlamentu Europejskiego i Rady 2009/73/WE	T		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.
	Operatorzy systemów dystrybucyjnych zdefiniowani w art. 2 pkt 6 dyrektywy 2009/73/WE				Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. –

	Operatorzy systemów przesyłowych zdefiniowani w art. 2 pkt 4 dyrektywy 2009/73/WE				Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie przesyłania paliw gazowych.
	Operatorzy systemów magazynowania zdefiniowani w art. 2 pkt 10 dyrektywy 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 LNG zdefiniowani w art. 2 pkt 12 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.
	Przedsiębiorstwa gazowe zdefiniowane w art. 2 pkt 1 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 instalacji służących do rafinacji i przetwarzania gazu ziemnego				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.

				Wodór	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 magazynowania wodoru.
e) Wodór	Operatorzy produkcji, magazynowania i przesyłu wodoru	T			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 dystrybucji wodoru.
Sektor 2. Transport			**Załącznik do projektu ustawy**	**Sektor 2. Transport**	
a) Transport lotniczy	Przewoźnicy lotniczy zdefiniowani w art. 3 pkt 4 rozporządzenia (WE) nr 300/2008, wykorzystywani do celów handlowych			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.
	— Zarządzający portem lotniczym zdefiniowani w art. 2 pkt 2 dyrektywy Parlamentu Europejskiego i Rady 2009/12/WE (6), porty lotnicze zdefiniowane w art. 2 pkt 1 tej dyrektywy, w tym porty lotnicze sieci bazowej wymienione w sekcji 2 załącznika II do rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1315/2013 (7), oraz jednostki				Zarządzający lotniskiem, o którym mowa w art. 2 pkt 7 ustawy z dnia 3 lipca 2002 r. – Prawo lotnicze.
					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.

	obsługujące urządzenia pomocnicze znajdujące się w portach lotniczych				– Prawo lotnicze, wykonujący zadania związane z kontrolą bezpieczeństwa.
	Operatorzy zarządzający ruchem lotniczym zapewniający służbę kontroli ruchu lotniczego (ATC) zdefiniowaną w art. 2 pkt 1 rozporządzenia (WE) nr 549/2004 Parlamentu Europejskiego i Rady				Instytucja zapewniająca służby żeglugi powietrznej, o której mowa w art. 127 ust. 1 ustawy z dnia 3 lipca 2002 r. – Prawo lotnicze.
b) Transport kolejowy	— Zarządcy infrastruktury zdefiniowani w art. 3 pkt 2 dyrektywy Parlamentu Europejskiego i Rady 2012/34/UE			Transport kolejowy	Zarządca infrastruktury kolejowej w rozumieniu art. 4 pkt 7 ustawy z dnia 28 marca 2003 r. o transporcie kolejowym z wyłączeniem zarządców wyłącznie infrastruktury nieczynnej, o której mowa w art. 4 pkt 1 lit. b tej ustawy, infrastruktury prywatnej, o której mowa w art. 4 pkt 1 lit. c, oraz infrastruktury kolei wąskotorowej, o której mowa w art. 4 pkt 1d tej ustawy.
	Przedsiębiorstwa kolejowe zdefiniowane w art. 3 pkt 1 dyrektywy 2012/34/UE oraz operatorzy obiektów infrastruktury usługowej zdefiniowani w art. 3 pkt 12 tej dyrektywy				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 funkcje operatora jest jednocześnie przewoźnikiem kolejowym.
c) Transport wodny	— Armatorzy śródlądowego, morskiego i przy brzeżnego wodnego transportu pasażerów i towarów zdefiniowani w odniesieniu do trans portu morskiego w załączniku I do rozporządzenia (WE) nr 725/2004, z wyłączeniem poszczególnych statków			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, z wyłączeniem poszczególnych statków, na których prowadzą działalność ci armatorzy.

	eksploatowanych przez tych armatorów				Armator, o którym mowa w art. 5 ust. 1 pkt 2 ustawy z dnia 21 grudnia 2000 r. o żegludze śródlądowej.
	Organy zarządzające portami zdefiniowanymi w art. 3 pkt 1 dyrektywy 2005/65/WE, w tym ich obiekty portowe zdefiniowane w art. 2 pkt 11 rozporządzenia (WE) nr 725/2004, oraz pod mioty wykonujące prace i operujące sprzętem znajdującym się w 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.
					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.
	Operatorzy systemów ruchu statków SRS zdefiniowanych w art. 3 lit. o) dyrektywy 2002/59/WE (10) Parlamentu Europejskiego i Rady				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.
d) Transport drogowy	Organy administracji drogowej zdefiniowane w art. 2 pkt 12 rozporządzenia delegowanego Komisji (UE) 2015/962 (11), odpowiedzialne za zarządzanie ruchem drogowym, z wyłączeniem podmiotów publicznych, dla których zarządza nie ruchem lub obsługa inteligentnych systemów transportowych stanowią inną niż istotna część ich ogólnej działalności			Transport drogowy	Organy, o których mowa w art. 19 ust. 2, 5 i 5a ustawy z dnia 21 marca 1985 r. o drogach publicznych, z wyłączeniem podmiotów publicznych, dla których zarządzanie ruchem lub obsługa inteligentnych systemów transportowych stanowią inną niż istotna część ich ogólnej działalności.
					Podmioty, o których mowa w art. 43a ust. 1 ustawy z dnia 21 marca 1985 r. o drogach publicznych.
	Operatorzy inteligentnych systemów transportowych zdefiniowanych w art.				

	4 pkt 1 dyrektywy Parlamentu Europejskiego i Rady 2010/40/UE			
e) Transport publiczny	Podmioty świadczące usługi publiczne zdefiniowane w art. 2 lit. d) rozporządzenia (WE) nr 1370/2007 (13) Parlamentu Europejskiego i Rady			Transport publiczny: Podmioty, o których mowa w art. 4 ust. 8 ustawy z dnia 16 Grudnia 2010 r. o publicznym transporcie zbiorowym.
Sektor 3. Bankowość			**Załącznik do projektu ustawy**	**Sektor 3.** Bankowość i infrastruktura rynków finansowych
— Instytucje kredytowe zdefiniowane w art. 4 ust. 1 pkt 1 rozporządzenia (UE) nr 575/2013				Bank krajowy, o którym mowa w art. 4 ust. 1 pkt 1 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe.
Sektor 4. infrastruktura rynków finansowych			**Załącznik do projektu ustawy**	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.
— Operatorzy systemów obrotu zdefiniowanych w art. 4 ust. 1 pkt 24 dyrektywy 2014/65/UE				Podmiot, o którym mowa w art. 3 pkt 49 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi.
Kontrahenci centralni (CCP) zdefiniowani w art. 2 pkt 1 rozporządzenia (UE) nr 648/2012				Centralny depozyt papierów wartościowych, 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.
				Podmiot, o którym mowa w art. 48 ust. 7 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi.
				Administratorzy kluczowych wskaźników referencyjnych.
				Podmiot, o którym mowa w art. 3 pkt 21a ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi mający siedzibę na terytorium Rzeczpospolitej Polskiej.

			Podmiot prowadzący ASO w rozumieniu art. 3 pkt 2 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi (Dz. U. z 2024 r. poz. 722). Podmiot prowadzący OTF w rozumieniu art. 3 pkt 10b ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi Giełda towarowa w rozumieniu art. 2 pkt 1 ustawy z dnia 26 października 2000 r. o giełdach towarowych. Izba rozliczeniowa, o której mowa w art. 67 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe.
Sektor 5. Zdrowie		**Załącznik do projektu ustawy**	**Sektor 4. Ochrona Zdrowia**
Świadczeniodawcy zdefiniowani w art. 3 lit. g) dyrektywy Parlamentu Europejskiego i Rady 2011/24/UE Laboratoria referencyjne UE, o których mowa w art. 15 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2371 — Podmioty prowadzące działania badawczo-rozwojowe w zakresie produktów leczniczych zdefiniowanych w art. 1 pkt 2 dyrektywy 2001/83/WE Parlamentu Europejskiego i Rady 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, w odniesieniu do których uznano, że mają one krytyczne znaczenie podczas stanu zagrożenia zdrowia publicznego („wykaz wyrobów medycznych o krytycznym znaczeniu w przypadku stanu zagrożenia zdrowia publicznego”) w			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. 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. Podmioty udzielające świadczeń opieki zdrowotnej, w rozumieniu art. 133 ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych. Jednostki organizacyjne podległe lub nadzorowane przez ministra kierującego działem administracji rządowej zdrowie. Urzędy obsługujące centralne organy nadzorowane przez ministra właściwego do spraw zdrowia.

rozumieniu art. 22 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/123 Podmioty posiadające pozwolenie na dystrybucję, o którym mowa w art. 79 dyrektywy 2001/83/WE			Produkcja, dystrybucja, obrót i magazynowanie substancji czynnych, produktów leczniczych i wyrobów medycznych	 Urzędy obsługujące organy Państwowej 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. 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. Przedsiębiorca prowadzący działalność polegającą na prowadzeniu hurtowni farmaceutycznej w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne. 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.
				Wytwórca lub importer produktu leczniczego w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne.
				Wytwórca, importer lub dystrybutor 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.
				Przedsiębiorca prowadzący działalność w formie apteki ogólnodostępnej w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne.
				Jednostki organizacyjne podległe lub nadzorowane przez ministra kierującego działem administracji rządowej zdrowie.
				Urzędy obsługujące centralne organy nadzorowane przez ministra właściwego do spraw zdrowia.
				Jednostki notyfikowane, jednostki oceniające zgodność, producenci, o których mowa w ustawie z dnia 7 kwietnia 2022 r. o wyrobach medycznych.
Sektor 6. Woda pitna		**Załącznik do projektu ustawy**	**Sektor 5.** Zapatrzenie w wodę pitną i jej dystrybucja	
— 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 (18), z wyłączeniem dystrybutorów, dla których dystrybucja wody przeznaczonej do spożycia przez ludzi stanowi jedynie inną niż istotna część ich ogólnej			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 , z wyłączeniem podmiotów, dla których dostarczanie wody przeznaczonej do spożycia przez ludzi jest inną niż istotną częścią ich ogólnej działalności.	

<table>
<tr><td>działalności polegającej na dystrybucji innych produktów i towarów</td><td></td><td></td><td></td></tr>
<tr><td>Sektor 7. Ścieki</td><td></td><td>Załącznik do projektu ustawy</td><td>Sektor 6. Zbiorowe odprowadzanie ścieków</td></tr>
<tr><td>Przedsiębiorstwa zbierające, odprowadzające lub oczyszczające ścieki komunalne, ścieki bytowe i ścieki przemysłowe zdefiniowane w art. 2 pkt 1, 2 i 3 dyrektywy Rady 91/271/EWG (19), z wyłączeniem przedsiębiorstw, dla których zbieranie, odprowadzanie lub oczyszczanie ścieków komunalnych, ścieków bytowych i ścieków przemysłowych stanowi inną niż istotna część ich ogólnej działalności</td><td></td><td></td><td>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.</td></tr>
<tr><td>Sektor 8. Infrastruktura cyfrowa</td><td></td><td>Załącznik do projektu ustawy</td><td>Sektor 7. Infrastruktura cyfrowa</td></tr>
<tr><td><table>
<tr><td>Dostawcy punktów wymiany ruchu internetowego zdefiniowanych w art. 6 pkt 18 dyrektywy (UE) 2022/2555</td></tr>
<tr><td>Dostawcy usług DNS zdefiniowani w art. 6 pkt 20 dyrektywy (UE) 2022/2555, z wyłączeniem operatorów głównych serwerów nazw</td></tr>
<tr><td>Rejestry nazw domen najwyższego poziomu zdefiniowane w art. 6 pkt 21 dyrektywy (UE) 2022/2555</td></tr>
<tr><td>Dostawcy usług chmurowych zdefiniowanych w art. 6 pkt 30 dyrektywy (UE) 2022/2555</td></tr>
<tr><td>Dostawcy usług przetwarzania danych zdefiniowanych w art. 6 pkt 31 dyrektywy (UE) 2022/ 2555</td></tr>
<tr><td>Dostawcy sieci dostarczania treści/danych/ zawartości zdefiniowanej w art. 6 pkt 32 dyrektywy (UE) 2022/2555</td></tr>
</table></td><td></td><td></td><td><table>
<tr><td rowspan="8">Infrastruktura cyfrowa z wyłączeniem komunikacji elektronicznej</td><td>Dostawca punktu wymiany ruchu internetowego.</td></tr>
<tr><td>Dostawca usług DNS, z wyłączeniem operatorów głównych serwerów nazw</td></tr>
<tr><td>Rejestr nazw domen najwyższego poziomu (TLD).</td></tr>
<tr><td>Dostawca usług chmurowych.</td></tr>
<tr><td>Dostawca usług ośrodka przetwarzania danych.</td></tr>
<tr><td>Dostawca sieci dostarczania treści.</td></tr>
<tr><td>Dostawca usług zaufania.</td></tr>
<tr><td>Podmiot świadczący usługę rejestracji nazw domen.</td></tr>
<tr><td>Komunikacja elektroniczna</td><td>Przedsiębiorca komunikacji elektronicznej.</td></tr>
</table></td></tr>
</table>

<table>
<tr><td>Dostawcy usług zaufania zdefiniowani w art. 3 pkt 19 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014

Dostawcy publicznych sieci łączności elektronicznej zdefiniowanych w art. 2 pkt 8 dyrektywy Parlamentu Europejskiego i Rady (UE) 2018/1972

Dostawcy usług łączności elektronicznej zdefiniowani w art. 2 pkt 4 dyrektywy (UE) 2018/1972, o ile ich usługi są publicznie dostępne</td><td></td><td></td><td></td></tr>
<tr><td>Sektor 9. Administracja publiczna</td><td></td><td>Załącznik do projektu ustawy</td><td>Sektor 8. Administracja publiczna</td></tr>
<tr><td>Podmioty administracji publicznej w ramach instytucji rządowych na szczeblu centralnym zdefiniowane przez państwa członkowskie zgodnie z prawem krajowym</td><td></td><td></td><td><table>
<tr><td>Podmioty publiczne</td><td>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 z wyłączeniem jednostek organizacyjnych podległych ministrowi właściwemu do spraw budżetu, finansów publicznych i instytucji finansowych lub przez niego nadzorowanych, urzędu obsługującego tego ministra oraz spółki celowej utworzonej do wykonywania niektórych zadań dotyczących informatyzacji w zakresie działów administracji rządowej budżet i finanse publiczne.</td></tr>
<tr><td></td><td>Jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 3, 5, 6, 8, 9, 11 i 12 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych, z wyłączeniem jednostek organizacyjnych obsługujących jednostki samorządu terytorialnego.</td></tr>
<tr><td></td><td>Podmiot, o którym mowa w art. 96 ust. 1 ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych.</td></tr>
<tr><td></td><td>Instytuty badawcze</td></tr>
<tr><td></td><td>Urząd Dozoru Technicznego</td></tr>
</table></td></tr>
</table>

				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.
				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
				Podmioty zarządzające/odpowiedzialne za stan techniczny oraz sprawność infrastruktury przeciwpowodziowej, budowli hydrotechnicznych i pozostałych obiektów o charakterze inżynierskim.
				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).
			Finanse publiczne	Centrum Informatyki Resortu Finansów.
				Spółka celowa, 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.
Sektor 10. Przestrzeń kosmiczna		**Załącznik do projektu ustawy**	**Sektor 9.** Przestrzeń kosmiczna
— Operatorzy infrastruktury naziemnej będącej własnością państw członkowskich lub podmiotów prywatnych i przez nie zarządzanej i obsługiwanej, którzy wspierają świadczenie usług kosmicznych, z wyłączeniem dostawców publicznych sieci łączności elektronicznej zdefiniowanych w art. 2 pkt 8 dyrektywy (UE) 2018/1972			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.
Sektor 11. Produkcja, przetwarzanie i dystrybucja żywności		**Załącznik do projektu ustawy**	**Sektor 10.** Produkcja, przetwarzanie i dystrybucja żywności
Przedsiębiorstwa spożywcze zdefiniowane w art. 3 pkt 2 rozporządzenia (WE) nr 178/2002 Parlamentu Europejskiego i Rady (22), zajmujące się wyłącznie logistyką i dystrybucją hurtową oraz produkcją przemysłową i przetwórstwem przemysłowym na dużą skalę			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.).

Odwrócona tabela zgodności

Projekt ustawy o zmianie ustawy o zarządzaniu kryzysowym oraz niektórych innych ustaw (UC47)

Jedn. red.	Treść przepisu projektu	Uzasadnienie wprowadzenia przepisu
Art. 1 pkt 4 lit. a, c, e, f, g h, j projektu ustawy (art. 3 pkt 1, 2b, 3, 3a, 8, 12, 14-16-18, 22, 29, 30 ustawy o zarządzaniu kryzysowym)	(Art. 3) 1) sytuacji kryzysowej – należy przez to rozumieć sytuację wpływającą negatywnie na poziom bezpieczeństwa ludzi, mienia w znacznych rozmiarach, środowiska lub dziedzictwa kulturowego, wywołującą znaczne ograniczenia w działaniu właściwych organów administracji publicznej ze względu na nieadekwatność posiadanych sił i środków lub zakłócenia obsługi tych organów; 2b) potencjalnej infrastrukturze krytycznej – należy przez to rozumieć obiekt, urządzenie, instalację, sieć, system oraz usługę lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje, sieci, systemy oraz usługi będące w fazie projektowania lub budowy, które po ich zakończeniu mogą być niezbędne do: a) realizacji ważnych interesów państwa, w tym zapewnienia funkcjonowania organów administracji publicznej, b) zapewnienia funkcjonowania przedsiębiorstw, c) zaspokajania oraz utrzymywania potrzeb obywateli, w tym potrzeb o charakterze lokalnym, d) zapewniające świadczenie usług kluczowych; 3) ochronie infrastruktury krytycznej - należy przez to rozumieć wszelkie działania zmierzające do zapewnienia funkcjonalności, ciągłości działania oraz integralności infrastruktury krytycznej; 3a) operatorze infrastruktury krytycznej – należy przez to rozumieć właściciela lub posiadacza obiektu, urządzenia, instalacji, sieci, systemu oraz usługi lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji, sieci, systemów oraz usług wpisanych do wykazu infrastruktury krytycznej;	Wdrożenie rozwiązań w zakresie zarządzania ryzykiem z uwzględnieniem rozwiązań zawartych w postanowieniach decyzji Parlamentu Europejskiego i Rady nr 1313/2013/EU z dnia 17 grudnia 2013 r. w sprawie Unijnego Mechanizmu Ochrony Ludności (Dz. Urz. UE L 347 z 20.12.2013, str. 924, L 250 z 04.10.2018, str. 1 oraz L 77A z 20.03.2019, str. 1) – dalej „UMOL” Słowniczek do ustawy uzupełniono o definicje niezbędne m.in. dla opracowania planów zarządzania kryzysowego, zawierających komponent zarządzania ryzykiem. Dostosowanie regulacji w obszarze infrastruktury krytycznej.

	8) siatce bezpieczeństwa – należy przez to rozumieć zestawienie potencjalnych zagrożeń ze wskazaniem podmiotu wiodącego oraz podmiotów współpracujących w realizacji działań, o których mowa w art. 2; 12) ryzyku – należy przez to rozumieć prawdopodobieństwo wystąpienia zagrożenia wraz z jego skutkami; 14) zarządzaniu ryzykiem – należy przez to rozumieć działania polegające na: a) ocenie ryzyka, b) planowaniu działań postępowania z ryzykiem, c) wdrażaniu działań postępowania z ryzykiem, d) osiąganiu gotowości do reagowania w przypadku wystąpienia sytuacji kryzysowej, f) okresowej ocenie osiągniętych efektów; 15) module zadaniowym – należy przez to rozumieć zestawienie przedsięwzięć i zadań przewidzianych do realizacji w sytuacji kryzysowej przez podmioty wskazane w siatce bezpieczeństwa, z wykorzystaniem własnych sił i środków, a także możliwego, zaplanowanego i uzgodnionego wsparcia ze strony innych podmiotów wskazanych w siatce bezpieczeństwa; 16) planach zarządzania kryzysowego – należy przez to rozumieć plany zarządzania ryzykiem oraz plany reagowania kryzysowego; 17) planach zarządzania ryzykiem – należy przez to rozumieć Krajowy Plan Zarządzania Ryzykiem, plany zarządzania ryzykiem ministrów kierujących działami administracji rządowej i kierowników urzędów centralnych oraz wojewódzkie, powiatowe i gminne plany zarządzania ryzykiem; 18) planach reagowania kryzysowego – należy przez to rozumieć Krajowy Plan Reagowania Kryzysowego, plany reagowania kryzysowego ministrów kierujących działami administracji rządowej i kierowników urzędów centralnych oraz wojewódzkie, powiatowe i gminne plany reagowania kryzysowego; 19) decyzji 1313/2013/UE – należy przez to rozumieć decyzję Parlamentu Europejskiego i Rady nr 1313/2013/EU z dnia 17 grudnia 2013 r. w sprawie Unijnego Mechanizmu Ochrony Ludności (Dz. Urz. UE L 347 z 20.12.2013, str. 924, z późn. zm.);	

	22) zagrożeniu hybrydowym - należy przez to rozumieć wrogie działania realizowane przy zastosowaniu środków politycznych, gospodarczych, dyplomatycznych, informacyjnych, militarnych lub innych, które nie stanowią agresji militarnej w ujęciu prawa międzynarodowego; 29) zdolności do ochrony informacji niejawnych – należy przez to rozumieć spełnienie wymagań określonych w ustawie z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych; 30) realizacji zadań z zakresu obrony cywilnej oraz ochrony ludności – należy przez to rozumieć realizacje zadań, o których mowa w ustawie z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej (Dz. U. poz. 1907 oraz z 2025 r. poz. 1705).”;	
Art. 1 pkt 5 projektu ustawy (projektowany art. 4 ust. 1 pkt 1a ustawy o zarządzaniu kryzysowym)	(Art. 4) 1a) prowadzenie oceny ryzyka	Wdrożenie rozwiązań zapewniających podstaw zarządzania ryzykiem, z uwzględnieniem postanowień UMOL.
Art. 1 pkt 7 (projektowany Rozdział 3 „Plany zarządzania kryzysowego art. 6g–6o ustawy o zarządzaniu kryzysowym)	Rozdział 3 Plany zarządzania kryzysowego Art. 6g. 1. Plany zarządzania ryzykiem zawierają: 1) cele strategiczne; 2) opis zasad współdziałania między podmiotami wskazanymi w siatce bezpieczeństwa; 3) uporządkowaną listę działań na rzecz ograniczenia ryzyka katastrof naturalnych lub awarii technicznych w zakresie organizacyjnym, technicznym i finansowym, 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. 2. Plany zarządzania ryzykiem opracowują:	Projektowana regulacja przewiduje konieczność opracowania Krajowego Planu Zarządzania Ryzkiem, z uwzględnieniem postanowień UMOL oraz Krajowego Planu Reagowania Kryzysowego. Dodatkowo regulacja wskazuje plany zarządzania kryzysowego obejmujące plany zarządzania ryzykiem oraz plany reagowania kryzysowego na pozostałych szczeblach.

	1) dyrektor Centrum - Krajowy Plan Zarządzania Ryzykiem, zwany dalej "KPZR"; 2) minister kierujący działem administracji rządowej - plan zarządzania ryzykiem ministra kierującego działem administracji rządowej; 3) Szef Agencji Bezpieczeństwa Wewnętrznego, Szef Agencji Wywiadu oraz Szef Centralnego Biura Antykorupcyjnego - plan zarządzania ryzykiem odpowiednio Szefa Agencji Bezpieczeństwa Wewnętrznego, Szefa Agencji Wywiadu oraz Szefa Centralnego Biura Antykorupcyjnego; 4) kierownik urzędu centralnego wskazany przez ministra kierującego działem administracji rządowej, któremu podlega lub jest przez tego ministra nadzorowany - plan zarządzania ryzykiem kierownika urzędu centralnego; 5) wojewoda – wojewódzki plan zarządzania ryzykiem; 6) starosta - powiatowy plan zarządzania ryzykiem; 7) wójt (burmistrz, prezydent miasta) - gminny plan zarządzania ryzykiem. 3. Plany zarządzania ryzykiem, o których mowa w ust. 2, opracowuje się z uwzględnieniem zagrożeń wskazanych w Krajowej Ocenie Ryzyka. 4. Plany zarządzania ryzykiem, o których mowa w ust. 1 pkt 2-5, opracowuje się z zachowaniem spójności z KPZR. 5. W planach, o których mowa w ust. 1 pkt 5 i 6 uwzględnia się postanowienia KPZR. Art. 6h. 1. Na potrzeby opracowania projektu KPZR dyrektor Centrum wydaje wytyczne do jego opracowania, obejmujące elementy, o których mowa w art. 6g ust. 1. 2. Dyrektor Centrum przekazuje wytyczne do opracowania projektu KPZR: 1) ministrom kierującym działami administracji rządowej; 2) Szefowi Agencji Bezpieczeństwa Wewnętrznego, Szefowi Agencji Wywiadu oraz Szefowi Centralnego Biura Antykorupcyjnego; 3) wojewodom; 4) innym niż wymienione w pkt 1-3 podmiotom, jeżeli jest to konieczne. 3. W zakresie swojej właściwości organy i podmioty, o których mowa w ust. 2, uwzględniając wytyczne przekazane przez dyrektora Centrum opracowują propozycje do ujęcia w projekcie KPZR. 4. Propozycje do ujęcia w projekcie KPZR wraz z danymi stanowiącymi podstawę do ich przygotowania, z wyłączeniem informacji niejawnych, organy i podmioty, o których mowa w ust. 2, przekazują dyrektorowi Centrum we wskazanym przez niego terminie.	

	5. Dyrektor Centrum może wystąpić do organów i podmiotów, o których mowa w ust. 2, o przekazanie dodatkowych propozycji do ujęcia w projekcie KPZR, jeżeli uzna, że ich umieszczenie w KPZR jest niezbędne. 6. Propozycje do ujęcia w projekcie KPZR przekazane przez ministra kierującego działem administracji rządowej uwzględniają wkład do propozycji do ujęcia w projekcie KPZR kierownika urzędu centralnego podległego temu ministrowi lub przez niego nadzorowanego. 7. Kierownik urzędu centralnego podległy ministrowi kierującego działem administracji rządowej lub przez niego nadzorowany opracowuje i przekazuje wkład do propozycji do ujęcia w projekcie KPZR ministra kierującego działem administracji rządowej. 8. Dyrektor Centrum przedkłada Radzie Ministrów projekt KPZR nie rzadziej niż raz na trzy lata. Rada Ministrów przyjmuje KPZR w drodze uchwały. 9. Na podstawie KPZR dyrektor Centrum opracowuje i udostępnia Komisji Europejskiej streszczenie istotnych elementów krajowej oceny zdolności zarządzania ryzykiem, o której mowa w art. 6 ust. 1 lit. b decyzji 1313/2013/UE. Art. 6i. 1. Plan zarządzania ryzykiem ministra kierującego działem administracji rządowej obejmuje własny plan zarządzania ryzykiem oraz plany zarządzania ryzykiem kierowników urzędów centralnych podległych temu ministrowi lub przez niego nadzorowanych. 2. Minister kierujący działem administracji, w zakresie swojej właściwości, wskazuje kierownika urzędu centralnego podległego lub nadzorowanego, który jest obowiązany do opracowania własnego planu zarządzania ryzykiem. 3. Plan zarządzania ryzykiem Ministra Obrony Narodowej uwzględnia plany zarządzania ryzykiem Szefa Służby Kontrwywiadu Wojskowego oraz Szefa Służby Wywiadu Wojskowego. 4. Minister kierujący działem administracji rządowej, Szef Agencji Bezpieczeństwa Wewnętrznego, Szef Agencji Wywiadu, Szef Centralnego Biura Antykorupcyjnego: 1) uzgadnia projekt planu zarządzania ryzykiem z dyrektorem Centrum pod względem spójności z KPZR; 2) zatwierdza uzgodniony plan zarządzania ryzykiem; 3) przekazuje kopię zatwierdzonego planu zarządzania ryzykiem dyrektorowi Centrum. 5. Kierownik urzędu centralnego, o którym mowa w ust. 2: 1) uzgadnia projekt planu zarządzania ryzykiem z ministrem kierującym działem administracji rządowej, któremu podlega lub przez którego jest nadzorowany;	

	2) uzgadnia projekt planu zarządzania ryzykiem z dyrektorem Centrum pod względem spójności z KPZR; 3) zatwierdza uzgodniony plan zarządzania ryzykiem; 4) przekazuje kopię zatwierdzonego planu zarządzania ryzykiem właściwemu ministrowi oraz dyrektorowi Centrum. 6. Wojewoda: 1) przekazuje projekt wojewódzkiego planu zarządzania ryzykiem do zatwierdzenia ministrowi właściwemu do spraw administracji publicznej; 2) przekazuje zatwierdzony wojewódzki plan zarządzania ryzykiem do wiadomości dyrektorowi Centrum. 7. Starosta przekazuje projekt powiatowego planu zarządzania ryzykiem do zatwierdzenia właściwemu wojewodzie. 8. Wójt (burmistrz, prezydent miasta) przekazuje projekt gminnego planu zarządzania kryzysowego do zatwierdzenia właściwemu staroście. Art. 6j. 1. Plany reagowania kryzysowego opracowują: 1) dyrektor Centrum - Krajowy Plan Zarządzania Ryzykiem, zwany dalej "KPRK"; 2) minister kierujący działem administracji rządowej - plan reagowania kryzysowego ministra kierującego działem administracji rządowej; 3) Szef Agencji Bezpieczeństwa Wewnętrznego, Szef Agencji Wywiadu oraz Szef Centralnego Biura Antykorupcyjnego - plan reagowania kryzysowego odpowiednio Szefa Agencji Bezpieczeństwa Wewnętrznego, Szefa Agencji Wywiadu oraz Szefa Centralnego Biura Antykorupcyjnego; 4) kierownik urzędu centralnego wskazany przez ministra kierującego działem administracji rządowej, któremu podlega lub jest przez tego ministra nadzorowany - plan reagowania kryzysowego kierownika urzędu centralnego; 5) wojewoda – wojewódzki plan reagowania kryzysowego; 6) starosta - powiatowy plan reagowania kryzysowego; 7) wójt (burmistrz, prezydent miasta) - gminny plan reagowania kryzysowego. 2. Plany reagowania kryzysowego, o których mowa w ust. 1, opracowuje się w odniesieniu do zagrożeń wskazanych w Krajowej Ocenie Ryzyka oraz z uwzględnieniem odpowiedniego planu zarządzania ryzykiem. 3. Plany reagowania kryzysowego, o których mowa w ust. 1 pkt 2-5, opracowuje się z zachowaniem spójności z KPRK. Art. 6k. 1. KPRK zawiera:	

	1) określenie zadań i obowiązków uczestników zarządzania kryzysowego w formie siatki bezpieczeństwa w zakresie reagowania w przypadku wystąpienia sytuacji kryzysowej oraz usuwania jej skutków; 2) zasady współdziałania między uczestnikami, o których mowa w pkt 1, w tym wymiany informacji w relacjach krajowych i międzynarodowych; 3) zestawienie sił i środków planowanych do wykorzystania w sytuacjach kryzysowych lub w zakresie realizacji zadań związanych z ochroną ludności oraz obroną cywilną; 4) zestawienie modułów zadaniowych pogrupowanych w katalogi; 5) załączniki określające: a) opis organizacji systemu monitorowania zagrożeń, ostrzegania i alarmowania, b) opis organizacji łączności, c) opis informowania ludności o zagrożeniach i sposobach postępowania na wypadek zagrożeń, d) procedury oceniania i dokumentowania strat i szkód, e) procedury uruchamiania rezerw strategicznych, f) procedury realizacji zadań związanych z ochroną ludności oraz obroną cywilną; g) procedury reagowania kryzysowego – standardowe procedury operacyjne, h) priorytety w zakresie ochrony oraz odtwarzania infrastruktury krytycznej. 2. Dyrektor Centrum we współpracy z podmiotami, o których mowa w art. 6j ust. 1 pkt 2-5, opracowuje projekt KPRK. 3. Dyrektor Centrum przedkłada projekt KPRK Radzie Ministrów nie rzadziej niż raz na trzy lata. Rada Ministrów przyjmuje KPRK w drodze uchwały. Art. 6l. 1. Plan reagowania kryzysowego ministra kierującego działem administracji rządowej, Szefa Agencji Bezpieczeństwa Wewnętrznego, Szefa Agencji Wywiadu, Szefa Centralnego Biura Antykorupcyjnego oraz kierownika urzędu centralnego podległego ministrowi kierującemu działem administracji rządowej lub przez niego nadzorowanego zawiera: 1) określenie zadań i obowiązków uczestników zarządzania kryzysowego w formie siatki bezpieczeństwa w zakresie reagowania w przypadku wystąpienia sytuacji kryzysowej oraz usuwania jej skutków; 2) określenie zadań w zakresie monitorowania zagrożeń; 3) zestawienie przedsięwzięć realizowanych w ramach przypisanych katalogów i modułów zadaniowych wraz z ich opisem; 4) określenie organizacji realizacji zadań z zakresu ochrony infrastruktury krytycznej lub zapewnienia ciągłości świadczenia usług kluczowych.	

	2. Plan reagowania kryzysowego ministra kierującego działem administracji rządowej obejmuje własny plan reagowania kryzysowego oraz plany reagowania kryzysowego kierowników urzędów centralnych podległych temu ministrowi lub przez niego nadzorowanych. 3. Minister kierujący działem administracji, w zakresie swojej właściwości, wskazuje kierownika urzędu centralnego podległego lub nadzorowanego, który jest zobowiązany do opracowania własnego planu reagowania kryzysowego. 4. Plan reagowania kryzysowego Ministra Obrony Narodowej uwzględnia plany zarządzania kryzysowego Szefa Służby Kontrwywiadu Wojskowego oraz Szefa Służby Wywiadu Wojskowego. 5. Minister kierujący działem administracji rządowej, Szef Agencji Bezpieczeństwa Wewnętrznego, Szef Agencji Wywiadu, Szef Centralnego Biura Antykorupcyjnego: 1) uzgadnia projekt planu reagowania kryzysowego z dyrektorem Centrum pod względem spójności z KPRK; 2) zatwierdza uzgodniony plan reagowania kryzysowego; 3) przekazuje kopię zatwierdzonego planu reagowania kryzysowego dyrektorowi Centrum. 6. Kierownik urzędu centralnego, o którym mowa w ust. 3: 1) uzgadnia projekt planu reagowania kryzysowego z ministrem kierującym działem administracji rządowej, któremu podlega lub przez którego jest nadzorowany; 2) uzgadnia projekt planu reagowania kryzysowego z dyrektorem Centrum pod względem spójności z KPRK; 3) zatwierdza uzgodniony plan reagowania kryzysowego; 4) przekazuje kopię zatwierdzonego planu reagowania kryzysowego właściwemu ministrowi oraz dyrektorowi Centrum. Art. 6m. 1. Wojewódzki plan reagowania kryzysowego zawiera: 1) elementy, o których mowa w art. 6k ust. 1 pkt 1–3 i 5 oraz art. 6l ust. 1 pkt 2 i 3; 2) zestawienie przedsięwzięć minimalizujących skutki zakłócenia funkcjonowania infrastruktury krytycznej dla ludności na terenie województwa wraz z ich opisem. 2. Wojewoda: 1) przekazuje projekt wojewódzkiego planu reagowania kryzysowego do zatwierdzenia ministrowi właściwemu do spraw administracji publicznej; 2) przekazuje zatwierdzony wojewódzki plan reagowania kryzysowego do wiadomości dyrektorowi Centrum.	

	Art. 6n. 1. Powiatowy plan zarządzania kryzysowego oraz gminny plan zarządzania kryzysowego zawiera: 1) elementy, o których mowa w art. 6k ust. 1 pkt 1–3 i 5 oraz art. 6l ust. 1 pkt 2 i 3; 2) zestawienie przedsięwzięć minimalizujących skutki zakłócenia funkcjonowania infrastruktury krytycznej dla ludności na terenie właściwej jednostki samorządu terytorialnego, wraz z ich opisem. 2. Starosta przekazuje projekt powiatowego planu zarządzania kryzysowego do zatwierdzenia właściwemu wojewodzie. 3. Wójt (burmistrz, prezydent miasta) przekazuje projekt gminnego planu zarządzania kryzysowego do zatwierdzenia właściwemu staroście. Art. 6o. 1. Plany zarządzania kryzysowego podlegają systematycznej aktualizacji w cyklu planowania nie dłuższym niż trzy lata. 2. Plany zarządzania kryzysowego uzgadnia się z właściwymi podmiotami, w zakresie ich dotyczącym, planowanymi do wykorzystania przy realizacji przedsięwzięć określonych w planie. 3. Przy opracowywaniu planów zarządzania kryzysowego uwzględnia się: 1) zawarte umowy i porozumienia, 2) plany opracowane na podstawie odrębnych przepisów, w tym wynikające z aktów Unii Europejskiej - niezbędne do realizacji przedsięwzięć określonych w planach zarządzania kryzysowego. 4. Minister kierujący działem administracji rządowej może wydać, w drodze zarządzenia, wytyczne do opracowania planów zarządzania kryzysowego kierowników urzędów centralnych podległych temu ministrowi lub przez niego nadzorowanych, kierując się zachowaniem spójności z planami zarządzania kryzysowego opracowywanego przez ministra.	
Art. 1 pkt 7 (rozdział 4 „Infrastruktura krytyczna, art. 6p-6q ustawy o zarządzaniu kryzysowym)	Rozdział 4 Infrastruktura krytyczna Art. 6p. Zadania dotyczące infrastruktury krytycznej obejmują: 1) identyfikację oraz wyznaczanie infrastruktury krytycznej; 2) gromadzenie i przetwarzanie informacji dotyczących zagrożeń infrastruktury krytycznej;	Przepisy dotyczące infrastruktury krytycznej zawierają szereg narzędzi, które w założeniu mają zapewnić maksymalnie efektywną i skuteczną ochronę infrastruktury krytycznej.

	3) opracowywanie i wdrażanie procedur na wypadek wystąpienia zagrożeń infrastruktury krytycznej; 4) odtwarzanie infrastruktury krytycznej; 5) współpracę między organami administracji publicznej a operatorami infrastruktury krytycznej w zakresie ochrony infrastruktury krytycznej. Art. 6q. 1. Organami właściwymi w sprawie identyfikacji infrastruktury krytycznej oraz współpracy z operatorami infrastruktury krytycznej, w zakresie swoich właściwości, są: 1) ministrowie kierujący działami administracji rządowej; 2) wojewodowie; 3) Komisja Nadzoru Finansowego. 2. Organy, o których mowa w ust. 1, w zakresie identyfikacji infrastruktury krytycznej współpracują z dyrektorem Centrum. 3. Minister kierujący działem administracji rządowej, wojewoda, Komisja Nadzoru Finansowego, w zakresie swojej właściwości, oraz dyrektor Centrum, zapewniają bieżącą współpracę z operatorem infrastruktury krytycznej, w szczególności przez: 1) prowadzenie bieżącej wymiany informacji na temat zagrożeń; 2) prowadzenie działań informacyjnych dotyczących dobrych praktyk, działań edukacyjnych na rzecz poszerzania wiedzy w zakresie bezpieczeństwa oraz zapewnienia funkcjonowania infrastruktury krytycznej, w tym organizowanie, konferencji, seminariów lub forów wymiany wiedzy; 3) udzielanie wsparcia merytorycznego operatorom infrastruktury krytycznej: a) w zakresie wdrażania dobrych praktyk oraz niezbędnych rozwiązań dotyczących ochrony infrastruktury krytycznej, b) w celu zapewnienia właściwego funkcjonowania infrastruktury krytycznej, jej ochrony lub odbudowy, c) w sytuacji kryzysowej lub w przypadku możliwości wystąpienia sytuacji kryzysowej.	
Art. 1 pkt 7 projektu ustawy (rozdział 5 „Identyfikowanie infrastruktury	Rozdział 5 Identyfikowanie infrastruktury krytycznej Art. 6r. 1. Dyrektor Centrum w celu zapewnienia:	Przepisy dotyczące infrastruktury krytycznej zawierają szereg narzędzi, które w założeniu mają zapewnić maksymalnie efektywną i skuteczną ochronę infrastruktury krytycznej.

krytycznej art. 6r-6x ustawy o zarządzaniu kryzysowym)	1) identyfikacji obiektu, urządzenia, instalacji, sieci, systemu oraz usługi lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji, sieci, systemów oraz usług jako infrastruktury krytycznej, 2) realizacji zadań w zakresie ochrony infrastruktury krytycznej – prowadzi wykaz infrastruktury krytycznej. 2. Wykaz infrastruktury krytycznej zawiera: 1) nazwę i lokalizację infrastruktury krytycznej, w tym wskazanie infrastruktury krytycznej niezbędnej do świadczenia usług kluczowych; 2) dane operatora infrastruktury krytycznej, w tym siedzibę i adres oraz numer identyfikacji podatkowej (NIP), jeżeli został nadany; 3) wskazanie organu identyfikującego infrastrukturę krytyczną. 3. Wykaz infrastruktury krytycznej prowadzony jest w postaci elektronicznej. Do wykazu stosuje się przepisy ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych. 4. Obiekt, urządzenie, instalacja, sieć, system oraz usługa lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje, sieci, systemy oraz usługi zostają wpisane do wykazu infrastruktury krytycznej w przypadku gdy spełniają kryteria, o których mowa w przepisach wydanych na podstawie ust. 5. 5. Rada Ministrów określi, w drodze uchwały, kryteria pozwalające identyfikować obiekt, urządzenie, instalację, sieć, system oraz usługę lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje, sieci, systemy oraz usługi jako infrastrukturę krytyczną, w tym: 1) kryteria sektorowe – progi, w tym progi liczbowe, charakteryzujące zdolność obiektu, urządzenia, instalacji, sieci, systemu oraz usługi lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji, sieci, systemów oraz usług do zapewnienia, funkcjonowania organów administracji publicznej, zapewnienia funkcjonowania przedsiębiorstw, zaspokajania potrzeb obywateli oraz zapewnienia świadczenia usług kluczowych; 2) kryteria przekrojowe – progi odnoszące się do znaczenia obiektu, urządzenia, instalacji, sieci, systemu oraz usługi lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji, sieci, systemów oraz usług obejmujące: a) kryteria ofiar w ludziach – oceniane w odniesieniu do ewentualnej liczby ofiar śmiertelnych lub liczby rannych, b) kryteria ewakuacji - oceniane w odniesieniu do liczby osób ewakuowanych lub czasu ewakuacji, c) kryteria skutków ekonomicznych – oceniane w odniesieniu do znaczenia strat ekonomicznych lub pogorszenia świadczenia jakości usług kluczowych,	

	d) kryteria skutków społecznych – oceniane w odniesieniu do wpływu na zaufanie opinii publicznej lub zakłócenia codziennego życia obywateli, w tym utraty usług kluczowych, e) kryteria wpływu międzynarodowego – oceniane w odniesieniu do pogorszenia wizerunku kraju na arenie międzynarodowej lub możliwości realizacji zobowiązań międzynarodowych, f) kryteria unikatowości - oceniane w odniesieniu do braku możliwości zastąpienia lub odtworzenia w akceptowalnym czasie -uwzględniając sektory i podsektory, o których mowa w załączniku do ustawy, znaczenie obiektu, urządzenia, instalacji, sieci, systemu oraz usługi lub połączone ze sobą funkcjonalnie obiektów, urządzeń, instalacji, sieci, systemów oraz usług dla realizacji interesów państwa, funkcjonowania przedsiębiorców, zaspokajania potrzeb obywateli, w tym potrzeb o charakterze lokalnym oraz zapewnienia świadczenia usług kluczowych. 6. Do uchwały stosuje się przepisy ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych. Art. 6s. 1. Dyrektor Centrum dokonuje wpisu do wykazu infrastruktury krytycznej na podstawie wniosku złożonego przez: 1) ministra kierującego działem administracji rządowej; 2) właściwego miejscowo wojewodę; 3) Przewodniczącego Komisji Nadzoru Finansowego. 2. Dyrektor Centrum opracowuje wyciągi z wykazu infrastruktury krytycznej znajdującej się na terenie poszczególnych województw i przekazuje je właściwym wojewodom. Art. 6t. 1. Minister kierujący działem administracji rządowej we współpracy z dyrektorem Centrum identyfikuje obiekt, urządzenie, instalację, sieć, system oraz usługę lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje, sieci, systemy oraz usługi mogące stanowić infrastrukturę krytyczną. 2. W przypadku identyfikacji prowadzonej przez ministra kierującego działem administracji rządowej, obiekt, urządzenie, instalację, sieć, system oraz usługę lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje, sieci, systemy oraz usługi zostają wpisane do wykazu infrastruktury krytycznej, jeżeli spełniają łącznie kryterium sektorowe, o którym mowa w art. 6r ust. 5 pkt 1, oraz co najmniej jedno z kryteriów przekrojowych, o których mowa w art. 6r ust. 5 pkt 2. 3. Minister kierujący działem administracji rządowej może wystąpić do właściciela lub posiadacza obiektu, urządzenia, instalacji, sieci, systemu oraz usługi lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji, sieci,	

	systemów oraz usług o udzielenie informacji, które umożliwią ocenę, czy spełniają one warunki do uznania ich za infrastrukturę krytyczną, przekazując dokumenty niezbędne do udzielenia informacji. 4. Minister kierujący działem administracji rządowej w wystąpieniu, o którym mowa w ust. 3, wskazuje termin udzielenia informacji. Wyznaczony termin nie może być krótszy niż 14 dni, licząc od dnia otrzymania wystąpienia przez podmiot. 5. Minister kierujący działem administracji rządowej składa do dyrektora Centrum wniosek o wpis obiektu, urządzenia, instalacji, sieci, systemu oraz usługi lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji, sieci, systemów oraz usługi do wykazu infrastruktury krytycznej. Wniosek zawiera informacje obejmujące: 1) nazwę i lokalizację obiektu, urządzenia, instalacji, sieci, systemu oraz usługi lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji, sieci, systemów oraz usług; 2) dane właściciela lub posiadacza obiektu, urządzenia, instalacji, sieci, systemu oraz usługi lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji, sieci, systemów oraz usług w tym siedzibę i adres oraz numer identyfikacji podatkowej (NIP), jeżeli został nadany. 6. Wniosek sporządza się i składa na piśmie utrwalonym w postaci elektronicznej, opatrzonym kwalifikowanym podpisem elektronicznym, podpisem osobistym, podpisem zaufanym albo kwalifikowaną pieczęcią elektroniczną. Art. 6u. 1. Wojewoda we współpracy z dyrektorem Centrum identyfikuje obiekt, urządzenie, instalację lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje oraz sieć, system lub usługę mogące stanowić infrastrukturę krytyczną na terenie województwa. 2. W przypadku identyfikacji prowadzonej przez wojewodę, obiekt, urządzenie, instalację, sieć, system oraz usługę lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje, sieci, systemy oraz usługi mogą zostać wpisane do wykazu infrastruktury krytycznej, jeżeli spełniają co najmniej jedno z kryteriów przekrojowych, o których mowa w art. 6r ust. 5 pkt 2. Przepisy art. 6t ust. 3-6 stosuje się odpowiednio. Art. 6v. 1. Komisja Nadzoru Finansowego, w zakresie swojej właściwości, we współpracy z dyrektorem Centrum, identyfikuje obiekt, urządzenie, instalację, sieć, system oraz usługę lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje, sieci, systemy oraz usługi mogące stanowić infrastrukturę krytyczną.	

	2. W przypadku identyfikacji prowadzonej przez Komisję Nadzoru Finansowego, obiekt, urządzenie, instalacja, sieć, system oraz usługa lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje, sieci, systemy oraz usługi mogą zostać wpisane do wykazu infrastruktury krytycznej, jeżeli spełniają łącznie kryterium sektorowe, o którym mowa w art. 6r ust. 5 pkt 1, oraz co najmniej jedno z kryteriów, o których mowa w art. 6r ust. 5 pkt 2. Przepis art. 6t ust. 3-6 stosuje się odpowiednio. Art. 6w. 1. Dyrektor Centrum informuje właściciela lub posiadacza obiektu, urządzenia, instalacji, sieci, systemu oraz usługi lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji, sieci, systemów oraz usług o dokonaniu wpisu do wykazu infrastruktury krytycznej oraz obowiązkach z tym związanych w terminie 30 dni od wpisu do wykazu. 2. Informacje o realizacji czynności, o których mowa w ust. 1, dyrektor Centrum przekazuje organowi wnioskującemu o wpis do wykazu. Art. 6x. Organy, o których mowa w art. 6s ust. 1, oraz dyrektor Centrum, prowadzą bieżącą wymianę informacji dotyczących realizacji czynności w zakresie identyfikacji obiektów, urządzeń, instalacji, sieci, systemów oraz usług lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji, sieci, systemów oraz usług, które mogą zostać wpisane do wykazu infrastruktury krytycznej.	
Art. 1 pkt 7 projektu ustawy (rozdział 6 „Identyfikowanie potencjalnej infrastruktury krytycznej art. 6y-6zd ustawy o zarządzaniu kryzysowym)	Rozdział 6 Identyfikowanie potencjalnej infrastruktury krytycznej Art. 6y. 1. Dyrektor Centrum w celu zapewnienia: 1) identyfikacji obiektu, urządzenia, instalacji, sieci, systemu oraz usługi lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji, sieci, systemów oraz usług, będących na etapie projektowania lub budowy jako potencjalnej infrastruktury krytycznej, 2) realizacji zadań w zakresie ochrony potencjalnej infrastruktury krytycznej – prowadzi wykaz potencjalnej infrastruktury krytycznej. 2. Wykaz potencjalnej infrastruktury krytycznej zawiera: 1) nazwę i lokalizację potencjalnej infrastruktury krytycznej; 2) dane podmiotu będącego inwestorem, w rozumieniu ustawy z dnia 7 lipca 1994 r. – Prawo budowlane (Dz. U. z 2025 r. poz. 418, 1080, 1535 i 1673),	Przepisy dotyczące infrastruktury krytycznej zawierają szereg narzędzi, które w założeniu mają zapewnić maksymalnie efektywną i skuteczną ochronę infrastruktury krytycznej.

	prowadzącego prace projektowe lub budowlane dotyczące potencjalnej infrastruktury krytycznej, w tym siedzibę i adres oraz numer identyfikacji podatkowej (NIP), jeżeli został nadany; 3) wskazanie organu identyfikującego potencjalną infrastrukturę krytyczną. 3. Wykaz potencjalnej infrastruktury krytycznej prowadzony jest w postaci elektronicznej. Do wykazu stosuje się przepisy ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych. 4. Obiekt, urządzenie, instalacja, sieć, system oraz usługa lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje, sieci, systemy oraz usługi, które są na etapie projektowania lub budowy mogą zostać wpisane do wykazu potencjalnej infrastruktury krytycznej w przypadku gdy z założeń wynika, że spełnią kryteria, o których mowa w przepisach wydanych na podstawie aktu wykonawczego wydanego na podstawie art. 6r ust. 5. Art. 6z. Dyrektor Centrum dokonuje wpisu do wykazu potencjalnej infrastruktury krytycznej na podstawie wniosku złożonego przez: 1) ministra kierującego działem administracji rządowej; 2) właściwego miejscowo wojewodę; 3) Komisję Nadzoru Finansowego. Art. 6za. 1. Minister kierujący działem administracji rządowej, we współpracy z dyrektorem Centrum oraz inwestorem identyfikuje potencjalną infrastrukturę krytyczną. Przepisy art. 6t ust. 2-6 stosuje się odpowiednio. 2. Wojewoda, we współpracy z dyrektorem Centrum oraz inwestorem identyfikuje potencjalną infrastrukturę krytyczną. Przepisy art. 6u ust. 2 oraz art. 6t ust. 3-6 stosuje się odpowiednio. 3. Komisja Nadzoru Finansowego, we współpracy z dyrektorem Centrum oraz inwestorem identyfikuje potencjalną infrastrukturę krytyczną. Przepisy art. 6v ust. 2 oraz art. 6t ust. 3-6 stosuje się odpowiednio. Art. 6zb. 1. Dyrektor Centrum informuje inwestora o dokonaniu wpisu do wykazu potencjalnej infrastruktury krytycznej oraz obowiązkach z tym związanych w terminie 30 dni od wpisu do wykazu. 2. Informacje o realizacji czynności, o których mowa w ust. 1, dyrektor Centrum przekazuje organowi wnioskującemu o wpis do wykazu. Art. 6zc. 1. Organy, o których mowa w art. 6z, w zakresie swojej właściwości, we współpracy z dyrektorem Centrum, przedstawiają inwestorowi informacje	

	oraz dokumenty pozwalające na uwzględnienie wymogów dotyczących infrastruktury krytycznej w dokumentacji projektowej lub podczas realizacji inwestycji oraz zapewniają bieżącą współpracę w zakresie, o którym mowa w art. 6p. 2. Do obowiązków inwestora w zakresie ochrony potencjalnej infrastruktury krytycznej nie stosuje się rozdziału 7 ustawy, z wyjątkiem przepisu art. 6ze ust. 1 pkt 1 i pkt 2 lit. a, pkt 3 lit. a oraz pkt 4, art. 6zf ust. 2 pkt 1 i 2 lit. a oraz pkt 4 lit. a. Art. 6zd. Podmioty, o których mowa w art. 6z oraz dyrektor Centrum, prowadzą bieżącą wymianę informacji dotyczących realizacji czynności w zakresie identyfikacji obiektów, urządzeń, instalacji, sieci, systemów oraz usług lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji, sieci, systemów oraz usług będących w fazie projektowania lub budowy, które mogą zostać wpisane do wykazu potencjalnej infrastruktury krytycznej.	
Art. 1 pkt 7 projektu ustawy (rozdział 7 „Obowiązki operatora infrastruktury krytycznej” art. 6ze-6zj ustawy o zarządzaniu kryzysowym)	Rozdział 7 Obowiązki operatora infrastruktury krytycznej Art. 6ze. 1. Operator infrastruktury krytycznej zapewnia jej ochronę, w szczególności przez: 1) prowadzenie systematycznej analizy zagrożeń dla infrastruktury krytycznej; 2) wdrażanie adekwatnych do wyników przeprowadzonej analizy zagrożeń rozwiązań w zakresie: a) bezpieczeństwa fizycznego, w tym ochrony fizycznej oraz zabezpieczeń technicznych uwzględniających kontrolę dostępu, b) bezpieczeństwa technicznego, c) bezpieczeństwa osobowego dotyczącego pracowników i dostawców zewnętrznych, d) cyberbezpieczeństwa, e) bezpieczeństwa prawnego, f) ciągłości działania i odtwarzania, w tym utrzymywania własnych systemów rezerwowych zapewniających bezpieczeństwo i podtrzymujących funkcjonowanie infrastruktury krytycznej do czasu jej pełnego odtworzenia; 3) bieżącą współpracę z organami zarządzania kryzysowego, służbami, stażami i inspekcjami oraz dyrektorem Centrum przez przekazywanie i odbieranie informacji o:	Przepisy dotyczące infrastruktury krytycznej zawierają szereg narzędzi, które w założeniu mają zapewnić maksymalnie efektywną i skuteczną ochronę infrastruktury krytycznej.

	a) zagrożeniach zakłócających lub mogących zakłócić funkcjonowanie infrastruktury krytycznej, b) spodziewanych przerwach lub zakłóceniach w funkcjonowaniu infrastruktury krytycznej; 4) sporządzanie i przekazywanie informacji w zakresie zapewnienia ochrony infrastruktury krytycznej na żądanie: a) odpowiednio: - ministra, o którym mowa w art. 6t ust. 1, - właściwego miejscowo wojewody, - Komisji Nadzoru Finansowego, b) dyrektora Centrum, c) Szefa Agencji Bezpieczeństwa Wewnętrznego; 5) zapewnienie zdolności do ochrony informacji niejawnych w zakresie realizacji przedsięwzięć związanych z ochroną infrastruktury krytycznej. 2. Operator infrastruktury krytycznej przeprowadza po raz pierwszy analizę zagrożeń, o której mowa w ust. 1 pkt 1, w terminie 6 miesięcy od dnia otrzymania informacji o dokonaniu wpisu do wykazu infrastruktury krytycznej. 3. Operator infrastruktury krytycznej wdraża rozwiązania, o których mowa w ust. 1 pkt 2 w terminie 6 miesięcy od dnia przeprowadzenia po raz pierwszy analizy zagrożeń, a następnie stosowanie do potrzeb, w zależności od wyników przeprowadzonej analizy zagrożeń. 4. Rada Ministrów określi, w drodze rozporządzenia, minimalne wymagania w zakresie bezpieczeństwa fizycznego, technicznego, osobowego, cyberbezpieczeństwa, prawnego oraz ciągłości działania, niezbędne do wdrażania rozwiązań, o których mowa w ust. 1 pkt 2, mając na uwadze: 1) rekomendacje o charakterze specjalistycznym w zakresie ochrony infrastruktury krytycznej, niezbędne do wdrażania rozwiązań w zakresie bezpieczeństwa infrastruktury krytycznej; 2) lokalizację i charakterystykę infrastruktury krytycznej; 3) potrzebę podejmowania działań zapewniających bezpieczeństwo infrastruktury krytycznej. 5. Operator infrastruktury krytycznej, przy opracowywaniu i zawieraniu umów zapewniających wdrażanie rozwiązań, o których mowa w ust. 1 pkt 2, żąda od usługodawców: 1) certyfikatów, uwzględniając dokumenty równoważne, zgodnie z zasadami wzajemnego uznawania w Unii Europejskiej lub w przypadku ich braku innych	

	dokumentów właściwych dla poszczególnych rozwiązań, potwierdzających posiadanie odpowiednich kompetencji i uprawnień niezbędnych do ich realizacji; 2) potwierdzenia zdolności do ochrony informacji niejawnych oraz stosowania przepisów o ochronie informacji niejawnych, jeżeli opracowanie, przygotowanie i wykonanie umowy wiążą się dostępem do informacji niejawnych. 6. Minister kierujący działem administracji rządowej, właściwy terytorialnie wojewoda lub Komisja Nadzoru Finansowego, po zasięgnięciu opinii właściwych sektorowych rad do spraw kompetencji, o których mowa w art. 4c ust. 1 pkt 2 ustawy z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości (Dz. U. z 2025 r. poz. 98), może opracować i udostępnić na stronie podmiotowej Biuletynu Informacji Publicznej zestawienie certyfikatów lub innych dokumentów właściwych dla realizacji rozwiązań wskazanych w ust. 1 pkt 2. 7. Minister kierujący działem administracji rządowej, właściwy terytorialnie wojewoda lub Komisja Nadzoru Finansowego, w zakresie swojej właściwości, we współpracy z dyrektorem Centrum ustalają klauzule tajności oraz szczegółowe wymagania dotyczące ochrony informacji niejawnych związanych z realizacją przez operatora infrastruktury krytycznej przedsięwzięć związanych z ochroną tej infrastruktury. Art. 6zf. 1. Operator infrastruktury krytycznej opracowuje, stosuje i na bieżąco aktualizuje dokumentację ochrony infrastruktury krytycznej. 2. Dokumentacja ochrony infrastruktury krytycznej, zawiera: 1) charakterystykę infrastruktury krytycznej oraz analizę zagrożeń, o której mowa w art. 6ze ust. 1 pkt 1; 2) opis zastosowanych, adekwatnie do przeprowadzonej analizy zagrożeń, rozwiązań w zakresie: a) bezpieczeństwa fizycznego, w tym opis organizacji i wykonywania ochrony fizycznej infrastruktury krytycznej, w tym zawierający dane specjalistycznej uzbrojonej formacji ochronnej chroniącej infrastrukturę krytyczną, 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) – jeżeli występuje, b) bezpieczeństwa technicznego, c) bezpieczeństwa osobowego, d) cyberbezpieczeństwa, e) bezpieczeństwa prawnego, f) ciągłości działania i odtwarzania; 3) opis:	

	a) zasobów umożliwiających podtrzymanie funkcjonowania infrastruktury krytycznej do czasu jej pełnego odtworzenia, b) współpracy z organami zarządzania kryzysowego, służbami, stażami i inspekcjami oraz dyrektorem Centrum dotyczący wymiany informacji o zdarzeniu zakłócającym lub mogącym zakłócić funkcjonowanie infrastruktury krytycznej oraz sposobu postępowania w przypadku takiego zdarzenia; 4) procedury: a) działania w sytuacji zagrożenia lub zakłócenia funkcjonowania infrastruktury krytycznej, b) zapewnienia ciągłości funkcjonowania infrastruktury krytycznej, c) odtwarzania infrastruktury krytycznej; 5) inne elementy niż wskazane w pkt 1-4, biorąc pod uwagę charakterystykę infrastruktury krytycznej. 3. Procedury, o których mowa w ust. 2 pkt 4 lit. a, uzgadnia się z właściwymi organami zarządzania kryzysowego, służbami, strażami i inspekcjami, w zakresie ich dotyczącym, planowanymi do wykorzystania w realizacji przedsięwzięć określonych w dokumentacji 4. Do dokumentacji ochrony infrastruktury krytycznej stosuje się przepisy ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych. 5. Operator infrastruktury krytycznej w terminie 15 miesięcy od uzyskania informacji o dokonaniu wpisu do wykazu infrastruktury krytycznej przedkłada oświadczenie o opracowaniu dokumentacji ochrony infrastruktury krytycznej, odpowiednio: 1) ministrowi, o którym mowa w art. 6t ust. 1; 2) właściwemu miejscowo wojewodzie; 3) Komisji Nadzoru Finansowego 4) dyrektorowi Centrum. 6. Operator infrastruktury krytycznej może dołączyć do oświadczenia o opracowaniu dokumentacji ochrony infrastruktury krytycznej informację o braku możliwości wdrożenia określonych rozwiązań, wskazując przyczynę tego braku, wraz z uzasadnieniem. Operator infrastruktury krytycznej uzgadnia odpowiednio z ministrem, wojewodą lub Komisją Nadzoru Finansowego działania mające na celu wdrożenie brakujących rozwiązań. 7. Operator infrastruktury krytycznej przekazuje dokumentację ochrony infrastruktury krytycznej na żądanie organów, o których mowa w ust. 4 pkt 1-3 oraz dyrektora Centrum. 8. Operator infrastruktury krytycznej będący jednocześnie podmiotem kluczowym w rozumieniu ustawy z dnia 5 lipca 2018 r. o krajowym systemie	

	cyberbezpieczeństwa, w dokumentacji ochrony infrastruktury krytycznej uwzględnia dokumentację dotyczącą bezpieczeństwa systemu informacyjnego, o której mowa w art. 10 tej ustawy. Art. 6zg. 1. Operator infrastruktury krytycznej sporządza, w terminie do dnia 31 marca każdego roku raport o stanie ochrony infrastruktury krytycznej za rok ubiegły. 2. Raport o stanie ochrony infrastruktury krytycznej zawiera w szczególności informacje dotyczące jej ochrony w zakresie zapewnienia: 1) bezpieczeństwa fizycznego; 2) bezpieczeństwa technicznego; 3) bezpieczeństwa osobowego; 4) cyberbezpieczeństwa; 5) bezpieczeństwa prawnego; 6) ciągłości działania i odtwarzania. 3. Raport o stanie ochrony infrastruktury krytycznej sporządza się z uwzględnieniem: 1) analizy zagrożeń dla infrastruktury krytycznej, o której mowa w art. 6ze ust. 1 pkt 1; 2) wdrożonych rozwiązań, o których mowa w art. 6ze ust. 1 pkt 2; 3) zagrożeń, które zakłóciły lub mogły zakłócić funkcjonowanie infrastruktury krytycznej, a nie były uwzględnione w analizie, o której mowa w art. 6ze ust. 1 pkt 1; 4) wyników przeprowadzonych kontroli i audytów odnoszących się do wdrożonych rozwiązań, o których mowa w art. 6ze ust. 1 pkt 2; 5) opisu działań podjętych przez operatora infrastruktury krytycznej w przypadkach wystąpienia zagrożeń. 4. Operator infrastruktury krytycznej przekazuje, w terminie do dnia 31 marca każdego roku, raport o stanie ochrony infrastruktury krytycznej odpowiednio: 1) ministrowi, o którym mowa w art. 6t ust. 1; 2) właściwemu miejscowo wojewodzie; 3) Komisji Nadzoru Finansowego. 5. Operator infrastruktury krytycznej przekazuje raport o stanie ochrony infrastruktury krytycznej na żądanie dyrektora Centrum, Szefa Agencji Bezpieczeństwa Wewnętrznego lub Szefa Agencji Wywiadu. 6. Do raportu o stanie ochrony infrastruktury krytycznej stosuje się przepisy ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych.	

	Art. 6zh.1. W przypadku pracownika zatrudnionego na stanowisku umożliwiającym dostęp do informacji o bezpieczeństwie obiektu infrastruktury krytycznej i osoby ubiegającej się o zatrudnienie na tym stanowisku, operator infrastruktury krytycznej żąda od pracownika i tej osoby przedłożenia informacji dotyczących karalności, w tym informacji, czy ich dane osobowe są zgromadzone w Krajowym Rejestrze Karnym. 2. Operator infrastruktury krytycznej żąda od pracownika danych biometrycznych w postaci odcisków linii papilarnych palców, głosu, obrazu rogówki, sieci żył palców lub biometrii twarzy, które są odpowiednie do wdrożonych środków kontroli dostępu niezbędnych dla ochrony szczególnie ważnych informacji o bezpieczeństwie infrastruktury krytycznej lub dostępu do stref, obiektów lub pomieszczeń wymagających szczególnej kontroli. 3. Operator infrastruktury krytycznej przetwarza informacje i dane, o których mowa w ust. 1 i 2 przez okres uzasadniony celem przetwarzania. Art. 6zi. 1. W celu realizacji zadań, o których mowa w art. 6ze ust. 1, art. 6zf ust. 1 oraz art. 6zg ust. 1, operator infrastruktury krytycznej wyznacza koordynatora ochrony infrastruktury krytycznej oraz zastępcę koordynatora ochrony infrastruktury krytycznej. 2. Operator infrastruktury krytycznej wyznacza koordynatora ochrony infrastruktury krytycznej oraz zastępcę koordynatora ochrony infrastruktury krytycznej w terminie 30 dni od dnia otrzymania informacji o ujęciu w wykazie infrastruktury krytycznej. 3. Zastępca koordynatora infrastruktury krytycznej zastępuje koordynatora w czasie jego nieobecności lub czasowej niemożności wykonywania przez niego obowiązków. 4. Koordynatorem ochrony infrastruktury krytycznej może być osoba, która: 1) jest pracownikiem operatora infrastruktury krytycznej albo żołnierzem lub funkcjonariuszem pełniącym służbę w jednostce organizacyjnej będącej operatorem infrastruktury krytycznej; 2) korzysta z pełni praw publicznych; 3) posiada wiedzę, umiejętności i doświadczenie w zakresie zarządzania bezpieczeństwem, z uwzględnieniem przedmiotu działalności operatora infrastruktury krytycznej; 4) nie była skazana prawomocnym wyrokiem za umyślne przestępstwo lub umyślne przestępstwo skarbowe; 5) spełnia wymagania bezpieczeństwa osobowego w zakresie dostępu do informacji niejawnych o klauzuli ustalonej w trybie określonym w art. 6ze ust. 7.	

	5. Koordynator ochrony infrastruktury krytycznej podlega bezpośrednio organowi zarządzającemu operatora infrastruktury krytycznej. 6. O wyznaczeniu koordynatora operator infrastruktury krytycznej informuje odpowiednio: 1) ministra, o którym mowa w art. 6t ust. 1; 2) właściwego miejscowo wojewodę; 3) Przewodniczącego Komisję Finansowego; 4) dyrektora Centrum. 7. Operator infrastruktury krytycznej zapewnia koordynatorowi ochrony infrastruktury krytycznej organizacyjne i techniczne warunki realizacji zadań, w tym dostęp do niezbędnych dokumentów i informacji. 8. Przepisy ust. 4-7 stosuje się do zastępcy koordynatora ochrony infrastruktury krytycznej. Art. 6zj. 1. Operator infrastruktury krytycznej informuje Prezesa Urzędu Komunikacji Elektronicznej o możliwości zastosowania urządzeń uniemożliwiających telekomunikację na określonym obszarze. 2. W celu zapewnienia ochrony infrastruktury krytycznej operator infrastruktury krytycznej w przypadkach o których mowa: 1) w art. 156ze ust. 1 ustawy z dnia 3 lipca 2002 r. - Prawo lotnicze (Dz. U. z 2025 r. poz. 1431 i 1688) lub 2) w art. 28a ust. 1 ustawy z dnia 4 września 2008 r. o ochronie żeglugi i portów morskich (Dz. U. z 2024 r. poz. 597 oraz ……), lub 3) w art. 11 pkt 17 ustawy z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej (Dz. U. z 2025 r. poz. 555, 820 i …) - może podjąć decyzję o dopuszczalności zastosowania urządzeń, o których mowa w ust. 1, przez czas niezbędny do wykonywania czynności przez pracowników ochrony specjalistycznych uzbrojonych formacji ochronnych, z uwzględnieniem konieczności minimalizacji skutków braku możliwości korzystania z usług telekomunikacyjnych. 3. O zastosowaniu urządzeń, o których mowa w ust. 1, operator infrastruktury krytycznej niezwłocznie informuje Prezesa Urzędu Komunikacji Elektronicznej.	

Art. 1 pkt 8 projektu ustawy (art. 7a ustawy o zarządzaniu kryzysowym)	w art. 7a w ust. 3 pkt 2 otrzymuje brzmienie: "2) zapewnienia właściwego funkcjonowania, ochrony, wzmocnienia oraz odbudowy infrastruktury krytycznej lub zapewnienia niezakłóconego świadczenia usługi kluczowej;";	Zmiany wynikowe do regulacji związanych ze świadczeniem usługi kluczowej przez podmiot krytyczny.
Art. 1 pkt 10 (projektowana zmiana art. 11 ustawy o zarządzaniu kryzysowym)	w art. 11: w pkt 1 lit. b otrzymuje brzmienie: b)opracowywanie i aktualizowanie Krajowego Planu Zarządzania Ryzykiem oraz Krajowego Planu Reagowania Kryzysowego,”, po ust. 1a dodaje się ust. 1b w brzmieniu: 1b. Centrum realizuje zadania, o których mowa w art. 22 ustawy z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej.";	
Art. 1 pkt 11 projektu ustawy (art. 11b ustawy o zarządzaniu kryzysowym)	"Art. 11b. W celu realizacji zadań planowania cywilnego wynikających z członkostwa Rzeczypospolitej Polskiej w Organizacji Traktatu Północnoatlantyckiego, Centrum: 1) koordynuje: a) udział przedstawicieli Rzeczypospolitej Polskiej w pracach Komitetu do spraw Odporności Organizacji Traktatu Północnoatlantyckiego oraz zapewnia wsparcie merytoryczne prowadzonych prac, b) opracowywanie stanowisk Rzeczypospolitej Polskiej na potrzeby procesów planowania cywilnego Organizacji Traktatu Północnoatlantyckiego; 2) zapewnienia funkcjonowanie punktu kontaktowego do przekazywania zadań oraz uruchamiania procedur wynikających z członkostwa Rzeczypospolitej Polskiej w Organizacji Traktatu Północnoatlantyckiego.”.	Zapewnienie narzędzia do całodobowej wymiany informacji na potrzeby zarządzania kryzysowego oraz analizy występujących lub mogących wystąpić zagrożeń.
Art. 1 pkt 12 projektu ustawy (art**.** 12 ustawy o zarządzaniu kryzysowym)	w art. 12: a) ust. 1 otrzymuje brzmienie: „1. Ministrowie kierujący działami administracji rządowej oraz kierownicy urzędów centralnych realizują, w zakresie swojej właściwości, zadania dotyczące zarządzania kryzysowego, w tym: 1) opracowują plany zarządzania kryzysowego;	

	2) organizują, prowadzą i koordynują szkolenia i ćwiczenia z zakresu zarządzania kryzysowego oraz biorą udział w ćwiczeniach krajowych i międzynarodowych; 3) współpracują z operatorami infrastruktury krytycznej lub podmiotami krytycznymi w zakresie realizacji zadań ochrony infrastruktury krytycznej oraz zapewnienia niezakłóconego świadczenia usług kluczowych; 4) zapewniają funkcjonowanie stałego dyżuru w ramach podwyższania gotowości obronnej państwa.", b) uchyla się ust. 2 i 2a, c) ust. 2c otrzymuje brzmienie: „2c. Do zadań zespołów, o których mowa w ust. 2b, należy: 1) dokonywanie okresowej oceny ryzyka na potrzeby Krajowej Oceny Ryzyka; 2) dokonywanie okresowej oceny gotowości do reagowania w przypadku wystąpienia sytuacji kryzysowej w zakresie organizacyjnym, technicznym i finansowym; 3) opiniowanie projektów planów zarządzania kryzysowego; 4) wypracowywanie wniosków i propozycji dotyczących zapobiegania i przeciwdziałania zagrożeniom.”;	
Art. 1 pkt 13 projektu ustawy (art. 14 ustawy o zarządzaniu kryzysowym)	w art. 14 ust. 3 otrzymują brzmienie: „3. Minister właściwy do spraw administracji publicznej w uzgodnieniu z ministrem właściwym do spraw wewnętrznych oraz po zasięgnięciu opinii dyrektora Centrum, wydaje, w drodze zarządzenia, wojewodom wytyczne do wojewódzkich planów zarządzania kryzysowego. Wytyczne do wojewódzkich planów zarządzania kryzysowego mogą zostać wydane w każdym czasie, niezależnie od cyklu planowania.";	
Art. 1 pkt 14 projektu ustawy **(art. 25 ustawy o zarządzaniu kryzysowym)**	w art. 25 w ust. 3 pkt 13 otrzymuje brzmienie: "13) wspieranie w wykonywaniu zadań związanych z naprawą i odbudową infrastruktury technicznej;";	

Art. 1 pkt 15 projektu ustawy (art. 25a-25d ustawy o zarządzaniu kryzysowym)	uchyla się art. 25a-25d;	
Art. 1 pkt 17 projektu ustawy (art. 26ustawy o zarządzaniu kryzysowym)	w art. 26 dodaje się ust. 4a i 4b w brzmieniu: „4a. Środki finansowe z rezerwy celowej, o której mowa w ust. 4, mogą być przeznaczone na realizację przedsięwzięć związanych z zarządzaniem ryzykiem, reagowaniem w przypadku wystąpienia sytuacji kryzysowej oraz usuwaniem jej skutków i odtwarzaniem zasobów, z uwzględnieniem planowanych działań z zakresu ochrony ludności i obrony cywilnej. 4b. Środki z rezerwy celowej, o której mowa w ust. 4, mogą być przeznaczane na pomoc finansową udzielaną innym jednostkom samorządu terytorialnego na realizację przez te jednostki przedsięwzięć, o których mowa w ust. 4a."	
Art. 2 projektu ustawy (zmiany w ustawie o drogach publicznych)	**Art. 2.** W ustawie z dnia 21 marca 1985 r. o drogach publicznych (Dz. U. z 2024 r. poz. 320 i 1222) dodaje się art. 20i w brzmieniu: "Art. 20i. 1. W sytuacji kryzysowej, jeżeli wymagają tego potrzeby obronności lub istotny interes bezpieczeństwa państwa, właściwy miejscowo wojewoda może, w drodze rozporządzenia porządkowego, po zasięgnięciu opinii zarządcy drogi, wprowadzić czasowe ograniczenia w korzystaniu z dróg publicznych, w tym czasowo wyłączyć je z ruchu; 2. Czasowe ograniczenia w korzystaniu z dróg publicznych, w tym ich czasowe wyłączenie z ruchu wprowadza się w sposób, który umożliwia przemieszczanie się w określonych kierunkach za pomocą innych dróg niepodlegających ograniczeniom w korzystaniu i niewyłączonych z ruchu. 3. Rozporządzenie porządkowe w zakresie, o którym mowa w ust. 1, określa: 1) odcinki dróg publicznych wyznaczone za pomocą współrzędnych geograficznych lub oznakowania umieszczonego na słupkach hektometrowych i kilometrowych, na których wprowadzono czasowe ograniczenia w korzystaniu lub czasowo zamknięte dla ruchu; 2) rodzaj ograniczenia w korzystaniu z dróg publicznych;	Wsparcie realizacji działań z zakresu zarządzania kryzysowego.

	3) okres, na który wprowadzono ograniczenia w korzystaniu z dróg publicznych lub czasowe wyłączenie z ruchu; 4) obowiązki zarządcy drogi, zarządzającego ruchem oraz innych organów i podmiotów w zakresie, o którym mowa w ust. 1. 4. Rozporządzenie porządkowe, o którym mowa w ust. 1, może być ogłoszone w drodze obwieszczenia lub za pomocą środków komunikacji elektronicznej, lub w inny sposób zwyczajowo przyjęty na danym terenie.”.	
Art. 3 projektu ustawy (zmiany w ustawie o Policji)	**Art. 3.** W ustawie z dnia 6 kwietnia 1990 r. o Policji Dz. U. z 2025 r. poz. 636, 718 i 1366) wprowadza się następujące zmiany: 1) w art. 16 ust. 1 otrzymuje brzmienie: „1. W przypadkach, o których mowa w art. 11 ustawy z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej (Dz. U. z 2024 r. poz. 383), policjanci mogą użyć środków przymusu bezpośredniego, o których mowa w art. 12 ust. 1 pkt 1−13 i 17−23 tej ustawy, lub wykorzystać te środki.”; 2) w art. 18c ust. 1 otrzymuje brzmienie: „1. Komendant Główny Policji, Komendant CBŚP, Komendant CBZC lub komendant wojewódzki Policji: 1) w celu realizacji zadań, o których mowa w art. 1 ust. 2 pkt 1, 2, 3a, 4a lub 2) w przypadkach o których mowa: a) w art. 156ze ust. 1 ustawy z dnia 3 lipca 2002 r. - Prawo lotnicze (Dz. U. z 2025 r. poz. 1431 i 1668), lub b) w art. 28a ust. 1 ustawy z dnia 4 września 2008 r. o ochronie żeglugi i portów morskich (Dz. U. z 2024 r. poz. 597 oraz …), lub c) w art. 11 pkt 17 ustawy z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej, lub 3) po wprowadzeniu trzeciego lub czwartego stopnia alarmowego, o których mowa odpowiednio w art. 16 ust. 5 lub ust. 6 ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych - może podjąć decyzję o dopuszczalności zastosowania przez Policję urządzeń uniemożliwiających telekomunikację na określonym obszarze, przez czas niezbędny do wyeliminowania zagrożenia lub jego skutków, z uwzględnieniem konieczności minimalizacji skutków braku możliwości korzystania z usług telekomunikacyjnych."; 3) w art. 36k po ust. 3 dodaje się ust. 3a w brzmieniu:	Zmiany wynikowe do ustawy o środkach przymusu bezpośredniego. Zapewnienie ochrony przeciwko dronom. Doprecyzowanie podmiotu wypłacającego świadczeń dla funkcjonariuszy Policji oddelegowanych do wykonywania zadań w urzędzie obsługującym ministra właściwego do spraw wewnętrznych albo w jednostce podległej lub nadzorowanej przez ministra właściwego do spraw wewnętrznych.

	3a. W przypadku policjantów oddelegowanych do wykonywania zadań służbowych w urzędzie obsługującym ministra właściwego do spraw wewnętrznych albo w jednostce podległej lub nadzorowanej przez ministra właściwego do spraw wewnętrznych należności, o których mowa w ust. 3, wypłaca jednostka organizacyjna Policji, w której policjant pełnił służbę bezpośrednio przed oddelegowaniem w uzgodnieniu z kierownikiem urzędu albo jednostki, do której policjant został oddelegowany.”.	
Art. 4. projektu ustawy (zmiany w ustawie o Straży Granicznej)	Art. 4. W ustawie z dnia 12 października 1990 r. o Straży Granicznej (Dz. U. z 2025 r. poz. 914 i 1366) wprowadza się następujące zmiany: 1) w art. 1 po ust. 3b dodaje się ust. 3c w brzmieniu: „3c. Straż Graniczna zapewnia koordynację działań podejmowanych przez organy i podmioty realizujące zadania w ramach Centrum Bezpieczeństwa Morskiego, o którym mowa w art. 25a ustawy z dnia 4 września 2008 r. o ochronie żeglugi i portów morskich (Dz. U. z 2024 r. poz. 597 oraz …) ."; 2) w art. 10e ust. 1 otrzymuje brzmienie: „1. Komendant Główny Straży Granicznej, Komendant BSWSG lub komendant oddziału Straży Granicznej: 1) w celu realizacji zadań, o których mowa w art. 1 ust. 2 pkt 1, 2, 4-5d i 10 lub 2) w przypadkach, o których mowa: a) w art. 156ze ust. 1 ustawy z dnia 3 lipca 2002 r. Prawo lotnicze (Dz. U. z 2025 r. poz. 1431 i 1668), lub b) w art. 28a ust. 1 ustawy z dnia 4 września 2008 r. o ochronie żeglugi i portów morskich, lub c) w art. 11 pkt 17 ustawy z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej (Dz. U. z 2025 r. poz. 555, 820 oraz …), lub	Zmiany wynikowe do ustawy o środkach przymusu bezpośredniego. Zapewnienie ochrony przeciwko dronom. Doprecyzowanie podmiotu wypłacającego świadczeń dla funkcjonariuszy Straży Granicznej oddelegowanych do wykonywania zadań w urzędzie obsługującym ministra właściwego do spraw wewnętrznych albo w jednostce podległej lub nadzorowanej przez ministra właściwego do spraw wewnętrznych.

	3) po wprowadzeniu trzeciego lub czwartego stopnia alarmowego, o których mowa odpowiednio w art. 16 ust. 5 lub ust. 6 ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych - może podjąć decyzję o dopuszczalności zastosowania urządzeń uniemożliwiających telekomunikację na określonym obszarze, przez czas niezbędny do wykonywania czynności przez Straż Graniczną, z uwzględnieniem konieczności minimalizacji skutków braku możliwości korzystania z usług telekomunikacyjnych. 3) w art. 23 ust. 1 otrzymuje brzmienie: „1. W przypadkach, o których mowa w art. 11 ustawy z 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej (Dz. U. z 2024 r. poz. 383), funkcjonariusze mogą użyć środków przymusu bezpośredniego, o których mowa w art. 12 ust. 1 pkt 1−13 i 16−23 tej ustawy, lub wykorzystać te środki.”; 4) w art. 41i dodaje się ust. 3 w brzmieniu: 3. W przypadku funkcjonariuszy oddelegowanych do wykonywania zadań służbowych w urzędzie obsługującym ministra właściwego do spraw wewnętrznych albo w jednostce podległej lub nadzorowanej przez ministra właściwego do spraw wewnętrznych należności, o których mowa w ust. 1, wypłaca jednostka organizacyjna, w której funkcjonariusz pełnił służbę przed oddelegowaniem w uzgodnieniu z kierownikiem urzędu albo jednostki, do której funkcjonariusz został oddelegowany.”.	
Art. 5. projektu ustawy **(zmiany w ustawie o ochronie przeciwpożarowej)**	Art. 5. W ustawie z dnia 24 sierpnia 1991 r. o ochronie przeciwpożarowej (Dz. U. z 2025 r. poz. 188) w art. 14fa ust. 3 otrzymuje brzmienie: "3. Plany ratownicze w zakresie zdarzeń z dużą liczbą poszkodowanych oraz działań ratowniczych i działań pomocowych podczas katastrof, klęsk żywiołowych i zdarzeń nadzwyczajnych są skorelowane z planami reagowania kryzysowego, o których mowa w art. 6j ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, oraz z planami postępowania awaryjnego, o których	Dostosowanie do zmian w przepisach ustawy o zarządzaniu kryzysowym.

	mowa w art. 84 ust.1 ustawy z dnia 29 listopada 2000 r. - Prawo atomowe (Dz.U. z 2024 r. poz. 1277, 1897 i 1907).".	
Art. 6 projektu ustawy **(zmiany w ustawie o Państwowej Straży Pożarnej)**	Art. 6. W ustawie z dnia 24 sierpnia 1991 r. o Państwowej Straży Pożarnej (Dz. U. z 2025 r. poz. 1312 i 1366) w art. 37r dodaje się ust. 3 w brzmieniu: „3. W przypadku strażaków oddelegowanych do wykonywania zadań służbowych w urzędzie obsługującym ministra właściwego do spraw wewnętrznych albo w jednostce podległej lub nadzorowanej przez ministra właściwego do spraw wewnętrznych, należności, o których mowa w ust. 1, wypłaca jednostka organizacyjna Państwowej Straży Pożarnej, w której strażak pełnił służbę przed oddelegowaniem w uzgodnieniu z kierownikiem urzędu albo jednostki, do której strażak został oddelegowany.”.	Dostosowanie do zmian w przepisach ustawy o zarządzaniu kryzysowym. Doprecyzowanie podmiotu wypłacającego świadczeń dla strażaków PSP oddelegowanych do wykonywania w urzędzie obsługującym ministra właściwego do spraw wewnętrznych albo w jednostce podległej lub nadzorowanej przez ministra właściwego do spraw wewnętrznych.
Art. 7 (zmiany w ustawie o ochronie osób i mienia)	**Art. 7.** W ustawie z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz. U. z 2021 r. poz. 1995) wprowadza się następujące zmiany: 1) w art. 5: a) w ust. 2: - w pkt 1 w lit. c wyrazy „ustawy z dnia 29 października 2010 r. o rezerwach strategicznych (Dz. U. z 2020 r. poz. 2051) ” zastępuje się wyrazami „ustawy z dnia 17 grudnia 2020 r. o rezerwach strategicznych (Dz. U. z 2024 r. poz. 1598 i 1907 oraz…)”, - w pkt 3 lit. a otrzymuje brzmienie: „a) zakłady, obiekty i urządzenia mające istotne znaczenie dla funkcjonowania powiatów lub miast na prawach powiatu, których zniszczenie lub uszkodzenie może stanowić zagrożenie dla życia i zdrowia ludzi oraz środowiska, w	Usprawnienie ochrony infrastruktury krytycznej.

	szczególności elektrownie i ciepłownie, ujęcia wody, wodociągi i oczyszczalnie ścieków,”, - pkt 5 otrzymuje brzmienie: „5) obiekt, urządzenie, instalację lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje ujęte w wykazie , o którym mowa w art. 6r ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2023 r. poz.122 oraz z 2024 r. poz. 834, 1222 i 1473).”, b) ust. 3 otrzymuje brzmienie: „3. Szczegółowe wykazy obszarów, obiektów i urządzeń, o których mowa w ust. 2, sporządzają i bieżąco aktualizują: Prezes Narodowego Banku Polskiego, Krajowa Rada Radiofonii i Telewizji, ministrowie, kierownicy urzędów centralnych i wojewodowie w stosunku do podległych, podporządkowanych lub nadzorowanych jednostek organizacyjnych, oraz Komisja Nadzoru Finansowego w stosunku do podmiotów podlegających nadzorowi Komisji Nadzoru Finansowego w rozumieniu ustawy z dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym (Dz. U. z 2024 r. poz. 135). Umieszczenie w wykazie określonego obszaru, obiektu lub urządzenia następuje w drodze decyzji administracyjnej.”, c) po ust. 3 dodaje się ust. 3a w brzmieniu: 3a. Do wykazów, o których mowa w ust. 3 , stosuje się przepisy ustawy z dnia 5 sierpnia 2010 r o ochronie informacji niejawnych (Dz. U. z 2025 r. poz. 1209).”, d) ust. 4 otrzymuje brzmienie: „4. Podmioty, o których mowa w ust. 3 , przekazują wykazy oraz ich aktualizacje właściwym terytorialnie wojewodom w terminie 14 dni odpowiednio od ich sporządzenia lub aktualizacji.", e) po ust. 4 dodaje się ust. 4a w brzmieniu: "4a. Starostowie i prezydenci miast na prawach powiatu informują wojewodę o zakładach, obiektach i urządzeniach, o których mowa w ust. 2 pkt 3 lit. a, znajdujących się na terenie powiatu.”,	

	f) ust. 5 otrzymuje brzmienie: 5. Wojewodowie prowadzą ewidencję obszarów, obiektów i urządzeń podlegających obowiązkowej ochronie, znajdujących się na terenie województwa. Do ewidencji stosuje się przepisy ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych.”, g) po ust. 5 dodaje się ust. 5a w brzmieniu: "5a. Ewidencja, o której mowa w ust. 5, zawiera dane dotyczące w szczególności: 1) numeru wpisu; 2) nazwy obszaru, obiektu lub urządzenia; 3) adresu obszaru, obiektu lub urządzenia; 4) nazwy stanowiska kierownika jednostki, która zarządza obszarem, obiektem lub urządzeniem; 5) organu, o którym mowa w ust. 3 , właściwego w stosunku do obszaru, obiektu lub urządzenia.", h) ust. 6 otrzymuje brzmienie: „6. Wojewoda, w drodze decyzji administracyjnej, może umieścić w ewidencji, o której mowa w ust. 5, znajdujące się na terenie województwa obszary, obiekty i urządzenia inne niż wpisane do wykazów, o których mowa w ust. 3 lub do wykazu infrastruktury krytycznej, o którym mowa w art. 6r ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, w tym zakłady, obiekty i urządzenia, o których mowa w ust. 2 pkt 3 lit. a.”, i) dodaje się ust. 7 i 8 w brzmieniu: „7. Wojewoda, po otrzymaniu wykazów lub ich aktualizacji od podmiotów, o których mowa w ust. 3, niezwłocznie aktualizuje ewidencję, o której mowa w ust. 5.	

	8. Wojewoda, niezwłocznie po umieszczeniu obszaru, obiektu lub urządzenia w ewidencji, o której mowa w ust. 5, informuje o tym kierownika jednostki, który bezpośrednio zarządza obszarami, obiektami i urządzeniami umieszczonymi w ewidencji oraz odpowiednio podmioty, o których mowa w ust. 3 , a także właściwego terytorialnie komendanta wojewódzkiego Policji oraz właściwego terytorialnie dyrektora delegatury Agencji Bezpieczeństwa Wewnętrznego.”; 2) po art. 5 dodaje się art. 5a w brzmieniu: „Art. 5a. Środki ochrony fizycznej oraz zabezpieczenia techniczne wykraczające poza granice obiektu lub urządzenia podlegającego obowiązkowej ochronie mogą być stosowane od strony wody w odniesieniu do: 1) obiektów, o których mowa w art. 5 ust. 1, będących jednocześnie obiektami portowymi w rozumieniu ustawy z 4 września 2008 r. o ochronie żeglugi i portów morskich (Dz. U. z 2024 r. poz. 597); 2) sztucznych wysp, konstrukcji i urządzeń w obszarach morskich Rzeczypospolitej Polskiej, o których mowa w art. 23 ust. 1 ustawy 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, 1535 i 1668); 3) kabli i rurociągów układanych i utrzymywanych w obszarach morskich Rzeczypospolitej Polskiej, o których mowa w art. 26 ust. 1 oraz art. 27 ust. 1 ustawy z dnia 21 marca 1991 r. o obszarach morskich Rzeczypospolitej Polskiej i administracji morskiej.”; 3) w art. 26 w ust. 1 w pkt 5 dodaje się lit. c w brzmieniu: "c) w art. 36 ust. 1a-1c;"; 4) w art. 36: a) w ust. 1 w pkt 4 wprowadzenie do wyliczenia i lit. a otrzymują brzmienie: „użycia lub wykorzystania środków przymusu bezpośredniego, o których mowa w art. 12 ust. 1 pkt 1 lit. a, b i d, pkt 2 lit. a, pkt 5, 7, 9, 11, pkt 12 lit. a, pkt 13 i	

	21-23 ustawy z 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej (Dz. U. z 2025 r. poz. 555 i 820 oraz …): a) w granicach chronionych obiektów i obszarów − w przypadkach, o których mowa w art. 11 pkt 2, 5, 8, 10, 13,15-17 tej ustawy,”, b) ust. 1a otrzymuje brzmienie: „1a. Środki przymusu bezpośredniego, o których mowa w art. 12 ust. 1 pkt 5 lub 11 ustawy z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej, mogą być wykorzystane wyłącznie zgodnie z art. 156ze ustawy z dnia 3 lipca 2002 r. - Prawo lotnicze (Dz. U. z 2025 r. poz. 1431 i 1668), art. 28a ustawy z dnia 4 września 2008 r. o ochronie żeglugi i portów morskich lub art. 11 pkt 17 ustawy z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej.”, c) po ust. 1a dodaje się ust. 1b–1c w brzmieniu: „1b. Pracownik ochrony przy wykonywaniu zadań ochrony obiektów, o których mowa w art. 5a pkt 1, w celu zabezpieczenia infrastruktury portowej przed uszkodzeniem, może patrolować ten obiekt jednostką pływającą od strony wody. 1c. Wykonując czynności, o których mowa w ust. 1b, pracownik ochrony ma prawo do wezwania osób przebywających w basenie portowym, a niemających do tego uprawnień, do jego opuszczenia, a także do podjęcia interwencji wobec tych osób, w tym ujęcia ich oraz użycia środków przymusu bezpośredniego określonych w art. 12 ust. 1 pkt 1 lit. a, b i d, pkt 2 lit. a, pkt 11, 13 i 21-23 ustawy z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej w przypadkach, o których mowa w art. 11 pkt 2, 5, 8, 10,13 i 15-17 tej ustawy."; 5) w art. 47 w ust. 2 wprowadzenie do wyliczenia otrzymuje brzmienie: "2. Współpracę, o której mowa w ust. 1, specjalistyczne uzbrojone formacje ochronne podejmują odpowiednio z właściwymi terytorialnie:"; 6) po art. 50b dodaje się art. 50c w brzmieniu:	

	"Art. 50c. 1. Kto nie będąc do tego uprawnionym, przebywa na obszarze lub obiekcie podlegającym obowiązkowej ochronie oraz takiego obszaru lub obiektu wbrew żądaniu osoby uprawnionej nie opuszcza, podlega grzywnie, karze ograniczenia wolności albo karze pozbawienia wolności do lat 2. 2. Kto nie będąc do tego uprawnionym, przebywając na obszarze lub obiekcie podlegającym obowiązkowej ochronie, utrudnia lub uniemożliwia korzystanie z tych obszarów, obiektów lub znajdujących się na ich terenie urządzeń lub instalacji, podlega grzywnie, karze ograniczenia wolności albo karze pozbawienia wolności do lat 5.".	
Art. 8 projektu ustawy (zmiany w ustawie o Żandarmerii Wojskowej i wojskowych organach porządkowych)	**Art. 8.** W ustawie z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych (Dz. U. z 2023 r. poz. 1266, 1860 oraz z 2024 r. poz. 1222 i 1248) wprowadza się następujące zmiany: 1) w art. 42 ust. 1 i 2 otrzymują brzmienie: „Art. 42. 1. W przypadkach, o których mowa w art. 11 pkt 1−6 i 8−16 ustawy z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej, żołnierze Żandarmerii Wojskowej mogą użyć środków przymusu bezpośredniego, o których mowa w art. 12 ust. 1 pkt 1−9, pkt 11, pkt 12 lit. a, c i d, pkt 13-14 i 17−23 tej ustawy, lub wykorzystać te środki. 2. W przypadkach, o których mowa w art. 45 pkt 1 lit. a-c i e, pkt 2-3 i pkt 4 lit. a i b oraz w art. 47 pkt 1-3 i 5-8 ustawy z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej, żołnierze Żandarmerii Wojskowej mogą użyć broni palnej lub ją wykorzystać.”; 2) w art. 51 ust. 2 i 3 otrzymują brzmienie: "2. W przypadkach, o których mowa w art. 11 pkt 1-6 i 8-14 ustawy z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej, żołnierze wojskowych organów porządkowych wchodzących w skład służby garnizonowej i służby wewnętrznej jednostki wojskowej w związku z wykonywaniem czynności służbowych mogą użyć środków przymusu bezpośredniego, o których mowa w	Zmiany wynikowe do ustawy o środkach przymusu bezpośredniego.

	art. 12 ust. 1 pkt 1-5, 7-9, 11, pkt 12 lit. a, c i d, pkt 13, 17, 19-23 tej ustawy, lub wykorzystać te środki. 3. W przypadkach, o których mowa w art. 45 pkt 1 lit. a-c i e, pkt 2, 3, pkt 4 lit. a i b oraz w art. 47 pkt 1-3, 5-8 ustawy z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej, żołnierze wojskowych organów porządkowych wchodzących w skład służby garnizonowej i służby wewnętrznej jednostki wojskowej w związku z wykonywaniem czynności służbowych mogą użyć broni palnej lub ją wykorzystać.”.	
Art. 9 projektu ustaw. (zmiany w ustawie o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu)	**Art. 9.** W ustawie z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2024 r. poz. 812, 1222 i 1562) wprowadza się następujące zmiany: 1) w art. 5 w ust. 1 pkt 2a otrzymuje brzmienie: „2a) rozpoznawanie, zapobieganie i wykrywanie zagrożeń godzących w bezpieczeństwo istotnych z punktu widzenia ciągłości funkcjonowania państwa systemów teleinformatycznych organów administracji publicznej lub systemu sieci teleinformatycznych objętych wykazem, o którym mowa w art. 6r ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2023 r. poz. 122 oraz z 2024 r. poz. 834, 1222 i 1473), a także systemów teleinformatycznych operatorów infrastruktury krytycznej, o których mowa w art. 3 pkt 3a tej ustawy;”; 2) w art. 32a ust. 1 otrzymuje brzmienie: „1. W celu zapobiegania, przeciwdziałania i zwalczania zdarzeń o charakterze terrorystycznym lub uprawdopodabniających popełnienie przestępstwa szpiegostwa, dotyczących istotnych z punktu widzenia ciągłości funkcjonowania państwa systemów teleinformatycznych organów administracji publicznej lub sieci teleinformatycznych objętych wykazem, o którym mowa w art. 6r ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, a także systemów teleinformatycznych operatorów infrastruktury krytycznej, o których mowa w art. 3 pkt 3a tej ustawy, lub danych przetwarzanych w tych systemach oraz rozpoznawania, zapobiegania i wykrywania przestępstw o charakterze	Zmiany wynikowe, związane ze zmianami ustawy o zarządzaniu kryzysowym.

	terrorystycznym lub przestępstwa szpiegostwa w tym obszarze oraz ścigania ich sprawców, ABW może przeprowadzać ocenę bezpieczeństwa tych systemów teleinformatycznych, zwaną dalej „oceną bezpieczeństwa”.”; 3) w art. 32aa ust. 1 otrzymuje brzmienie: „1. W celu zapobiegania, przeciwdziałania i zwalczania zdarzeń o charakterze terrorystycznym lub uprawdopodabniających popełnienie przestępstwa szpiegostwa, dotyczących istotnych z punktu widzenia ciągłości funkcjonowania państwa systemów teleinformatycznych organów administracji publicznej lub sieci teleinformatycznych objętych wykazem, o których mowa w art. 6r ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, a także systemów teleinformatycznych operatorów infrastruktury krytycznej, o których mowa w art. 3 pkt 3a tej ustawy, lub danych przetwarzanych w tych systemach oraz rozpoznawania, zapobiegania i wykrywania przestępstw o charakterze terrorystycznym lub przestępstwa szpiegostwa w tym obszarze oraz ścigania ich sprawców, ABW wdraża w tych podmiotach system wczesnego ostrzegania o zagrożeniach występujących w sieci Internet, zwany dalej „systemem ostrzegania”, prowadzi go i koordynuje jego funkcjonowanie.”.	
Art. 10 projektu ustawy (zmiany w ustawie o transporcie kolejowym)	**Art. 10.** W ustawie z dnia 28 marca 2003 r. o transporcie kolejowym (Dz. U. z 2024 r. poz. 697 i 731) dodaje się art. 25g w brzmieniu: "Art. 25g. 1. W sytuacji kryzysowej, jeżeli wymagają tego potrzeby obronności lub istotny interes bezpieczeństwa państwa, właściwy miejscowo wojewoda może, w drodze rozporządzenia porządkowego, po zasięgnięciu opinii zarządcy infrastruktury kolejowej, wprowadzić czasowe ograniczenia w dostępie do infrastruktury kolejowej, w tym całkowicie wyłączyć dostęp do infrastruktury kolejowej. 2. Rozporządzenie porządkowe w zakresie, o którym mowa w ust. 1 określa: 1) linie kolejowe, opisane zgodnie z wykazem linii kolejowych zawartym w regulaminie sieci, wraz ze wskazaniem kilometraża odcinków linii kolejowych,	Mechanizm wsparcia realizacji zadań z zakresu zarządzania kryzysowego.

	na których wprowadzono czasowe ograniczenia w dostępie do infrastruktury kolejowej, w tym całkowicie wyłączono dostęp do infrastruktury kolejowej; 2) rodzaj ograniczenia w dostępie do infrastruktury kolejowej, w tym wskazuje przewozy priorytetowe lub ładunki z pierwszeństwem dostępu do infrastruktury kolejowej oraz przejazdu; 3) okres, na który wprowadzono ograniczenia w dostępie do infrastruktury kolejowej, w tym całkowicie wyłączono dostęp do infrastruktury kolejowej; 4) koordynatora przewozów priorytetowych lub ładunków z pierwszeństwem dostępu do infrastruktury kolejowej oraz przejazdu na liniach kolejowych, o których mowa w pkt 1. 3. Rozporządzenie porządkowe, o którym mowa w ust. 1, może być ogłoszone w drodze obwieszczenia lub za pomocą środków komunikacji elektronicznej, lub w inny sposób zwyczajowo przyjęty na danym terenie. 4. Operatorzy obiektów infrastruktury usługowej zapewniają pierwszeństwo w obsłudze przewozom priorytetowym lub ładunkom z pierwszeństwem dostępu do infrastruktury kolejowej oraz przejazdu, w zakresie wskazanym przez koordynatora, o którym mowa w ust. 2 pkt 4. 5. Jeżeli w opinii, o której mowa w ust. 1, zarządca infrastruktury kolejowej wskazuje na konieczność wprowadzenia czasowego ograniczenia w dostępie do infrastruktury kolejowej, w tym całkowitego wyłączenia dostępu do infrastruktury kolejowej zlokalizowanej poza obszarem właściwości wojewody wydającego rozporządzenie porządkowe, wojewoda przekazuje tę opinię pozostałym właściwym miejscowo wojewodom.".	

Art. 11 projektu ustawy (zmiany w ustawie o ochronie zdrowia zwierząt oraz zwalczaniu chorób zakaźnych zwierząt)	**Art. 11.** W ustawie z dnia 11 marca 2004 r. o ochronie zdrowia zwierząt oraz zwalczaniu chorób zakaźnych zwierząt (Dz. U. z 2023 r. poz. 1075 oraz z 2025 r. poz. 1795) dodaje się art. 47d-47g w brzmieniu: "Art. 47d. 1. W przypadku nakazu odstrzału, o którym mowa w art. 46 ust. 3 pkt 8, jeżeli jest to niezbędne ze względu na rodzaj i skalę zagrożenia, minister właściwy do spraw wewnętrznych, na wniosek wojewody, może przekazać do jego dyspozycji doraźne zgrupowanie zadaniowe sformowane z policjantów, funkcjonariuszy Straży Granicznej lub funkcjonariuszy Państwowej Straży Pożarnej, którzy posiadają uprawnienia do wykonywania polowania, celem ich użycia do odstrzału sanitarnego zwierząt wolno żyjących (dzikich) na określonych obszarach. 2. Dowodzenie doraźnymi zgrupowaniami zadaniowymi, o których mowa w ust. 1, powierzane jest odpowiednio policjantowi, funkcjonariuszowi Straży Granicznej lub funkcjonariuszowi Państwowej Straży Pożarnej wskazanemu przez właściwego miejscowo komendanta odpowiednio Policji, Straży Granicznej lub Państwowej Straży Pożarnej, a w przypadku stworzenia doraźnego zgrupowania zadaniowego złożonego z policjantów, funkcjonariuszy Straży Granicznej lub funkcjonariuszy Państwowej Straży Pożarnej – policjantowi wskazanemu przez właściwego miejscowo komendanta Policji. Art. 47e. 1. Jeżeli w sytuacji kryzysowej użycie innych sił i środków jest niemożliwe lub może okazać się niewystarczające, Minister Obrony Narodowej, na wniosek wojewody, może przekazać do jego dyspozycji doraźne zgrupowanie zadaniowe sformowane z żołnierzy, którzy posiadają uprawnienia do wykonywania polowania, celem użycia ich do odstrzału, o którym mowa w art. 46 ust. 3 pkt 8, zwierząt wolno żyjących (dzikich) na określonych obszarach. 2. Dowodzenie doraźnymi zgrupowaniami zadaniowymi, o których mowa w ust. 1, odbywa się na zasadach określonych w regulaminach wojskowych i według procedur obowiązujących w Siłach Zbrojnych Rzeczypospolitej Polskiej. 3. Użycie doraźnych zgrupowań zadaniowych w sytuacji kryzysowej nie może zagrozić zdolności Sił Zbrojnych do realizacji zadań wynikających z Konstytucji Rzeczypospolitej Polskiej i ratyfikowanych umów międzynarodowych.	Zmiany wynikowa, związana ze zmianą ustawy o zarzadzaniu kryzysowym.

	Art. 47f. 1. W przypadkach, o których mowa w art. 47d i art. 47e, odpowiednio policjanci, funkcjonariusze Straży Granicznej, funkcjonariusze Państwowej Straży Pożarnej i żołnierze używają broni myśliwskiej prywatnej lub użyczonej zgodnie z przepisami ustawy z dnia 21 maja 1999 r. o broni i amunicji (Dz. U. z 2024 r. poz. 485). 2. Odpowiedzialność za szkody wyrządzone przez policjantów, funkcjonariuszy Straży Granicznej, funkcjonariuszy Państwowej Straży Pożarnej i żołnierzy realizujących zadania, o których mowa w ust. 1, ponosi wojewoda. 3. W przypadkach, o których mowa w art. 47d i art. 47e: 1) nie stosuje się przepisów ustawy dotyczących ryczałtu; 2) policjanci, funkcjonariusze Straży Granicznej, funkcjonariusze Państwowej Straży Pożarnej i żołnierze współpracują z zarządcą lub dzierżawcą obwodu łowieckiego. Art. 47g. W przypadkach, o których mowa w art. 47d i art. 47e, do obowiązków wojewody należy: 1) zapewnienie amunicji do broni, o której mowa w art. 47f ust. 1; 2) zwrot kosztów transportu, zakwaterowania i wyżywienia doraźnych zgrupowań zadaniowych; zwrot kosztów zakwaterowania lub wyżywienia nie przysługuje w przypadku zapewnienia w miejscu wykonywania czynności bezpłatnego zakwaterowania lub wyżywienia.	
Art. 12 projektu ustawy (zmiany w ustawie o ochronie żeglugi i portów morskich)	**Art. 12.** W ustawie z dnia 4 września 2008 r. o ochronie żeglugi i portów morskich (Dz. U. z 2024 r. poz. 597) wprowadza się następujące zmiany: 1) w art. 1 w ust. 3 w pkt 4 kropkę zastępuje się średnikiem i dodaje się punkt 5 w brzmieniu: „5) terminalu morskiego przeładunku ropy i paliw ciekłych w Gdańsku."; 2) w art. 24 ust. 5 otrzymuje brzmienie:	Zmiany zwiększające bezpieczeństwo infrastruktury krytycznej.

	„5. W przypadku wprowadzenia poziomu ochrony 3 stosuje się odpowiednio art. 21 i art. 25 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U z 2023 r. poz. 122 oraz z 2024 r. poz. 834, 1222 i 1473).”; 3) po art. 25 dodaje się art. 25a-25d w brzmieniu: „Art. 25a. 1 W celu zapewnienia wsparcia wymiany informacji pomiędzy organami lub podmiotami realizującymi zadania w zakresie zapobiegania, ograniczania lub usuwania poważnego niebezpieczeństwa grożącego: 1) obiektom portowym i portom morskim oraz związanej z nimi infrastrukturze, 2) obiektom, urządzeniom i instalacjom wchodzącym w skład infrastruktury zapewniającej dostęp do portów o podstawowym znaczeniu dla gospodarki narodowej, 3) zlokalizowanym na polskich obszarach morskich obiektom, urządzeniom i instalacjom wchodzącym w skład infrastruktury służącej do: a) wytwarzania lub przesyłania źródeł energii lub surowców energetycznych, w tym morskim farmom wiatrowym w rozumieniu art. 3 pkt 3 ustawy o promowaniu i zespołom urządzeń służącym do wyprowadzenia mocy w rozumieniu art. 3 pkt 13 ustawy o promowaniu, oraz podmorskim sieciom elektroenergetycznym i światłowodowym lub rurociągom, a także związanej z nimi infrastrukturze, b) telekomunikacji w rozumieniu ustawy z dnia 12 lipca 2024 r. Prawo komunikacji elektronicznej (Dz. U. poz. 1221), 4) wykorzystywanym w wyłącznej strefie ekonomicznej sztucznym wyspom, konstrukcjom i urządzeniom przeznaczonym do gospodarczego badania i eksploatacji zasobów wyłącznej strefy ekonomicznej - zwanych dalej „infrastrukturą morską” oraz statkom, a także zadania w zakresie ochrony granicy państwowej na morzu oraz ochrony życia lub zdrowia ludzi, mienia w znacznych rozmiarach lub środowiska zlokalizowanych na polskich obszarach morskich w rozumieniu ustawy z dnia 21 marca 19912 r. o obszarach	

	morskich Rzeczypospolitej Polskiej i administracji morskiej, tworzy się Centrum Bezpieczeństwa Morskiego, zwane dalej „CBM”. 2. CBM umiejscowione jest we wskazanym przez Komendanta Głównego Straży Granicznej oddziale Straży Granicznej. 3. CBM kieruje wyznaczony przez Komendanta Głównego Straży Granicznej komendant oddziału Straży Granicznej lub jego zastępca, zwany dalej „Szefem CBM”. 4. Do zadań CBM należy: 1) bieżące monitorowanie zagrożeń, 2) wspieranie wymiany informacji pomiędzy organami lub podmiotami, o których mowa w art. 25b ust. 1, 3) wspieranie współpracy z właściwymi organami innych państw, 4) wspieranie procesu decyzyjnego właściwych organów lub podmiotów oraz podejmowanych przez nich działań, 5) opracowywanie raportów dotyczących zagrożeń - w odniesieniu do żeglugi, infrastruktury morskiej, statków, granicy państwa na morzu, życia lub zdrowia ludzi, mienia w znacznych rozmiarach lub ochrony środowiska na polskich obszarach morskich 5. CBM realizuje zadania w systemie całodobowym przez 7 dni w tygodniu. 6.Koordynację wspólnej realizacji zadań określonych w ust. 4 zapewnia Szef CBM.” Art. 25b. 1. W ramach CBM współdziałają przedstawiciele Ministra Obrony Narodowej, Szefa Służby Kontrwywiadu Wojskowego, Szefa Agencji Bezpieczeństwa Wewnętrznego, Szefa Służby Wywiadu Wojskowego, Szefa Agencji Wywiadu, Komendanta Głównego Policji, Komendanta Głównego Państwowej Straży Pożarnej, Szefa Krajowej Administracji Skarbowej, Dyrektora Morskiej Służby Poszukiwania i Ratownictwa (Służby SAR), dyrektorów	

	urzędów morskich oraz właściwych terytorialnie wojewodów i operatorów infrastruktury krytycznej, którzy wspólnie ze Strażą Graniczą realizują zadania określone w art. 25a ust. 4, na zasadach określonych w porozumieniu zawartym między właściwym organem lub podmiotem a Komendantem Głównym Straży Granicznej. 2. Wspólna realizacja zadań określonych w art. 25a ust. 4 w przypadku przedstawicieli: 1) Ministra Obrony Narodowej, Szefa Agencji Bezpieczeństwa Wewnętrznego, Dyrektora Morskiej Służby Poszukiwania i Ratownictwa (Służby SAR) oraz dyrektorów urzędów morskich – jest wykonywana w siedzibie CBM; 2) Szefa Agencji Wywiadu, Szefa Służby Kontrwywiadu Wojskowego, Szefa Służby Wywiadu Wojskowego, Komendanta Głównego Policji, Komendanta Głównego Państwowej Straży Pożarnej, Szefa Krajowej Administracji Skarbowej, właściwych terytorialnie wojewodów i operatorów infrastruktury krytycznej – jest wykonywana w siedzibie CBM lub w siedzibie organu lub podmiotu, którego jest przedstawicielem. 3. Komendant Główny Straży Granicznej występuje do organu lub podmiotu, o którym mowa w ust. 1, z wnioskiem o wyznaczenie przedstawicieli oraz zawarcie porozumienia. 4. Wniosek, o którym mowa w ust. 3, zawiera w szczególności: 1) zakres zadań i obowiązków oraz kwalifikacje, uprawnienia lub umiejętności wymagane do ich wykonywania; 2) wymagania w zakresie posiadania poświadczenia bezpieczeństwa upoważniającego do dostępu do informacji niejawnych i okresu jego ważności; 3) proponowany czas pracy albo służby przedstawicieli organu lub podmiotu, o którym mowa w ust. 1, z uwzględnieniem możliwości jej wykonywania w systemie zmianowym;	

	4) miejsce wykonywania zadań określonych w art. 25a ust. 4 przez przedstawicieli organu lub podmiotu, o którym mowa w ust. 1; 5) liczbę przedstawicieli organu lub podmiotu, o którym mowa w ust. 1, niezbędną do wykonywania zadań określonych w art. 25a ust. 4, w celu zapewnienia ciągłości działania CBM. 5. Wniosek, o którym mowa w ust. 3, może zawierać imię i nazwisko przedstawiciela, organu lub podmiotu, o którym mowa w ust. 1. Organ lub podmiot, o którym mowa w ust. 1, może odmówić wyznaczenia osoby, której dotyczy wniosek, jeżeli jest to uzasadnione potrzebami tego organu lub podmiotu. 6. Organ lub podmiot, o którym mowa w ust. 1, w terminie 7 dni od dnia otrzymania wniosku, o którym mowa w ust. 3, zawiadamia Komendanta Głównego Straży Granicznej o wyznaczonych przedstawicielach. 7. Porozumienie, o którym mowa w ust. 1, określa w szczególności: 1) datę zawarcia porozumienia; 2) miejsce wspólnego wykonywania zadań CBM; 3) imiona i nazwiska przedstawicieli; 4) stopnie przedstawicieli, w przypadku gdy są oni funkcjonariuszami albo żołnierzami; 5) numery poświadczeń bezpieczeństwa wydanych przedstawicielom, daty ich wydania i wystawcę takich poświadczeń oraz okres ważności i oznaczenie klauzuli upoważniających do przetwarzania informacji niejawnych; 6) zakres zadań i obowiązków przedstawicieli oraz sposób organizacji wykonywania tych zadań i obowiązków; 7) ustalony czas pracy albo służby; 8) osobę odpowiedzialną za organizację i koordynację wykonywanych zadań w CBM oraz monitorowanie ich realizacji.	

	8. W przypadku planowanej zmiany przedstawiciela organ lub podmiot, o którym mowa w ust. 1, wskazuje kolejnego przedstawiciela w celu zapewnienia ciągłości działania CBM. W takim przypadku dokonuje się zmiany zawartego porozumienia poprzez wskazanie nowego przedstawiciela. 9. Organ lub podmiot, o którym mowa w ust. 1, wypłaca swoim przedstawicielom uposażenie albo wynagrodzenie i inne świadczenia oraz należności pieniężne. Art. 25c. 1. W szczególnie uzasadnionych przypadkach związanych z zagrożeniem wystąpienia poważnego niebezpieczeństwa, Szef CBM powołuje sztab koordynacyjny, w skład którego wchodzą przedstawiciele wyznaczeni przez organy lub podmioty, o których mowa w art. 25b ust. 1. 2. Do zadań sztabu koordynacyjnego należy dokonywanie aktualnej oceny stopnia zagrożenia infrastruktury morskiej, statków lub granicy państwowej na morzu oraz wydawania rekomendacji zmierzających do odpowiedniego zabezpieczenia tej infrastruktury, statków lub granicy. Art. 25d. Komendant Główny Straży Granicznej, w terminie do dnia 31 marca każdego roku kalendarzowego, przedstawia ministrowi właściwemu do spraw wewnętrznych sprawozdanie z działania CBM w poprzednim roku kalendarzowym.”. 4) w art. 27 w ust. 1 po pkt 5 dodaje się pkt 6 w brzmieniu: "6) terminalowi morskiego przeładunku ropy i paliw ciekłych w Gdańsku"; 5) po rozdziale 6 dodaje się rozdział 6a w brzmieniu: „Rozdział 6a Zapobieganie bezprawnemu wykonywaniu operacji z użyciem bezzałogowych obiektów pływających Art. 28a. 1. Bezzałogowy obiekt pływający może zostać zniszczony, unieruchomiony albo może nad nim zostać przejęta kontrola, w przypadku gdy: 1) przebieg operacji lub działanie bezzałogowego obiektu pływającego:	

	a) zagraża lub może zagrozić życiu lub zdrowiu ludzi lub zwierząt, b) stwarza lub może stworzyć zagrożenie dla chronionych obiektów, urządzeń lub obszarów, c) stwarza lub może stworzyć uzasadnione podejrzenie, że może zostać użyty jako środek ataku terrorystycznego, d) stwarza lub może stworzyć zagrożenie bezpieczeństwa jednostki pływającej lub życia lub zdrowia załogi lub pasażerów znajdujących się na jej pokładzie, e) utrudnia lub może utrudnić ruch w portach morskich lub powoduje lub może spowodować jego wstrzymanie lub ograniczenie; 2) bezzałogowy obiekt pływający wbrew zakazowi wykonuje operację na polskich obszarach morskich. 2. Do zniszczenia, unieruchomienia bezzałogowego obiektu pływającego albo przejęcia nad nim kontroli, w związku z realizacją zadań ustawowych, są uprawnieni na zasadach określonych w ustawie z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej (Dz. U. z 2024 r. poz. 383 i 1248) funkcjonariusze Policji, Straży Granicznej, Służby Ochrony Państwa oraz, zgodnie z zakresem właściwości miejscowej, pracownicy ochrony specjalistycznych uzbrojonych formacji ochronnych, o których 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 oraz …). 3. Do zniszczenia, unieruchomienia bezzałogowego obiektu pływającego albo przejęcia nad nim kontroli, w związku z realizacją zadań ustawowych, na terenie chronionych obiektów Sił Zbrojnych Rzeczypospolitej Polskiej oraz jednostek organizacyjnych podległych, podporządkowanych lub nadzorowanych przez Ministra Obrony Narodowej są uprawnieni na zasadach określonych w ustawie z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej żołnierze Żandarmerii Wojskowej oraz Sił Zbrojnych Rzeczypospolitej Polskiej. 4. Za szkody powstałe w wyniku zniszczenia, unieruchomienia albo przejęcia kontroli nad bezzałogowym obiektem pływającym w przypadkach, o których mowa w ust. 1, odpowiada właściciel lub operator lub armator bezzałogowego	

	obiektu pływającego zniszczonego, unieruchomionego albo nad którym przejęto kontrolę.”.	
Art. 13 projektu ustawy (zmiany w ustawie o szczególnych uprawnieniach ministra właściwego do spraw aktywów państwowych oraz ich wykonywaniu w niektórych spółkach kapitałowych lub grupach kapitałowych prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych)	**Art. 13.** W ustawie z dnia 18 marca 2010 r. o szczególnych uprawnieniach ministra właściwego do spraw aktywów państwowych oraz ich wykonywaniu w niektórych spółkach kapitałowych lub grupach kapitałowych prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych (Dz. U. z 2020 r. poz. 2173 oraz z 2024 r. poz. 834) wprowadza się następujące zmiany: 1) w art. 1 ust. 1 otrzymuje brzmienie: „1. Ustawa określa szczególne uprawnienia przysługujące ministrowi właściwemu do spraw aktywów państwowych w spółkach kapitałowych lub grupach kapitałowych, w rozumieniu art. 3 ust. 1 pkt 44 ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2023 r. poz. 120, 295 i 1598 oraz z 2024 r. poz. 619), prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych, których mienie zostało ujawnione w wykazie, o którym mowa w art. 6r ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2023 r. poz. 122 oraz z 2024 r. poz. 834, 1222 i 1473), zwanych dalej „spółkami”.”; 2) w art. 2: a) ust. 3 otrzymuje brzmienie: „3. Sprzeciw jest wyrażany w formie decyzji administracyjnej, w terminie 45 dni od dnia otrzymania przez ministra właściwego do spraw aktywów państwowych od pełnomocnika do spraw ochrony infrastruktury krytycznej, o którym mowa w art. 5, informacji o podjęciu przez organy spółki uchwały lub dokonaniu przez zarząd spółki czynności prawnej, o której mowa w ust. 1 i 2, jednak nie później niż w terminie 60 dni od dnia ich dokonania.", b) po ust. 3 dodaje się ust. 3a w brzmieniu:	Zwiększenie nadzoru nad zapewnieniem infrastruktury krytycznej.

	"3a. Sprzeciw jest wyrażany po zasięgnięciu opinii odpowiednio ministra właściwego do spraw energii lub ministra właściwego do spraw gospodarki surowcami energetycznymi. Opinię wydaje się w terminie 10 dni od dnia otrzymania wniosku o jej wydanie. Niewyrażenie opinii w tym terminie uważa się za brak uwag.”, c) ust. 5 otrzymuje brzmienie: „5. W przypadku złożenia wniosku o ponowne rozpatrzenie sprawy termin na jej załatwienie wynosi 30 dni od dnia otrzymania wniosku.”, d) w ust. 6 pkt 1 otrzymuje brzmienie: „1) minister właściwy do spraw aktywów państwowych przekazuje skargę do właściwego sądu administracyjnego wraz z aktami sprawy i odpowiedzią na skargę w terminie 30 dni od dnia jej wniesienia przez stronę;”, e) ust. 8 otrzymuje brzmienie: „8. W sprawach nieuregulowanych w ust. 1-7 do postępowania w sprawie sprzeciwu stosuje się przepisy ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (Dz. U. z 2025 r. poz. 1691).", 3) w art. 4 ust. 2 otrzymuje brzmienie: „2. Minister właściwy do spraw aktywów państwowych, po otrzymaniu od dyrektora Rządowego Centrum Bezpieczeństwa informacji o ujęciu spółki w wykazie lub wyciągu, o którym mowa w ust. 1, powiadamia spółkę o ujęciu w wykazie składników jej mienia, o których mowa w art. 1 ust. 1 i 2.”; 4) w art. 5 wprowadza się następujące zmiany: a) ust. 1 „1. Zarząd spółki, w porozumieniu z ministrem właściwym do spraw aktywów państwowych oraz dyrektorem Rządowego Centrum Bezpieczeństwa, powołuje i odwołuje pełnomocnika do spraw ochrony infrastruktury krytycznej oraz jego zastępcę, przy czym powołanie pełnomocnika następuje w terminie 30 dni,	

	a powołanie jego zastępcy w terminie 60 dni od dnia otrzymania powiadomienia, o którym mowa w art. 4 ust. 2.", b) po ust. 1 dodaje się ust. 1a w brzmienie: „1a. Minister właściwy do spraw aktywów państwowych niezwłocznie informuje odpowiednio ministra właściwego do spraw energii lub ministra właściwego do spraw gospodarki surowcami energetycznymi o powołaniu lub odwołaniu pełnomocnika do spraw infrastruktury krytycznej oraz jego zastępcy.”, c) ust. 4 otrzymuje brzmienie: „4. Pełnomocnik do spraw ochrony infrastruktury krytycznej może jednocześnie pełnić funkcję koordynatora ochrony infrastruktury krytycznej lub pełnomocnika bezpieczeństwa usługi kluczowej, o których mowa odpowiednio w art. 6zi ust. 1 i art. 6zzd ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym.", d) po ust. 5 dodaje się ust. 6 w brzmieniu: „6. Do zastępcy pełnomocnika postanowienia art. 5 ust. 2-5 stosuje się odpowiednio.”, 5) art. 6 wprowadza się następujące zmiany: a) ust. 1 otrzymuje brzmienie: „1. Zarząd spółki zobowiązany jest do przekazywania pełnomocnikowi do spraw ochrony infrastruktury krytycznej lub jego zastępcy, dokumentów lub informacji o podjęciu uchwały lub o dokonaniu przez organy spółki czynności prawnych, o których mowa w art. 2 ust. 1 i 2, w terminie 3 dni od dnia ich podjęcia lub dokonania.", b) ust. 2 otrzymuje brzmienie: "2. Zarząd spółki powiadamia pełnomocnika do spraw ochrony infrastruktury krytycznej lub jego zastępcę o każdym planowanym posiedzeniu dotyczącym spraw, o których mowa w art. 2 ust. 1 i 2.",	

	c) w ust. 3 wstęp do wyliczenia otrzymuje brzmienie: „3. Pełnomocnik do spraw ochrony infrastruktury krytycznej albo jego zastępca, sporządza dla zarządu spółki oraz rady nadzorczej raport doraźny, okresowy, raport półroczny i roczny o stanie ochrony infrastruktury krytycznej. Raport doraźny sporządzany jest w terminie 1 dnia od zidentyfikowania zagrożenia lub wystąpienia sytuacji stwarzającej zagrożenie dla funkcjonowania, ciągłości działania oraz integralności infrastruktury krytycznej. Raport okresowy jest sporządzany, co kwartał lub na żądanie zarządu spółki lub rady nadzorczej. Raport powinien zawierać informacje dotyczące ochrony infrastruktury krytycznej w zakresie:”, d) po ust. 3 dodaje się ust. 3a w brzmieniu: "3a. Raport roczny i półroczny zawiera informację, o których mowa w ust. 3, poszerzone o: 1) rejestr stwierdzonych incydentów wraz z informacją o przeprowadzonych działaniach korygujących; 2) informację o przeprowadzonych kontrolach i audytach dotyczących ochrony infrastruktury krytycznej; 3) informację o posiadanych certyfikatach systemów i rozwiązań dotyczących ochrony infrastruktury krytycznej;", e) ust. 4 otrzymuje brzmienie: „4. Raport doraźny oraz raport półroczny i roczny są przekazywane ministrowi właściwemu do spraw aktywów państwowych, dyrektorowi Rządowego Centrum Bezpieczeństwa oraz odpowiednio ministrowi właściwemu do spraw energii lub ministrowi właściwemu do spraw gospodarki surowcami energetycznymi. Jeżeli raporty są niepełne, zawierają nieścisłości lub nie przedstawiają dokładnie stanu faktycznego w zakresie spraw w nim zawartych, pełnomocnik do spraw ochrony infrastruktury krytycznej lub jego zastępca jest zobowiązany, na wezwanie ministra właściwego do spraw aktywów państwowych lub dyrektora Rządowego Centrum Bezpieczeństwa, lub odpowiednio ministra właściwego do spraw energii	

	lub ministra właściwego do spraw gospodarki surowcami energetycznymi, do uzupełnienia raportów we wskazanym zakresie i terminie.”, f) ust. 5 otrzymuje brzmienie: „5. Pełnomocnik do spraw ochrony infrastruktury krytycznej lub w razie jego nieobecności jego zastępca, sporządza sprawozdania półroczne i roczne z wykonanych obowiązków, które składa ministrowi właściwemu do spraw aktywów państwowych, dyrektorowi Rządowego Centrum Bezpieczeństwa oraz odpowiednio ministrowi właściwemu do spraw energii lub ministrowi właściwemu do spraw gospodarki surowcami energetycznymi.”, g) ust. 6 otrzymuje brzmienie: „6. Pełnomocnik do spraw ochrony infrastruktury krytycznej lub w razie jego nieobecności jego zastępca, w terminie 4 dni od dnia otrzymania dokumentów lub informacji o podjęciu uchwały lub o dokonaniu przez organy spółki czynności prawnych, o których mowa w art. 2 ust. 1 i 2, przekazuje ministrowi właściwemu do spraw aktywów państwowych, dyrektorowi Rządowego Centrum Bezpieczeństwa oraz odpowiednio ministrowi właściwemu do spraw energii lub ministrowi właściwemu do spraw gospodarki surowcami energetycznymi pisemną informację w tej sprawie oraz stanowisko odnośnie do wniesienia sprzeciwu, wraz z jego uzasadnieniem. Stanowisko powinno zawierać informacje dotyczące faktów i okoliczności podjętych przez spółkę czynności prawnych, o których mowa w art. 2 ust. 1 i 2 wraz ze wskazaniem motywów podejmowanych działań i tła historycznego”, h) ust. 8 otrzymuje brzmienie: "8. Prezes Rady Ministrów określi, w drodze rozporządzenia: 1) szczegółowy tryb powoływania i odwoływania pełnomocnika do spraw ochrony infrastruktury krytycznej oraz jego zastępcy, 2) sposób wykonywania obowiązku monitorowania działalności spółki w zakresie, o którym mowa w art. 2) ust. 1 i 2	

	- uwzględniając konieczność efektywnego wykonywania szczególnych uprawnień ministra właściwego do spraw aktywów państwowych w spółkach kapitałowych lub grupach kapitałowych."; 6) po art. 7 dodaje się art. 7a w brzmieniu: „Art. 7a. 1. Zarząd spółki może podlegać karze pieniężnej za nierealizowanie zadań: 1) o których mowa w art. 5 ust. 1 – w wysokości do 50 000 zł; 2) o których mowa w art. 6 ust. 1 – w wysokości do 100 000 zł; 3) o których mowa w art. 6 ust. 2 – w wysokości do 50 000 zł. 2. Jeżeli zarząd spółki uporczywie narusza przepisy ustawy, może podlegać karze w wysokości do 1 000 000 zł. 3. Kary pieniężne nakłada w drodze decyzji minister właściwy do spraw aktywów państwowych. 4. W przypadku nierealizowania przez pełnomocnika do spraw ochrony infrastruktury krytycznej, lub jego zastępcę, obowiązków wskazanych w art. 5 ust. 2, minister właściwy do spraw aktywów państwowych może uznać, że pełnomocnik przestał dawać rękojmię prawidłowego wykonywania obowiązków, o czym powiadamia zarząd spółki. 5. Zarząd spółki w terminie 30 dni od powiadomienia, o którym mowa w art. 7a ust. 4 zobowiązany jest do odwołania pełnomocnika w trybie określonym w art. 5 ust. 1 ustawy.";	

Art. 14 projektu ustawy (zmiany w ustawie o odpadach)	**Art. 14.** W ustawie z dnia 14 grudnia 2012 r. o odpadach (Dz. U. z 2023 r. poz. 1587, 1597, 1688, 1852 i 2029) w art. 25 w ust. 6i pkt 2 otrzymuje brzmienie: „2) stanowiącego element infrastruktury krytycznej ujętej w wykazie, o którym mowa w art. 6r ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2023 r. poz. 122 oraz z 2024 r. poz. 834, 1222 i 1473);”.	Zmiana wynikowa – dostosowanie treści przepisu do zmian w ustawie o zarządzaniu kryzysowym.
Art. 15 projektu ustawy (zmiany w ustawie o środkach przymusu bezpośredniego i broni palnej)	**Art. 15.** W ustawie z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej (Dz. U. z 2024 r. poz. 383) wprowadza się następujące zmiany: 1) w art. 4: a) w pkt 8 lit. b otrzymuje brzmienie: „b) obiekty, urządzenia, instalacje, sieci, systemy oraz usługi lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje, sieci, systemy oraz usługi ujęte w wykazie infrastruktury krytycznej, o którym mowa w art. 6r ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2023 r. poz. 122 oraz z 2024 r. poz. 834, 1222 i 1473),", b) pkt 9 otrzymuje brzmienie: „9) wykorzystaniu środka przymusu bezpośredniego – należy przez to rozumieć zastosowanie środka przymusu bezpośredniego: a) wobec zwierzęcia, b) w celu zatrzymania, zablokowania lub unieruchomienia pojazdu lub pokonania przeszkody, c) w przypadku bezzałogowego statku powietrznego – w celu jego zniszczenia, unieruchomienia albo przejęcia kontroli nad jego lotem, d) w przypadku bezzałogowego obiektu pływającego – w celu jego zniszczenia, unieruchomienia albo przejęcia nad nim kontroli,	Rozwiązania zapewniające ochronę fizyczną infrastruktury krytycznej.

	e) w przypadku bezzałogowego obiektu lądowego – w celu jego zniszczenia, unieruchomienia albo przejęcia nad nim kontroli;"; 2) w art. 11 w pkt 15 kropkę zastępuje się średnikiem i dodaje się pkt 16 i 17 w brzmieniu: „16) zniszczenia, unieruchomienia bezzałogowego obiektu pływającego albo przejęcia nad nim kontroli, w przypadkach, o których mowa w art. 28a ust. 1 ustawy z dnia 4 września 2008 r. o ochronie żeglugi i portów morskich (Dz. U. z 2024 r. poz. 597 oraz…); 17) zniszczenia, unieruchomienia bezzałogowego obiektu lądowego albo przejęcia nad nim kontroli, w przypadku gdy: a) zagraża lub może zagrozić życiu lub zdrowiu ludzi lub zwierząt, b) stwarza lub może stworzyć zagrożenie dla chronionych obiektów, urządzeń lub obszarów, c) zakłóca lub może zakłócić przebieg zgromadzenia lub imprezy masowej albo zagraża bezpieczeństwu ich uczestników, d) stwarza lub może stworzyć uzasadnione podejrzenie, że może zostać użyty jako środek ataku o charakterze terrorystycznym."; 3) w art. 12 w ust. 1 w pkt 21 kropkę zastępuje się średnikiem i dodaje się pkt 22 i 23 w brzmieniu: „22) środki i urządzenia przeznaczone do zniszczenia, unieruchomienia bezzałogowego obiektu pływającego albo przejęcia nad nim kontroli; 23) środki i urządzenia przeznaczone do zniszczenia, unieruchomienia bezzałogowego obiektu lądowego albo przejęcia nad nim kontroli."; 4) art. 23 otrzymuje brzmienie:	

	„Art. 23.1. Pocisków niepenetracyjnych miotanych z broni palnej, broni pneumatycznej lub urządzeń do tego przeznaczonych można użyć lub wykorzystać w przypadkach, o których mowa w art. 11 pkt 2–5, 7–11, 13 i 15–17. 2. W przypadku zbiorowego zakłócenia porządku publicznego użycie pocisków niepenetracyjnych poprzedza się strzałem ostrzegawczym lub salwą ostrzegawczą w bezpiecznym kierunku, z wyjątkiem sytuacji, gdy miałoby to nastąpić w pomieszczeniach, obiektach aresztu śledczego, zakładu karnego, strzeżonego ośrodka lub aresztu dla cudzoziemców. 3. Pocisków niepenetracyjnych używa się w celu obezwładnienia osób lub wykorzystuje się w celu obezwładnienia zwierzęcia przez zadanie bólu fizycznego, przy czym nie celuje się w głowę lub szyję, oraz w celu zniszczenia albo unieruchomienia bezzałogowego statku powietrznego, bezzałogowego obiektu pływającego lub bezzałogowego obiektu lądowego. 4. Można użyć lub wykorzystać także pociski niepenetracyjne zawierające chemiczne środki obezwładniające lub barwiące.”; 5) po art. 33a dodaje się art. 33b i 33c w brzmieniu: „Art. 33b. 1. Środki i urządzenia przeznaczone do zniszczenia, unieruchomienia bezzałogowego obiektu pływającego albo przejęcia nad nim kontroli można wykorzystać w przypadku, o którym mowa w art. 11 pkt 16. 2. Zniszczenie, unieruchomienie bezzałogowego obiektu pływającego albo przejęcie nad nim kontroli może nastąpić przez wykorzystanie: 1) bezzałogowych statków powietrznych; 2) pocisków niepenetracyjnych lub innych przedmiotów miotanych za pomocą przeznaczonych do tego urządzeń oraz za pomocą broni palnej i broni pneumatycznej; 3) urządzeń emitujących skumulowaną wiązkę energii lub fal elektromagnetycznych;	

	4) urządzeń zakłócających działanie systemów pozycjonowania obiektu pływającego; 5) urządzeń zakłócających komunikację pomiędzy operatorem a obiektem pływającym; 6) urządzeń technicznych przymocowanych do dna morskiego i służących do ochrony fizycznej; 7) bezzałogowych obiektów pływających. Art. 33c. 1. Środki i urządzenia przeznaczone do zniszczenia, unieruchomienia bezzałogowego obiektu lądowego albo przejęcia nad nim kontroli można wykorzystać w przypadku, o którym mowa w art. 11 pkt 17. 2. Zniszczenie, unieruchomienie bezzałogowego obiektu lądowego albo przejęcie nad nim kontroli może nastąpić przez wykorzystanie: 1) bezzałogowych statków powietrznych; 2) pocisków niepenetracyjnych lub innych przedmiotów miotanych za pomocą przeznaczonych do tego urządzeń oraz za pomocą broni palnej i broni pneumatycznej; 3) urządzeń emitujących skumulowaną wiązkę energii lub fal elektromagnetycznych; 4) urządzeń zakłócających działanie systemów pozycjonowania obiektu lądowego; 5) urządzeń zakłócających komunikację pomiędzy operatorem a obiektem lądowym; 6) bezzałogowych obiektów lądowych.”; 6) w art. 47 w pkt 7 kropkę zastępuje się średnikiem i dodaje się pkt 8 w brzmieniu: „8) zniszczenia lub unieruchomienia bezzałogowego obiektu lądowego, w przypadkach, o których mowa w art. 11 pkt 17.”.	

Art. 16 projektu ustawy (zmiany w ustawie o działaniach antyterrorystycznych)	**Art. 16.** W ustawie z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (Dz. U. z 2024 r. poz. 92 i 1248) wprowadza się następujące zmiany: 1) w art. 2 uchyla się pkt 3; 2) art. 4 otrzymuje brzmienie: „Art. 4. 1. Organy administracji publicznej lub operatorzy infrastruktury krytycznej współpracują z organami, służbami i instytucjami właściwymi w sprawach bezpieczeństwa i zarządzania kryzysowego przy realizacji działań antyterrorystycznych. 2. Organy i podmioty, o których mowa w ust. 1, przekazują niezwłocznie Szefowi ABW będące w ich posiadaniu informacje dotyczące zagrożeń o charakterze terrorystycznym, w tym zagrożeń dla funkcjonowania systemów i sieci energetycznych, wodno-kanalizacyjnych, ciepłowniczych oraz teleinformatycznych istotnych z punktu widzenia bezpieczeństwa państwa. 3. W przypadku powzięcia informacji o możliwości wystąpienia zdarzenia o charakterze terrorystycznym zagrażającego infrastrukturze krytycznej, życiu lub zdrowiu ludzi, mieniu w znacznych rozmiarach, dziedzictwu narodowemu lub środowisku, Szef ABW może wydawać polecenia organom i podmiotom, o których mowa w ust. 1, z wyłączeniem podmiotów, o których mowa w art. 7, zagrożonym tymi zdarzeniami, mające na celu przeciwdziałanie zagrożeniom, ich usunięcie albo minimalizację, oraz przekazywać im informacje niezbędne do tego celu. Organy i podmioty, o których mowa w zdaniu pierwszym, informują Szefa ABW o podjętych działaniach w tym zakresie. 4. Szef ABW o podjętych działaniach, o których mowa w ust. 3, informuje niezwłocznie Ministra Koordynatora Służb Specjalnych, jeżeli został powołany.”; 3) w art. 12: „a) w ust. 1 pkt 1 i 2 otrzymują brzmienie: „1) Policja – w obiektach infrastruktury krytycznej wskazanych przez Komendanta Głównego Policji w uzgodnieniu z Szefem ABW;	Zapewnienie efektywności w zakresie ochrony infrastruktury krytycznej.

	2) Żandarmeria Wojskowa – w obiektach stanowiących siedzibę urzędu obsługującego Ministra Obrony Narodowej oraz w obiektach należących do komórek i jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych albo administrowanych przez te komórki i jednostki organizacyjne wskazanych przez Ministra Obrony Narodowej w uzgodnieniu z Szefem SKW.”, b) po ust. 2 dodaje się ust. 3 w brzmieniu: „3. Komendant Główny Policji i Szef ABW, określą w drodze porozumienia, tryb wskazywania obiektów infrastruktury krytycznej, o których mowa w ust.1 pkt 1. ”; 4) w art. 15 w ust. 9 wyraz „zadania” zastępuje się wyrazem „przedsięwzięcia”; 5) w art. 16 w ust. 1 pkt 4 otrzymuje brzmienie: „4) dla określonych obiektów jednostek organizacyjnych administracji publicznej, prokuratury, sądów lub obiektów infrastruktury krytycznej;”; 6) w art. 17: a) ust. 1 otrzymuje brzmienie: „1. W przypadku wprowadzenia pierwszego lub drugiego stopnia alarmowego lub pierwszego lub drugiego stopnia alarmowego CRP w trybie art. 16 ust. 1, Szef ABW może powołać sztab koordynacyjny, w skład którego wchodzą przedstawiciele wyznaczeni przez podmioty, o których mowa w art. 5 ust. 1.”, b) po ust. 1 dodaje się ust. 1a w brzmieniu: „1a. W przypadku wprowadzenia trzeciego lub czwartego stopnia alarmowego lub trzeciego lub czwartego stopnia alarmowego CRP, w trybie art. 16 ust. 1, Szef ABW powołuje sztab koordynacyjny, o którym mowa w ust. 1.”, c) ust. 3 otrzymuje brzmienie: „3. Do zadań sztabu koordynacyjnego należy:	

	1) rekomendowanie zmiany lub odwołania stopnia alarmowego lub stopnia alarmowego CRP; 2) dokonywanie oceny stopnia zagrożenia infrastruktury krytycznej zlokalizowanej na obszarze objętym obowiązywaniem stopnia alarmowego lub stopnia alarmowego CRP oraz wydawanie rekomendacji zmierzających do jej odpowiedniego zabezpieczenia; 3) rekomendowanie form i zakresu współdziałania podmiotów wchodzących w skład sztabu koordynacyjnego i biorących udział w jego pracach.”.	
Art. 17 projektu ustawy (zmiany w ustawie Prawo wodne)	Art. 17. W ustawie z dnia 20 lipca 2017 r. - Prawo wodne (Dz. U. z 2025 r. poz. 960 i 1535) w art. 240 w ust. 3 pkt 24 otrzymuje brzmienie: "24) współdziałają z wojewodami w zakresie opracowywania wojewódzkiego planu zarządzania ryzykiem oraz wojewódzkiego planu reagowania kryzysowego;".	Zmiany wynikowe do ustawy o zarządzaniu kryzysowym.
Art. 18 projektu ustawy (zmiany w ustawie o Służbie Ochrony Państwa)	**Art. 18.** W ustawie z dnia 8 grudnia 2017 r. o Służbie Ochrony Państwa (Dz. U. z 2025 r. poz. 34, z 2024 r. poz. 1871 oraz z 2025 r. poz. 179, 718 i 1366) wprowadza się następujące zmiany: 1) w art. 37 ust. 1 i 2 otrzymują brzmienie: „1. W przypadkach, o których mowa w art. 11 pkt 1–6 i 9–16 ustawy z 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej (Dz. U. z 2025 r. poz. 555, 820 oraz …), funkcjonariusz może użyć środków przymusu bezpośredniego, o których mowa w art. 12 ust. 1 pkt 1, pkt 2 lit. a, pkt 5, 7, 9, 11, pkt 12 lit. a, c i d, pkt 13 i 17–23 tej ustawy, lub wykorzystać te środki. 2. W przypadkach, o których mowa w art. 45 pkt 1 lit. a-c i e, pkt 2 i pkt 3 lit. a z wyłączeniem pościgu za osobą, o której mowa w art. 45 pkt 1 lit. d, oraz w art. 47	Zmiany wynikowe do ustawy o środkach przymusu bezpośredniego. Zapewnienie ochrony antydronowej. Doprecyzowanie podmiotu wypłacającego świadczeń dla funkcjonariuszy SOP Granicznej oddelegowanych do wykonywania zadań służbowych w urzędzie obsługującym ministra właściwego do spraw wewnętrznych albo w jednostce podległej lub nadzorowanej przez ministra właściwego do spraw wewnętrznych.

	pkt 1, pkt 2 lit. a i pkt 3-8 ustawy z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej, funkcjonariusz może użyć broni palnej lub ją wykorzystać.”; 2) w art. 39 ust. 1 otrzymuje brzmienie: „1. Komendant SOP: 1) w celu realizacji zadań, o których mowa w art. 3 pkt 1 lub 2) w przypadkach o których mowa: a) w art. 156ze ust. 1 ustawy z dnia 3 lipca 2002 r. Prawo lotnicze (Dz. U. z 2025 r. poz. 1431 i 1668), lub b) w art. 28a ust. 1 ustawy z dnia 4 września 2008 r. o ochronie żeglugi i portów morskich (Dz. U. z 2024 r. poz. 597 oraz …), lub c) w art. 11 pkt 17 ustawy z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej - może podjąć decyzję o dopuszczalności zastosowania urządzeń uniemożliwiających telekomunikację na określonym obszarze przez czas niezbędny do wykonywania czynności przez SOP, z uwzględnieniem konieczności minimalizacji skutków braku możliwości korzystania z usług telekomunikacyjnych. 3) w art. 98 dodaje się ust. 3 w brzmieniu: 3. W przypadku funkcjonariusza oddelegowanego do wykonywania zadań służbowych w urzędzie obsługującym ministra właściwego do spraw wewnętrznych albo w jednostce podległej lub nadzorowanej przez ministra właściwego do spraw wewnętrznych, należności, o których mowa w ust. 1, wypłaca komórka organizacyjna SOP właściwa w sprawach finansowych w uzgodnieniu z kierownikiem urzędu albo jednostki, do której funkcjonariusz został oddelegowany.”.	

Art. 19 projektu ustawy **(zmiany w ustawie o krajowym systemie cyberbezpieczeństwa)**	**Art. 19.** W ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2023 r. poz. 913, 1703 oraz z 2024 r. poz. 834) wprowadza się następujące zmiany: 1) w art. 10 w ust. 4 wyrazy „właścicielem, posiadaczem samoistnym albo posiadaczem zależnym obiektów, instalacji, urządzeń lub usług wchodzących w skład infrastruktury krytycznej, wymienionych w 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 oraz z 2024 r. poz. 834)” zastępuje się wyrazami „operatorem infrastruktury krytycznej, o którym mowa w art. 3 pkt 3a ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2023 r. poz. 122, z późn. zm.[12)])”; 2) w art. 15 w ust. 7 w pkt 2 wyrazy „właścicielem, posiadaczem samoistnym albo posiadaczem zależnym obiektów, instalacji, urządzeń lub usług wchodzących w skład infrastruktury krytycznej, wymienionych w wykazie, o którym mowa w art. 5b ust. 7 pkt 1” zastępuje się wyrazami „operatorem infrastruktury krytycznej, o którym mowa w art. 3 pkt 3a”; 3) w art. 26: a) w ust. 2 wyrazy „właścicieli, posiadaczy samoistnych albo posiadaczy zależnych obiektów, instalacji, urządzeń lub usług wchodzących w skład infrastruktury krytycznej, wymienionych w wykazie, o którym mowa w art. 5b ust. 7 pkt 1” zastępuje się wyrazami „operatorów infrastruktury krytycznej, o których mowa w art. 3 pkt 3a”, b) w ust. 5 pkt 1 otrzymuje brzmienie: „1) podmioty podległe Ministrowi Obrony Narodowej lub przez niego nadzorowane, w tym podmioty, których systemy teleinformatyczne lub sieci teleinformatyczne objęte są wykazem, o których mowa w art. 6r ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym;”, c) w ust. 7 pkt 5 i 6 otrzymują brzmienie:	Dostosowanie do zmian w ustawie o zarządzaniu kryzysowym.

	„5) inne niż wymienione w pkt 1–4 oraz ust. 5 podmioty, których systemy teleinformatyczne lub sieci teleinformatyczne objęte są wykazem, o którym mowa w art. 6i ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym; 6) podmioty, o których mowa w ust. 6, jeżeli incydent dotyczy systemów teleinformatycznych lub sieci teleinformatycznych objętych wykazami, o których mowa w art. 6i ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym.”, d) w art. 46 po ust. 1 dodaje się ust. 1a w brzmieniu: "1a. System, o którym mowa w ust. 1, zapewnia wymianę informacji między organami do spraw podmiotów krytycznych, o których mowa w art. 6v ustawy z dnia 27 kwietnia 2007 r. o zarządzaniu kryzysowym, dyrektorem Rządowego Centrum Bezpieczeństwa a podmiotami krytycznymi, o których mowa w art. 3 pkt 1a tej ustawy.".	
Art. 20 projektu ustawy (zmiany w ustawie o rezerwach strategicznych)	**Art. 20.** W ustawie z dnia 17 grudnia 2020 r. o rezerwach strategicznych (Dz. U. z 2024 r. poz. 1598) wprowadza się następujące zmiany: 1) w art. 2: a) pkt 1 otrzymuje brzmienie: "1) infrastruktura krytyczna - infrastrukturę, o której mowa w art. 3 pkt 2 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2023 r. poz. 122 oraz z 2024 r. poz. 834, 1222 i 1473), b) po pkt dodaje się pkt 1a i 1b w brzmieniu: "1a) podmiot krytyczny - podmiot, o którym mowa w art. 3 pkt 1a ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym; 1b) usługa kluczowa - usługa, o której mowa w art. 3 pkt 1d ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym;", c) po pkt 4 dodaje się pkt 4a w brzmieniu:	Dostosowanie do zmian w ustawie o zarządzaniu kryzysowym. Usprawnienie mechanizmów zarządzania rezerwami strategicznymi w sytuacjach kryzysowych.

	„4a) wirtualne środowisko informatyczne – wydzielona przestrzeń wielosystemowa oparta o ograniczone zasoby fizyczne;”; 2) art. 4 otrzymuje brzmienie: „Art. 4. Rezerwy strategiczne mogą stanowić surowce, materiały, urządzenia, maszyny, konstrukcje, elementy infrastruktury krytycznej, wirtualne środowisko informatyczne, fizyczne i wirtualne zasoby teleinformatyczne, produkty naftowe, produkty rolne i rolno–spożywcze, środki spożywcze i ich składniki, wyroby medyczne, produkty lecznicze, produkty lecznicze weterynaryjne oraz substancje czynne w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne (Dz. U. z 2025 r. poz. 750, 905, 924, 1416 i 1537), materiały wybuchowe, broń, amunicja oraz ich istotne części, ładunki miotające oraz wyroby i technologie o przeznaczeniu wojskowym lub policyjnym w rozumieniu ustawy z dnia 13 czerwca 2019 r. o wykonywaniu działalności gospodarczej w zakresie wytwarzania i obrotu materiałami wybuchowymi, bronią, amunicją oraz wyrobami i technologią o przeznaczeniu wojskowym lub policyjnym (Dz. U. z 2023 r. poz. 1743), produkty biobójcze, a także inne produkty – niezbędne do realizacji celów, o których mowa w art. 3."; 3) w art. 5 dotychczasową treść oznacza się jako ust. 2 i dodaje się ust. 1 w brzmieniu: „Art. 5. 1. Agencja w imieniu własnym dokonuje zakupu asortymentu, o którym mowa w art. 4, z przeznaczeniem do rezerw strategicznych oraz zawiera umowy, o których mowa w art. 17 i art. 18 w celu utworzenia rezerw strategicznych.”; 4) art. 7 otrzymuje brzmienie: „Art. 7. Do decyzji wydawanych przez ministra właściwego do spraw wewnętrznych w zakresie rezerw strategicznych oraz decyzji, o której mowa w art. 32 ust. 1, a także do decyzji wydawanych przez organy i podmioty, o których mowa w art. 8 ust. 2, w przypadku, o którym mowa w art. 29, nie stosuje się przepisów ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (Dz. U. z 2025 r. poz. 1691).”; 5) w art. 8:	

	a) w ust. 2 pkt 5 otrzymuje brzmienie: „5) minister właściwy do spraw gospodarki surowcami energetycznymi;”, b) w ust. 4 pkt 1-3 otrzymują brzmienie: "1) ocenę ryzyka zidentyfikowanych zagrożeń, uwzględniającą sposoby i środki reagowania na te zagrożenia, zawartą w opracowanych planach zarządzania kryzysowego, o których mowa w art. 2 pkt 16 ustawy o zarządzaniu kryzysowym; 2) wnioski wynikające z wykonania postanowień Strategii Oporności Podmiotów Krytycznych, o której mowa w art. 6f ustawy o zarządzaniu kryzysowym, w zakresie sprawowania nadzoru nad infrastrukturą krytyczną oraz podmiotami krytycznymi zapewniającymi świadczenie usług kluczowych; 3) wykazy potrzeb wynikających z oceny ryzyka, dotyczących utworzenia rezerw strategicznych w danym asortymencie i ilości, w podziale na poszczególne lata wraz z uzasadnieniem;”, 6) w art. 9 w ust. 1 pkt 1 i 2 otrzymują brzmienie: „1) wnioski dotyczące tworzenia, utrzymywania i likwidacji rezerw wynikające z oceny ryzyka zidentyfikowanych zagrożeń zawartej w Krajowej Ocenie Ryzyka, o której mowa w art. 6e ustawy o zarządzaniu kryzysowym, oraz wnioski, o których mowa w art. 8 ust. 4 pkt 2; 2) dane dotyczące asortymentów rezerw strategicznych i ich ilości, jakie należy utworzyć w poszczególnych latach wraz z uzasadnieniem;”; 7) w art. 10: a) ust. 2 otrzymuje brzmienie: „2. Minister właściwy do spraw wewnętrznych, po przyjęciu Programu przez Radę Ministrów, niezwłocznie przekazuje: 1) Program – Agencji i organom, o których mowa w art. 8 ust. 2 pkt 1–3;	

	2) wyciąg z Programu, zawierający informacje o rodzaju i ilości rezerw strategicznych ujętych w Programie, z podziałem na poszczególne lata – organom i podmiotom, o których mowa w art. 8 ust. 2 pkt 4–22.”; b) dodaje się ust. 3 w brzmieniu: „3. Przepis ust. 2 stosuje się odpowiednio w przypadku aktualizacji Programu.”; 8) w art. 11 w ust. 2: a) w pkt 1 lit. a i b otrzymują brzmienie: „a) zakupu asortymentu w celu utworzenia rezerw strategicznych oraz odtworzenia udostępnionych rezerw strategicznych, b) utrzymywania i przechowywania rezerw strategicznych, w tym ich zamiany, wymiany i konserwacji,”, b) pkt 2 otrzymuje brzmienie: „2) dotacji podmiotowej przeznaczonej na dofinansowanie kosztów w terminie ich zapłaty dotyczących działalności bieżącej Agencji realizującej zadania państwa w zakresie określonym w ustawie oraz inne zadania, z wyłączeniem zadań realizowanych przez Agencję w zakresie zapasów interwencyjnych określonych w ustawie o zapasach ropy naftowej, produktów naftowych i gazu ziemnego.”; 9) w art. 12 ust. 1 otrzymuje brzmienie: „1. W budżecie państwa tworzy się rezerwę celową z przeznaczeniem na finansowanie działań ministra właściwego do spraw wewnętrznych w sytuacjach zagrożeń, o których mowa w art. 3, na skutek zdarzeń, których nie można było przewidzieć ani im przeciwdziałać, w szczególności na finansowanie kosztów: 1) udostępnienia rezerw strategicznych, w tym wydawania, przetransportowania i dystrybucji udostępnionych rezerw strategicznych do ostatecznych odbiorców;	

	2) innych usług niezbędnych do udostępnienia rezerw strategicznych ostatecznym odbiorcom; 3) przetworzenia i przetrzymania udostępnionych rezerw strategicznych, jeżeli jest to konieczne; 4) zakupu danego asortymentu rezerw lub usług w ramach udostępnienia rezerw utrzymywanych na podstawie umów, o których mowa w art. 17 i art. 18; 5) niezbędnych czynności Agencji i organów, na których rzecz rezerwy strategiczne udostępniono, oraz podmiotów, którym je wydano, w zakresie organizacji i realizacji udostępnienia rezerw strategicznych, na zasadach określonych w ustawie; 6) utworzenia i utrzymywania rezerw strategicznych nieobjętych Programem, o których mowa w art. 14; 7) odtworzenia udostępnionych rezerw strategicznych objętych Programem, o których mowa w art. 13; 8) realizacji zadań, o których mowa w art. 32.”; 10) w art. 13: a) ust. 2 otrzymuje brzmienie: „2. Decyzja o utworzeniu rezerw strategicznych określa w szczególności: 1) sposób utworzenia rezerw strategicznych przez Agencję; 2) rodzaj i ilość asortymentu rezerw strategicznych.”, b) ust. 4 otrzymuje brzmienie: „4. Wykonując decyzję o utworzeniu rezerw strategicznych, Agencja: 1) dokonuje nabycia określonej ilości asortymentu rezerw strategicznych; 2) przechowuje zakupiony asortyment rezerw strategicznych;	

	3) zawiera umowy, o których mowa w art. 17 lub w art. 18; 4) może przyjąć określony asortyment w formie darowizny z przeznaczeniem do rezerw strategicznych.”, c) ust. 5 otrzymuje brzmienie: „5. W przypadkach, w których nie mają zastosowania przepisy o zamówieniach publicznych, Agencja, dokonując zakupu asortymentu rezerw strategicznych lub usług związanych z utrzymywaniem rezerw strategicznych, lub zawierając umowy, o których mowa w art. 17 i art. 18, stosuje przejrzyste, niedyskryminacyjne i konkurencyjne warunki wyłaniania sprzedawcy tego asortymentu, usługi lub podmiotu, z którym zostanie zawarta umowa, o której mowa w art. 17 i art. 18, w szczególności: 1) przesyła zapytania ofertowe do podmiotów wykonujących działalność gospodarczą w zakresie produkcji, handlu, świadczenia określonych usług, w tym przechowywania oraz dysponujących odpowiednią bazą magazynową i gwarantujących odpowiednią jakość poszukiwanego asortymentu rezerw strategicznych, a także zapewniających ochronę informacji niejawnych, zgodnie z odrębnymi przepisami; 2) zaprasza do negocjacji podmioty oferujące najkorzystniejsze ekonomicznie warunki sprzedaży, świadczenia usług i przechowywania asortymentu rezerw strategicznych, biorąc pod uwagę relację ceny do jakości; 3) przeprowadza negocjacje cenowe z uwzględnieniem cen rynkowych w zakresie zakupu określonej ilości asortymentu rezerw strategicznych lub zakupu określonych usług.”; 11) w art. 14 dodaje się ust. 3 w brzmieniu: „3. Do decyzji, o której mowa w ust. 1, przepisy art. 13 ust. 2–6 stosuje się odpowiednio.”; 12) w art. 17 w ust. 2 pkt 1–3 otrzymują brzmienie:	

	„1) wysokość wynagrodzenia za utrzymywanie rezerw z możliwością ich zakupu lub najmu na rzecz Agencji; 2) zobowiązanie podmiotu, z którym zawarto umowę, do stałej gotowości sprzedaży lub najmu na rzecz Agencji asortymentu przechowywanych rezerw; 3) tryb i warunki, w tym cenę sprzedaży asortymentu będącego przedmiotem umowy na rzecz Agencji lub wysokość czynszu najmu tego asortymentu, do którego uiszczenia będzie zobowiązana Agencja w przypadku wydania, przez upoważniony organ, decyzji o udostępnieniu rezerw strategicznych.”; 13) w art. 19: a) w ust. 5: – pkt 4–5 otrzymują brzmienie: „4) wskazanie czy udostępnienie rezerw strategicznych następuje bez obowiązku zwrotu, z obowiązkiem zwrotu lub z obowiązkiem zwrotu niewykorzystanej części udostępnionych rezerw strategicznych; 5) inne szczególne warunki udostępnienia rezerw strategicznych, w tym w szczególności dotyczące obowiązku przetransportowania rezerw, montażu, zainstalowania lub ich przetworzenia lub obowiązku pokrycia kosztów przeglądów, demontażu, jeżeli jest to konieczne ze względu na właściwości udostępnionego asortymentu rezerw strategicznych lub jest uzasadnione innymi względami;”, – w pkt 5 kropkę zastępuje się średnikiem i dodaje się pkt 6 i 7 w brzmieniu: „6) określenie, czy udostępnione bez obowiązku zwrotu rezerwy strategiczne podlegają odtworzeniu wraz ze wskazaniem ilości oraz źródeł finansowania; 7) określenie źródła finansowania kosztów udostępnienia.”, b) dodaje się ust. 9–11 w brzmieniu: „9. W przypadku wydania decyzji o udostępnieniu rezerw strategicznych bez obowiązku zwrotu własność asortymentu rezerw strategicznych przechodzi na	

	organ lub podmiot, któremu rezerwy strategiczne zostały wydane z chwilą jego wydania. 10. W przypadku wydania decyzji o udostępnieniu rezerw strategicznych z obowiązkiem zwrotu utrzymanie wydanych rezerw strategicznych w należytym stanie, w tym dokonywanie wymaganych przeglądów, konserwacji i napraw, obciąża, podmiot lub organ, któremu rezerwy strategiczne zostały wydane. 11. Do zakupu usług transportowych oraz innych usług logistycznych związanych z wykonaniem decyzji o udostępnieniu rezerw strategicznych nie stosuje się przepisów ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych (Dz. U. z 2024 r. poz. 1320), jeżeli wartość zamówienia jest mniejsza niż progi unijne, o których mowa art. 3 ust. 1 tej ustawy."; 14) w art. 20 w ust. 2 pkt 6 otrzymuje brzmienie: „6) zwraca Agencji niewykorzystaną część udostępnionych rezerw strategicznych, jeżeli zostały udostępnione z obowiązkiem zwrotu niewykorzystanej części;"; 15) w art. 21: a) ust. 1 otrzymuje brzmienie: „1. Minister właściwy do spraw wewnętrznych może, w drodze decyzji, udostępnić określony specjalistyczny asortyment techniczny rezerw strategicznych, mając na względzie potrzebę przeciwdziałania lub usuwania skutków klęski żywiołowej lub sytuacji kryzysowej lub wsparcia realizacji celów społecznych lub przedsięwzięć gospodarczych, w szczególności związanych z odtworzeniem, budową, modernizacją lub remontem infrastruktury. Przepisy art. 19 ust. 2 i 4 oraz ust. 5 pkt 1–3 stosuje się odpowiednio.", b) ust. 3 otrzymuje brzmienie: „3. Udostępnienie specjalistycznego asortymentu technicznego rezerw strategicznych, jest dokonywane nieodpłatnie na rzecz państwowych jednostek organizacyjnych, jednostek samorządu terytorialnego lub utworzonych przez nie jednostek organizacyjnych w przypadku wystąpienia klęski żywiołowej lub sytuacji kryzysowej lub w celu zaspokojenia potrzeb społecznych lub	

	gospodarczych, w szczególności związanych z odtworzeniem, budową, modernizacją lub remontem infrastruktury.”; 16) art. 22 otrzymuje brzmienie: „Art. 22. 1. Agencja może odpłatnie udostępnić określony specjalistyczny asortyment techniczny rezerw strategicznych na rzecz jednostek samorządu terytorialnego, utworzonych przez nie jednostek organizacyjnych, służb, inspekcji lub innych jednostek, o których mowa w art. 8 ust. 2 pkt 22, oraz na rzecz przedsiębiorców mając na względzie potrzebę wsparcia w realizacji celów społecznych lub przedsięwzięć gospodarczych. 2. Udostępnienie specjalistycznego asortymentu technicznego rezerw strategicznych, jest dokonywane na wniosek podmiotów określonych w ust. 1. 3. Specjalistyczny asortyment techniczny rezerw strategicznych, o którym mowa w ust. 1 jest udostępniany na podstawie umowy zawartej na czas oznaczony między Agencją a podmiotem, o którym mowa w ust. 1. 4. Umowa, o której mowa w ust. 3, określa w szczególności warunki udostępnienia specjalistycznego asortymentu technicznego rezerw strategicznych oraz jego zwrotu.”; 17) w art. 23 ust. 5 otrzymuje brzmienie: „5. Umowa, o której mowa w ust. 4, określa w szczególności warunki udostępnienia specjalistycznego asortymentu medycznego rezerw strategicznych oraz jego zwrotu.”; 18) po art. 23 dodaje się art. 23a w brzmieniu: „Art. 23a. 1. Minister właściwy do spraw wewnętrznych może, w drodze decyzji, udostępnić wirtualne środowisko informatyczne oraz fizyczne lub wirtualne zasoby informatyczne mając na względzie potrzebę wsparcia realizacji celów związanych z cyberbezpieczeństwem państwa oraz konieczność odtworzenia zasobów cyfrowych. Przepisy art. 19 ust. 2 i 4 oraz ust. 5 pkt 1–3 stosuje się odpowiednio.	

	2. Decyzję, o której mowa w ust. 1, wykonuje Agencja. 3. Udostępnienie, o którym mowa w ust. 1, jest dokonywane odpłatnie na rzecz państwowych jednostek organizacyjnych, jednostek samorządu terytorialnego lub utworzonych przez nie jednostek organizacyjnych w przypadku wystąpienia zagrożenia cyberbezpieczeństwa państwa lub konieczności odtworzenia zasobów cyfrowych. 4. Wirtualne środowisko informatyczne oraz fizyczne lub wirtualne zasoby informatyczne są udostępniane na podstawie umowy zawartej na czas oznaczony pomiędzy Agencją a podmiotem, o którym mowa w ust. 3. 5. Umowa, o której mowa w ust. 4, w szczególności warunki udostępnienia asortymentu określonego w ust. 1 oraz jego zwrotu.”; 19) art. 24 otrzymuje brzmienie: „Art. 24. Minister właściwy do spraw wewnętrznych określi, w drodze rozporządzenia, szczegółową procedurę udostępnienia rezerw strategicznych, w tym czasowego, zwrotnego udostępnienia specjalistycznego asortymentu technicznego rezerw strategicznych oraz specjalistycznego asortymentu medycznego rezerw strategicznych, procedurę zwrotu asortymentu rezerw strategicznych, oraz szczegółowe czynności przy udostępnieniu lub wydaniu rezerw strategicznych, uwzględniając konieczność zapewnienia prawidłowej i efektywnej realizacji zadań Agencji.”; 20) w art. 27a w ust. 1 wprowadzenie do wyliczenia otrzymuje brzmienie: „1. Minister właściwy do spraw wewnętrznych może zlikwidować, w drodze decyzji, określony asortyment rezerw strategicznych, ze względu na konieczność:”; 21) uchyla się art. 28; 22) art. 29: a) ust. 2 otrzymuje brzmienie:	

	"2. W przypadkach, o których mowa w ust. 1, organ lub podmiot powierzający Agencji określone zadanie wskazuje, rodzaj i ilość asortymentu, zakres jego przechowania, w tym czas tego przechowania, oraz organy lub podmioty, którym dany asortyment zostanie wydany oraz warunki wydania, a także określa wysokość środków finansowych przeznaczonych na finansowanie zadania.", b) po ust. 3 dodaje się ust. 3a i 3b w brzmieniu: 3a. Środki finansowe na realizację powierzonego zadania oraz na pokrycie kosztów, o których mowa w ust. 3, organ lub podmiot powierzający Agencji określone zadanie przekazuje Agencji na podstawie zawartego z nią porozumienia. 3b. Środki finansowe, o których mowa w ust. 3a, nie stanowią przychodu Agencji, a ich przekazanie nie wymaga dokonywania zmian w planie finansowym Agencji."; 23) po art. 29 dodaje się art. 29a w brzmieniu: „Art. 29a. 1. Agencja, za zgodą ministra właściwego do spraw wewnętrznych, może wykonywać zadania związane z: 1) przeciwdziałaniem wystąpieniu zagrożenia bezpieczeństwa i obronności państwa, porządku i zdrowia publicznego, klęski żywiołowej lub sytuacji kryzysowej; 2) udzielaniem pomocy humanitarnej ludności znajdującej się w sytuacji zagrożenia życia lub zdrowia – na podstawie przepisów prawa międzynarodowego publicznego, procedur organizacji międzynarodowych oraz porozumień tworzących wiążące zobowiązanie wobec Agencji. 2. Agencja może realizować zadania, o których mowa w ust. 1, po zapewnieniu środków finansowych na ich realizację, w tym na pokrycie wydatków niekwalifikowanych, zgodnie z ustawą o finansach publicznych.”; 24) w art. 31:	

	a) w ust. 1 – pkt 3 otrzymuje brzmienie: „3) wykonywanie decyzji organów lub podmiotów, o których mowa w art. 8 ust. 2, dotyczących zakupu, przechowywania, dystrybucji i wydawania określonych asortymentów towarów zgodnie z zasadami określonymi w rozdziale 6;”, – po pkt 8 dodaje się pkt 8a w brzmieniu: „8a) wykonywanie zadań, o których mowa w art. 29a ust. 1;”, – pkt 10 i 11 otrzymują brzmienie: „10) opracowywanie informacji o asortymencie rezerw strategicznych, ilości i wartości rezerw strategicznych oraz ich finansowaniu, wykorzystaniu i rozmieszczeniu, w terminach do dnia 15 września każdego roku za I półrocze i do dnia 31 marca każdego roku za rok poprzedni; 11) przekazywanie Ministrowi Obrony Narodowej, ministrowi właściwemu do spraw transportu, ministrowi właściwemu do spraw wewnętrznych i Szefowi Agencji Bezpieczeństwa Wewnętrznego informacji o ilości i rozmieszczeniu rezerw strategicznych, ujętych w Programie w terminach do dnia 15 września każdego roku za I półrocze i do dnia 31 marca każdego roku za rok poprzedni;” - po pkt 13 kropkę zastępuje się średnikiem i dodaje się pkt 14 w brzmieniu: „14) prowadzenie działalności informacyjnej, promocyjnej i edukacyjnej w zakresie zadań Agencji.”, b) ust. 2 otrzymuje brzmienie: „2. Do czynności realizowanych przez Agencję w ramach zadań, o których mowa w ust. 1 pkt 5, nie stosuje się przepisów art. 38–41 ustawy z dnia 16 grudnia 2016 r. o zasadach zarządzania mieniem państwowym (Dz. U. z 2024 r. poz. 125 i 834).”;	

	25) art. 32 otrzymuje brzmienie: „Art. 32. 1. Minister właściwy do spraw wewnętrznych może powierzyć Agencji, w drodze decyzji, realizację innych zadań niż określone w art. 31, na terytorium Rzeczypospolitej Polskiej lub w porozumieniu z ministrem właściwym do spraw zagranicznych poza jej granicami, związanych z: 1) wystąpieniem zagrożenia bezpieczeństwa i obronności państwa, porządku i zdrowia publicznego, klęski żywiołowej lub sytuacji kryzysowej; 2) wypełnieniem zobowiązania międzynarodowego albo udzieleniem pomocy lub wsparcia: a) podmiotowi prawa międzynarodowego publicznego, b) podmiotowi krajowemu, zagranicznemu lub międzynarodowemu podejmującemu działania w zakresie niesienia pomocy humanitarnej lub usuwania skutków sytuacji kryzysowej – w szczególności w przypadkach określonych w pkt 1. 2. Realizując zadania, o których mowa w ust. 1, Agencja jest uprawniona w szczególności do: 1) nabywania, zbywania, transportowania, przechowywania, wydawania oraz do wywozu poza terytorium Rzeczypospolitej Polskiej i przywozu z terytorium innego państwa określonego asortymentu; 2) nabywania oraz świadczenia usług, w szczególności usług o charakterze logistycznym, transportowym i magazynowym, na terytorium Rzeczypospolitej Polskiej lub poza jej granicami; 3) zlecania wykonania robót budowlanych oraz usług związanych z ich wykonaniem; 4) przyjmowania i przekazywania darowizn.	

	3. Powierzając zadania, o których mowa w ust. 1, minister właściwy do spraw wewnętrznych zapewnia Agencji na ten cel odpowiednie środki finansowe. 4. Wydając decyzję, o której mowa w ust. 1, minister właściwy do spraw wewnętrznych może nadać jej rygor natychmiastowej wykonalności. Decyzja nie wymaga uzasadnienia. 5. Do udzielania zamówień niezbędnych do realizacji decyzji, o której mowa w ust. 1, nie stosuje się przepisów ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych, jeżeli wartość zamówienia jest mniejsza niż progi unijne, o których mowa art. 3 ust. 1 tej ustawy. 6. Agencja, w terminie 30 dni od dnia udzielenia zamówienia, o którym mowa w ust. 5, zamieszcza w Biuletynie Zamówień Publicznych informację o udzieleniu tego zamówienia, w której podaje: 1) datę i miejsce zawarcia umowy lub informację o zawarciu umowy drogą elektroniczną, 2) opis przedmiotu umowy, z wyszczególnieniem odpowiednio ilości rzeczy lub innych dóbr oraz zakresu usług, 3) cenę albo cenę maksymalną, jeżeli cena nie jest znana w chwili zamieszczenia ogłoszenia, 4) wskazanie okoliczności faktycznych uzasadniających udzielenie zamówienia bez zastosowania przepisów ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych, 5) nazwę (firmę) podmiotu albo imię i nazwisko osoby, z którymi została zawarta umowa – z wyłączeniem przypadków, w których udzielenie zamówienia wiąże się z korzystaniem z informacji niejawnych.”; 26) w art. 36 dodaje się ust. 5 w brzmieniu:	

	„5. Przepisów ust. 1–4 nie stosuje się do naboru wewnętrznego spośród pracowników Agencji do zatrudnienia na wolne stanowiska pracy w Agencji.”; 27) art. 40 otrzymuje brzmienie: „Art. 40. Pracownicy Agencji zatrudnieni: 1) na stanowisku głównego księgowego, 2) na stanowisku zastępcy dyrektora biura lub na stanowisku równorzędnym, 3) na stanowisku kierownika działu lub na stanowisku równorzędnym, 4) na stanowisku kierownika składnicy lub na stanowisku równorzędnym – składają Prezesowi Agencji oświadczenia o stanie majątkowym na zasadach, w trybie i w terminach określonych w przepisach ustawy z dnia 21 sierpnia 1997 r. o ograniczeniu prowadzenia działalności gospodarczej przez osoby pełniące funkcje publiczne oraz podlegają ograniczeniom w prowadzeniu działalności gospodarczej, takim jak pracownicy agencji państwowych, o których mowa w art. 2 pkt 10 ustawy z dnia 21 sierpnia 1997 r. o ograniczeniu prowadzenia działalności gospodarczej przez osoby pełniące funkcje publiczne (Dz. U. z 2023 r. poz. 1090).”; 28) po art. 40 dodaje się art. 40a w brzmieniu: „Art. 40a. Agencja wykonuje obowiązek, o którym mowa w art. 13 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) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.), zwanego dalej „rozporządzeniem 2016/679”, przez udostępnienie informacji, o których mowa w art. 13 ust. 1 i 2 rozporządzenia 2016/679, na swojej stronie internetowej lub w Biuletynie Informacji Publicznej na stronie podmiotowej Agencji. W takim przypadku Agencja, podczas pozyskiwania danych osobowych, informuje osobę, której dane dotyczą, o miejscu udostępnienia tych informacji.”;	

	29) w art. 41: a) w ust. 2 pkt 2 otrzymuje brzmienie: „2) dotacje celowe na realizację zadań, o których mowa w art. 12 ust. 1;” b) w ust. 2 w pkt 9 kropkę zastępuje się średnikiem i dodaje się pkt 10 w brzmieniu: „10) środki pochodzące z budżetu Unii Europejskiej.” c) ust. 3 otrzymuje brzmienie: „3. Przychody, o których mowa w ust. 2 pkt 4–7, przeznacza się na realizację zadań Agencji, o których mowa w art. 31 i art. 32, oraz na bieżącą działalność Agencji, w tym wynagrodzenia jej pracowników.”; d) po ust. 3a dodaje się ust. 3b w brzmieniu: „3b. Przychody Agencji, o których mowa w ust. 2 pkt 10, przeznacza się na realizację zadań Agencji, o których mowa w art. 31 ust. 1, w szczególności w pkt 8a.”; 30) w art. 42: a) w ust. 1 w pkt 3 lit. b otrzymuje brzmienie: „b) realizacji zadań określonych w ustawie oraz w ustawie o zapasach ropy naftowej, produktów naftowych i gazu ziemnego, z uwzględnieniem: – kosztów realizacji tych zadań przez inne podmioty, – zakupu towarów i usług;”, b) ust. 3 otrzymuje brzmienie: „3. Agencja w terminie 30 dni od ogłoszenia ustawy budżetowej na dany rok, przekazuje ministrowi właściwemu do spraw wewnętrznych plan rzeczowy rezerw strategicznych stanowiący załącznik do planu finansowego Agencji.”,	

	c) ust. 4 otrzymuje brzmienie: „4. Agencja sporządza i przekazuje ministrowi właściwemu do spraw wewnętrznych sprawozdania finansowe i związane z nimi informacje, w trybie i na zasadach określonych w ustawie o finansach publicznych oraz ustawie o rachunkowości.”; 31) w art. 44 ust. 1 otrzymuje brzmienie: „1. Należności i wierzytelności Agencji mające charakter cywilnoprawny, w szczególności z tytułu wykonywania zadań, o których mowa w art. 31 ust. 1 pkt 1, 2, 4–8 i 13, mogą być umarzane w całości albo w części lub ich spłata może być odraczana, lub rozkładana na raty.”; 32) w art. 46 w ust. 1 dodaje się pkt 1a w brzmieniu: „1a) minister właściwy do spraw gospodarki surowcami energetycznymi – w zakresie należności i wierzytelności wynikających z wykonywania zadań, o których mowa w art. 31 ust. 1 pkt 8, z zastrzeżeniem pkt 1;”; 33) po art. 46 dodaje się art. 46a w brzmieniu: „Art. 46a. Przepisów art. 44–46 nie stosuje się do zawarcia ugody na podstawie art. 54a ustawy o finansach publicznych.”.	
Art. 21 projektu ustawy (zmiany w ustawie z dnia o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa)	**Art. 21.** W ustawie z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa (Dz. U. poz. 1662) w art. 2 w ust. 4 po pkt 1a dodaje się pkt 1b w brzmieniu: "1b) wpływy z kar pieniężnych, o których mowa w art. 6zzo ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2023 r. poz. 122 oraz z 2024 r. poz. 834, 1222, 1473, 1572 i 1907);".	Zmiana wynikowa do zmian w ustawie o zarządzaniu kryzysowym. Wskazanie funduszu właściwego do gromadzenia środków finansowych pochodzących z kar nakładanych na podmioty krytyczne.

Art. 22 projektu ustawy (zmiany w ustawie – Prawo komunikacji elektronicznej)	**Art. 22.** 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) wprowadza się następujące zmiany: 1) uchyla się art. 42; 2) po art. 67 dodaje się art. 67a w brzmieniu: „Art. 67a. 1. Prezes UKE, w uzgodnieniu z ministrem właściwym do spraw wewnętrznych, zapewnia odpowiednie częstotliwości do realizacji zadań z zakresu komunikacji głosowej i transmisji danych do zapewnienia bezpiecznej radiowej łączności mobilnej w celu: zapewnienia ciągłości i bezpieczeństwa funkcjonowania administracji państwowej oraz ochrony ludności i obrony cywilnej. 2. Podmiot będący przedsiębiorcą telekomunikacyjnym lub podmiot prowadzący działalność telekomunikacyjną, o którym mowa w art. 79 ustawy z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej (Dz. U. poz. 1907, z 2025 r. poz. 1705 oraz …), któremu minister właściwy do spraw wewnętrznych zlecił zadania związane z organizacją, budową, utrzymaniem i modernizacją Systemu Bezpiecznej Łączności Państwowej, wykorzystuje częstotliwości do wykonywania zadań, o których mowa w ust. 1, na podstawie decyzji o rezerwacji częstotliwości wydanej przez Prezesa UKE po uzgodnieniu z ministrem właściwym do spraw wewnętrznych. 3. Do rezerwacji częstotliwości, o której mowa w ust. 1 przepisu art. 104 ust. 3 nie stosuje się.”.	Zmiana wynikowa do zmian w ustawie o zarządzaniu kryzysowym.
Art. 23 projektu ustawy (zmiany w ustawie o ochronie ludności i obronie cywilnej)	**Art. 23.** W ustawie z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej (Dz. U. poz. 1907 oraz z 2025 r. poz. 1705) wprowadza się następujące zmiany: 1) w art. 5 ust. 2 otrzymuje brzmienie: „2. Podmioty ochrony ludności i obrony cywilnej są obowiązane do współpracy z organami ochrony ludności i obrony cywilnej, stosownie do swoich możliwości, kompetencji, obszaru działania oraz zakresu działania ujętego w planach zarządzania kryzysowego, o których mowa w art. 6g ust. 2 oraz art. 6j ust. 1 ustawy	Zmiany wynikowe do zmian w ustawie o zarządzaniu kryzysowym.

	z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, i planach ciągłości działania.”; 2) w art. 15 w ust. 1 pkt 6 otrzymuje brzmienie: „6) analizowanie wniosków z ocen ryzyka mających wpływ na bezpieczeństwo i ochronę ludności i obronę cywilną, o których mowa w Krajowej Ocenie Ryzyka, o której mowa w art. 6e ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, i informacji pochodzących z raportów Rządowego Centrum Bezpieczeństwa oraz centrów służb podległych mu i nadzorowanych przez niego, a także przedstawianie propozycji rozwiązań w tym zakresie;”; 3) w art. 38, wprowadzenie do wyliczenia otrzymuje brzmienie: "Organy ochrony ludności i Dyrektor Rządowego Centrum Bezpieczeństwa uwzględniają w planach, o których mowa w art. 6g ust. 2 oraz art. 6j ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym:”; 4) art. 40 otrzymuje brzmienie: „Art. 40. 1. Dyrektor Rządowego Centrum Bezpieczeństwa opracowuje krajowy plan ewakuacji ludności we współpracy z Szefem Sztabu Generalnego Wojska Polskiego. 2. Krajowy plan ewakuacji opracowuje się na podstawie wojewódzkich planów ewakuacji ludności. 3. Krajowy plan ewakuacji oraz wojewódzkie plany ewakuacji opracowuje się na okres 3 lat. 4. Plany, o których mowa w ust. 3 mogą być aktualizowane w przypadku zmian dotyczących sytuacji, o których mowa w art. 39 ust. 1. 5. Krajowy plan ewakuacji jest zatwierdzany przez ministra właściwego do spraw wewnętrznych.”; 5) art. 44 otrzymuje brzmienie:	

	„Art. 44. Wojewódzki plan ewakuacji ludności stanowi załącznik funkcjonalny do wojewódzkiego planu reagowania kryzysowego. Wkłady, o których mowa w art. 43, stanowią załączniki funkcjonalne do planów reagowania kryzysowego odpowiednio gminy i powiatu.”; 6) po art. 79 dodaje się art. 79a w brzmieniu: „Art. 79a. 1. Zlecenie zadań związanych z organizacją budową, utrzymaniem i modernizacją SBŁP przedsiębiorcy spełniającemu łącznie warunki, o których mowa w art. 79, może nastąpić w drodze decyzji administracyjnej, wydawanej przez ministra właściwego do spraw wewnętrznych. 2. Wykonywanie zadań, w zakresie określonym w ust. 1, następuje na podstawie umowy zawartej pomiędzy przedsiębiorcą oraz ministrem właściwym do spraw wewnętrznych. 3. W umowie, o której mowa w ust. 2, określa się w szczególności zakres zadań, warunki finansowania i sposób współpracy z operatorem SBŁP."; 7) w art. 206 dotychczasową treść oznacza się jako ust. 1 i dodaje się ust. 2 w brzmieniu: "2. Postanowień ust. 1 nie stosuje się dla zamierzenia budowlanego, wobec którego przed dniem wejścia w życie niniejszej ustawy złożono wniosek o wydanie decyzji o środowiskowych uwarunkowaniach zgody na realizację przedsięwzięcia.".	

Projekt

R O Z P O R Z Ą D Z E N I E

M I N I S T R A S P R A W W E W N Ę T R Z N Y C H I A D M I N I S T R A C J I

z dnia

w sprawie szczegółowej procedury udostępnienia rezerw strategicznych

Na podstawie art. 24 ustawy z dnia 17 grudnia 2020 r. o rezerwach strategicznych (Dz. U. …) zarządza się, co następuje:

§ 1. Rozporządzenie określa szczegółową procedurę udostępnienia rezerw strategicznych, w tym czasowego, zwrotnego udostępnienia specjalistycznego asortymentu technicznego rezerw strategicznych oraz specjalistycznego asortymentu medycznego rezerw strategicznych, zwaną dalej „procedurą”.

§ 2. Procedura udostępnienia rezerw strategicznych obejmuje następujące czynności:

1) wydania określonego asortymentu w celu użycia lub wykorzystania, następującego z magazynów:
   a) własnych Agencji,
   b) podmiotów, którym oddano dany asortyment rezerw strategicznych na przechowanie,
   c) podmiotów utrzymujących na podstawie odpłatnej umowy rezerwy strategiczne stanowiące ich własność,

   podmiotów, które zawarły umowy o utrzymywaniu zdolności produkcyjnych;
2) zrealizowania określonej usługi na podstawie umowy o pozostawaniu w gotowości do świadczenia usług;
3) w celu zapewnienia prawidłowości, rzetelności i sprawnego realizowania powierzonych Agencji zadań oraz należytego przepływu informacji i dokumentacji pomiędzy Agencją i innymi podmiotami.

§ 3. Ilekroć w procedurze jest mowa o:

1) decyzji o udostępnieniu rezerw strategicznych - należy przez to rozumieć decyzję ministra właściwy do spraw wewnętrznych, o której mowa w art. 19 ustawy z dnia 17 grudnia 2020 r. o rezerwach strategicznych;

2) rezerwach - należy przez to rozumieć rezerwy strategiczne, w rozumieniu ustawy o rezerwach strategicznych;
3) organie - należy przez to rozumieć organ lub podmiot, o którym mowa w art. 8 ust. 2 ustawy o rezerwach strategicznych, na rzecz którego udostępnione zostaną rezerwy;
4) odbiorcy - należy przez to rozumieć podmiot, któremu udostępnione rezerwy będą wydane do użycia lub wykorzystania;
5) przetrzymaniu rezerw - należy przez to rozumieć krótki okres przechowywania udostępnionych rezerw, na określonym terenie w pomieszczeniach, magazynach, placach, zagrodach, środkach transportu lub wydzielonych obszarach, do momentu ich użycia w celach określonych w decyzji o udostępnieniu rezerw strategicznych;
6) przetworzeniu rezerw - należy przez to rozumieć uporządkowany i celowy proces biologicznego, chemicznego, fizycznego lub mechanicznego przekształcania lub transformacji określonego asortymentu udostępnionej rezerwy utrzymywanej w postaci surowców lub półproduktów, prowadzony zgodnie z obowiązującymi procedurami technologicznymi, prowadzący do uzyskania produktów i substancji służących do dalszego racjonalnego użycia lub wykorzystania zgodnie z przeznaczeniem określonym w decyzji o udostępnieniu rezerw strategicznych;
7) niewykorzystanej części udostępnionych rezerw - należy przez to rozumieć pozostałą w dyspozycji odbiorcy część udostępnionego asortymentu rezerw, która bez nadmiernych nakładów finansowych lub czynności dostosowawczych lub technologicznych, bez względu na upływ czasu, może być przyjęta przez Agencję;
8) umowie przechowania, należy przez to rozumieć umowę, na podstawie której Agencja oddała innemu podmiotowi dany asortyment rezerw na przechowanie;
9) podmiocie przechowującym, należy przez to rozumieć podmiot świadczący usługi na podstawie umowy przechowania;
10) umowie utrzymywania, należy przez to rozumieć umowę, na podstawie której Agencja utrzymuje rezerwy stanowiące własność innych podmiotów;
11) podmiocie utrzymującym, należy przez to rozumieć podmiot świadczący usługi utrzymywania;
12) podmiocie utrzymującym zdolności produkcyjne, należy przez to rozumieć podmiot zobowiązany do utrzymywania mocy produkcyjnych na podstawie umowy o utrzymywaniu zdolności produkcyjnych;

13) umowie o utrzymywaniu zdolności produkcyjnych, należy przez to rozumieć umowę, na podstawie której Agencja zobowiązuje podmiot do utrzymywania zdolności produkcyjnych w zakresie danego asortymentu rezerw;
14) podmiocie pozostającym w gotowości do świadczenia usług, należy przez to rozumieć podmiot zobowiązany do utrzymania mocy usługowych na podstawie umowy pozostawania w gotowości do świadczenia usług;
15) umowie o pozostawaniu w gotowości do świadczenia usług, należy przez to rozumieć umowę, na podstawie której Agencja zobowiązuje podmiot do utrzymywania zdolności usługowych w zakresie danego asortymentu rezerw;
16) wydawaniu lub wydaniu, należy przez to rozumieć czynności podejmowane w celu fizycznego przekazania rezerw wskazanym w decyzji podmiotom;
17) wykorzystaniu rezerw, należy przez to rozumieć użycie udostępnionych rezerw w celach określonych w decyzji o udostępnieniu rezerw strategicznych.

§ 4. 1. Prezes Agencji, po otrzymaniu decyzji, przekazuje dyspozycję właściwej komórce organizacyjnej Agencji, prowadzącej sprawy związane z danym asortymentem rezerw.

2. Komórka organizacyjna Agencji weryfikuje pozostające w jej dyspozycji informacje dotyczące stanu rezerw utrzymywanych w magazynach własnych oraz u podmiotów przechowujących lub utrzymujących, uwzględniając w szczególności rodzaj asortymentu, jego ilość, rozmieszczenie i inne szczególne właściwości, a następnie wskazuje obiekty, z których udostępnienie rezerw będzie miało miejsce, określając ilość i asortyment dla poszczególnych obiektów oraz, jeżeli zachodzi taka potrzeba, wymogi w zakresie ewentualnego przetransportowania lub przetrzymania rezerw przez odbiorcę.

§ 5. 1. W przypadkach, w których:
1) ma nastąpić przetworzenie udostępnionych rezerw przed ich wydaniem;
2) udostępnieniu podlegają rezerwy objęte obowiązkiem zapłaty podatku akcyzowego;
3) udostępnieniu podlegają rezerwy objęte umową utrzymywania;
4) udostępnianiu podlegają rezerwy na podstawie umowy o utrzymywaniu zdolności produkcyjnych lub umowy o pozostawaniu w gotowości do świadczenia usług;
5) udostępnieniu bezzwrotnemu podlegają rezerwy, których nieodpłatne przekazanie podlega opodatkowaniu podatkiem VAT, a decyzja nie określa źródeł lub trybu finansowania wydatków związanych z przetworzeniem, zapłatą akcyzy, zapłatą podatku VAT, nabyciem lub wynajmem utrzymywanych rezerw, Agencja występuje niezwłocznie

do ministra właściwego do spraw wewnętrznych z wnioskiem o ich wskazanie, określając szacunkową wysokość kosztów z tytułu dokonania tych czynności lub z tytułu koniecznych do poniesienia opłat.

2. Przekazanie wniosku wskazanego w ust. 1 nie wstrzymuje dalszych czynności podejmowanych w związku z udostępnieniem rezerw.

§ 6. Agencja zapewnia przetransportowanie udostępnionych rezerw oraz organizuje inne usługi logistyczne, o ile wskazano tak w decyzji o udostępnieniu rezerw strategicznych.

§ 7. 1. Agencja informuje:

1) odbiorcę o podjęciu czynności mających na celu wykonanie decyzji, a w szczególności przekazuje informacje dotyczące miejsca, z którego nastąpi wydanie rezerw, o ile odbiorca będzie dokonywał odbioru rezerw we własnym zakresie lub uzyskuje informacje o miejscu dostawy, do którego rezerwy zostaną przetransportowane;
2) odbiorcę o wymaganiach dotyczących właściwego przetransportowania rezerw w przypadku, gdy odbiorca organizuje przetransportowanie we własnym zakresie;
3) odbiorcę o wymaganiach w zakresie ewentualnego przetrzymania rezerw - jeżeli zachodzi taka potrzeba;
4) odbiorcę o jego obowiązkach wynikających z przepisów o rezerwach strategicznych oraz o uprawnieniu Agencji do dokonania sprawdzenia warunków przetransportowania rezerw oraz ich przetrzymania;
5) odbiorcę o obowiązku:
   a) zwrotu rezerw w przypadku udostępnienia rezerw z obowiązkiem ich zwrotu lub
   b) zwrotu niewykorzystanej części udostępnionych rezerw.

2. Niezależnie od przekazania informacji wskazanych w ust. 1, Agencja podejmuje czynności mające na celu przygotowanie rezerw do wydania, w szczególności uzyskuje od organu lub odbiorcy informacje dotyczące osoby lub osób upoważnionych do fizycznego odbioru rezerw oraz uzgadnia termin wydania rezerw, jeżeli nie został on określony w decyzji ministra właściwego do spraw wewnętrznych.

3. Informacje, o których mowa w ust. 1 i 2, mogą być przekazywane lub uzyskiwane w formie pisemnej lub w formie dokumentu elektronicznego opatrzonego kwalifikowanym podpisem elektronicznym. Informacje mogą być przekazywane lub uzyskiwane także ustnie, pisemnie w formie adnotacji, telefonicznie, za pomocą środków komunikacji elektronicznej

w rozumieniu art. 2 pkt 5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2020 r. poz. 344) lub za pomocą innych środków łączności.

4. W przypadku, gdy informacje zostały przekazane lub uzyskane ustnie lub telefonicznie, ich treść powinna być stwierdzona w formie pisemnej lub dokumentowej.

§ 8. 1. Agencja sporządza „Polecenie wydania".

2. „Polecenie wydania" może być sporządzone w formie pisemnej lub w formie dokumentu elektronicznego opatrzonego kwalifikowanym podpisem elektronicznym. „Polecenie wydania" może być sporządzone także ustnie, pisemnie w formie adnotacji, telefonicznie, za pomocą środków komunikacji elektronicznej w rozumieniu art. 2 pkt 5 ustawy o świadczeniu usług drogą elektroniczną lub za pomocą innych środków łączności.

3. W przypadku, gdy „Polecenie wydania" zostało wydane ustnie lub telefonicznie, jego istotne elementy powinny być stwierdzone w formie pisemnej lub dokumentowej.

4. „Polecenie wydania" zawiera w szczególności:

1) oznaczenie podmiotu, obowiązanego do wydania rezerw;
2) oznaczenie miejsca, z którego ma nastąpić wydanie rezerwy;
3) oznaczenie, ilość, jednostki miary i ewentualnie inne dane identyfikujące rezerwy;
4) oznaczenie odbiorcy rezerwy.

§ 9. 1. Rezerwy mogą być wydane wyłącznie osobom uprawnionym do reprezentowania organu lub odbiorcy wskazanego w decyzji. Organ lub odbiorca wskazany w decyzji zobowiązany jest przekazać Agencji w formie pisemnej lub dokumentowej upoważnienie do odbioru.

2. Z wydania rezerw sporządza się „Protokół wydania", który jest podpisywany przez przedstawiciela Agencji oraz odbierającego rezerwy, z zastrzeżeniem § 10 ust. 1. Jeden egzemplarz „Protokołu wydania" przekazywany jest odbierającemu rezerwy.

3. Sporządza się odrębne protokoły wydania, jeżeli udostępnienie rezerw i ich wydanie następuje dla wielu podmiotów lub z wielu magazynów.

4. W przypadku transportowania rezerw przez podmiot trzeci, działający na podstawie zlecenia Agencji, „Protokół wydania" podpisywany jest wyłącznie przez umocowanego przedstawiciela Agencji. Potwierdzenie odbioru udostępnionych odbiorcy rezerw stanowi list przewozowy.

5. W przypadkach uzasadnionych szczególnymi okolicznościami nie sporządza się „Protokołu wydania", o którym mowa w ust. 2 i 3. W takim przypadku wydanie rezerw

z magazynu dokumentuje się podpisem na dokumencie magazynowym wydania zewnętrznego (WZ) lub na innym dokumencie.

6. W przypadku wydania rezerw odbiorcom zagranicznym, Agencja zobowiązana jest do przygotowania wszystkich niezbędnych dokumentów wymaganych w międzynarodowym obrocie towarami oraz do zapewnienia zgodności tych dokumentów z przepisami celnymi.

§ 10.1. Szczegółowe zasady postępowania w przypadku udostępnienia rezerw, w szczególności ich wydania przez podmioty przechowujące, przez podmioty utrzymujące rezerwy lub podmioty utrzymujące zdolności produkcyjne bądź pozostające w gotowości do świadczenia usług, określają odpowiednio umowy: przechowania, utrzymywania, o utrzymywaniu zdolności produkcyjnych oraz o pozostawaniu w gotowości do świadczenia usług.

2. Przepis § 9 ust. 1-4 stosuje się odpowiednio w przypadku „Protokołu wydania" sporządzonego przez podmiot przechowujący, utrzymujący rezerwy, podmiot utrzymujący zdolności produkcyjne bądź pozostający w gotowości do świadczenia usług.

§ 11. W przypadku, w którym decyzja ministra właściwego do spraw wewnętrznych zobowiązuje Agencję do zapewnienia przetworzenia rezerw przed ich wydaniem, właściwa komórka organizacyjna Agencji określa zasady oraz tryb i miejsce przetworzenia rezerw, zgodnie z treścią decyzji, z właściwością surowców lub półproduktów, stosownie do zawartych umów przechowania lub umów utrzymywania rezerw, jeżeli zawierają takie postanowienia, lub umów zawartych z innymi podmiotami uprawnionymi do prowadzenia procesu przetworzenia, jeżeli takie umowy zawarto.

§ 12. 1. W przypadku stwierdzenia przeszkody w wykonaniu decyzji, w zakresie zapewnienia przez Agencję przetworzenia rezerw, wynikającej w szczególności z obowiązujących przepisów prawa, w tym:

1) określających nakazy uzyskania stosownych zezwoleń, decyzji lub przeprowadzenia innych czynności;
2) wprowadzających zakazy wprowadzania do obrotu określonych towarów;
3) nakładających obowiązek przeprowadzenia postępowań mających na celu wyłonienie podmiotów uprawnionych do przeprowadzenia określonych czynności oraz zawarcia z nimi umowy

– Prezes Agencji informuje ministra właściwego do spraw wewnętrznych o stwierdzonej przeszkodzie w wykonaniu decyzji oraz przedstawia propozycje dalszych działań.

2. Kolejne czynności podejmowane są przez Agencję po wskazaniu przez ministra właściwego do spraw wewnętrznych dalszego sposobu postępowania w związku ze stwierdzeniem przeszkody w wykonaniu decyzji.

§ 13. 1. W przypadku udostępnienia rezerw z obowiązkiem zwrotu udostępnienie następuje na podstawie umowy zawartej w formie pisemnej pomiędzy Agencją a podmiotem, któremu udostępnione rezerwy zostały wydane, która określa w szczególności:

1) przedmiot umowy;
2) okres obowiązywania umowy;
3) termin i miejsce udostępnienia rezerw;
4) wysokość wynagrodzenia za udostępnienie, w przypadku odpłatnego udostępnienia;
5) kary umowne w przypadku niewywiązywania się z postanowień umowy w przypadku udostępnienia rezerw strategicznych na podstawie art. 21-23 ustawy o rezerwach strategicznych;
6) zabezpieczenie należytego wykonania umowy w przypadku udostępnienia rezerw strategicznych na podstawie art. 21-23 ustawy o rezerwach strategicznych;
7) zobowiązanie podmiotu, któremu udostępniono rezerwy do:
   a) poniesienia wszelkich kosztów związanych z udostępnieniem i zwrotem rezerw oraz ich eksploatacją w okresie udostępnienia o ile decyzja nie wskazuje inaczej,
   b) zwrotu udostępnionych rezerw w stanie niewykraczającym ponad normalne zużycie,
   c) używania rezerw zgodnie z ich przeznaczeniem,
   d) przestrzegania określonych zasad używania, przeglądów, bieżącej konserwacji i innych warunków wynikających z gwarancji jakości lub zaleceń producenta lub dostawcy albo zaleceń technicznych określonych w odrębnych przepisach,
   e) ponoszenia kosztów napraw powstałych z niewłaściwego używania rezerw;
   f) pokrycia wydatków poniesionych przez Agencję po dokonaniu zwrotu rezerw w celu przywrócenia towaru do stanu umożliwiającego użytkowanie towaru zgodnie z jego przeznaczeniem,
   g) konieczność przeprowadzenia zabezpieczenia antykorozyjnego w przypadku odpłatnego udostępnienia specjalistycznego asortymentu rezerw strategicznych w postaci konstrukcji mostowych,
8) warunki przetrzymania i przetransportowania rezerw, jeżeli jest to zasadne;
9) termin, miejsce i inne warunki zwrotu rezerw do Agencji.

2. Udostępnienie rezerw następuje na zasadach określonych w § 4 - § 10.

3. W szczególnie uzasadnionych przypadkach wydanie rezerw może nastąpić przed sporządzeniem i podpisaniem umowy, o której mowa w ust. 1. W takim przypadku umowa na piśmie zostanie sporządzona i podpisana niezwłocznie, nie później niż w terminie 30 dni od dnia wydania rezerwy.

4. Zasady oraz tryb uzgodnienia umowy oraz jej podpisania, w braku odmiennych postanowień w decyzji o udostępnieniu rezerwy, określa Agencja.

§ 14. 1. W przypadku zwrotu niewykorzystanej części udostępnionych rezerw, Agencja po uzyskaniu od odbiorcy lub organu informacji o zamiarze zwrotu niewykorzystanej części rezerw, uzgadnia z odbiorcą lub organem szczegółowe warunki zwrotu.

2. Agencja może sprawdzić warunki przetrzymania rezerw lub zażądać udokumentowania warunków przetrzymania rezerw, jak również dokonać oceny, czy spełnione są inne wymagania określone w stosunku do jakości i innych właściwości rezerw.

3. Na podstawie informacji, o których mowa w ust. 1, Agencja uzgadnia z odbiorcą lub organem termin oraz sposób przetransportowania niewykorzystanej części udostępnionych rezerw do miejsca wskazanego przez Agencję.

4. Agencja odmawia przyjęcia zwrotu, jeżeli stan towaru nie pozwala na jego ponowne wprowadzenie na stan rezerw lub jeżeli przywrócenie towaru do stanu umożliwiającego używanie zgodnie z przeznaczeniem wymaga nadmiernych nakładów.

§ 15. W przypadku udostępnienia bez obowiązku zwrotu odbiorca rezerw staraniem własnym i na własny koszt dokonuje utylizacji lub likwidacji niewykorzystanej części rezerw, których termin ważności upłynął lub gdy nastąpiło jego zużycie techniczne.

§ 16. Rozporządzenie wchodzi w życie z dniem następującym po dniu ogłoszenia.

MINISTER SPRAW
WEWNĘTRZNYCH
I ADMINISTRACJI

UZASADNIENIE

Rozporządzenie określa szczegółową procedurę udostępnienia *rezerw strategicznych*, w tym czasowego, zwrotnego udostępnienia specjalistycznego asortymentu technicznego *rezerw strategicznych* oraz specjalistycznego asortymentu medycznego *rezerw strategicznych*, uwzględniając konieczność zapewnienia prawidłowej i efektywnej realizacji zadań Agencji, zwanej dalej „procedurą".

Procedura udostępnienia rezerw strategicznych określa czynności podejmowane przez Rządową Agencję Rezerw Strategicznych, dalej zwaną „Agencją", realizowane w procesie udostępnienia rezerw strategicznych na rzecz określonego organu, w tym czynności:

- ✓ wydania określonego asortymentu w celu użycia lub wykorzystania,
- ✓ zrealizowania określonej usługi na podstawie umowy o pozostawaniu w gotowości do świadczenia usług,
- ✓ celem zapewnienia prawidłowości, rzetelności i sprawnego realizowania powierzonych Agencji zadań oraz należytego przepływu informacji i dokumentacji pomiędzy Agencją i innymi podmiotami.

Procedurę stosuje się w przypadku udostępnienia rezerw strategicznych w drodze decyzji wydanej przez ministra właściwego do spraw wewnętrznych.

Minister właściwy do spraw wewnętrznych może wydać decyzję w formie pisemnej lub w formie dokumentu elektronicznego opatrzonego kwalifikowanym podpisem elektronicznym. Decyzja może być wydana także ustnie lub pisemnie w formie adnotacji.

W przypadku, gdy decyzja została wydana ustnie, jej istotne elementy, o których mowa w art. 19 ust. 5 ustawy o rezerwach strategicznych, powinny być stwierdzone w formie pisemnej lub dokumentowej.

Osoby wykonujące zadania określone procedurą obowiązane są działać bez zbędnej zwłoki, z zachowaniem należytej staranności i rzetelności, przestrzegając przepisów prawa powszechnie obowiązującego i obowiązujących w Agencji procedur wewnętrznych. W uzasadnionych przypadkach Prezes Agencji może delegować pracownika lub pracowników Agencji celem dokonania sprawdzenia warunków przetransportowania udostępnionych rezerw oraz ich przetrzymania.

W przypadku stwierdzenia, niedających się usunąć przed udostępnieniem rezerw, naruszeń obowiązujących przepisów prawa albo wymogów wynikających z niniejszej procedury, o których Agencja poinformowała organ lub odbiorcę, Prezes Agencji informuje ministra właściwego do spraw wewnętrznych o stwierdzonych naruszeniach oraz przedstawia propozycje dalszych działań.

Prezes Agencji, po otrzymaniu decyzji, przekazuje dyspozycję właściwej komórce organizacyjnej Agencji, prowadzącej sprawy związane z danym asortymentem rezerw.

Komórka organizacyjna Agencji weryfikuje pozostające w jej dyspozycji informacje dotyczące stanu rezerw utrzymywanych w magazynach własnych oraz u podmiotów przechowujących lub utrzymujących, uwzględniając w szczególności rodzaj asortymentu, jego ilość, rozmieszczenie i inne szczególne właściwości, a następnie wskazuje obiekty, z których udostępnienie rezerw będzie miało miejsce, określając ilość i asortyment dla poszczególnych obiektów oraz, jeżeli zachodzi taka potrzeba, wymogi w zakresie ewentualnego przetransportowania lub przetrzymania rezerw przez odbiorcę.

Agencja zapewnia przetransportowanie udostępnionych rezerw oraz organizuje inne usługi logistyczne, o ile wskazano tak w decyzji.

Agencja informuje:

- ✓ odbiorcę o podjęciu czynności mających na celu wykonanie decyzji, a w szczególności przekazuje informacje dotyczące miejsca, z którego nastąpi wydanie rezerw, o ile odbiorca będzie dokonywał odbioru rezerw we własnym zakresie lub uzyskuje informacje o miejscu dostawy, do którego rezerwy zostaną przetransportowane;
- ✓ odbiorcę o wymaganiach dotyczących właściwego przetransportowania rezerw w przypadku, gdy odbiorca organizuje przetransportowanie we własnym zakresie;
- ✓ odbiorcę o wymaganiach w zakresie ewentualnego przetrzymania rezerw - jeżeli zachodzi taka potrzeba;
- ✓ odbiorcę o jego obowiązkach wynikających z przepisów o rezerwach strategicznych oraz o uprawnieniu Agencji do dokonania sprawdzenia warunków przetransportowania rezerw oraz ich przetrzymania;
- ✓ odbiorcę o obowiązku.

Niezależnie od przekazania informacji wskazanych Agencja podejmuje czynności mające na celu przygotowanie rezerw do wydania, w szczególności uzyskuje od organu lub odbiorcy informacje dotyczące osoby lub osób upoważnionych do fizycznego odbioru rezerw oraz uzgadnia termin wydania rezerw, jeżeli nie został on określony w decyzji ministra właściwego do spraw wewnętrznych. Informacje mogą być przekazywane lub uzyskiwane w formie pisemnej lub w formie dokumentu elektronicznego opatrzonego kwalifikowanym podpisem elektronicznym. Informacje mogą być przekazywane lub uzyskiwane także ustnie, pisemnie w formie adnotacji, telefonicznie, za pomocą środków komunikacji elektronicznej w rozumieniu art. 2 pkt 5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2020 r. poz. 344) lub za pomocą innych środków łączności. W przypadku, gdy informacje zostały przekazane lub uzyskane ustnie lub telefonicznie, ich treść powinna być stwierdzona w formie pisemnej lub dokumentowej.

Agencja sporządza „Polecenie wydania". „Polecenie wydania" może być sporządzone w formie pisemnej lub w formie dokumentu elektronicznego opatrzonego kwalifikowanym podpisem elektronicznym. „Polecenie wydania" może być sporządzone także ustnie, pisemnie w formie adnotacji, telefonicznie, za pomocą środków komunikacji elektronicznej w rozumieniu art. 2 pkt 5 ustawy o świadczeniu usług drogą elektroniczną lub za pomocą innych środków łączności. W przypadku, gdy „Polecenie wydania" zostało wydane ustnie lub telefonicznie, jego istotne elementy powinny być stwierdzone w formie pisemnej lub dokumentowej.

Rezerwy mogą być wydane wyłącznie osobom uprawnionym do reprezentowania organu lub odbiorcy wskazanego w decyzji. Organ lub odbiorca wskazany w decyzji zobowiązany jest przekazać Agencji w formie pisemnej lub dokumentowej upoważnienie do odbioru.

Z wydania rezerw sporządza się „Protokół wydania", który jest podpisywany przez przedstawiciela Agencji oraz odbierającego rezerwy. Jeden egzemplarz „Protokołu wydania" przekazywany jest odbierającemu rezerwy.

Sporządza się odrębne protokoły wydania, jeżeli udostępnienie rezerw i ich wydanie następuje dla wielu podmiotów lub z wielu magazynów.

W przypadku transportowania rezerw przez podmiot trzeci, działający na podstawie zlecenia Agencji, „Protokół wydania" podpisywany jest wyłącznie przez umocowanego przedstawiciela Agencji. Potwierdzenie odbioru udostępnionych odbiorcy rezerw stanowi list przewozowy.

W przypadkach uzasadnionych szczególnymi okolicznościami nie sporządza się „Protokołu wydania". W takim przypadku wydanie rezerw z magazynu dokumentuje się podpisem na dokumencie magazynowym wydania zewnętrznego (WZ) lub na innym dokumencie. W przypadku wydania rezerw odbiorcom zagranicznym, Agencja zobowiązana jest do przygotowania wszystkich niezbędnych dokumentów wymaganych w międzynarodowym obrocie towarami oraz do zapewnienia zgodności tych dokumentów z przepisami celnymi.

Szczegółowe zasady postępowania w przypadku udostępnienia rezerw, w szczególności ich wydania przez podmioty przechowujące, przez podmioty utrzymujące rezerwy lub podmioty utrzymujące zdolności produkcyjne bądź pozostające w gotowości do świadczenia usług, określają odpowiednio umowy: przechowania, utrzymywania, o utrzymywaniu zdolności produkcyjnych oraz o pozostawaniu w gotowości do świadczenia usług.

W przypadku, w którym decyzja ministra właściwego do spraw wewnętrznych zobowiązuje Agencję do zapewnienia przetworzenia rezerw przed ich wydaniem, właściwa komórka organizacyjna Agencji określa zasady oraz tryb i miejsce przetworzenia rezerw, zgodnie z treścią decyzji, z właściwością surowców lub półproduktów, stosownie do zawartych umów przechowania lub umów utrzymywania rezerw, jeżeli zawierają takie postanowienia, lub umów zawartych z innymi podmiotami uprawnionymi do prowadzenia procesu przetworzenia, jeżeli takie umowy zawarto.

W przypadku stwierdzenia przeszkody w wykonaniu decyzji, w zakresie zapewnienia przez Agencję przetworzenia rezerw, wynikającej w szczególności z obowiązujących przepisów prawa, w tym określających nakazy uzyskania stosownych zezwoleń, decyzji lub przeprowadzenia innych czynności, wprowadzających zakazy wprowadzania do obrotu określonych towarów, nakładających obowiązek przeprowadzenia postępowań mających na celu wyłonienie podmiotów uprawnionych do przeprowadzenia określonych czynności oraz zawarcia z nimi umowy – Prezes Agencji informuje ministra właściwego do spraw wewnętrznych o stwierdzonej przeszkodzie w wykonaniu decyzji oraz przedstawia propozycje dalszych działań.

Kolejne czynności podejmowane są przez Agencję po wskazaniu przez ministra właściwego do spraw wewnętrznych dalszego sposobu postępowania w związku ze stwierdzeniem przeszkody w wykonaniu decyzji.

W przypadku udostępnienia rezerw z obowiązkiem zwrotu udostępnienie następuje na podstawie umowy zawartej w formie pisemnej pomiędzy Agencją a podmiotem, któremu udostępnione rezerwy zostały wydane.

W szczególnie uzasadnionych przypadkach wydanie rezerw może nastąpić przed sporządzeniem i podpisaniem umowy, o której mowa w ust. 1. W takim przypadku umowa na piśmie zostanie sporządzona i podpisana niezwłocznie, nie później niż w terminie 30 dni od dnia wydania rezerwy.

W przypadku zwrotu niewykorzystanej części udostępnionych rezerw, Agencja po uzyskaniu od odbiorcy lub organu informacji o zamiarze zwrotu niewykorzystanej części rezerw, uzgadnia z odbiorcą lub organem szczegółowe warunki zwrotu.

Agencja może sprawdzić warunki przetrzymania rezerw lub zażądać udokumentowania warunków przetrzymania rezerw, jak również dokonać oceny, czy spełnione są inne wymagania określone w stosunku do jakości i innych właściwości rezerw.

Na podstawie informacji, o których mowa w ust. 1, Agencja uzgadnia z odbiorcą lub organem termin oraz sposób przetransportowania niewykorzystanej części udostępnionych rezerw do miejsca wskazanego przez Agencję.

Agencja odmawia przyjęcia zwrotu, jeżeli stan towaru nie pozwala na jego ponowne wprowadzenie na stan rezerw lub jeżeli przywrócenie towaru do stanu umożliwiającego używanie zgodnie z przeznaczeniem wymaga nadmiernych nakładów.

W przypadku udostępnienia bez obowiązku zwrotu odbiorca rezerw staraniem własnym i na własny koszt dokonuje utylizacji lub likwidacji niewykorzystanej części rezerw, których termin ważności upłynął lub gdy nastąpiło jego zużycie techniczne.

Projektowane rozwiązania wejdą w życie po upływie 14 od dnia ogłoszenia

Projekt rozporządzenia nie podlega notyfikacji zgodnie z przepisami dotyczącymi funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych.

Projekt rozporządzenia nie jest sprzecznym 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.

Nazwa projektu Rozporządzenie Ministra Spaw Wewnętrznych i Administracji w sprawie szczegółowej procedury udostępniania rezerw strategicznych **Ministerstwo wiodące i ministerstwa współpracujące** **Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu** **Kontakt do opiekuna merytorycznego projektu**	**Data sporządzenia** 19.05.2025 r. **Źródło:** **Nr w wykazie prac …….**

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

W celu efektywnego i transparentnego dysponowania rezerwami strategicznymi niezbędna jest procedura ich udostępniania.

2. Rekomendowane rozwiązanie, w tym planowane narzędzia interwencji, i oczekiwany efekt

Rozporządzenie określa szczegółową procedurę udostępnienia *rezerw strategicznych*, w tym czasowego, zwrotnego udostępnienia specjalistycznego asortymentu technicznego *rezerw strategicznych* oraz specjalistycznego asortymentu medycznego *rezerw strategicznych*, uwzględniając konieczność zapewnienia prawidłowej i efektywnej realizacji zadań Agencji, zwanej dalej „procedurą”.

3. Jak problem został rozwiązany w innych krajach, w szczególności krajach członkowskich OECD/UE?

4. Podmioty, na które oddziałuje projekt

Grupa	Wielkość	Źródło danych	Oddziaływanie
(dodaj/usuń)			
(dodaj/usuń)			
(dodaj/usuń)			
(dodaj/usuń)			
(dodaj/usuń)			

5. Informacje na temat zakresu, czasu trwania i podsumowanie wyników 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												
budżet państwa												
JST												
pozostałe jednostki (oddzielnie)												
Wydatki ogółem												
budżet państwa												
JST												
pozostałe jednostki (oddzielnie)												
Saldo ogółem												
budżet państwa												
JST												
pozostałe jednostki (oddzielnie)												

Źródła finansowania	
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							
	(dodaj/usuń)							
W ujęciu niepieniężnym	duże przedsiębiorstwa							
	sektor mikro-, małych i średnich przedsiębiorstw							
	rodzina, obywatele oraz gospodarstwa domowe							
	(dodaj/usuń)							
Niemierzalne	(dodaj/usuń)							
	(dodaj/usuń)							

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:	☐ zwiększenie liczby dokumentów ☐ zwiększenie liczby procedur ☐ wydłużenie czasu na załatwienie sprawy ☐ inne:
Wprowadzane obciążenia są przystosowane do ich elektronizacji.	☐ tak ☐ nie ☐ nie dotyczy

Komentarz:

9. Wpływ na rynek pracy

10. Wpływ na pozostałe obszary

☐ środowisko naturalne ☐ sytuacja i rozwój regionalny ☐ sądy powszechne, administracyjne lub wojskowe	☐ demografia ☐ mienie państwowe ☐ inne:	☐ informatyzacja ☐ zdrowie

Omówienie wpływu	

11. Planowane wykonanie przepisów aktu prawnego

12. W jaki sposób i kiedy nastąpi ewaluacja efektów projektu oraz jakie mierniki zostaną zastosowane?

13. Załączniki (istotne dokumenty źródłowe, badania, analizy itp.)

Projekt

R O Z P O R Z Ą D Z E N I E

R A D Y M I N I S T R Ó W

z dnia

w sprawie minimalnych wymagań w zakresie bezpieczeństwa fizycznego, technicznego, osobowego, cyberbezpieczeństwa, prawnego oraz ciągłości działania infrastruktury krytycznej

Na podstawie art. 6ze ust. 4 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym zarządza się, co następuje:

§ 1. Minimalne wymagania w zakresie bezpieczeństwa fizycznego, technicznego, osobowego, cyberbezpieczeństwa, prawnego oraz ciągłości działania, niezbędne do wdrażania rozwiązań w zakresie ochrony infrastruktury krytycznej, są określone w załączniku do rozporządzenia.

§ 2. Rozporządzenie wchodzi w życie po upływie 14 dni od ogłoszenia.

P R E Z E S R A D Y M I N I S T R Ó W

Załącznik
do rozporządzenia Rady Ministrów
z dnia
Dz. U. poz.

Minimalne wymagania w zakresie bezpieczeństwa fizycznego, technicznego, osobowego, cyberbezpieczeństwa, prawnego oraz ciągłości działania infrastruktury krytycznej

Bezpieczeństwa fizyczne

1. W ramach bezpieczeństwa fizycznego operator:
   1) zapewnia bezpośrednią ochronę fizyczną (osobową),
   2) instaluje i utrzymuje systemy zabezpieczeń technicznych (SZT),
   3) wprowadza zabezpieczenia mechaniczne i budowlane.

3. Rozwiązania proceduralne bezpieczeństwa fizycznego IK polegają na:
   1) stosowaniu działań prewencyjnych;
   2) zapewnieniu możliwie najwcześniejszego wykrycia intruza;
   3) przekazywaniu informacji o wykryciu intruza, w tym alarmowaniu;
   4) stosowaniu środków spowalniających dotarcie intruza do stref chronionych;
   5) podejmowaniu interwencji przez personel ds. ochrony infrastruktury krytycznej w celu zapewnienia bezpieczeństwa obiektu oraz rejestracji zdarzeń.

4. W celu zapewnienia skutecznej ochrony operator integruje systemy bezpośredniej ochrony fizycznej z systemami zabezpieczeń technicznych (SZT).

5. Operator zapewnia wdrożenie systemu bezpieczeństwa fizycznego IK w sposób systemowy i udokumentowany, obejmujący w szczególności:
   1) identyfikację i ustalenie chronionych zasobów;
   2) przyjęcie podstawowych założeń projektowych dla systemu bezpieczeństwa fizycznego, w tym określenie potencjalnych intruzów oraz charakterystyki ich działania, z uwzględnieniem przewidywanych scenariuszy ataków;

3) ocenę możliwości wyeliminowania przewidywanych scenariuszy ataków, a w przypadkach, gdy nie jest to możliwe – określenie niezbędnych czasów spowolnienia działania potencjalnych intruzów, powiązanych z rzeczywistym czasem interwencji sił bezpośredniej ochrony fizycznej;

4) ustalenie chronionych obszarów i stref oraz zasad dostępu do nich;

5) przeprowadzenie szacowania ryzyka w celu doboru adekwatnych systemów zabezpieczeń technicznych, z uwzględnieniem zabezpieczeń mechanicznych i budowlanych;

6) dobór systemów zabezpieczeń technicznych, z uwzględnieniem zabezpieczeń mechanicznych i budowlanych;

7) opracowanie procedur reagowania uwzględniających specyfikę chronionych obiektów oraz rodzaj identyfikowanych zagrożeń;

8) zapewnienie przeszkolenia personelu ds. ochrony infrastruktury krytycznej w zakresie podejmowania właściwych działań dla identyfikowanych zagrożeń;

9) instalację i konfigurację systemów zabezpieczeń technicznych;

10) testowanie systemów zabezpieczeń technicznych oraz całego systemu bezpieczeństwa fizycznego IK;

11) przegląd i korektę procedur;

12) systematyczne przeglądy systemu bezpieczeństwa fizycznego IK, obejmujące w szczególności kontrole działania, konserwacje oraz usuwanie zdiagnozowanych niesprawności, a w przypadkach gdy nie jest to możliwe – stosowanie środków zastępczych o parametrach umożliwiających utrzymanie funkcjonowania systemu zgodnie z dokumentacją powykonawczą;

13) systematyczny audyt lub certyfikację zainstalowanych systemów zabezpieczeń technicznych na zgodność z właściwymi Polskimi Normami.

6. Operator zapewnia kontrolę osób oraz ładunków przemieszczających się do i z obszaru chronionego infrastruktury krytycznej.

7. Kontrola, o której mowa w pkt. 6 obejmuje w szczególności pracowników operatora, kontrahentów, dostawców, wykonawców, podwykonawców oraz gości.

8. Operator określa zasady kontroli osób i ładunków w procedurach wewnętrznych, obejmujących w szczególności zasady wejścia, wjazdu, wyjścia i wyjazdu do i z obiektu oraz stref ochronnych, a także zasady poruszania się po obszarze chronionym.
9. Procedury, o których mowa w pkt. 8, uwzględniają przypadki stosowania odrębnych zasad wobec określonych osób lub grup osób, jeżeli operator dopuszcza takie rozwiązania.
10. Kontrola ładunków przemieszczających się do i z obszaru chronionego może być prowadzona w sposób pełny lub wyrywkowy, w zależności od wyników oceny ryzyka oraz poziomu zagrożenia, przy uwzględnieniu przepisów Ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (Dz.U. 2025 poz. 194).
11. Poruszanie się gości po obszarze chronionym odbywa się pod nadzorem osoby upoważnionej przez operatora, od momentu wejścia do chwili opuszczenia obiektu, jeżeli operator nie określi inaczej w procedurach.
12. Operator zapewnia zarządzanie dostępem do stref ochrony poprzez nadawanie, zmianę oraz cofanie uprawnień dostępu, w szczególności z wykorzystaniem:
    1) przepustek (identyfikatorów lub kart dostępu);
    2) kodów dostępu, w tym kodów pierwszego logowania;
    3) kluczy do pomieszczeń lub obszarów chronionych.
13. Operator określa zasady:
    1) wydawania, ewidencjonowania i odbierania przepustek, identyfikatorów, kart i kluczy;
    2) przechowywania kluczy oraz zarządzania kodami dostępu;
    3) okresowej weryfikacji oraz aktualizacji uprawnień dostępu.
14. Przepustki, identyfikatory lub karty dostępu podlegają indywidualizacji oraz ewidencjonowaniu w sposób umożliwiający identyfikację osoby uprawnionej.
15. Operator zapewnia, aby przepustki, identyfikatory lub karty dostępu posiadały zabezpieczenia utrudniające ich przerabianie lub nieuprawnione wykorzystanie.
16. Przepustki stałe oraz okresowe umożliwiające samodzielne poruszanie się po obszarze chronionym umożliwiają jednoznaczną identyfikację ich posiadacza.

17. Przepustki jednorazowe mogą być wydawane na czas określony i podlegają zwrotowi po opuszczeniu obszaru chronionego. Operator zapewnia rozwiązania uniemożliwiające ich wykorzystanie po upływie okresu ważności.
18. Przepustki nie zawierają informacji, których ujawnienie mogłoby ułatwić ich nieuprawnione wykorzystanie w przypadku utraty.
19. Operator stosuje środki techniczne służące identyfikacji i weryfikacji osób wchodzących do obiektów infrastruktury krytycznej, w tym rozwiązania biometryczne, jeżeli jest to uzasadnione oceną ryzyka.
20. Stosowanie środków, o których mowa w pkt. 19, uwzględnia zasadę proporcjonalności oraz zakres niezbędny do zapewnienia bezpieczeństwa fizycznego infrastruktury krytycznej.
21. Operator zapewnia doraźną lub stałą bezpośrednią ochronę fizyczną infrastruktury krytycznej, jeżeli wynika to z oceny zagrożeń oraz charakterystyki chronionej infrastruktury krytycznej.
22. Wymogu stałej bezpośredniej ochrony fizycznej nie stosuje się dla obiektów liniowych (rurociągi, linie energetyczne, drogi i linie kolejowe) oraz obiektów bez stałej obsługi.
23. Bezpośrednia ochrona fizyczna może być realizowana przez operatora w formie Wewnętrznej Służby Ochrony albo zapewniana przez podmiot zewnętrzny posiadający koncesję na prowadzenie działalności gospodarczej w zakresie usług ochrony osób i mienia.
24. Operator zapewnia, aby pracownicy ochrony fizycznej posiadali broń na podstawie świadectwa broni, o którym mowa w art. 29 ust. 1 pkt 1 i 2 ustawy z dnia 21 maja 1999 r. o broni i amunicji (Dz. U. z 2024 r. poz. 485), jeżeli wynika to z oceny zagrożeń.
25. Operator zapewnia fizyczną barierę oddzielającą strefę zewnętrzną od pozostałych stref ochronnych infrastruktury krytycznej.
26. Fizyczna bariera, o której mowa w pkt. 25, stanowi element systemu bezpieczeństwa fizycznego IK i ma na celu istotne utrudnienie nieuprawnionego przedostania się intruza do obszarów chronionych.

27. Fizyczna bariera jest realizowana w szczególności jako jeden lub kombinacja kilku elementów, którymi mogą być:
    1) ogrodzenie,
    2) ściana budynku,
    3) naturalna, ukształtowana przeszkoda terenowa lub obszar wodny,
    4) zabezpieczenie drogowe antyterrorystyczne,
    5) inny element konstrukcyjny, architektoniczny lub krajobrazowy spełniający funkcję ochronną.
28. Rozwiązania, o których mowa w pkt. 27, zapewniają odporność adekwatną do zidentyfikowanych zagrożeń oraz charakterystyki i lokalizacji chronionego obszaru.
29. W zakresie ogrodzeń, bram i furtek stosuje się przepisy rozporządzenia ministra infrastruktury z 12 kwietnia 2002 r. w sprawie warunków technicznych, jakim powinny odpowiadać budynki i ich usytuowanie (tj. Dz. U. z 2022 r. poz. 1225);
30. Operator zapewnia, aby bramy i furtki stanowiące element fizycznej bariery:
    1) odpowiadały wysokości oraz charakterystyce bariery fizycznej;
    2) uwzględniały odporność na nieuprawnione sforsowanie lub staranowanie, stosownie do wyników oceny zagrożeń;
    3) były wyposażone w środki umożliwiające kontrolę ruchu osobowego i pojazdów.
31. Operator stosuje dodatkowe zabezpieczenia wjazdów, w szczególności urządzenia zaporowe lub kontrolne, jeżeli wynika to z analizy zagrożeń.
32. Bramy i urządzenia zamykane automatycznie są wyposażone w rozwiązania uniemożliwiające ich zamknięcie w czasie trwania ruchu osobowego lub pojazdów oraz w środki ostrzegawcze.
33. Jeżeli fizyczna bariera nie spełnia wymagań wynikających z charakterystyki i lokalizacji infrastruktury krytycznej, operator zapewnia zastosowanie rozwiązań kompensacyjnych zapewniających równoważny poziom bezpieczeństwa.
34. Rozwiązania kompensacyjne mogą obejmować w szczególności:

1) systemy ochrony obwodowej;
2) systemy dozoru wizyjnego (VSS);
3) zwiększenie liczby posterunków ochrony, patroli lub innych środków organizacyjnych.

35. Fizyczna bariera jest projektowana i utrzymywana w sposób umożliwiający skuteczną integrację z systemami zabezpieczeń technicznych.
36. Operator zapewnia możliwość obserwacji fizycznej bariery oraz punktów wejścia i wjazdu do stref ochronnych.
37. Jeżeli fizyczną barierę stanowi ściana budynku, operator zapewnia, aby jej konstrukcja oraz stan techniczny zapewniały poziom ochrony nie niższy niż w przypadku ogrodzenia.
38. W przypadku drzwi lub okien stanowiących element fizycznej bariery operator zapewnia zastosowanie rozwiązań proceduralnych, technicznych lub organizacyjnych uniemożliwiających ich pozostawienie bez nadzoru.
39. Drzwi i okna, których dostępność może powodować nieakceptowalne ryzyko nieuprawnionego wejścia, zapewniają odporność adekwatną do wymaganego czasu spowolnienia potencjalnego intruza albo są zabezpieczone innymi równoważnymi rozwiązaniami.
40. Operator oznacza fizyczną barierę informacją o zakazie nieuprawnionego wstępu na obszar chroniony.
41. Operator zapewnia warunki do skutecznej obserwacji strefy zewnętrznej oraz patrolowania strefy peryferyjnej, jeżeli wynika to z charakterystyki i lokalizacji infrastruktury krytycznej.
42. Jeżeli jest to uzasadnione oceną ryzyka, operator stosuje rozwiązania umożliwiające wczesną detekcję naruszenia fizycznej bariery, w szczególności z wykorzystaniem systemów zabezpieczeń technicznych.
43. Systemy zabezpieczeń technicznych powinny być zaprojektowane, wykonane i skonfigurowane w taki sposób, aby czas pomiędzy wykryciem intruza a reakcją personelu ds. ochrony IK był krótszy niż czas potrzebny do uszkodzenia lub narażenia bezpieczeństwa zasobów IK.

44. Systemy zabezpieczeń technicznych powinny:

    1) spełniać wymagania co najmniej stopnia 3 określone w Polskiej Normie odpowiedniej dla danego systemu;

    2) wykorzystywać optymalne parametry techniczne urządzeń;

    3) funkcjonować poprawnie w przewidzianych dla nich warunkach środowiska pracy;

    4) nie utrudniać codziennej pracy personelu, przy czym sposób ich działania powinien być uzgodniony z personelem ds. ochrony IK;

    5) być wykonane w wykonaniu przeciwwybuchowym i iskrobezpiecznym – jeżeli występuje ryzyko wybuchowe,

45. Zabrania się stosowania w systemach zabezpieczeń technicznych kamer, których ustawienia fabryczne można przywrócić programowo (zdalnie) bez konieczności ingerencji fizycznej.

46. Czynności obejmujące projektowanie, instalowanie, konserwację i naprawy systemów zabezpieczeń technicznych są wykonywane przez:

    1) personel ds. ochrony infrastruktury krytycznej, lub

    2) uprawnionych usługodawców zewnętrznych.

47. Osoby wykonujące czynności, o których mowa w pkt. 46, posiadają kwalifikacje, kompetencje oraz uprawnienia odpowiednie do zakresu realizowanych czynności, a w szczególności:

    1) zaświadczenie o ukończeniu kursu pracownika zabezpieczenia technicznego wydane przez wyspecjalizowaną w tym zakresie placówkę kształcenia ustawicznego działającą w systemie oświaty;

    2) dokument potwierdzający odbycie szkolenia aktualizującego, jeśli zaświadczenie, o którym mowa w pkt. 1 zostało wydane wcześniej niż 3 lata przed rozpoczęciem czynności, o których mowa w pkt. 46;

    3) dokumenty potwierdzające ukończenie szkoleń produktowych właściwych dla zastosowanych systemów STZ;

4) inne uprawnienia niezbędne do realizacji powierzonych czynności, jeżeli wynika to z ich charakteru.

48. Operator zapewnia, aby usługodawcy zewnętrzni realizujący czynności w zakresie SZT posiadali kompetencje potwierdzone odpowiednimi certyfikatami lub innymi dokumentami, zgodnie z art. 6ze ust. 5 pkt. 1 ustawy, mając na względzie zestawienie, o którym mowa w art. 6ze ust. 6 ustawy.

49. Operator weryfikuje spełnienie wymagań, o których mowa w pkt. 47 i 48 przed rozpoczęciem realizacji czynności oraz w trakcie ich trwania.

50. Operator zapewnia przeprowadzenie szkolenia personelu ds. ochrony infrastruktury krytycznej w zakresie obsługi i eksploatacji zainstalowanych systemów zabezpieczeń technicznych.

51. Szkolenie, o którym mowa w pkt. 50, odbywa się na podstawie programu zatwierdzonego przez operatora i uwzględnia dokumentację oraz instrukcje użytkowania systemów.

52. Operator zapewnia utrzymanie uzyskanego poziomu zabezpieczenia systemów zabezpieczeń technicznych poprzez systematyczne przeglądy, konserwacje oraz naprawy.

53. Przeglądy i konserwacje przeprowadza się w okresach określonych w właściwych Polskich Normach lub dokumentacji powykonawczej systemów.

54. Operator zapewnia rozpoczęcie czynności utrzymaniowych niezwłocznie po zainstalowaniu systemów.

55. Operator prowadzi rejestr konserwacji, przeglądów technicznych i napraw obejmujący w szczególności:

    1) przeglądy, konserwacje i naprawy;

    2) modernizacje i rozbudowy systemów;

    3) awarie, uszkodzenia oraz przypadki nieprawidłowego działania systemów.

56. Przed odbiorem końcowym systemu zabezpieczeń technicznych operator zapewnia przeprowadzenie okresu próbnego działania systemu.

57. Okres próbny, o którym mowa w pkt. 56, trwa przez czas określony w dokumentacji technicznej wykonawczej, adekwatny do złożoności systemu.

58. W czasie okresu próbnego system zabezpieczeń technicznych funkcjonuje w normalnych warunkach pracy.

59. Operator zapewnia monitorowanie działania systemu w okresie próbnym przez personel ds. ochrony infrastruktury krytycznej, w szczególności w zakresie identyfikacji nieprawidłowości w jego działaniu oraz okoliczności ich występowania.

60. Zidentyfikowane w okresie próbnym nieprawidłowości są niezwłocznie zgłaszane podmiotowi, który zainstalował system, w celu ich usunięcia.

61. Po zakończeniu okresu próbnego, jeżeli nie stwierdzono nieprawidłowości w działaniu systemu zabezpieczeń technicznych lub jeżeli zostały one skutecznie usunięte, operator dokonuje odbioru końcowego systemu.

62. Odbiór końcowy systemu zabezpieczeń technicznych obejmuje w szczególności weryfikację:

    1) dokumentacji technicznej powykonawczej;

    2) zgodności zainstalowanych urządzeń i elementów z dokumentacją techniczną powykonawczą;

    3) oprogramowania systemu;

    4) posiadania ważnych licencji uprawniających do korzystania z oprogramowania;

    5) parametrów technicznych systemu zabezpieczeń technicznych oraz urządzeń wchodzących w jego skład;

    6) poprawności działania systemu oraz wszystkich jego elementów we wszystkich konfiguracjach przewidzianych dokumentacją techniczną;

    7) zdolności systemu do pracy w normalnych warunkach pracy oraz w stanie alarmu przez czas co najmniej 15 minut przy zasilaniu podstawowym;

    8) zdolności systemu do pracy w normalnych warunkach pracy oraz w stanie alarmu przez czas co najmniej 15 minut przy zasilaniu rezerwowym, przez okres określony dla tego źródła zasilania, bez zaniku napięcia;

9) jakości wykonanych prac, w tym sposobu wykonania połączeń wewnętrznych oraz oznakowania elementów systemu, kabli i przewodów.

63. Jeżeli system zabezpieczeń technicznych został poddany certyfikacji i uzyskał certyfikat zgodności z właściwą dla danego systemu zabezpieczeń Polską Normą, wydany przez właściwą w tym zakresie jednostkę certyfikującą, odbioru końcowego, o którym mowa w pkt. 62 lit. a–i nie przeprowadza się.

64. W przypadku, o którym mowa w pkt. 63, podstawą odbioru systemu zabezpieczeń technicznych jest certyfikat zgodności.

65. Jeżeli certyfikacja systemu zabezpieczeń technicznych jest podstawą odbioru końcowego tego systemu, operator zapewnia przeprowadzenie oceny zgodności dokumentacji wykonawczej systemu przed rozpoczęciem procesu certyfikacji.

66. Ocenę zgodności dokumentacji wykonawczej, o której mowa w pkt. 65, przeprowadza jednostka certyfikująca realizująca certyfikację systemu zabezpieczeń technicznych.

67. Ocena zgodności dokumentacji wykonawczej obejmuje w szczególności weryfikację:

1) zgodności przyjętych rozwiązań projektowych z właściwymi Polskimi Normami;

2) spójności dokumentacji wykonawczej z wynikami oceny zagrożeń przeprowadzonej dla infrastruktury krytycznej;

3) kompletności i jednoznaczności dokumentacji wykonawczej w zakresie niezbędnym do certyfikacji systemu.

68. Stwierdzenie niezgodności w dokumentacji wykonawczej skutkuje obowiązkiem ich usunięcia przed kontynuowaniem procesu certyfikacji systemu zabezpieczeń technicznych.

69. Wyniki oceny zgodności dokumentacji wykonawczej stanowią element dokumentacji procesu certyfikacji systemu zabezpieczeń technicznych.

70. Operator zapewnia funkcjonowanie systemu transmisji alarmów oraz alarmowego centrum odbiorczego, stanowiących element systemu bezpieczeństwa fizycznego infrastruktury krytycznej.

71. Obowiązki, o których mowa w pkt. 70, operator realizuje:

1) w ramach własnych struktur organizacyjnych, albo

2) poprzez powierzenie ich wykonywania uprawnionemu podmiotowi zewnętrznemu, w szczególności koncesjonowanemu podmiotowi wykonującemu działalność gospodarczą w zakresie usług ochrony osób i mienia.

72. Powierzenie wykonywania obowiązków podmiotowi zewnętrznemu nie zwalnia operatora z odpowiedzialności za zapewnienie bezpieczeństwa fizycznego infrastruktury krytycznej.

73. System transmisji alarmów zapewnia przekazywanie informacji o stanie systemów alarmowych z obiektów infrastruktury krytycznej do alarmowego centrum odbiorczego.

74. Transmisja informacji alarmowych jest realizowana w sposób ciągły, niezawodny i bezpieczny, adekwatnie do poziomu ryzyka, charakterystyki oraz lokalizacji chronionej infrastruktury krytycznej.

75. System transmisji alarmów zapewnia redundancję, w szczególności poprzez zastosowanie co najmniej dwóch niezależnych torów transmisji.

76. Przekazywanie informacji alarmowych odbywa się z potwierdzeniem odbioru oraz umożliwia bieżący nadzór nad dostępnością transmisji.

77. Przerwanie transmisji alarmowej lub utrata łączności z obiektem chronionym jest traktowana jako zdarzenie o charakterze technicznym albo sabotażowym i podlega procedurom reagowania.

78. Funkcjonowanie systemu transmisji alarmów podlega bieżącemu nadzorowi, analizie dostępności oraz dokumentowaniu, a zapisy dotyczące jego pracy są przechowywane przez okres umożliwiający ocenę ciągłości i niezawodności działania.

79. Alarmowe centrum odbiorcze zapewnia całodobowe przyjmowanie, przetwarzanie i obsługę sygnałów alarmowych.

80. Alarmowe centrum odbiorcze może być zlokalizowane w obiekcie operatora albo funkcjonować jako wyodrębniona jednostka organizacyjna podmiotu zewnętrznego realizującego zadania ochrony fizycznej.

81. Operator zapewnia ciągłość funkcjonowania alarmowego centrum odbiorczego poprzez utrzymywanie zapasowego alarmowego centrum odbiorczego, zlokalizowanego w innym miejscu niż centrum podstawowe.
82. Centrum monitorowania alarmów funkcjonuje w pomieszczeniach zabezpieczonych przed nieuprawnionym dostępem oraz zdarzeniami mogącymi zakłócić jego pracę i jest objęte systemami zabezpieczeń technicznych.
83. Informacje o stanie bezpieczeństwa centrum monitorowania alarmów są przekazywane do innego, niezależnego centrum monitorowania.
84. Centrum monitorowania alarmów posiada zasilanie rezerwowe umożliwiające jego nieprzerwaną pracę przez okres odpowiadający wymaganiom ciągłości działania infrastruktury krytycznej.
85. Obsługa zdarzeń alarmowych obejmuje ciągłe monitorowanie sygnałów z chronionych obiektów oraz podejmowanie działań adekwatnych do rodzaju zdarzenia.
86. Operator zapewnia priorytetyzację obsługi zdarzeń alarmowych, w szczególności w odniesieniu do zdarzeń o charakterze napadu, włamania, sabotażu lub awarii technicznej.
87. Postępowanie z informacjami alarmowymi odbywa się zgodnie z zatwierdzonymi procedurami, spójnymi z planem ochrony chronionego obiektu.
88. Operator zapewnia możliwość niezwłocznego dysponowania grupami interwencyjnymi oraz skuteczną koordynację działań interwencyjnych z wykorzystaniem odpowiednich środków łączności.
89. Gotowość operacyjna grup interwencyjnych podlega bieżącemu nadzorowi, w tym monitorowaniu ich stanu i dostępności.
90. Personel centrum monitorowania alarmów posiada kwalifikacje i uprawnienia adekwatne do realizowanych zadań.
91. Obsługa centrum monitorowania alarmów odbywa się z zachowaniem zasad identyfikacji i autoryzacji użytkowników oraz rejestracji podejmowanych działań.
92. Komunikacja związana z obsługą zdarzeń alarmowych podlega rejestracji i archiwizacji przez okres umożliwiający analizę zdarzeń oraz prowadzenie postępowań wyjaśniających krótszy niż 6 miesięcy.

Bezpieczeństwo techniczne

1. W ramach bezpieczeństwa technicznego operator:
    1) prowadzi analizę ryzyka operacyjnego związanego z zawodnością urządzeń, instalacji technologicznych oraz systemów organizacyjnych;
    2) wdraża zintegrowane zarządzanie bezpieczeństwem technicznym obiektu IK obejmujące:
        a) nośność i stateczność konstrukcji,
        b) bezpieczeństwo pożarowe,
        c) higienę, zdrowie i środowisko,
        d) bezpieczeństwo użytkowania i dostępność,
        e) ochronę przed hałasem,
        f) oszczędność energii i izolacyjność cieplną,
        g) zrównoważone wykorzystania zasobów naturalnych;
    3) analizuje potencjalne zakłócenia dla niezawodności technicznej poszczególnych instalacji i wdraża środki ponoszące niezawodność poprzez:
        a) redundancję urządzeń,
        b) skracanie czasu naprawy,
        c) stały nadzór lub monitoring stanu technicznego,
        d) dobór elementów składowych o podwyższonej jakości.
    4) zapewnia zdolność serwisową poprzez:
        a) remonty zapobiegawcze planowane,
        b) remonty wyznaczone na podstawie analizy stanu technicznego;
    5) ogranicza możliwość powstania uszkodzeń IK na skutek zaniku zaopatrzenia w wodę i czynniki chłodzące, przerwanie transmisji danych albo braku energii elektrycznej;
    6) zapewnia podtrzymanie zasilania w energię elektryczną zgodnie ze wzorem: czas podtrzymania = 4 godziny + czas przygotowania kopi danych (backup) + czas niezbędny do bezpiecznego zamknięcia procesów;
    7) w celu utrzymania zarządzania bezpieczeństwem technicznym obiektu IK wyznacza lokalizację zapasową.
2. Wymóg zapewnienia awaryjnego zasilania w energie elektryczną nie dotyczy jednostek wytwórczych w rozumieniu prawa energetycznego oraz obiektów IK, dla których 8 godzinna przerwa w dostawach energii elektrycznej nie wpływa na ciągłość działania.
3. Zawierając umowy serwisowe operator określa dopuszczalny czas reakcji serwisu (umowy SLA).

Bezpieczeństwo osobowe

1. W ramach bezpieczeństwa osobowego operator:

1) posiada opracowaną, wdrożoną i poddawaną okresowym przeglądom politykę bezpieczeństwa osobowego;
2) zdefiniował role i odpowiedzialności oraz przydzielił uprawnienia w obszarze bezpieczeństwa osobowego;
3) prowadzi analizę ryzyka związaną z możliwym negatywnym oddziaływaniem na bezpieczeństwo IK własnego personelu i usługodawców;
4) posiada procedurę ustalania tożsamości osób przed dopuszczeniem do pracy;
5) dokonuje weryfikacji kwalifikacji i kompetencji personelu związanego z funkcjonowaniem IK;
6) posiada i stosuje procedurę sprawdzania przeszłości kryminalnej kandydatów i pracowników związanych z funkcjonowaniem IK;
7) udziela dostępu do pomieszczeń, systemów i informacji wyłącznie w zakresie niezbędnym do wykonywania obowiązków;
8) posiada procedury udzielania czasowego dostępu do pomieszczeń, systemów i informacji dla usługobiorców realizujących czynności serwisowe i naprawcze;
9) zapewnia jednoznaczną identyfikację wizualną personelu związanego z IK (identyfikatory, przepustki, odróżnienie pracowników, gości, podwykonawców);
10) organizuje okresowo szkolenia dla personelu w zakresie bezpieczeństwa fizycznego, technicznego, osobowego, prawnego i ciągłości działania adekwatnie do ról realizowanych w organizacji.

2. W przypadku powierzania części procesów związanych z funkcjonowaniem IK podwykonawcom operator posiada uregulowanie w umowach z usługodawcami zewnętrznymi wymagania bezpieczeństwa osobowego (weryfikacja personelu, szkolenia, zasady dostępu, odpowiedzialność).
3. W umowach operator posiada uregulowane zagadnienia związane z dostępem do obiektów, w tym zasady dostępu zdalnego oraz szczegółowe wymagania co do kompetencji pracowników podwykonawcy lub usługobiorcy wynikające z charakterystyki IK.
4. Operator posiada procedury reagowania w zakresie:
   1) niezwłocznego zwrotu wszystkich aktywów przekazanych pracownikowi (sprzęt, identyfikatory, karty dostępu, dokumenty, nośniki, urządzenia MFA) w przypadku rozwiązania umowy o pracę lub umowy z podwykonawcą lub usługodawcą;
   2) niezwłocznego zablokowania uprawnień i dostępów (fizycznych i teleinformatycznych), zmianę haseł/kodów wspólnych, aktualizację rejestrów dostępu) w przypadku zaistnienia zagrożenia lub incydentu związanego z działalnością pracownika podwykonawcy lub usługodawcy.
5. Operator minimum raz do roku i po każdej zmianie stanowiska przeprowadza weryfikację, czy uprawnienia i dostępy przyznane pracownikowi pozostają adekwatne do aktualnie realizowanych obowiązków.

Cyberbezpieczeństwo w zakresie przetwarzania i przechowywania informacji

1. W ramach cyberbezpieczenstwa w zakresie przetwarzania i przechowywania informacji operator:
    1) przydziela uprawnienia i okresowo weryfikuje poprawność przydzielonych uprawnień do zasobów i usług teleinformatycznych wyłącznie w zakresie wykonywanych obowiązków służbowych;
    2) chroni tożsamość osób posiadających uprawnienia do zasobów i usług teleinformatycznych poprzez dwuetapową identyfikację, a w przypadku dostępu zdalnego i dostępu do kluczowych zasobów stosuje rozwiązania oparte o klucze sprzętowe FIDO2;
    3) chroni dostęp do zasobów poprzez logiczny lub fizyczny podział sieci na segmenty i stosuje kontrolę przepływu danych pomiędzy poszczególnymi segmentami;
    4) stosuje szyfrowanie danych wrażliwych przesyłanych wewnątrz sieci i wszystkich danych przesyłanych poza sieć wewnętrzną;
2. zapewnia możliwość odzyskania danych poprzez proces backupu przy założeniu, że wykonywane są minimum 3 kopie, które są przechowywane w minimum 2 różnych lokalizacjach z czego jedna jest przechowywana poza siedzibą podmiotu lub w chmurze obliczeniowej.

Cyberbezpieczeństwo systemów sterowania przemysłowego

1. W ramach cyberbezpieczenstwa systemów sterowania przemysłowego operator:
    1) ogranicza dostęp do kodów, aplikacji i sieci zarządzających urządzeniami i systemami sterowania przemysłowego wyłącznie do osób, które muszą taki dostęp posiadać ze względu na realizowane obowiązki służbowe;
    2) w przypadku podwykonawców i serwisantów udziela wyłącznie czasowego dostępu do systemów sterowania przemysłowego po wcześniejszej weryfikacji danych osoby ubiegającej się o taki dostęp;
    3) ewidencjonuje dane osoby, które taki dostęp otrzymały, czas udzielenia dostępu i czynności wykonywane w okresie udzielenia dostępu;
    4) stosuje rozwiązania techniczne lub organizacyjne eliminujące możliwość przełamania ochrony sieci OT przez nośniki i urządzenia wykorzystywane przez podwykonawców i serwisantów;
    5) zapewnia fizyczną separację systemów IT i OT z wykorzystaniem bram jednokierunkowych na potrzeby badania stanu sieci OT i zbierania danych generowanych w ramach tej sieci;
    6) przechowuje kody źródłowe służące do sterowania urządzeniami OT oraz kolejne wersje tych kodów i możliwością przywrócenia ostatniej poprawnie działającej wersji;
    7) przechowuje we własnych zasobach dane generowane przez urządzenia OT;
    8) zapewnia zdolności do analizy danych generowanych przez urządzenia OT.

2. W przypadku powierzenia obsługi urządzeń i systemów sterowania przemysłowego (OT) podmiotowi zewnętrznemu operator:
    1) w oparciu o zawartą umowę lub w oparciu o postanowienia rozporządzenia Parlamentu Europejskiego i Rady (UE) 2023/2854 (tzw. Data Act) żąda od usługodawcy wszelkich danych generowanych przez urządzenia i sieci OT i przechowuje te dane we własnych zasobach;
    2) zapewnia zdolność do analizy zgromadzonych danych w oparciu o zasoby własne lub zasoby innego podmiotu niż podmiot, któremu powierzono obsługę urządzeń i systemów OT;
    3) w zawartej umowie gwarantuje, że po jej zakończeniu i w razie zaprzestania jej dalszej realizacji niezależnie od przyczyny, podmiot któremu powierzono obsługę urządzeń i systemów sterowania przemysłowego nie będzie miał prawa do naruszenia poufności, integralności ani dostępności danych generowanych przez OT;
    4) wdraża mechanizmy czasowego dostępu do systemów sterowania przemysłowego po wcześniejszej weryfikacji danych osoby ubiegającej się o taki dostęp i po wcześniejszym zarchiwizowaniu danych, które mogą być zmieniane za skutek udzielonego dostępu.
3. W przypadku stosowania lokalnych pulpitów operatorskich (Human Machine Interface -HMI) operator chroni je przed nieupoważnionym dostępem fizycznym, ogranicza ich funkcjonalność wyłącznie do interfejsów użytkownika i blokuje możliwość dostępu do portów fizycznych urządzenia.
4. Jeżeli do sterowania wykorzystywana jest sieć bezprzewodowa operator separuje tę sieć od pozostałych sieci wewnętrznych, szyfruje transmisję danych, wyłącza rozgłaszanie SSID (service set identifier), blokuje dostęp do sieci poprzez mechanizm dozwolonych adresów MAC oraz ogranicza zasięg sieci wyłącznie do stref, gdzie dostęp do sieci jest wymagany.

Cyberbezpieczeństwo przetwarzania danych w chmurze obliczeniowej

1. W ramach cyberbezpieczeństwa przetwarzania danych w chmurze obliczeniowej operator w zawieranej umowie z dostawcą usługi przestrzega zastępujących zasad:
    1) dostawca chmury publicznej jest przedsiębiorstwem zlokalizowanym w UE;
    2) prawo właściwe dla umowy z dostawcą chmury publicznej musi być prawem polskim lub innego kraju członkowskiego Unii Europejskiej;
    3) dane pozostają wyłączną własnością i pod kontrolą operatora IK;
    4) dane są szyfrowane zarówno w spoczynku, jak i podczas transmisji;
    5) dostawca zapewnia wybór lokalizacji danych (centrum lub centra przetwarzania danych, także w postaci tzw. regionu);

6) dostawca dla konkretnej usługi chmurowej posiada system zarządzania bezpieczeństwem informacji opracowany zgodnie z normą ISO 27001, wraz z ważnym certyfikatem wydanym przez akredytowany podmiot;
7) dostawca posiada plan ciągłości działania potwierdzony ważnym certyfikatem zgodności z normą ISO 22301, którego zakres obejmuje konkretną usługę;
8) dostawca zapewnia kontraktowo standard dostępności rozwiązania chmurowego na poziomie co najmniej 99%;
9) dostawca zapewnia kontraktowo odpowiedzialność za swoich poddostawców (pod przetwarzających), a ich lista jest dostępna;
10) dostawca zapewnia kontraktowo proces zgłaszania incydentów bezpieczeństwa;
11) dostawca zapewnia bezpośrednie wsparcie techniczne w Polsce.

2. Na wypadek zagrożenia utraty własnych obiektów, w których przetwarzane są dane (wzrost ryzyka związanego z możliwością ataku kinetycznego) operator posiada i okresowo aktualizuje Plan Ewakuacji do Chmury Obliczeniowej.
3. Operator posiada umowę z podmiotem lub ekspertami zewnętrznymi na wypadek konieczności odbudowy zasobów po incydencie cyber. W umowie operator określa warunki przestrzegania bezpieczeństwa osobowego (weryfikacja personelu), zasady ochrony informacji niejawnych (wymagane poświadczenia) oraz zasady udzielania czasowego dostępu niezbędnego do usunięcia następstw incydentu.
4. Operator posiada i stale aktualizuje plan lub plany reakcji na incydent cyber. Plany uwzględniają komunikację z podmiotami zewnętrznymi, w tym Policją i innymi służbami, dostawcami usług sieciowych, właściwym Zespołem Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT) oraz mediami.

Bezpieczeństwo prawne

1. W ramach bezpieczeństwa prawnego operator zapewnia:
   1) zgodność procesów ochrony IK z przepisami prawa;
   2) chroni kluczowe zasoby IK przed działaniami prawnymi innych podmiotów.
2. W zakresie zgodności z przepisami operator:
   1) posiada wdrożony mechanizm systematycznej identyfikacji nowych i zmieniających się przepisów, wytycznych, standardów, regulacji oraz wymagań dotyczących IK;
   2) komunikuje zmiany właściwym pracownikom i komórkom organizacyjnym;
   3) implementuje obowiązki wynikające ze zmian otoczenia prawnego i monitoruje ich wdrażanie
   4) każdorazowo przy zawieraniu umów z dostawcami i podwykonawcami dokonuje analizy ryzyka wynikającego z tych umów pod kątem wpływu na ciągłość i bezpieczeństwo IK.
3. W zakresie ochrony kluczowych zasobów operator:

1) posiada tytuł prawny (np. własność, użytkowanie, licencje) do kluczowych zasobów niezbędnych do funkcjonowania IK;
2) tytuły prawne do kluczowych zasobów (umowy, decyzje administracyjne, licencje, zgody regulacyjne) są udokumentowane i aktualizowane.
3) przy zawieraniu umów z dostawcami i podwykonawcami eliminuje zapisy prowadzące do uzależnienia od jednego dostawcy (tzw. vendor lock – VL);
4) w zawieranych umowach uwzględnia zasady usuwania wykrytych podatności, których wykorzystanie może powodować ryzyko zakłócenia funkcjonowania IK, a w przypadku oprogramowania uwzględnia zasady dostępu do kodu źródłowego zarówno w trakcie obowiązywania umowy jak i po jej zakończeniu.

4. Operator posiada zasady wymiany informacji z właściwym wojewodą, ministrem i Dyrektorem Rządowego Centrum Bezpieczeństwa o zagrożeniach i incydentach mogących spowodować zakłócenia w funkcjonowaniu IK, w tym o zagrożeniach związanych z dzielnością prawną innych podmiotów, w tym:
   1) możliwość wrogiego przejęcia;
   2) zmiana struktury właścicielskiej mogąca naruszać zasady kontroli inwestycji bezpośrednich;
   3) zmiana struktury właścicielskiej stwarzająca ryzyko naruszenia obowiązujących sankcji.

Ciągłość działania

1. W zakresie ciągłości działania IK operator:
   1) posiada i stale aktualizuje dokumentację w zakresie systemu ciągłości działania obejmującą:
   a) role poszczególnych osób w systemie,
   b) analizę BIA ,
   c) analizę zagrożeń dla procesów krytycznych,
   d) strategię ciągłości działania,
   e) plany ciągłości działania,
   f) scenariusze testów i raportów z przeprowadzonych testów i przeglądów;
   2) minimum raz na dwa lata dokonuje analizy poprawności działania systemu ciągłości działania bazując na wynikach audytów, wynikach testów i przeglądów oraz wnioskach z zaistniałych incydentów;
   3) stale doskonali system ciągłości działania opierając się na cyklu Deminga.
2. Na wypadek wystąpienia incydentu lub sytuacji kryzysowej operator:
   1) sporządza plan zarządzania kryzysowego - opisujący zasady organizacji i postępowania jednostki kierującej i koordynującej działaniami podejmowanymi w ramach reakcji na zdarzenie kryzysowe;
   2) plany/procedury awaryjne (contingency plan) koncentrujące się na przywróceniu/wznowieniu działania procesów i zasobów po wystąpieniu awarii;

3) plany/procedury odtworzenia utraconych zasobów (DRP – disaster recovery plan);
4) ustala docelowy czas przywrócenia (RTO) i docelowy moment przywrócenia (RPO).

UZASADNIENIE

Projektowane rozporządzenie stanowi wykonanie upoważnienia ustawowego z art. 6ze. ust. 4 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, zwanej dalej „ustawą" i określa minimalne wymagania w zakresie bezpieczeństwa fizycznego, technicznego, osobowego, cyberbezpieczeństwa, prawnego oraz ciągłości działania, niezbędne do wdrażania rozwiązań, o których mowa w ust. 1 pkt 2 ustawy, mając na uwadze:
1) rekomendacje o charakterze specjalistycznym w zakresie ochrony infrastruktury kry-tycznej, niezbędne do wdrażania rozwiązań w zakresie bezpieczeństwa infrastruktury krytycznej;
2) lokalizację i charakterystykę infrastruktury krytycznej;
3) potrzebę podejmowania działań zapewniających bezpieczeństwo infrastruktury kry-tycznej.

Projektowane rozporządzenie będzie wykorzystywane przez operatorów infrastruktury krytycznej podmioty krytyczne w procesie wdrażania adekwatnych do przeprowadzonej analizy zagrożeń w zakresie: bezpieczeństwa fizycznego, technicznego, osobowego, cyberbezpieczeństwa, prawnego oraz ciągłości działania.

Operatorzy infrastruktury krytycznej, spośród których wyodrębniane będą podmioty krytyczne, dotychczas nie posiadali odpowiednich narzędzi do selekcji dla środków w zakresie bezpieczeństwa i w zakresie odporności. Wdrażanie wskazanych w Narodowym Programie Ochrony Infrastruktury Krytycznej działań w zakresie bezpieczeństwa fizycznego, technicznego, osobowego, teleinformatycznego, prawnego oraz ciągłości działania opierało się dotychczas na zaleceniach zawartych w Załączniku 1 do NPOIK - *Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje.* System oparty na zaleceniach nie jest wystarczająco efektywny i uniemożliwia szybkie i optymalne dostosowywanie operatorów IK do nowych zagrożeń, a w szczególności uniemożliwia wdrożenie zintegrowanego systemu zarządzania bezpieczeństwem świadczenia usługi kluczowej w wypadku przekształcenia w podmiot krytyczny.

Regulacja zapewnia:

- jednolite i spójne podeście do ochrony IK, w uwzględnieniem:
  - wymagań dla sześciu obszarów bezpieczeństwa IK, które od kilkunastu lat opisywane są w narodowym programie ochrony infrastruktury krytycznej,
  - zasad szacowania ryzyka, obowiązków, wytycznych i zaleceń w zakresie wdrażania adekwatnych środków organizacyjno-technicznych,
- podniesienie odporności systemowej na zróżnicowane zagrożenia,
- zgodność z wymaganiami Dyrektywy CER w sprawie odporności podmiotów krytycznych i uchylającej dyrektywę rady 2008/114/WE,
- ułatwienie i zwiększenie efektywności procesów inwestycyjnych,
- potencjalne zmniejszenie kosztów po stronie operatorów IK dzięki ograniczeniu ryzyka popełniania błędów w procesach inwestycyjnych,
- zwiększenie efektywności opracowywania, stosowania i aktualizacji dokumentacji ochrony IK,
- poprawienie efektywności współpracy pomiędzy operatorami IK, a organami zarządzania kryzysowego, służbami, stażami i inspekcjami oraz dyrektorem centrum
- poprawienie efektywności nadzorów i kontroli nad operatorami IK,
- stymulację rynku usług doradczych, audytorskich i szkoleniowych w zakresie ochrony IK,
- promuje standardy oparte na normach europejskich i międzynarodowych w innych sektorach gospodarki

Proponowane minimalne wymagania są komplementarne do Załącznika 1 do NPOIK - *Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje.*

Projektowane rozporządzenie wejdzie w życie po upływie 14 od dnia ogłoszenia

Projekt rozporządzenia nie podlega notyfikacji zgodnie z przepisami dotyczącymi funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych.

Projekt rozporządzenia nie jest sprzeczny 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.

Nazwa projektu Rozporządzenie Rady Ministrów w sprawie minimalnych wymagań w zakresie bezpieczeństwa fizycznego, technicznego, osobowego, cyberbezpieczeństwa, prawnego oraz ciągłości działania infrastruktury krytycznej **Ministerstwo wiodące i ministerstwa współpracujące** **Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu** **Kontakt do opiekuna merytorycznego projektu**	**Data sporządzenia** **Źródło:** **Nr w wykazie prac …….**

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

Podejście do harmonizacji wymagań w zakresie zapewniania bezpieczeństwa i odporności podmiotów będących operatorami infrastruktury krytycznej zawarte w Dyrektywie CER w sprawie odporności podmiotów krytycznych i uchylającej dyrektywę Rady 2008/114/WE wprost wskazuje na konieczność dostosowania do dynamicznego krajobrazu zagrożeń hybrydowych i terrorystycznych. Operatorzy infrastruktury krytycznej, spośród których wyodrębniane będą podmioty krytyczne, dotychczas nie posiadali odpowiednich narzędzi do selekcji dla środków w zakresie bezpieczeństwa i w zakresie odporności. Wdrażanie wskazanych w Narodowym Programie Ochrony Infrastruktury Krytycznej działań w zakresie bezpieczeństwa fizycznego, technicznego, osobowego, teleinformatycznego, prawnego oraz ciągłości działania opierało się dotychczas na zaleceniach zawartych w Załączniku 1 do NPOIK - *Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje.* System oparty na zaleceniach nie jest wystarczająco efektywny i uniemożliwia szybkie i optymalne dostosowywanie operatorów IK do nowych zagrożeń, a w szczególności uniemożliwia wdrożenie zintegrowanego systemu zarządzania bezpieczeństwem świadczenia usługi kluczowej w wypadku przekształcenia w podmiot krytyczny.

Mając na względzie zapewnienie ochrony infrastruktury krytycznej, operatorzy IK, zgodnie z projektem ustawy, są zobligowani do prowadzenia systematycznej analizy zagrożeń dla infrastruktury krytycznej i wdrożenia adekwatnych do wyników przeprowadzonej analizy zagrożeń rozwiązań w zakresie:

a) bezpieczeństwa fizycznego, w tym ochrony fizycznej oraz zabezpieczeń technicznych uwzględniających kontrolę dostępu,
b) bezpieczeństwa technicznego,
c) bezpieczeństwa osobowego dotyczącego pracowników i dostawców zewnętrznych,
d) cyberbezpieczeństwa,
e) bezpieczeństwa prawnego,
f) ciągłości działania i odtwarzania, w tym utrzymywania własnych systemów rezerwowych zapewniających bezpieczeństwo i podtrzymujących funkcjonowanie infrastruktury krytycznej do czasu jej pełnego odtworzenia;

Dlatego też, w projekcie ustawy zawarto upoważnienie ustawowe, na podstawie którego Rada Ministrów określi, w drodze rozporządzenia minimalne wymagania w powyższym zakresie.

2. Rekomendowane rozwiązanie, w tym planowane narzędzia interwencji, i oczekiwany efekt

Wydanie rozporządzenia zawierającego minimalne wymagania w zakresie bezpieczeństwa fizycznego, technicznego, osobowego, cyberbezpieczeństwa, prawnego oraz ciągłości działania. Rozwiązanie zapewnia zgodność z celami zawartymi w Dyrektywie CER w sprawie odporności podmiotów krytycznych i uchylającej dyrektywę Rady 2008/114/WE.

Wdrożone zostanie spójne i jednolite podejście do ochrony IK, które umożliwi podniesienie poziomu odporności systemowej, tym bardziej, że podstawą minimalnych wymagań są szeroko stosowane normy europejskie i międzynarodowe.

Rozporządzenie ma nie tylko bezpośredni i pozytywny wpływ na odporność fizyczną, cyfrową i organizacyjną IK, ale także na zdolności operatorów IK do reagowania na incydenty i skuteczność współpracy z organami zarządzania kryzysowego, służbami oraz RCB.

Regulacja znacząco ułatwia procesy inwestycyjne w środki zapewniające bezpieczeństwo – operatorzy IK zyskują przejrzyste narzędzie do selekcji, co przekłada się na zmniejszenie problemów organizacyjnych, prawnych, finansowych i w konsekwencji optymalizację całego systemu zapewniania ochrony IK.

Co więcej, projektowane przepisy wspierają i optymalizują skuteczność działań kontrolnych i nadzorczych.

3. Jak problem został rozwiązany w innych krajach, w szczególności krajach członkowskich OECD/UE?

4. Podmioty, na które oddziałuje projekt

Grupa	Wielkość	Źródło danych	Oddziaływanie
(dodaj/usuń)			
(dodaj/usuń)			
(dodaj/usuń)			
(dodaj/usuń)			
(dodaj/usuń)			

5. Informacje na temat zakresu, czasu trwania i podsumowanie wyników 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												
budżet państwa												
JST												
pozostałe jednostki (oddzielnie)												
Wydatki ogółem												
budżet państwa												
JST												
pozostałe jednostki (oddzielnie)												
Saldo ogółem												
budżet państwa												
JST												
pozostałe jednostki (oddzielnie)												

Źródła finansowania	Rozporządzenie nie powoduje konieczności wydatkowania środków finansowych z budżet państwa.
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	Nie dotyczy

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							
	(dodaj/usuń)							
W ujęciu niepieniężnym	duże przedsiębiorstwa							
	sektor mikro-, małych i średnich przedsiębiorstw							
	rodzina, obywatele oraz gospodarstwa domowe							
	(dodaj/usuń)							
Niemierzalne	(dodaj/usuń)							
	(dodaj/usuń)							

Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	

8. Zmiana obciążeń regulacyjnych (w tym obowiązków informacyjnych) wynikających z projektu

X 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:	☐ zwiększenie liczby dokumentów ☐ zwiększenie liczby procedur ☐ wydłużenie czasu na załatwienie sprawy ☐ inne:
Wprowadzane obciążenia są przystosowane do ich elektronizacji.	☐ tak ☐ nie ☐ nie dotyczy

Komentarz:

9. Wpływ na rynek pracy

10. Wpływ na pozostałe obszary

☐ środowisko naturalne ☐ sytuacja i rozwój regionalny ☐ sądy powszechne, administracyjne lub wojskowe	☐ demografia ☐ mienie państwowe ☐ inne:	☐ informatyzacja ☐ zdrowie
Omówienie 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?

Nie dotyczy.

13. Załączniki (istotne dokumenty źródłowe, badania, analizy itp.)

Nie dotyczy.

Projekt

R O Z P O R Z Ą D Z E N I E

R A D Y M I N I S T R Ó W

z dnia

w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych[1]

Na podstawie art. 6zp ust. 3 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z … poz. …) zarządza się, co następuje:

§ 1. Wykaz usług kluczowych oraz progi istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych, są określone w załączniku do rozporządzenia.

§ 2. Rozporządzenie wchodzi w życie po upływie 14 od dnia ogłoszenia.

P R E Z E S R A D Y M I N I S T R Ó W

[1] Niniejsze rozporządzenie w zakresie swojej regulacji wdraża dyrektywę 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 333 z 27.12.2022 r. str. 164).

Załącznik

do rozporządzenia Rady Ministrów

z dnia

Dz. U. poz.

WYKAZ USŁUG KLUCZOWYCH ORAZ PROGI ISTOTNOŚCI SKUTKU ZAKŁÓCAJĄCEGO INCYDENTU DLA ŚWIADCZENIA USŁUG

Sektor	**Podsektor**	**Rodzaj podmiotu**	**Usługa kluczowa**	**Próg istotności skutku zakłócającego incydentu dla świadczenia usługi kluczowej**
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.	1. Wydobywanie gazu ziemnego	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora: ***ilość wydobytego gazu ziemnego na terenie kraju w roku poprzednim wynosząca minimum 11 TWh lub udział wielkości rocznego wydobycia gazu ziemnego w łącznym krajowym zużyciu gazu ziemnego w roku poprzednim wynosząca minimum 15%.***
		Podmioty prowadzące działalność gospodarczą w zakresie wydobywania ropy naftowej na podstawie	2. Wydobywanie ropy naftowej	1. Inne czynniki charakterystyczne dla danego podsektora: ***udział wydobytego surowca w dostawach ropy naftowej dla poszczególnych***

		koncesji, o której mowa w art. 22 ust. 1 ustawy z dnia 9 czerwca 2011 r. – Prawo geologiczne i górnicze.		***rafinerii zlokalizowanych na terytorium RP, określony jako procent w dostawach rocznych wynoszący minimum 10%.***
		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.	3. Wydobywanie węgla brunatnego	1. Inne czynniki charakterystyczne dla danego podsektora: ***ilość wydobytego węgla brunatnego w tonach wynosząca minimum 10 mln ton rocznie.***
		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.	4. Wydobywanie węgla kamiennego	1. Inne czynniki charakterystyczne dla danego podsektora: ***ilość wydobytego węgla kamiennego w tonach wynosząca rocznie minimum 8 mln ton***
		Podmioty prowadzące działalność gospodarczą w zakresie wydobywania pozostałych kopalin na podstawie koncesji, o której mowa w art. 22 ust. 1	5. Wydobywanie miedzi	1. Inne czynniki charakterystyczne dla danego podsektora: ***ilość produkcji miedzi wynosząca minimum 50 tys. ton rocznie***

		ustawy z dnia 9 czerwca 2011 r. – Prawo geologiczne i górnicze.		
	Energia elektryczna	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.	6. Wytwarzanie energii elektrycznej	1. Inne czynniki charakterystyczne dla danego podsektora: ***moc zainstalowana elektryczna wynosząca minimum 120 MW brutto lub procentowy udział wytworzonej i sprzedanej energii elektrycznej w produkcji energii elektrycznej ogółem w kraju wynoszący minimum 0,4% w rocznej produkcji energii elektrycznej, w tym posiadanie Jednostki Wytwórczej Centralnie Dysponowanej***
		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.	7. Przesyłanie energii elektrycznej	1. Inne czynniki charakterystyczne dla danego podsektora: ***długość sieci przesyłowej wynosząca minimum 500 km lub zarządzanie Głównym Punktem Zasilania.***

		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.	8. Dystrybucja energii elektrycznej	1. liczba użytkowników zależnych od usługi kluczowej świadczonej przez dany podmiot: **liczba odbiorców wynosząca minimum 500 tys.,** 2. Inne czynniki charakterystyczne dla danego podsektora: ***długość sieci dystrybucyjnej/trakcyjnej wynosząca minimum 500 km***
		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.	9. Obrót energią elektryczną	1. liczba użytkowników zależnych od usługi kluczowej świadczonej przez dany podmiot: ***liczba odbiorców końcowych wynosząca minimum 500 tys. rocznie,*** 2. Inne czynniki charakterystyczne dla danego podsektora: ***udział ilości sprzedanej energii elektrycznej przez przedsiębiorstwo w stosunku do ilości energii elektrycznej dostarczonej ogółem do odbiorców końcowych w kraju wynoszący minimum 3,5%***
		Podmioty o których mowa w art. 3 pkt 28b ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne.	10. Wykonywanie zadań związanych z jednolitym łączeniem rynków dnia następnego lub dnia bieżącego	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***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 11j ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne.	11. Zmiana zużycia energii elektrycznej odbiorcy końcowego w stosunku do jego zwykłego lub bieżącego zużycia energii elektrycznej w odpowiedzi na sygnały rynkowe	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***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, świadczący usługę, o której mowa w art. 3 pkt 6f tej ustawy	12. Łączenie wielkości mocy lub energii elektrycznej oferowanej przez odbiorców, wytwórców energii elektrycznej lub posiadaczy magazynów energii elektrycznej	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***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 w/w ustawy***
		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.	13. Zarządzanie punktem ładowania i jego obsługę	1. Udział podmiotu krytycznego w rynku w odniesieniu do świadczonej usługi kluczowej: ***min. 10 % udziału w rynku.***

		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.	14. Magazynowanie energii elektrycznej	1. Inne czynniki charakterystyczne dla danego podsektora: ***moc magazynu wynosząca minimum 50 MW brutto***
			15. Przetwarzanie energii elektrycznej	1. Inne czynniki charakterystyczne dla danego podsektora: ***moc magazynu do przetwarzania energii elektrycznej wynosząca minimum 50 MW brutto***
	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.	16. Wytwarzanie ciepła	1. liczba użytkowników zależnych od usługi kluczowej świadczonej przez dany podmiot: ***minimum wynosząca 150 tys. odbiorców końcowych oraz użytkowników lokali mieszkalnych i użytkowych w budynkach wielolokalowych, zamieszkiwanych lub użytkowanych przez osoby niebędące odbiorcami (w odniesieniu do których umowa z przedsiębiorstwem energetycznym została zawarta przez odbiorcę),*** 2. Wpływ, jaki incydent, jeżeli chodzi o skalę i czas trwania, mógłby mieć na działalność gospodarczą i społeczną lub bezpieczeństwo publiczne: **wpływ**

				na co najmniej 50% odbiorców, o których mowa w pkt. 1,
		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.	17. Obrót ciepłem	1. liczba użytkowników zależnych od usługi kluczowej świadczonej przez dany podmiot: ***wynosząca minimum 150 tys. odbiorców końcowych oraz użytkowników lokali mieszkalnych i użytkowych w budynkach wielolokalowych, zamieszkiwanych lub użytkowanych przez osoby niebędące odbiorcami (w odniesieniu do których umowa z przedsiębiorstwem energetycznym została zawarta przez odbiorcę),*** 2. Wpływ, jaki incydent, jeżeli chodzi o skalę i czas trwania, mógłby mieć na działalność gospodarczą i społeczną lub bezpieczeństwo publiczne: ***wpływ na co najmniej 50% odbiorców, o których mowa w pkt. 1***
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na	18. Przesyłanie ciepła	1. liczba użytkowników zależnych od usługi kluczowej świadczonej przez dany podmiot: ***wynosząca minimum 150 tys. odbiorców końcowych oraz użytkowników lokali mieszkalnych i użytkowych w***

		wykonywanie działalności gospodarczej w zakresie przesyłania ciepła.		***budynkach wielolokalowych, zamieszkiwanych lub użytkowanych przez osoby niebędące odbiorcami (w odniesieniu do których umowa z przedsiębiorstwem energetycznym została zawarta przez odbiorcę),*** 2. Wpływ, jaki incydent, jeżeli chodzi o skalę i czas trwania, mógłby mieć na działalność gospodarczą i społeczną lub bezpieczeństwo publiczne: ***wpływ na co najmniej 50% odbiorców, o których mowa w pkt. 1,***
		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.	19. Dystrybucja ciepła	1. liczba użytkowników zależnych od usługi kluczowej świadczonej przez dany podmiot: ***wynosząca minimum 150 tys. odbiorców końcowych oraz użytkowników lokali mieszkalnych i użytkowych w budynkach wielolokalowych, zamieszkiwanych lub użytkowanych przez osoby niebędące odbiorcami (w odniesieniu do których umowa z przedsiębiorstwem energetycznym została zawarta przez odbiorcę),***

				2. Wpływ, jaki incydent, jeżeli chodzi o skalę i czas trwania, mógłby mieć na działalność gospodarczą i społeczną lub bezpieczeństwo publiczne: ***wpływ na co najmniej 50% odbiorców, o których mowa w pkt. 1,***
	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.	20. Wytwarzanie paliw ciekłych	1. Inne czynniki charakterystyczne dla danego podsektora: ***ilość wytworzonych paliw ciekłych w roku poprzednim wynosząca minimum 5 mln ton lub wielkość przerobu ropy naftowej w roku poprzednim wynosząca minimum 5 mln ton.***
		Podmioty prowadzące działalność gospodarczą w zakresie przesyłania ropy naftowej.	21. Przesyłanie ropy naftowej	1. Inne czynniki charakterystyczne dla danego podsektora: ***wielkość przesyłu ropy naftowej wynosząca minimum 10 mln ton średniorocznie z ostatnich 3 lat***
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy	22. Przesyłanie paliw ciekłych	1. Inne czynniki charakterystyczne dla danego podsektora: ***wielkość przesyłu paliw ciekłych w roku***

		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.		***poprzednim wynosząca minimum 1 mln ton rocznie***
		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.	23. Magazynowanie ropy naftowej	1. Inne czynniki charakterystyczne dla danego podsektora: ***magazynowanie minimum 500 tys. ton ropy naftowej średniorocznie z ostatnich 3 lat***
		Podmioty prowadzące działalność gospodarczą w zakresie przeładunku ropy naftowej.	24. Przeładunek ropy naftowej	1. Inne czynniki charakterystyczne dla danego podsektora: ***przeładunek minimum 1 mln ton ropy naftowej średniorocznie z ostatnich 3 lat***
		Przedsiębiorstwo energetyczne, o którym	25. Magazynowanie paliw ciekłych	1. Inne czynniki charakterystyczne dla danego podsektora: ***suma***

		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.		***pojemności nominalnej magazynów podmiotu świadczącego usługę magazynowania wynosząca minimum 100 tys. m³***
		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	26. Przeładunek paliw ciekłych	1. Inne czynniki charakterystyczne dla danego podsektora: ***wielkość przeładunku w roku poprzednim dokonana przez podmiot świadczący usługę przeładunku wynosząca minimum 500 tys. m3 rocznie***

		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.	27. Obrót paliwami ciekłymi lub obrót paliwami ciekłymi z zagranicą	1. Inne czynniki charakterystyczne dla danego podsektora: ***przywóz minimum 400 tys. m3 paliw ciekłych w roku poprzednim lub liczba stacji paliw ciekłych wykorzystywanych do prowadzenia działalności w roku poprzednim: wynosząca minimum 250 stacji***
		Podmioty prowadzące działalność gospodarczą w zakresie wytwarzania paliw syntetycznych.	28. Wytwarzanie paliw syntetycznych	1. Inne czynniki charakterystyczne dla danego podsektora: ***wytwarzanie minimum 100 tys. m3 paliw syntetycznych średniorocznie z ostatnich 3 lat***
		Agencja wykonawcza utworzona na podstawie ustawy z dnia 17 grudnia 2020 r. o rezerwach strategicznych (Dz. U. z 2023 r. poz. 294 oraz z 2024 r. poz. 834).	29. Zapewnienie strategicznych rezerw produktów żywnościowych, medycznych i technicznych oraz zapasów paliw	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***Agencja wykonawcza utworzona na podstawie ustawy z dnia 17 grudnia 2020 r. o rezerwach strategicznych***

				(Dz. U. z 2023 r. poz. 294 oraz z 2024 r. poz. 834).
	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.	30. Wytwarzanie paliw gazowych	1. Inne czynniki charakterystyczne dla danego podsektora: ***ilość wytworzonych paliw gazowych w roku poprzednim wynosząca minimum 110 TWh***
		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.	31. Przesyłanie paliw gazowych	1. Inne czynniki charakterystyczne dla danego podsektora: ***ilość przesłanych paliw gazowych w roku poprzednim wynosząca minimum 110 TWh***
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na	32. Obrót paliwami gazowymi i obrót gazem ziemnym z zagranicą	1. Inne czynniki charakterystyczne dla danego podsektora: ***ilość przywiezionego gazu ziemnego w roku poprzednim wynosząca minimum 100 TWh lub procentowy stosunek wielkości przywozu gazu***

		wykonywanie działalności gospodarczej w zakresie obrotu gazem ziemnym z zagranicą lub na wykonywanie działalności gospodarczej w zakresie obrotu paliwami gazowymi.		***ziemnego do krajowego zużycia gazu ziemnego w roku poprzednim wynoszący minimum 60%, lub ilość sprzedanych paliw gazowych do odbiorców końcowych w roku poprzednim wynosząca minimum 27 TWh***
		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.	33. Przesyłanie paliw gazowych	1. Inne czynniki charakterystyczne dla danego podsektora: ***ilość przesłanych paliw gazowych w roku poprzednim wynosząca minimum 110 TWh***
		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.	34. Dystrybucja paliw gazowych	1. Inne czynniki charakterystyczne dla danego podsektora: ***ilość dystrybuowanych paliw gazowych w roku poprzednim wynosząca minimum 90 TWh***
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 26 ustawy	35. Magazynowanie paliw gazowych	1. Inne czynniki charakterystyczne dla danego podsektora: ***poziom pojemności czynnych***

		z dnia 10 kwietnia 1997 r. - Prawo energetyczne, będące wyznaczonym przez Prezesa Urzędu Regulacji Energetyki operatorem systemu magazynowania paliw gazowych.		***udostępnianych użytkownikom w roku poprzednim wynoszący minimum 30 TWh***
		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.	36. Skraplanie i regazyfikacja LNG oraz sprowadzanie i wyładunek LNG	1. Inne czynniki charakterystyczne dla danego podsektora: ***ilość regazyfikowanego gazu skroplonego w roku poprzednim wynosząca minimum 10 TWh***
		Przedsiębiorstwa energetyczne prowadzące działalność gospodarczą w zakresie rafinacji i przetwarzania gazu ziemnego.	37. Rafinacja i przetwarzania gazu ziemnego	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***ilość wytwarzanych produktów i półproduktów handlowych w skali rocznej minimum 5 TWh***
	Wodór	Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, prowadzące działalność w	38. Produkcja wodoru	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***ilość wytwarzanego wodoru w roku poprzednim minimum 100 tys. ton***

		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 magazynowania wodoru	39. Magazynowanie wodoru	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***zdolność magazynowania wodoru pow. 5 tys. ton***
		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	40. Przesyłanie wodoru	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***przesył wodoru w roku poprzednim minimum 5 tys. ton***
		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.	41. Dystrybucja wodoru	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***dystrybucja wodoru w roku poprzednim minimum 5 tys. ton***

	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.	42. Unieszkodliwianie odpadów promieniotwórczych	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***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.***
			43. Składowanie odpadów promieniotwórczych	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***powierzchnia składowania po 2 tys. m3***
			44. Wytwarzanie energii elektrycznej lub cieplnej	1. Inne czynniki charakterystyczne dla danego podsektora: ***moc zainstalowana elektryczna wynosząca minimum 2 GW brutto, w tym posiadanie Jednostki Wytwórczej Centralnie Dysponowanej***
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	45. Transport lotniczy pasażerski	1. Liczba użytkowników zależnych od usługi kluczowej świadczonej przez dany podmiot: ***przewóz minimum 3 mln pasażerów rocznie określany: – na podstawie uśrednionych danych***

		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).		***statystycznych za 3 lata poprzedzające wydanie decyzji o uznaniu za operatora usługi kluczowej lub – w przypadku podmiotów działających na rynku krócej niż 3 lata, na podstawie danych statystycznych za 2 pełne lata lub 1 pełny rok poprzedzający wydanie decyzji,***
		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).	46. Transport lotniczy towarów	1. Udział podmiotu świadczącego usługę kluczową w rynku: ***wynoszący minimum 25% udział realizowanych lotów transportu towarów w skali rynku krajowego obliczony: – na podstawie uśrednionych danych statystycznych za 3 lata poprzedzające wydanie decyzji o uznaniu za operatora usługi kluczowej lub – w przypadku podmiotów działających na rynku krócej niż 3 lata, na podstawie danych statystycznych za 2 pełne lata lub 1 pełny rok poprzedzający wydanie decyzji,***
		Zarządzający lotniskiem, o którym mowa w art. 2 pkt 7 ustawy z dnia 3 lipca 2002 r. – Prawo lotnicze (Dz. U. z	47. Działalność usługowa wspomagająca transport	1. Liczba użytkowników zależnych od usługi kluczowej świadczonej przez dany podmiot: ***obsługa minimum 3 mln pasażerów rocznie***

		2023 r. poz. 2110 oraz z 2024 r. poz. 731 i 1222).	lotniczy przez zarządzającego lotniskiem	***określana: – na podstawie uśrednionych danych statystycznych za 3 lata poprzedzające wydanie decyzji o uznaniu za operatora usługi kluczowej lub – w przypadku podmiotów działających na rynku krócej niż 3 lata, na podstawie danych statystycznych za 2 pełne lata lub 1 pełny rok poprzedzający wydanie decyzji lub – w przypadku nowych podmiotów, których przewidywany zakres działania spełni wymogi progu uznania za operatora usługi kluczowej, na podstawie planu generalnego, o którym mowa w art. 55 ust. 6 ustawy z dnia 3 lipca 2002 r. – Prawo lotnicze,***
		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	48. Działalność usługowa wspomagająca transport lotniczy przez przedsiębiorę, posiadającego status zarejestrowanego agenta	1. Inne czynniki charakterystyczne dla danego podsektora: – ***realizowanie przez podmiot kontroli bezpieczeństwa ładunku lub poczty lotniczej wraz z nadawaniem skontrolowanym ładunkom statusów SPX, SCO oraz SHR w myśl rozporządzenia wykonawczego Komisji (UE) 2015/1998 z dnia 5 listopada 2015 r. ustanawiającego***

		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 Instytucja zapewniająca służby żeglugi powietrznej, o której mowa w art. 127 ust. 1 ustawy z dnia 3 lipca 2002 r. – Prawo lotnicze.		***szczegółowe środki w celu wprowadzenia w życie wspólnych podstawowych norm ochrony lotnictwa cywilnego, lub – świadczenie usługi elektronicznego przekazu informacji o statusie ochrony nadanym przesyłce, przekazywanej drogą lotniczą do punktu docelowego***
		Podmiot posiadający status zarejestrowanego agenta obsługi naziemnej o którym mowa w rozporządzeniu Parlamentu Europejskiego i Rady (WE) nr 300/2008 z dnia 11 marca 2008 w sprawie wspólnych zasad ochrony lotnictwa cywilnego i uchylające rozporządzenie (WE) nr 2320/2002 wraz z aktami wykonawczym	49. Działalność usługowa wspomagająca transport lotniczy przez przedsiębiorę, posiadającego status zarejestrowanego agenta obsługi naziemnej	1. Inne czynniki charakterystyczne dla danego podsektora: ***podmiot posiadający status zarejestrowanego agenta obsługi naziemnej o którym mowa w rozporządzeniu Parlamentu Europejskiego i Rady (WE) nr 300/2008 z dnia 11 marca 2008 w sprawie wspólnych zasad ochrony lotnictwa cywilnego i uchylające rozporządzenie (WE) nr 2320/2002 wraz z aktami wykonawczym***
		Instytucja zapewniająca służby żeglugi powietrznej, o której mowa w art. 127 ust. 1 ustawy z dnia 3 lipca 2002 r. – Prawo lotnicze.	50. Działalność usługowa wspomagająca transport lotniczy przez instytucję zapewniającą służby żeglugi powietrznej	1. Zdolność podmiotu do utrzymywania wystarczającego poziomu świadczenia usługi kluczowej przy uwzględnieniu dostępności alternatywnych sposobów jej świadczenia: ***brak***

				alternatywy dla świadczonej usługi i możliwości jej realizowania przez inną służbę w przypadku wystąpienia incydentu, 2. Inne czynniki charakterystyczne dla danego podsektora: ***usługa zapewniana jest dla więcej niż 10 tys. lotów rocznie, niezależnie od maksymalnej masy startowej i liczby miejsc pasażerskich w statku powietrznym, przy lotach liczonych jako suma startów i lądowań oraz obliczanych jako średnia z ubiegłych 3 lat***
	Transport kolejowy	Zarządca infrastruktury kolejowej w rozumieniu art. 4 pkt 7 ustawy z dnia 28 marca 2003 r. o transporcie kolejowym (Dz. U. z 2024 r. poz. 697 i 731), 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	51. Konstrukcja rozkładu jazdy pociągów	1. Wpływ, jaki incydent, jeżeli chodzi o skalę i czas trwania, mógłby mieć na działalność gospodarczą i społeczną lub bezpieczeństwo publiczne: ***a) strata finansowa z tytułu niezrealizowania przewozu: wynosząca 500 tys. złotych dziennie,*** ***b) brak możliwości uruchomienia pociągów: w liczbie 5 tys. sztuk dziennie,***

		mowa w art. 4 pkt 1d tej ustawy.		***c) brak możliwości realizacji dostaw paliw kopalnych (węgiel), płynnych (paliwa) powyżej 12 godzin,*** ***d) brak możliwości realizacji przejazdów pociągów pasażerskich (transport publiczny) powyżej 12 godzin,*** 2. Udział podmiotu świadczącego usługę kluczową w rynku: **udział w rynku zarządców infrastruktury kolejowej: powyżej 50% długości eksploatowanych linii kolejowych (wg aktualnych danych publikowanych przez Prezesa Urzędu Transportu Kolejowego),** 3. Inne czynniki charakterystyczne dla danego podsektora: ***liczba składanych przez przewoźników wniosków o konstrukcję rozkładu jazdy – nie mniej niż 800 tys. rocznie***
		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	52. Transport kolejowy pasażerski	1. Udział podmiotu świadczącego usługę kluczową w rynku: ***udział przewoźnika w rynku wynoszący powyżej 25%, liczony wg wykonanej pracy przewozowej lub liczby pasażerów (na podstawie danych publikowanych przez***

		infrastruktury usługowej, o którym mowa w art. 4 pkt 52 ustawy z dnia 28 marca 2003 r. o transporcie kolejowym.		***Prezesa Urzędu Transportu Kolejowego),*** 2. Zasięg geograficzny związany z obszarem, którego mógłby dotyczyć incydent: ***świadczenie usługi na obszarze co najmniej 9 województw,***
		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.	53. Transport kolejowy towarów	1. Udział podmiotu świadczącego usługę kluczową w rynku: ***udział przewoźnika w rynku wynoszący powyżej 25%, liczony wg wykonanej pracy przewozowej lub przewiezionej masy towarów (na podstawie danych publikowanych przez Prezesa Urzędu Transportu Kolejowego),***
	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	54. Transport morski pasażerski	1. Liczba użytkowników zależnych od usługi kluczowej świadczonej przez dany podmiot: **przewóz minimum 100 tys. pasażerów rocznie,**

		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 wyłączeniem poszczególnych statków, na których prowadzą działalność ci armatorzy.		
		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 wyłączeniem poszczególnych statków, na których prowadzą działalność ci armatorzy.	55. Transport morski towarów	1. Inne czynniki charakterystyczne dla danego podsektora: ***przewóz minimum 1 mln ton towarów rocznie***

		Armator, o którym mowa w art. 5 ust. 1 pkt 2 ustawy z dnia 21 grudnia 2000 r. o żegludze śródlądowej (Dz. U. z 2024 r. poz. 395 i 731).	56. Transport wodny śródlądowy pasażerski	1. Udział podmiotu świadczącego usługę kluczową w rynku: ***przewóz co najmniej 30% pasażerów transportu pasażerskiego żeglugi śródlądowej,***
		Armator, o którym mowa w art. 5 ust. 1 pkt 2 ustawy z dnia 21 grudnia 2000 r. o żegludze śródlądowej (Dz. U. z 2024 r. poz. 597).	57. Transport wodny śródlądowy towarów	1. Udział podmiotu świadczącego usługę kluczową w rynku: ***realizowanie co najmniej 40% przewozów towarów rocznie w transporcie śródlądowym krajowym,***
		Podmiot zarządzający portem, o którym mowa w art. 2 pkt 6 ustawy z dnia 20 grudnia 1996 r. o portach i przystaniach morskich (Dz. U. z 2023 r. poz. 1796).	58. Zarządzanie portem morskim	1. Inne czynniki charakterystyczne dla danego podsektora: ***zarządzanie portem należącym do sieci bazowej TEN-T, o której mowa w rozporządzeniu Parlamentu Europejskiego i Rady (UE) nr 1315/2013 z dnia 11 grudnia 2013 r. w sprawie unijnych wytycznych dotyczących rozwoju transeuropejskiej sieci transportowej i uchylającym decyzję nr 661/2010/UE (Dz. Urz. UE L 348/1 z 20.12.2013, str.1)***
		Podmiot zarządzający obiektem portowym, o którym mowa w art. 2 pkt 11	59. Obsługa transportu morskiego pasażerów i towarów	1. Liczba użytkowników zależnych od usługi kluczowej świadczonej przez dany podmiot: **obsługa**

		rozporządzenia (WE) 725/2004 Parlamentu Europejskiego i Rady z dnia 31 marca 2004 r. w sprawie podniesienia ochrony statków i obiektów portowych.		**minimum 100 tys. pasażerów przewożonych w transporcie morskim rocznie,** 2. Inne czynniki charakterystyczne dla danego podsektora: ***obsługa minimum 3 mln ton towarów przewożonych w transporcie morskim rocznie.***
		Podmioty prowadzące na terenie portu działalność wspomagającą transport morski zakwalifikowaną w PKD pod numerem 52.22. A	60. Działalność usługowa wspomagająca transport morski	1. Inne czynniki charakterystyczne dla danego podsektora: ***każdy podmiot wykonujący usługi, o których mowa w art. 1 ust. 2 lit. a, c, f oraz g rozporządzenia Parlamentu Europejskiego i Rady (UE) 2017/352 z dnia 15 lutego 2017 r. ustanawiające ramy w zakresie świadczenia usług portowych oraz wspólne zasady dotyczące przejrzystości finansowej portów (Dz. Urz. UE L 57/1 z 03.03.2017, str. 1)***
		VTS (Służba Kontroli Ruchu Statków) -–aparat pomocniczy dyrektora urzędu morskiego powołany w celu monitorowania ruchu statków i przekazywania informacji, stanowiący część	61. Monitorowanie ruchu statków	1.Inne czynniki charakterystyczne dla danego podsektora: ***Służba Kontroli Ruchu Statków - podmiot powołany w celu monitorowania ruchu statków i przekazywania informacji, stanowiący część składową Narodowego Systemu***

		składową Narodowego Systemu SafeSeaNet, o którym mowa w art. 91 ustawy z dnia 18 sierpnia 2011 r. o bezpieczeństwie morskim (Dz. U. z 2023 r. poz. 1666 i 2005).		***SafeSeaNet, o którym mowa w art. 91 ustawy z dnia 18 sierpnia 2011 r. o bezpieczeństwie morskim (Dz. U. z 2023 r. poz. 1666 i 2005).***
	Transport publiczny	Podmioty, o których mowa w art. 4 ust. 8 ustawy z dnia 16 Grudnia 2010 r. o publicznym transporcie zbiorowym.	62. Transport publiczny	1. Liczba użytkowników zależnych od usługi kluczowej świadczonej przez dany podmiot: ***3 mln pasażerów średnio rocznie z ostatnich 3 lat.***
	Transport drogowy	Organy, o których mowa w art. 19 ust. 2, 5 i 5a ustawy z dnia 21 marca 1985 r. o drogach publicznych (Dz. U. z 2024 r. poz. 320).	63. Zarządzanie drogami	Spełnienie poniższych kryteriów łącznie: 1.Zasięg geograficzny związany z obszarem, którego mógłby dotyczyć incydent: **minimum 15% wszystkich dróg krajowych,** 2. Inne czynniki charakterystyczne dla danego podsektora: ***minimum 500 tys. pojazdów samochodowych na drogach krajowych rocznie***
		Podmioty, o których mowa w art. 43a ust. 1 ustawy z	64. Inteligentne systemy transportowe	Spełnienie poniższych kryteriów łącznie:

		dnia 21 marca 1985 r. o drogach publicznych.		1. Wpływ, jaki incydent, jeżeli chodzi o skalę i czas trwania, mógłby mieć na działalność gospodarczą i społeczną lub bezpieczeństwo publiczne: ***każdy negatywny wpływ na bezpieczeństwo ruchu drogowego lub prawidłowość poboru opłat za przejazd*** 2. Zasięg geograficzny związany z obszarem, którego mógłby dotyczyć incydent: ***minimum 15% wszystkich dróg krajowych,*** 3. Inne czynniki charakterystyczne dla danego podsektora: ***minimum 500 tys. pojazdów samochodowych na drogach krajowych rocznie***

Bankowość i infrastruktura rynków finansowych		Bank krajowy, o którym mowa w art. 4 ust. 1 pkt 1 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe.	65. Przyjmowanie wkładów pieniężnych płatnych na żądanie lub z nadejściem oznaczonego terminu oraz prowadzenie rachunków tych wkładów	1. Udział podmiotu świadczącego usługę kluczową w rynku: ***świadczenie usługi kluczowej przez bank istotny pod względem wielkości, organizacji wewnętrznej oraz rodzaju, zakresu i złożoności prowadzonej działalności, który spełnia co najmniej jeden z warunków: – udział banku w aktywach sektora bankowego jest nie mniejszy niż 2%, – udział banku w depozytach sektora bankowego jest nie mniejszy niż 2%, – udział banku w funduszach własnych sektora bankowego jest nie mniejszy niż 2%,*** 2. Inne czynniki charakterystyczne dla danego podsektora: ***został uznany za bank istotny przez Komisję Nadzoru Finansowego, w drodze decyzji administracyjnej zgodnie z art. 4b ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe***
		Bank krajowy, o którym mowa w art. 4 ust. 1 pkt 1 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe.	66. Prowadzenie innych rachunków bankowych	1. Udział podmiotu świadczącego usługę kluczową w rynku: ***świadczenie usługi kluczowej przez bank istotny pod względem wielkości, organizacji wewnętrznej oraz rodzaju, zakresu i złożoności***

				prowadzonej działalności, który spełnia co najmniej jeden z warunków: – udział banku w aktywach sektora bankowego jest nie mniejszy niż 2%, – udział banku w depozytach sektora bankowego jest nie mniejszy niż 2%, – udział banku w funduszach własnych sektora bankowego jest nie mniejszy niż 2%, 2. Inne czynniki charakterystyczne dla danego podsektora: ***został uznany za bank istotny przez Komisję Nadzoru Finansowego, w drodze decyzji administracyjnej zgodnie z art. 4b ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe***
		Bank krajowy, o którym mowa w art. 4 ust. 1 pkt 1 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe.	67. Udzielanie kredytów	1. Udział podmiotu świadczącego usługę kluczową w rynku: ***świadczenie usługi kluczowej przez bank istotny pod względem wielkości, organizacji wewnętrznej oraz rodzaju, zakresu i złożoności prowadzonej działalności, który spełnia co najmniej jeden z warunków: – udział banku w aktywach sektora bankowego jest nie mniejszy niż 2%, – udział banku w depozytach sektora bankowego***

				jest nie mniejszy niż 2%, – udział banku w funduszach własnych sektora bankowego jest nie mniejszy niż 2%, 2. Inne czynniki charakterystyczne dla danego podsektora: ***został uznany za bank istotny przez Komisję Nadzoru Finansowego, w drodze decyzji administracyjnej zgodnie z art. 4b ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe***
		Bank krajowy, o którym mowa w art. 4 ust. 1 pkt 1 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe.	68. Przeprowadzanie bankowych rozliczeń pieniężnych	1. Udział podmiotu świadczącego usługę kluczową w rynku: ***świadczenie usługi kluczowej przez bank istotny pod względem wielkości, organizacji wewnętrznej oraz rodzaju, zakresu i złożoności prowadzonej działalności, który spełnia co najmniej jeden z warunków: – udział banku w aktywach sektora bankowego jest nie mniejszy niż 2%, – udział banku w depozytach sektora bankowego jest nie mniejszy niż 2%, – udział banku w funduszach własnych sektora bankowego jest nie mniejszy niż 2%,***

				2. Inne czynniki charakterystyczne dla danego podsektora: ***został uznany za bank istotny przez Komisję Nadzoru Finansowego, w drodze decyzji administracyjnej zgodnie z art. 4b ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe***
		Bank krajowy, o którym mowa w art. 4 ust. 1 pkt 1 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe.	69. Udzielanie pożyczek pieniężnych	1. Udział podmiotu świadczącego usługę kluczową w rynku: ***świadczenie usługi kluczowej przez bank istotny pod względem wielkości, organizacji wewnętrznej oraz rodzaju, zakresu i złożoności prowadzonej działalności, który spełnia co najmniej jeden z warunków: – udział banku w aktywach sektora bankowego jest nie mniejszy niż 2%, – udział banku w depozytach sektora bankowego jest nie mniejszy niż 2%, – udział banku w funduszach własnych sektora bankowego jest nie mniejszy niż 2%,*** 2. Inne czynniki charakterystyczne dla danego podsektora: ***został uznany za bank istotny przez Komisję Nadzoru Finansowego, w drodze decyzji administracyjnej***

				zgodnie z art. 4b ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe
		Bank krajowy, o którym mowa w art. 4 ust. 1 pkt 1 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe.	70. Świadczenie usług płatniczych oraz wydawanie pieniądza elektronicznego	1. Udział podmiotu świadczącego usługę kluczową w rynku: ***świadczenie usługi kluczowej przez bank istotny pod względem wielkości, organizacji wewnętrznej oraz rodzaju, zakresu i złożoności prowadzonej działalności, który spełnia co najmniej jeden z warunków: – udział banku w aktywach sektora bankowego jest nie mniejszy niż 2%, – udział banku w depozytach sektora bankowego jest nie mniejszy niż 2%, – udział banku w funduszach własnych sektora bankowego jest nie mniejszy niż 2%,*** 2. Inne czynniki charakterystyczne dla danego podsektora: ***został uznany za bank istotny przez Komisję Nadzoru Finansowego, w drodze decyzji administracyjnej zgodnie z art. 4b ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe***
			71. Świadczenie usług zaufania oraz wydawanie środków identyfikacji elektronicznej	1. Udział podmiotu świadczącego usługę kluczową w rynku: ***świadczenie usługi kluczowej przez***

			w rozumieniu przepisów o usługach zaufania	***bank istotny pod względem wielkości, organizacji wewnętrznej oraz rodzaju, zakresu i złożoności prowadzonej działalności, który spełnia co najmniej jeden z warunków: – udział banku w aktywach sektora bankowego jest nie mniejszy niż 2%, – udział banku w depozytach sektora bankowego jest nie mniejszy niż 2%, – udział banku w funduszach własnych sektora bankowego jest nie mniejszy niż 2%,*** 2. Inne czynniki charakterystyczne dla danego podsektora: ***został uznany za bank istotny przez Komisję Nadzoru Finansowego, w drodze decyzji administracyjnej zgodnie z art. 4b 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.	72. Wykonywanie czynności, o których mowa w art. 3 ustawy z dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo- -kredytowych w zakresie określonym w tym przepisie	1. liczba użytkowników zależnych od usługi kluczowej świadczonej przez dany podmiot: ***świadczenia usługi kluczowej przez spółdzielczą kasę oszczędnościowo-kredytową, której średnioroczna liczba członków przekracza 600 tys. osób,***

		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).	73. Prowadzenie rynku regulowanego lub innej działalności w zakresie organizowania obrotu instrumentami finansowymi oraz działalności związanej z tym obrotem	1. Inne czynniki charakterystyczne dla danego podsektora: ***wszystkie podmioty świadczące tę usługę, posiadające zezwolenie Komisji Nadzoru Finansowego (zgodnie z art. 25 ust. 1 ustawy o obrocie instrumentami finansowymi (Dz. U. z 2024 r. poz. 722 z późn. zm).***
		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.).	74. Prowadzenie alternatywnego systemu obrotu ASO)	1. Inne czynniki charakterystyczne dla danego podsektora: ***wszystkie podmioty świadczące tę usługę, posiadające zezwolenie Komisji Nadzoru Finansowego (zgodnie z art. 16 ust. 3 ustawy o obrocie instrumentami finansowymi (Dz. U. z 2024 r. poz. 722 z późn zm.).***
		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.).	75. Prowadzenie platformy aukcyjnej	1. Inne czynniki charakterystyczne dla danego podsektora: ***wszystkie podmioty świadczące tę usługę, posiadające zezwolenie Komisji Nadzoru Finansowego zgodnie z art. 29a ust. 1 lub ust. 2 ustawy o obrocie instrumentami finansowymi (Dz. U. z 2024 r. poz. 722 z późn zm.).***
		Podmiot prowadzący rynek regulowany, o którym mowa w art. 14 ust. 1 ustawy z dnia	76. Prowadzenie zorganizowanej platformy obrotu (OTF)	1. Inne czynniki charakterystyczne dla danego podsektora: ***wszystkie podmioty świadczące tę usługę,***

		29 lipca 2005 r. o obrocie instrumentami finansowymi (Dz. U. z 2024 r. poz. 722 z późn zm.).		***posiadające zezwolenie Komisji Nadzoru Finansowego (zgodnie z art. 16 ust. 5 ustawy o obrocie instrumentami finansowymi (Dz. U. z 2024 r. poz. 722 z późn zm.).***
		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.).	77. Prowadzenie działalności jako dostawca usług w zakresie udostępniania informacji.	1. Inne czynniki charakterystyczne dla danego podsektora: ***wszystkie podmioty świadczące tę usługę, posiadające zezwolenie Europejskiego Urzędu Nadzoru Giełd i Papierów Wartościowych (zgodnie z art. 27c ust. 1 Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 600/2014 z dnia 15 maja 2014 r. w sprawie rynków instrumentów finansowych oraz zmieniające rozporządzenie (UE) nr 648/2012 Dz.U.UE.L.2014.173.84 z dnia 2014.06.12) w zw. z art. 29c ust. 1 ustawy o obrocie instrumentami finansowymi (Dz. U. z 2024 r. poz. 722 z późn zm.).***
		Podmiot prowadzący rynek regulowany, o którym mowa w art. 14 ust. 1 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi	78. Prowadzenie działalności polegającej na świadczeniu usług finansowania społecznościowego.	1. Inne czynniki charakterystyczne dla danego podsektora: ***wszystkie podmioty świadczące tę usługę, posiadające zezwolenie wydane zgodnie z art. 12 ust. 1 rozporządzenia Parlamentu***

		(Dz. U. z 2024 r. poz. 722 z późn zm.).		***Europejskiego i Rady (UE) 2020/1503 z dnia 7 października 2020 r. w sprawie europejskich dostawców usług finansowania społecznościowego dla przedsięwzięć gospodarczych oraz zmieniające rozporządzenie (UE) 2017/1129 i dyrektywę (UE) 2019/1937 (Dz.U.UE.L.2020.347.1 z dnia 2020.10.20) w zw. z art. 21 ust. 2c ustawy o obrocie instrumentami finansowymi (Dz. U. z 2024 r. poz. 722 z późn zm.).***
		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.).	79. Organizowanie obrotu towarami giełdowymi.	1. Inne czynniki charakterystyczne dla danego podsektora: ***wszystkie podmioty świadczące tę usługę, które zawiadomiły Komisję Nadzoru Finansowego zgodnie z art. 21 ust. 3a ustawy o obrocie instrumentami finansowymi (Dz. U. 2024 r. poz. 722 z późn zm.) i wobec których Komisja Nadzoru Finansowego nie zgłosiła sprzeciwu wobec rozpoczęcia organizowania przez spółkę prowadzącą rynek regulowany obrotu towarami giełdowymi albo jego kontynuowania zgodnie z art. 21 ust. 3c ustawy 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 (Dz. U. z 2024 r. poz. 722 z późn zm.).	80. Działanie pomiędzy kontrahentami kontraktów będących w obrocie na co najmniej jednym rynku finansowym, polegające na staniu się nabywcą dla każdego sprzedawcy i sprzedawcą dla każdego nabywcy (CCP)	1. Inne czynniki charakterystyczne dla danego podsektora: ***wszystkie podmioty świadczące tę usługę, posiadające zezwolenie Komisji Nadzoru Finansowego (zgodnie z art. 14 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 648/2012 z dnia 4 lipca 2012 r. w sprawie instrumentów pochodnych będących przedmiotem obrotu poza rynkiem regulowanym, kontrahentów centralnych i repozytoriów transakcji (Dz.U.UE.L.2012.201.1 z dnia 2012.07.27).***
		Podmiot, o którym mowa w art. 48 ust. 7 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi (Dz. U. z 2024 r. poz. 722 z późn zm.).	81. Zadania, o których mowa w art. 48 ust. 1 pkt 1-6, ust. 2 i ust. 3 pkt 2 i 3 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi(Dz. U. z 2024 r. poz. 722 z późn zm.).	1. Inne czynniki charakterystyczne dla danego podsektora: ***wszystkie podmioty świadczące tę usługę na podstawie umowy z Krajowym Depozytem Papierów Wartościowych S.A.***
		Administratorzy kluczowych wskaźników referencyjnych.	82. Administrowanie kluczowych wskaźników referencyjnych.	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***wpisanie opracowywanego przez danego***

				Administratora wskaźnika referencyjnego na listę kluczowych wskaźników referencyjnych prowadzoną przez Komisję Europejską na podstawie art. 20 ust. 1 Rozporządzenia 2016/1011
		Centralny depozyt papierów wartościowych, o którym mowa w art. 3 pkt 21a ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi (Dz. U. z 2024 r. poz. 722, z późn zm.) mający siedzibę na terytorium Rzeczpospolitej Polskiej..	83. Prowadzenie systemu rozrachunku papierów wartościowych i świadczenie co najmniej jednej z następujących usług: pierwsza rejestracja papierów wartościowych w systemie zapisów księgowych lub zapewnianie i prowadzenie rachunków papierów wartościowych na najwyższym poziomie ewidencji	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***wszystkie podmioty świadczące tę usługę, , posiadające zezwolenie Komisji Nadzoru Finansowego (zgodnie z art. 16 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 909/2014 z dnia 23 lipca 2014 r. w sprawie usprawnienia rozrachunku papierów wartościowych w Unii Europejskiej i w sprawie centralnych depozytów papierów wartościowych, zmieniające dyrektywy 98/26/WE i 2014/65/UE oraz rozporządzenie (UE) nr 236/2012 (Dz.U.UE.L.2014.257.1 z dnia 2014.08.28).***
		Podmiot prowadzący ASO w rozumieniu art. 3 pkt 2 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami	84. Prowadzenie poza rynkiem regulowanym wielostronnego systemu kojarzącego oferty kupna i	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***podmiot prowadzący ASO w rozumieniu art. 3 pkt 2 ustawy z dnia 29 lipca 2005***

		finansowymi (Dz. U. z 2024 r. poz. 722).	sprzedaży instrumentów finansowych	***r. o obrocie instrumentami finansowymi (Dz. U. 2024 r. poz. 722, z późn zm.), który otrzymał zezwolenie na prowadzenie ASO wydane przez Komisję Nadzoru Finansowego***
		Podmiot prowadzący OTF w rozumieniu art. 3 pkt 10b ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi	85. Prowadzenie wielostronnego systemu kojarzącego w sposób uznaniowy składane przez odmioty trzecie oferty kupna i sprzedaży obligacji, strukturyzowanych produktów finansowych, uprawnień do emisji, instrumentów pochodnych lub produktów energetycznych będących przedmiotem obrotu hurtowego	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***podmiot prowadzący OTF w rozumieniu art. 3 pkt 10b ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi (Dz. U. 2024 r. poz. 722, z późn zm.), który otrzymał zezwolenie na prowadzenie OTF wydane przez Komisję Nadzoru Finansowego***
		Giełda towarowa, w rozumieniu art. 2 pkt 1 ustawy z dnia 26 października 2000 r. o giełdach towarowych (Dz. U. z 2024 r, poz. 910 z późn. zm.)	86. Prowadzenie giełdy towarowej.	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***wszystkie podmioty świadczące tę usługę, posiadające zezwolenie na prowadzenie giełdy towarowej (zgodnie z art. 7 ust. 1 ustawy z dnia 26 października 2000 r. o***

				giełdach towarowych (Dz. U. z 2024 r, poz. 910 z późn. zm.)
		Giełda towarowa, w rozumieniu art. 2 pkt 1 ustawy z dnia 26 października 2000 r. o giełdach towarowych (Dz. U. z 2024 r, poz. 910 z późn. zm.)	87. Prowadzenie rynku regulowanego w rozumieniu przepisów ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi (Dz. U. z 2024 r. poz. 722 z późn zm.), z uwzględnieniem ograniczeń z art. 5 ust. 2c ustawy z dnia 26 października 2000 r. o giełdach towarowych (Dz. U. z 2024 r, poz. 910 z późn. zm.)	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***wszystkie podmioty świadczące tę usługę, posiadające zezwolenie Komisji Nadzoru Finansowego (zgodnie z art. 25 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi (Dz. U. z 2024 r. poz. 722 z późn zm.) w zw. z art. 5 ust. 2b ustawy z dnia 26 października 2000 r. o giełdach towarowych (Dz. U. z 2024 r, poz. 910 z późn. zm.).***
		Giełda towarowa, w rozumieniu art. 2 pkt 1 ustawy z dnia 26 października 2000 r. o giełdach towarowych (Dz. U. z 2024 r. poz. 910,z późn. zm.)	88. Prowadzenie platformy aukcyjnej zgodnie z art. 5 ust. 2f ustawy z dnia 26 października 2000 r. o giełdach towarowych (Dz. U. z 2024 r. poz. 910, z późn. zm.)	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***wszystkie podmioty świadczące tę usługę, posiadające zezwolenie Komisji Nadzoru Finansowego zgodnie z art. 29a ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi (Dz. U. z 2024 r. poz. 722, z późn zm.) w zw. z art. 5 ust. 2f ustawy z dnia 26 października 2000 r. o giełdach towarowych (Dz. U. z 2024 r. poz. 910, z późn. zm.).***

		Giełda towarowa, w rozumieniu art. 2 pkt 1 ustawy z dnia 26 października 2000 r. o giełdach towarowych (Dz. U. z 2024 r, poz. 910 z późn. zm.)	89. Prowadzenie zorganizowanej platformy obrotu zgodnie z art. 5 ust. 2h i ust. 2i ustawy z dnia 26 października 2000 r. o giełdach towarowych (Dz. U. z 2024 r, poz. 910 z późn. zm.)	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***wszystkie podmioty świadczące tę usługę, , posiadające zezwolenie Komisji Nadzoru Finansowego (zgodnie z art. 25 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi (Dz. U. z 2024 r. poz. 722 z późn zm.) w zw. z art. 5 ust. 2j w zw. z ust. 2h i 2i ustawy z dnia 26 października 2000 r. o giełdach towarowych (Dz. U. z 2024 r, poz. 910 z późn. zm.).***
		Giełda towarowa, w rozumieniu art. 2 pkt 1 ustawy z dnia 26 października 2000 r. o giełdach towarowych (Dz. U. z 2024 r, poz. 910 z późn. zm.)	90. Prowadzenie działalności polegającej na świadczeniu usług finansowania społecznościowego	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***wszystkie podmioty świadczące tę usługę, , posiadające zezwolenie wydane zgodnie z art. 12 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2020/1503 z dnia 7 października 2020 r. w sprawie europejskich dostawców usług finansowania społecznościowego dla przedsięwzięć gospodarczych oraz zmieniające rozporządzenie (UE) 2017/1129 i dyrektywę (UE)***

				2019/1937 (Dz.U.UE.L.2020.347.1 z dnia 2020.10.20) w zw. z art. 21 ust. 2c ustawy o obrocie instrumentami finansowymi (Dz. U. z 2024 r. poz. 722 z późn zm.) w zw. z art. 5 ust. 2l ustawy z dnia 26 października 2000 r. o giełdach towarowych (Dz. U. z 2024 r. poz. 910, z późn. zm.).
		Giełda towarowa, w rozumieniu art. 2 pkt 1 ustawy z dnia 26 października 2000 r. o giełdach towarowych (Dz. U. z 2024 r, poz. 910 z późn. zm.)	91. Dokonywanie rozliczeń zgodnie z art. 5 ust. 3 ustawy z dnia 26 października 2000 r. o giełdach towarowych (Dz. U. z 2024 r, poz. 910 z późn. zm.)	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***wszystkie podmioty świadczące tę usługę, posiadające zezwolenie (zgodnie z art. 7 ustawy z dnia 26 października 2000 r. o giełdach towarowych (Dz. U. z 2024 r, poz. 910 z późn. zm.)***
		Giełdowa izba rozrachunkowa, w rozumieniu art. 2 pkt 4 ustawy z dnia 26 października 2000 r. o giełdach towarowych (Dz. U. z 2024 r, poz. 910 z późn. zm.)	92. Obsługa finansowa transakcji giełdowych oraz organizacja i prowadzenie rozliczeń transakcji giełdowych, a także zapewnienie przeprowadzania rozliczeń z tytułu transakcji giełdowych.	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***wszystkie podmioty świadczące tę usługę, , posiadające zezwolenie (zgodnie z art. 14 ust. 1 ustawy z dnia 26 października 2000 r. o giełdach towarowych (Dz. U. z 2024 r, poz. 910 z późn. zm.).***
		Izba rozliczeniowa w rozumieniu art. 68a ust. 1	93. Organizacja i prowadzenie rozliczeń	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora

		ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi (Dz. U. z 2024 r. poz. 722 z późn zm.).		jeżeli występują: ***wszystkie podmioty świadczące tę usługę, posiadające zezwolenie Komisji Nadzoru Finansowego (zgodnie z art. 68a ust. 5 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi (Dz. U. z 2024 r. poz. 722 z późn zm.).***
		Izba rozrachunkowa w rozumieniu art. 68a ust. 2 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi (Dz. U. z 2024 r. poz. 722 z późn zm.).	94. Organizacja i prowadzenie rozrachunku transakcji	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***wszystkie podmioty świadczące tę usługę, , posiadające zezwolenie (zgodnie z art. 68a ust. 5 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi (Dz. U. z 2024 r. poz. 722 z późn zm.).***
		Krajowa Izba Rozliczeniowa S.A.	95. Przetwarzanie i rozliczanie transakcji międzybankowych	1. Udział podmiotu krytycznego w rynku w odniesieniu do świadczonej usługi kluczowej, ***minimum 10 % udziału w rynku*** 2. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***podmiot świadczący tę usługę***

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.	96. Udzielanie świadczenia opieki zdrowotnej przez podmiot leczniczy	1. Inne czynniki charakterystyczne dla danego podsektora: ***świadczeniodawca zakwalifikowany do systemu podstawowego szpitalnego zabezpieczenia świadczeń opieki zdrowotnej w ramach tzw. „sieci szpitali" oraz posiadający Szpitalny Oddział Ratunkowy***
			97. Świadczenie usługi: Szpitalnego Oddziału Ratunkowego, Centrum Urazowego lub Centrum Urazowego dla Dzieci.	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***podmioty posiadające Szpitalny Oddział Ratunkowy, Centrum Urazowego lub Centrum Urazowego dla Dzieci***
		Podmiot leczniczy, o którym mowa w art. 4 ust. 1 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej.	98. Kierowanie jednostkami systemu Państwowego Ratownictwa Medycznego	1. Inne czynniki charakterystyczne dla danego podsektora: ***zapewnienie dostępu do usługi dla wszystkich usługobiorców.***
		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	99. Wykonywanie analiz medycznych	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***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***

		decyzji nr 1082/2013/UE (Dz. Urz. UE L 314 z 06.12.2022, str. 1)		***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.	100. Gromadzenie i udostępnianie Elektronicznej Dokumentacji Medycznej	1. Inne czynniki charakterystyczne dla danego podsektora: ***zapewnienie dostępu do usługi dla wszystkich usługobiorców***
		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 2024 r. poz. 652 i 1222).	101. Utrzymanie Systemu Wspomagania Dowodzenia Państwowego Ratownictwa Medycznego	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***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 2024 r. poz. 652 i 1222).***
		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. 281 i 1229).	102. Pozyskiwanie gromadzenie, konserwacja, przechowywanie i przekazywanie krwi i jej składników	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują ***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. 281 i 1229) o***

				znaczeniu krajowym i wojewódzkim.
		Podmioty udzielające świadczeń opieki zdrowotnej, w rozumieniu art. 133 ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (Dz. U. z 2024 r. poz. 146, 858 i 1222).	103. Zlecanie przez świadczeniodawców podwykonawcom udzielania świadczeń opieki zdrowotnej w ramach umowy o udzielanie świadczeń opieki zdrowotnej	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***podmioty udzielające świadczeń opieki zdrowotnej, w rozumieniu art. 133 ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych***

	Produkcja, dystrybucja, obrót i magazynowanie substancji czynnych, produktów leczniczych i wyrobów medycznych	Urząd Rejestracji Produktów Leczniczych, Wyrobów Medycznych i Produktów Biobójczych.	104. Prowadzenie rejestru produktów leczniczych, wyrobów medycznych i produktów biobójczych	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: **Urząd Rejestracji Produktów Leczniczych, Wyrobów Medycznych i Produktów Biobójczych.**
		Urzędy obsługujące organy Inspekcji Farmaceutycznej.	105. Obsługa organów inspekcji farmaceutycznej	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: **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.).	106. Prowadzenie działalności badawczo-rozwojowej w zakresie produktów leczniczych	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***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***
		Przedsiębiorca prowadzący działalność polegającą na prowadzeniu hurtowni	107. Obrót, dystrybucja, magazynowanie produktów leczniczych	1. Udział podmiotu krytycznego w rynku w odniesieniu do świadczonej

		farmaceutycznej w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne (Dz. U. z 2024 r. poz. 686).		usługi kluczowej, ***minimum 10 % udziału w rynku*** 2. Inne czynniki charakterystyczne dla danego podsektora: ***zapewnienie dostępu do usługi dla wszystkich usługobiorców***
		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.	108. Dopuszczenie do obrotu produktu leczniczego	1. Inne czynniki charakterystyczne dla danego podsektora: ***kwota refundacji produktów leczniczych powyżej 1 mld PLN za ostatni rok kalendarzowy***
		Wytwórca lub importer produktu leczniczego w rozumieniu ustawy z dnia 6 września 2001 r.– Prawo farmaceutyczne	109. Wytwarzanie lub Import produktów leczniczych	1. Inne czynniki charakterystyczne dla danego podsektora: ***kwota refundacji produktów leczniczych znajdujących się w wykazach produktów leczniczych, wyrobów medycznych oraz środków spożywczych specjalnego przeznaczenia żywieniowego***

				zagrożonych brakiem dostępności na terytorium RP, wydawanych na podstawie art. 37av ust. 14 ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne – powyżej 50 mln PLN za ostatni rok kalendarzowy
		Wytwórca, importer lub dystrybutor substancji czynnej w rozumieniu ustawy z dnia 6 września 2001 r.– Prawo farmaceutyczne	110. Produkcja, Obrót i dystrybucja substancji czynnej	1. Inne czynniki charakterystyczne dla danego podsektora: ***kwota refundacji produktów leczniczych znajdujących się w wykazach produktów leczniczych, wyrobów medycznych oraz środków spożywczych specjalnego przeznaczenia żywieniowego zagrożonych brakiem dostępności na terytorium RP, wydawanych na podstawie art. 37av ust. 14 ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne – powyżej 50 mln PLN za ostatni rok kalendarzowy***

		Importer równoległy w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne.	111. Obrót i dystrybucja produktów leczniczych	1. Inne czynniki charakterystyczne dla danego podsektora: ***kwota refundacji produktów leczniczych znajdujących się w wykazach produktów leczniczych, wyrobów medycznych oraz środków spożywczych specjalnego przeznaczenia żywieniowego zagrożonych brakiem dostępności na terytorium RP, wydawanych na podstawie art. 37av ust. 14 ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne – powyżej 50 mln PLN za ostatni rok kalendarzowy***

		Przedsiębiorca prowadzący działalność w formie apteki ogólnodostępnej w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne.	112. Obrót, dystrybucja produktów leczniczych	1. Inne czynniki charakterystyczne dla danego podsektora: ***przedsiębiorca prowadzący działalność gospodarczą polegającą na prowadzeniu co najmniej 4 aptek ogólnodostępnych zapewniających dostępność świadczeń w porze nocnej, niedzielę, święta i inne dni wolne od pracy na podstawie uchwały rady powiatu w trybie określonym w art. 94 ust. 1 i 2 ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne***
		Podmiot o którym mowa w art. 96 ust 1. ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (Dz.U.2024.0.146)	113. Świadczenie opieki zdrowotnej	1. Inne czynniki charakterystyczne dla danego podsektora: ***objęcie usługą wszystkich świadczeniodawców mających zawartą umowę o udzielanie świadczeń opieki zdrowotnej***
		Podmiot o którym mowa w art. 1 ustawy o Agencji Badań Medycznych.	114. Innowacje w zakresie dostępności i zwiększenia bezpieczeństwa oraz terapeutyczności produktów leczniczych	1. Inne czynniki charakterystyczne dla danego podsektora: ***objęcie usługą wszystkich świadczeniodawców mających zawartą umowę o udzielanie świadczeń opieki zdrowotnej***

		Podmiot o którym mowa w art. 95 i 95a ustawy prawo farmeceutyczne	115. Zapewnienie dostępności produktów leczniczych i wyrobów medycznych	1. Inne czynniki charakterystyczne dla danego podsektora: ***objęcie usługą wszystkich świadczeniodawców mających zawartą umowę o udzielanie świadczeń***
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.	116. Ujmowanie wody	1. Liczba użytkowników zależnych od usługi kluczowej: ***ujmowanie wody dla minimum 500 tys. podłączonych mieszkańców w ramach zbiorowego zaopatrzenia w wodę,***
		Podmiot dostarczający wodę przeznaczoną do spożycia przez ludzi, w tym przedsiębiorstwo wodociągowo-kanalizacyjne	117. Uzdatnianie wody	1. Liczba użytkowników zależnych od usługi kluczowej: ***uzdatnianie wody dla minimum 500 tys. podłączonych mieszkańców w***

		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.		***ramach zbiorowego zaopatrzenia w wodę***,
		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	118. Dostarczanie wody	1. Liczba użytkowników zależnych od usługi kluczowej: ***dostarczanie wody dla minimum 500 tys. podłączonych mieszkańców w ramach zbiorowego zaopatrzenia w wodę***

		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 istotna częścią ich ogólnej działalności.	119. 119. Odprowadzanie ścieków	1. liczba użytkowników zależnych od usługi kluczowej świadczonej przez dany podmiot: ***obsługa aglomeracji o równoważnej liczbie mieszkańców (RLM), o której mowa w art. 86 ust. 3 pkt 2 ustawy z dnia 20 lipca 2017 r. – Prawo wodne, powyżej 500 tys.***
		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	120. Oczyszczanie ścieków	1. liczba użytkowników zależnych od usługi kluczowej świadczonej przez dany podmiot: ***obsługa aglomeracji o równoważnej liczbie mieszkańców (RLM), o której mowa w art. 86 ust. 3 pkt 2 ustawy z dnia 20 lipca 2017 r. – Prawo wodne, powyżej 500 tys.,***

		oczyszczanie ścieków jest inną niż istotna częścią ich ogólnej działalności.		
Infrastruktura cyfrowa	Infrastruktura cyfrowa z wyłączeniem komunikacji elektronicznej	Dostawca punktu wymiany ruchu internetowego.	121. Wymiana ruchu internetowego	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***podmiot świadczący tę usługę***
		Dostawca usług DNS, z wyłączeniem operatorów głównych serwerów nazw.	122. Prowadzenie autorytatywnego serwera DNS	1. Inne czynniki charakterystyczne dla danego podsektora: ***minimalnie 100 tys. nazw domen, dla których serwer jest autorytatywny***
		Rejestr nazw domen najwyższego poziomu (TLD).	123. Prowadzenie rejestru domeny najwyższego poziomu (TLD)	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***podmiot świadczący tę usługę***
		Dostawca usług chmurowej.	124. Dostarczanie usług chmurowych	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***podmiot świadczący tę usługę***
		Dostawca usług ośrodka przetwarzania danych.	125. Dostarczanie usług ośrodka przetwarzania danych	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***podmiot świadczący tę usługę***
		Dostawca sieci dostarczania treści.	126. Dostarczanie treści	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora

				jeżeli występują: ***podmiot świadczący tę usługę***
		Dostawca usług zaufania.	127. Dostarczanie usług zaufania	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***podmiot świadczący tę usługę***
		Podmiot świadczący usługę rejestracji nazw domen.	128. Świadczenie usługi rejestracji nazw domen	1. Inne czynniki charakterystyczne dla danego podsektora: ***prowadzenie przynajmniej jednego rejestru domeny najwyższego poziomu (TLD) dla co najmniej 100 tys. abonentów***
	Komunikacja elektroniczna	Przedsiębiorca komunikacji elektronicznej.	129. Świadczenie usług telekomunikacyjnych	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***podmiot będący przedsiębiorcą telekomunikacyjnym lub podmiot świadczący publicznie dostępną usługę komunikacji interpersonalnej niewykorzystującą numerów***
			130. Świadczenie usług komunikacji interpersonalnej niewykorzystującej numerów	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***podmiot świadczący publicznie dostępną usługę***
		Jednostki sektora finansów publicznych, o których	131. Zapewnienie dostępu do służb ratowniczych	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora

Administracja publiczna		mowa w art. 9 pkt 1 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych oraz urzędy je obsługujące	132. Zapewnienie możliwości przekraczania granic RP 133. Zapewnienia dostępu do rejestrów państwowych 134. Zapewnienia dostępu do rejestrów publicznych uznanych za bardzo istotne 135. Zapewnienie dostępu do systemu Informacyjnego Schengen 136. Zapewnienie dostępu do usług udostępnianych poprzez portal w domenie gov.pl	jeżeli występują: ***podmiot świadczący tę usługę***
		Jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 3, 5, 6 8, 9, 11 i 12 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych	137. Zapewnienie dostępu do służb ratowniczych 138. Zapewnienie możliwości przekraczania granic RP 139. Zapewnienia dostępu do rejestrów państwowych 140. Zapewnienia dostępu do rejestrów publicznych uznanych za bardzo istotne 141. Zapewnienie dostępu do systemu Informacyjnego Schengen 142. Zapewnienie dostępu do usług udostępnianych	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***podmiot świadczący tę usługę***

			poprzez portal w domenie gov.pl	
		Instytuty badawcze o których mowa w art. 1.1 ustawy z dnia 30 kwietnia 2010 r. o instytutach badawczych (Dz. U. 2010 Nr 96 poz. 618)	143. Prowadzenie badania naukowe i prace rozwojowe ukierunkowane na ich wdrożenie i zastosowanie w praktyce	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***podmiot świadczący tę usługę***
		Bank Gospodarstwa Krajowego o którym mowa w ustawie z dnia 14 marca 2003 r. o Banku Gospodarstwa Krajowego	144. Realizacja zadań wskazanych w ustawie z dnia 14 marca 2003 r. o Banku Gospodarstwa Krajowego	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***podmiot świadczący tę usługę***
		Urząd Dozoru Technicznego o którym mowa w ustawie z dnia 21 grudnia 2000 r. o dozorze technicznym Dz. U. 2000 Nr 122 poz. 1321	145. Realizacja zadań wskazanych w ustawie z dnia 21 grudnia 2000 r. o dozorze technicznym	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***podmiot świadczący tę usługę***
		Polska Agencja Żeglugi Powietrznej o której mowa w ustawie z dnia 8 grudnia 2006 r. o Polskiej Agencji Żeglugi Powietrznej Dz. U. 2006 Nr 249 poz. 1829	146. Realizacja zadań wskazanych w ustawie z dnia 8 grudnia 2006 r. o Polskiej Agencji Żeglugi Powietrznej	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***podmiot świadczący tę usługę***
		Polskie Centrum Akredytacji o którym mowa w art. 58 ustawy z dnia 30 sierpnia	147. Realizacja zadań przypisanych Polskiemu Centrum Akredytacji	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora

		2002 r. o systemie oceny zgodności Dz. U. 2002 Nr 166 poz. 1360	zawartych w ustawie z dnia 30 sierpnia 2002 r. o systemie oceny zgodności	jeżeli występują: ***podmiot świadczący tę usługę***
		Urząd Komisji Nadzoru Finansowego o którym mowa w art. 3.1 ustawy z dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym Dz. U. 2006 Nr 157 poz. 1119	148. Realizacja zadań przypisanych Komisji Nadzoru Finansowego zawartych w ustawie dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***podmiot świadczący tę usługę***
		Polska Agencja Prasowa o której mowa w ustawie z dnia 31 lipca 1997 r. o Polskiej Agencji Prasowej Dz. U. 1997 Nr 107 poz. 687	149. Uzyskiwanie i przekazywanie odbiorcom rzetelne, obiektywne i wszechstronne informacje z kraju i z zagranicy	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***podmiot świadczący tę usługę***
		Państwowe Gospodarstwo Wodne Wody Polskie, o którym mowa w ustawie z dnia 20 lipca 2017 r. – Prawo wodne (Dz. U. z 2024 r. poz. 1087 i 1089)	150. Kształtowanie i ochrona zasobów wodnych, korzystanie z wód oraz zarządzanie zasobami wodnymi	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***podmiot świadczący tę usługę***
		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	151. Funkcjonowanie systemu instytucji rozwoju	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***podmiot świadczący tę usługę***

		Narodowy Fundusz Ochrony Środowiska i Gospodarki Wodnej o którym mowa w ustawie z dnia 27 kwietnia 2001 r. - Prawo ochrony środowiska (Dz. U. z 2024 r. poz. 54, z późn. zm.).	152. Ochrona środowiska i warunki korzystania z jego zasobów	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***podmiot świadczący tę usługę***
		Państwowy Fundusz Rehabilitacji Osób Niepełnosprawnych o którym mowa w ustawie z dnia 27 sierpnia 1997 r. o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych Dz. U. 1997 Nr 123 poz. 776	153. Realizacja zadań przez Państwowy Fundusz Rehabilitacji Osób Niepełnosprawnych	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***podmiot świadczący tę usługę***
		Zakład Unieszkodliwiania Odpadów Promieniotwórczych z siedzibą w Otwocku Świerku	154. Unieszkodliwianie odpadów promieniotwórczych	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***podmiot świadczący tę usługę***
		Spółki prawa handlowego wykonujące zadania – o charakterze użyteczności publicznej w rozumieniu art. 1 ust. 2 ustawy z dnia 20 grudnia 1996 r. o gospodarce	155. Realizacja zadań o charakterze użyteczności publicznej, których celem jest bieżące i nieprzerwane zaspokajanie zbiorowych potrzeb ludności w drodze	1. Udział podmiotu krytycznego w rynku w odniesieniu do świadczonej usługi kluczowej: ***minimum 10 % udziału w rynku*** 2. Inne czynniki charakterystyczne dla danego sektora lub podsektora

		komunalnej (Dz. U. z 2021 r. poz. 679).	świadczenia usług powszechnie dostępnych	jeżeli występują: ***podmiot świadczący tę usługę***
		Podmioty zarządzające/odpowiedzialne za stan techniczny oraz sprawność infrastruktury przeciwpowodziowej, budowli hydrotechnicznych i pozostałych obiektów o charakterze inżynierskim.	156. Utrzymanie infrastruktury przeciwpowodziowej, budowli hydrotechnicznych i pozostałych obiektów o charakterze inżynierskim w należytym stanie technicznym	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***podmiot świadczący tę usługę***
Przestrzeń kosmiczna		Operator infrastruktury naziemnej, który wspiera świadczenie usług kosmicznych, z wyjątkiem przedsiębiorców publicznej sieci łączności elektronicznej.	157. System satelitarny wspomagający GPS	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***podmiot świadczący tę usługę***
		Podmiot o którym mowa w art. 1.1. ustawy z dnia 26 września 2014 r. o Polskiej Agencji Kosmicznej Dz. U. 2014 poz. 1533	158. Realizacja zadań wskazanych w art.3 ustawy z dnia 26 września 2014 r. o Polskiej Agencji Kosmicznej	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***podmiot świadczący tę usługę***
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.	159. Produkcja, przetwarzanie i dystrybucja żywności	1. Udział podmiotu krytycznego w rynku w odniesieniu do świadczonej usługi kluczowej: ***minimum 10 % udziału w rynku***

		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.).		2. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***podmiot świadczący tę usługę***
	Produkcja pasz	Podmioty wskazane w art. 3 ust. 4 rozporządzenia (WE) nr 178/2002 Parlamentu Europejskiego i Rady z dnia 28 stycznia 2002 r. ustanawiającego ogólne zasady i wymagania prawa żywnościowego, powołującego Europejski Urząd do Spraw Bezpieczeństwa Żywności oraz ustanawiającego procedury w sprawie bezpieczeństwa żywności.	160. Produkcja pasz	1. Udział podmiotu krytycznego w rynku w odniesieniu do świadczonej usługi kluczowej: ***minimum 10 % udziału w rynku*** 2. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***podmiot świadczący tę usługę***

	Utylizacja	Zakłady przetwórcze kategorii 1, 2 i 3 oraz spalarnie, w rozumieniu rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 1069/2009 z dnia 21 października 2009 r. określającego przepisy sanitarne dotyczące produktów ubocznych pochodzenia zwierzęcego, nieprzeznaczonych do spożycia przez ludzi, i uchylającego rozporządzenie (WE) nr 1774/2002 (rozporządzenie o produktach ubocznych pochodzenia zwierzęcego).	161. Utylizacja	1. Udział podmiotu krytycznego w rynku w odniesieniu do świadczonej usługi kluczowej: ***minimum 10 % udziału w rynku*** 2. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***podmiot świadczący tę usługę***
Zarządzanie usługami ICT		Dostawca usług zarządzanych	162. Dostawca usług ICT	1. Udział podmiotu krytycznego w rynku w odniesieniu do świadczonej usługi kluczowej: ***minimum 10 % udziału w rynku*** 2. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***podmiot świadczący tę usługę***

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.	163. Produkcja oraz wytwarzanie i dystrybucja substancji lub mieszanin substancji chemicznych	1. Udział podmiotu krytycznego w rynku w odniesieniu do świadczonej usługi kluczowej: ***minimum 10 % udziału w rynku*** 2. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***podmiot świadczący tę usługę***
		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.	164. Wytwarzanie z substancji lub mieszanin wyrobów chemicznych	1. Udział podmiotu krytycznego w rynku w odniesieniu do świadczonej usługi kluczowej: ***minimum 10 % udziału w rynku*** 2. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***podmiot świadczący tę usługę***
Usługi pocztowe		Operator pocztowy, o którym mowa w art. 3 pkt 12 ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe.	165. Dystrybucja pocztowa i kurierska	1. Udział podmiotu krytycznego w rynku w odniesieniu do świadczonej usługi kluczowej: **minimum 10 % udziału w rynku** 2. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***podmiot świadczący tę usługę***
Gospodarowanie odpadami	Zbieranie odpadów	Przedsiębiorstwa świadczące usługi w rozumieniu ustawy z dnia 14 grudnia 2012 r. o	166. Zbieranie odpadów	1. Udział podmiotu krytycznego w rynku w odniesieniu do świadczonej

		odpadach (Dz. U. z 2023 r. poz.1587, 1597, 1688, 1852 i 2029), polegające na zbieraniu odpadów, zobowiązane do uzyskania wpisu w rejestrze, o którym mowa w art. 49 ust. 1 ustawy o odpadach.		usługi kluczowej: ***minimum 10 % udziału w rynku*** 2. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli wytępują: ***podmiot świadczący tę usługę***
	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.	167. Transport odpadów	1. Udział podmiotu krytycznego w rynku w odniesieniu do świadczonej usługi kluczowej: ***minimum 10 % udziału w rynku*** 2. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***podmiot świadczący tę usługę***
			168. Transport odpadów zakaźnych	1. Udział podmiotu krytycznego w rynku w odniesieniu do świadczonej usługi kluczowej: ***minimum 10 % udziału w rynku*** 2. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***podmiot świadczący tę usługę***
			169. Transport innych odpadów niebezpiecznych	1. Udział podmiotu krytycznego w rynku w odniesieniu do świadczonej

				usługi kluczowej: ***minimum 10 % udziału w rynku*** 2. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***podmiot świadczący tę usługę***
			170. Transport odpadów komunalnych	1. Liczba użytkowników zależnych od usługi kluczowej świadczonej przez dany podmiot: ***minimum 250 tys. mieszkańców*** 2. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***podmiot świadczący tę usługę***
	Przetwarzanie odpadów 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, 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	171. Przetwarzanie odpadów, wraz z nadzorem nad wymienionymi działaniami, a także późniejsze postępowanie z miejscami unieszkodliwiania odpadów	1. Liczba użytkowników zależnych od usługi kluczowej świadczonej przez dany podmiot: ***min. 250 tys. mieszkańców*** 2. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***podmiot świadczący tę usługę***

		ustawy z dnia 14 grudnia 2012 r. o odpadach.		
	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.	172. Działania wykonywane w charakterze sprzedawcy odpadów lub pośrednika w obrocie odpadami	1. Udział podmiotu krytycznego w rynku w odniesieniu do świadczonej usługi kluczowej: ***minimum 10 % udziału w rynku*** 2. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***podmiot świadczący tę usługę***

			173. Termiczne przekształcanie i składowanie odpadów niebezpiecznych i komunalnych	1. Udział podmiotu krytycznego w rynku w odniesieniu do świadczonej usługi kluczowej: ***minimum 10 % udziału w rynku*** 2. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***podmiot świadczący tę usługę***
			174. Termiczne przekształcanie odpadów zakaźnych, medycznych i zakaźnych weterynaryjnych	1. Udział podmiotu krytycznego w rynku w odniesieniu do świadczonej usługi kluczowej: ***minimum 10 % udziału w rynku*** 2. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***podmiot świadczący tę usługę***
			175. Gospodarowanie pozostałymi odpadami	1. Udział podmiotu krytycznego w rynku w odniesieniu do świadczonej usługi kluczowej: ***minimum 10 % udziału w rynku*** 2. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***podmiot świadczący tę usługę***

Finanse publiczne		Bank, o którym mowa w art. 2 ustawy z dnia 14 marca 2003 r. o Banku Gospodarstwa Krajowego (Dz. U. z 2024 r. poz. 441 z późn. zm.)	176. Wspieranie zrównoważonego rozwoju społeczno-gospodarczego Polski.	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***podmiot świadczący tę usługę***
		Podmiot, o którym mowa w art. 67 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe (Dz. U. z 2023 r. poz. 2488 z późn. zm.)	177. Ustalanie wierzytelności zleceń płatniczych	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***podmiot świadczący tę usługę***
		Podmiot, o którym mowa w art. 66 ustawa z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych (Dz. U. z 2024 r. poz. 497)	178. Nadzorowanie systemu ubezpieczeń społecznych	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***podmiot świadczący tę usługę***
		Podmiot, o którym mowa w art. 2 ust. 1 ustawy z dnia 20 grudnia 1990 r. o ubezpieczeniu społecznym rolników (Dz. U. z 2024 r. poz. 90 z późn. zm.)	179. Nadzorowanie systemu ubezpieczeń społecznych rolników	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***podmiot świadczący tę usługę***
		Spółka, o której mowa w pkt 17 załącznika do rozporządzenia Prezesa Rady Ministrów z dnia 24 września 2021 r. w sprawie	180. Produkcja krajowych dokumentów identyfikacyjnych	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***podmiot świadczący tę usługę***

		wykazu spółek o istotnym znaczeniu dla gospodarki państwa (Dz. U. poz. 1782).		
		Spółka, o której mowa w pkt 17 załącznika do rozporządzenia Prezesa Rady Ministrów z dnia 24 września 2021 r. w sprawie wykazu spółek o istotnym znaczeniu dla gospodarki państwa (Dz. U. poz. 1782).	181. Produkcja i personalizacja krajowych dokumentów komunikacyjnych	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***podmiot świadczący tę usługę***
		Podmiot, o którym mowa w § 1 załącznika do zarządzenia Ministra Finansów, Funduszy i Polityki Regionalnej z dnia 27 listopada 2020 r. w sprawie nadania statutu Centrum Informatyki Resortu Finansów (Dz. Urz. MF z 2022 r. poz. 68 z późn. zm.)	182. Świadczenie usług Teleinformatycznych na rzecz Ministerstwa Finansów	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***podmiot świadczący tę usługę***

		Spółka celowa, o której mowa w art. 2 ust. 1 obwieszczenia Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 22 stycznia 2021 r. w sprawie ogłoszenia jednolitego tekstu ustawy o szczególnych zasadach wykonywania niektórych zadań dotyczących informatyzacji w zakresie działów administracji rządowej budżet i finanse publiczne (Dz.U. 2021 poz. 186).	183. Zadania dotyczące informatyzacji w zakresie działów administracji rządowej budżet i finanse publiczne.	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora jeżeli występują: ***podmiot świadczący tę usługę***

UZASADNIENIE

Projektowane rozporządzenie stanowi wykonanie upoważnienia ustawowego z art. 6zp ust. 3 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, zwanej dalej „ustawą" i określa wykaz usług kluczowych oraz progi istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych.

Przedmiotowy projekt rozporządzenia w zakresie swojej regulacji wdraża do polskiego porządku prawnego dyrektywę 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 333 z 27.12.2022 r. str. 164).

Wykaz usług kluczowych będący załącznikiem do niniejszego rozporządzenia uwzględnia podział na sektory, podsektory, rodzaje podmiotów określone w załączniku ustawy oraz progi istotności skutku zakłócającego incydentu dla usługi kluczowej.

Wykaz usług kluczowych został sporządzony w oparciu o usługi kluczowe wskazane przez organy właściwe organy do spraw podmiotów krytycznych. Wykaz usług kluczowych będzie wykorzystywany w procesie identyfikacji i uznawania operatora infrastruktury krytycznej w danym sektorze lub podsektorze, wymienionych w załączniku do ustawy, za podmiot krytyczny.

W procesach inicjowania wpisów do wykazu organy do spraw podmiotów krytycznych będą dokonywać oceny, czy określona usługa znajduje się w załączniku do niniejszego rozporządzenia. Następnie właściwy organ określi jaki jest poziom skutku zakłócającego dla świadczonej usługi kluczowej.

Ustalenie wykazu usług kluczowych oraz progów istotności skutku zakłócającego nastąpiło we współpracy z organami do spraw podmiotów krytycznych, które będą przedkładać wnioski o wpis do wykazu podmiotów krytycznych.

Projektowane rozwiązania wejdą w życie po upływie 14 od dnia ogłoszenia

Projekt rozporządzenia nie podlega notyfikacji zgodnie z przepisami dotyczącymi funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych.

Projekt rozporządzenia nie jest sprzecznym 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.

Nazwa projektu Rozporządzenie Rady Ministrów w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych **Ministerstwo wiodące i ministerstwa współpracujące** **Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu** **Kontakt do opiekuna merytorycznego projektu**	**Data sporządzenia** **Źródło:** **Nr w wykazie prac …….**

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym przewiduje identyfikację podmiotów krytycznych przez organy do spraw podmiotów krytycznych. Uznanie operatora infrastruktury krytycznej za podmiot krytyczny nastąpi w przypadku dokonania jego wpisu do wykazu podmiotów krytycznych.

Operator infrastruktury krytycznej zostaje wpisany do wykazu podmiotów krytycznych w przypadku gdy:
1) świadczy co najmniej jedną usługę kluczową;
2) incydent miałby istotny skutek zakłócający dla świadczenia usługi kluczowej.

Dlatego też w ustawie zawarto upoważnienie ustawowe, w którym Rada Ministrów określi, w drodze rozporządzenia wykaz usług kluczowych w podziale na sektory, podsektory i kategorie podmiotów wymienionych w załączniku do ustawy oraz progi istotności skutku zakłócającego dla świadczenia usług kluczowych, wymienionych w wykazie usług kluczowych.

2. Rekomendowane rozwiązanie, w tym planowane narzędzia interwencji, i oczekiwany efekt

Wydanie rozporządzenia określającego wykaz usług kluczowych oraz progi istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych.
Rozporządzenie zawiera wykaz usług kluczowych oraz progi istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych, które są niezbędne do identyfikacji podmiotów krytycznych w celu wpisania ich do wykazu podmiotów krytycznych, a tym samym nałożenia obowiązków wynikających z ustawy o zarządzaniu kryzysowym.

Wykaz usług kluczowych będzie wykorzystywany przez organy do spraw podmiotów krytycznych do wyłaniania podmiotów w poszczególnych sektorach i podsektorach. W procesie ujmowania w wykazie organy właściwe będą dokonywać oceny, czy określona usługa znajduje się w załączniku do niniejszego rozporządzenia. W kolejnych krokach w oparciu o stworzony wykaz właściwy organ będzie określał jaki jest poziom skutku zakłócającego dla świadczonej usługi kluczowej.

3. Jak problem został rozwiązany w innych krajach, w szczególności krajach członkowskich OECD/UE?

4. Podmioty, na które oddziałuje projekt

Grupa	Wielkość	Źródło danych	Oddziaływanie
(dodaj/usuń)			
(dodaj/usuń)			
(dodaj/usuń)			
(dodaj/usuń)			
(dodaj/usuń)			

5. Informacje na temat zakresu, czasu trwania i podsumowanie wyników 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												
budżet państwa												
JST												
pozostałe jednostki (oddzielnie)												
Wydatki ogółem												
budżet państwa												
JST												
pozostałe jednostki (oddzielnie)												
Saldo ogółem												
budżet państwa												
JST												
pozostałe jednostki (oddzielnie)												

Źródła finansowania	Rozporządzenie nie powoduje konieczności wydatkowania środków finansowych z budżet państwa.
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	Nie dotyczy

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							
	(dodaj/usuń)							
W ujęciu niepieniężnym	duże przedsiębiorstwa							
	sektor mikro-, małych i średnich							

	przedsiębiorstw	
	rodzina, obywatele oraz gospodarstwa domowe	
	(dodaj/usuń)	
Niemierzalne	(dodaj/usuń)	
	(dodaj/usuń)	

Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	

8. Zmiana obciążeń regulacyjnych (w tym obowiązków informacyjnych) wynikających z projektu

X 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:	☐ zwiększenie liczby dokumentów ☐ zwiększenie liczby procedur ☐ wydłużenie czasu na załatwienie sprawy ☐ inne:
Wprowadzane obciążenia są przystosowane do ich elektronizacji.	☐ tak ☐ nie ☐ nie dotyczy

Komentarz:

9. Wpływ na rynek pracy

10. Wpływ na pozostałe obszary

☐ środowisko naturalne ☐ sytuacja i rozwój regionalny ☐ sądy powszechne, administracyjne lub wojskowe	☐ demografia ☐ mienie państwowe ☐ inne:	☐ informatyzacja ☐ zdrowie

Omówienie 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?

Nie dotyczy.

13. Załączniki (istotne dokumenty źródłowe, badania, analizy itp.)

Nie dotyczy.

Projekt

R O Z P O R Z Ą D Z E N I E

R A D Y M I N I S T R Ó W

z dnia

w sprawie wykazu norm, które podmiot krytyczny uwzględnia przy wdrażaniu rozwiązań organizacyjno-technicznych

Na podstawie art. 6zt ust. 5 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. …) zarządza się, co następuje:

§ 1. Wykaz norm oraz wytycznych do ich stosowania, które podmiot krytyczny uwzględnia przy wdrażaniu rozwiązań organizacyjno-technicznych, o których mowa w art. 6zt ust 1 pkt 2 ustawy o zarządzaniu kryzysowym, jest określony w załączniku do rozporządzenia.

§ 2. Rozporządzenie wchodzi w życie po upływie 14 dni od ogłoszenia.

P R E Z E S R A D Y M I N I S T R Ó W

Załącznik
do rozporządzenia Rady Ministrów
z dnia
Dz. U. poz.

Wykaz norm oraz wytycznych do ich stosowania

L.p.	Normy	Wytyczne do stosowania norm
1	PN-EN ISO/IEC 27001 Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności. Systemy zarządzania bezpieczeństwem informacji. Wymagania	PN-EN ISO/IEC 27002 Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności. Zabezpieczanie informacji
2	PN-EN ISO 22301 Bezpieczeństwo i odporność. Systemy zarządzania ciągłością działania. Wymagania	PN-EN ISO 22313 Bezpieczeństwo i odporność. Systemy zarządzania ciągłością działania. Wytyczne dotyczące stosowania ISO 22301
3	PN-EN 50131-1 Systemy alarmowe. Systemy sygnalizacji włamania i napadu. Część 1: Wymagania systemowe	PKN-CLC/TS 50131-7 Systemy alarmowe. Systemy sygnalizacji włamania i napadu. Część 7: Wytyczne stosowania
4	PN-EN 60839-11-1 Systemy alarmowe i elektroniczne systemy zabezpieczeń. Część 11-1: Elektroniczne systemy kontroli dostępu. Wymagania dotyczące systemów i komponentów	PN-EN 60839-11-2 Systemy alarmowe i elektroniczne systemy zabezpieczeń. Część 11-2: Elektroniczne systemy kontroli dostępu. Wytyczne stosowania

5	PN-EN 62676-1-1 Systemy dozoru wizyjnego stosowane w zabezpieczeniach. Część 1-1: Wymagania systemowe. Postanowienia ogólne	PN-EN 62676-4 Systemy dozoru wizyjnego stosowane w zabezpieczeniach. Część 4: Wytyczne stosowania

UZASADNIENIE

Projektowane rozporządzenie stanowi wykonanie upoważnienia ustawowego z art. 6zt. ust. 5 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, zwanej dalej „ustawą" i określa wykaz norm, które podmiot krytyczny uwzględnia przy wdrażaniu rozwiązań organizacyjno-technicznych, o których mowa w art. 6zt. ust. 1 pkt. 2.

Przedmiotowy projekt rozporządzenia w zakresie swojej regulacji wdraża do polskiego porządku prawnego dyrektywę 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 333 z 27.12.2022 r. str. 164).

Rozporządzenie będzie wykorzystywane przez podmioty krytyczne w procesie wdrażania zintegrowanego systemu zarządzania bezpieczeństwem świadczenia usługi kluczowej, w zakresie stosowanych rozwiązań organizacyjno-technicznych. Zgodnie z art. 6zt. ust. 2, rozwiązania organizacyjno-techniczne, o których mowa w art. 6zt ust. 1 pkt 2, powinny spełniać wymagania określone w normach, wskazanych w akcie wykonawczym wydanym na podstawie ust. 5.

Wykaz norm w tym rozporządzeniu został opracowany z uwzględnieniem celów wyznaczanych przez Dyrektywę CER i odnosi się do:

1) zarządzania bezpieczeństwem informacji;
2) zarządzania ciągłością działania usługi kluczowej;
3) zapewnienia bezpieczeństwa fizycznego, w tym ochrony fizycznej budynków i terenów należących do podmiotu krytycznego oraz zabezpieczeń technicznych, uwzględniających kontrolę dostępu.

Dla powyższych aspektów istnieją powszechnie rozpoznawalne i stosowane na rynku normy, które w sposób komplementarny umożliwiają nie tylko wdrożenie odpowiednich i proporcjonalnych do wyników oceny ryzyka rozwiązań organizacyjno-technicznych, ale także ich audyt, o którym mowa w art. 6zz. ust. 1.

Uwzględnienie norm umożliwia:

1. podniesienie poziomu bezpieczeństwa systemowego i operacyjnego poprzez:
    - eliminowanie niespójności interpretacyjnych i wdrożeniowych,
    - wzrost odporności IK na zagrożenia,
    - skuteczne i mierzalne zarządzanie ryzykiem,
2. ułatwienie procesów inwestycyjnych poprzez:
    - ograniczenie konieczności opracowywania od podstaw własnych wymagań projektowych, proceduralnych i testowych przez inwestorów,
    - skrócenie czasu opracowania dokumentacji przetargowej,
    - redukcję kosztów poprzez redukcję ryzyka realizacji wadliwych rozwiązań organizacyjno-technicznych,
    - optymalizację kosztową przy zachowaniu wymaganego poziomu bezpieczeństwa (zasada proporcjonalności i adekwatności środków do ryzyk),
3. zwiększenie interoperacyjności systemów bezpieczeństwa poprzez:
    - integrację systemów,
    - łatwość późniejszych modernizacji i rozbudowy zastosowanych rozwiązań (np. systemów zabezpieczeń technicznych),
    - redukcję ryzyka,
4. zwiększenie przejrzystości wymagań i redukcji ryzyka prawnego poprzez:
    - zmniejszenie liczby sporów interpretacyjnych pomiędzy zamawiającymi (podmiotami krytycznymi), wykonawcami i organami nadzoru,
    - zwiększeniem efektywności audytowania, certyfikacji lub kontroli,
    - wzmocnienie pozycji inwestora (podmiotu krytycznego) wobec wykonawców dzięki powoływaniu się na obiektywnie weryfikowalne wymagania,
5. wspieranie innowacyjności i transferu technologii poprzez:

- ułatwione wdrażanie innowacji zgodnych z prawem,
- sprzyjanie przenoszeniu nowych technologii z rynku międzynarodowego do krajowych projektów w zakresie IK,
- zgodność z unijnymi politykami w np. zakresie transformacji cyfrowej,

6. spójność z polityką unii europejskiej i ułatwienie transgranicznej współpracy poprzez:
   - zgodność krajowych regulacji z prawem UE,
   - ułatwienie współpracy z zagranicznymi dostawcami rozwiązań organizacyjno-technicznych,
7. zwiększenie skuteczności nadzoru i kontroli poprzez
   - możliwość wczesnego identyfikowania niezgodności i lub bezpieczeństwa,
   - zwiększenie efektywności i transparentności audytów, certyfikacji i kontroli.

Projektowane rozporządzenie wejdzie w życie po upływie 14 od dnia ogłoszenia

Projekt rozporządzenia nie podlega notyfikacji zgodnie z przepisami dotyczącymi funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych.

Projekt rozporządzenia nie jest sprzeczny 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.

Nazwa projektu Rozporządzenie Rady Ministrów w sprawie wykazu norm, które podmiot krytyczny uwzględnia przy wdrażaniu rozwiązań organizacyjno-technicznych **Ministerstwo wiodące i ministerstwa współpracujące** **Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu** **Kontakt do opiekuna merytorycznego projektu**	**Data sporządzenia** **Źródło:** **Nr w wykazie prac …….**

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

Podejście do zapewniania bezpieczeństwa i odporności podmiotów krytycznych zawarte w Dyrektywie CER w sprawie odporności podmiotów krytycznych i uchylającej dyrektywę Rady 2008/114/WE wprost uwzględnia stosowanie europejskich i międzynarodowych norm i specyfikacji technicznych istotnych dla środków w zakresie bezpieczeństwa i w zakresie odporności mających zastosowanie do podmiotów krytycznych.

Standaryzacja oparta na normach i specyfikacjach technicznych zapewnia jednolite podejście do wymagań dotyczących odporności podmiotów krytycznych i ciągłości działania usług kluczowych, a co więcej umożliwia realizację procesów audytowania lub certyfikacji, które również stanowią cel wdrożeniowy Dyrektywy CER.

Dlatego też, mając na względzie optymalizację procesu budowania odporności podmiotów krytycznych, w projekcie ustawy zaproponowano aby wdrożenie odpowiednich i proporcjonalnych do wyników oceny ryzyka rozwiązań organizacyjno-technicznych przez podmioty krytyczne, w ramach zintegrowanego systemu zarządzania bezpieczeństwem świadczenia usługi kluczowej, oparte było na wymaganiach określonych w normach. Zawarto więc w projekcie ustawy upoważnienie ustawowe, na podstawie którego Rada Ministrów określi, w drodze rozporządzenia, wykaz tychże norm.

2. Rekomendowane rozwiązanie, w tym planowane narzędzia interwencji, i oczekiwany efekt

Wydanie rozporządzenia zawierającego wykaz norm, których wymagania powinny spełniać stosowane w podmiotach rozwiązania organizacyjno-techniczne.
Wprowadzenie jednolitych standardów opierających się na normach pozwala na skuteczniejsze działanie systemu zarządzania bezpieczeństwem świadczenia usługi kluczowej, eliminację jego słabych punktów (np. w zakresie ograniczenia błędów popełnianych w procesie inwestycji w środki służące zapewnieniu bezpieczeństwa fizycznego, co może przełożyć się na obniżenie kosztów) oraz wzmocnienie interoperacyjności pomiędzy podmiotami odpowiedzialnymi za bezpieczeństwo.

Bardzo istotnym elementem wprowadzenia rozporządzenia jest dostosowanie do obligatoryjności prowadzenia przez podmioty krytyczne okresowych audytów (co jest realizacją celu Dyrektywy CER) zintegrowanego systemu zarządzania bezpieczeństwem świadczenia usługi kluczowej – audyt należy bowiem prowadzić w odniesieniu do ustalonych standardów, które powinny być transparentne i jednolite dla wszystkich podmiotów krytycznych.

Zakres norm pokrywa się z określonymi w projekcie ustawy obowiązkami podmiotów krytycznych w zakresie wdrażania rozwiązań organizacyjno-technicznych.

3. Jak problem został rozwiązany w innych krajach, w szczególności krajach członkowskich OECD/UE?

Dyrektywa CER w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE wprost wskazuje, że normy i specyfikacje techniczne powinny być uwzględniane w przepisach krajowych państw członkowskich.

4. Podmioty, na które oddziałuje projekt

Grupa	Wielkość	Źródło danych	Oddziaływanie
(dodaj/usuń)			
(dodaj/usuń)			
(dodaj/usuń)			

(dodaj/usuń)			
(dodaj/usuń)			

5. Informacje na temat zakresu, czasu trwania i podsumowanie wyników 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												
budżet państwa												
JST												
pozostałe jednostki (oddzielnie)												
Wydatki ogółem												
budżet państwa												
JST												
pozostałe jednostki (oddzielnie)												
Saldo ogółem												
budżet państwa												
JST												
pozostałe jednostki (oddzielnie)												

Źródła finansowania	Rozporządzenie nie powoduje konieczności wydatkowania środków finansowych z budżet państwa.
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	Nie dotyczy

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							
	(dodaj/usuń)							

W ujęciu niepieniężnym	duże przedsiębiorstwa	
	sektor mikro-, małych i średnich przedsiębiorstw	
	rodzina, obywatele oraz gospodarstwa domowe	
	(dodaj/usuń)	
Niemierzalne	(dodaj/usuń)	
	(dodaj/usuń)	

Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	

8. Zmiana obciążeń regulacyjnych (w tym obowiązków informacyjnych) wynikających z projektu

X 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:	☐ zwiększenie liczby dokumentów ☐ zwiększenie liczby procedur ☐ wydłużenie czasu na załatwienie sprawy ☐ inne:
Wprowadzane obciążenia są przystosowane do ich elektronizacji.	☐ tak ☐ nie ☐ nie dotyczy

Komentarz:

9. Wpływ na rynek pracy

10. Wpływ na pozostałe obszary

☐ środowisko naturalne ☐ sytuacja i rozwój regionalny ☐ sądy powszechne, administracyjne lub wojskowe	☐ demografia ☐ mienie państwowe ☐ inne:	☐ informatyzacja ☐ zdrowie

Omówienie 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?
Nie dotyczy.
13.Załączniki (istotne dokumenty źródłowe, badania, analizy itp.)
Nie dotyczy.

Projekt

R O Z P O R Z Ą D Z E N I E

R A D Y M I N I S T R Ó W

z dnia

w sprawie progów uznania incydentu za istotny

Na podstawie art. 6zv ust. 4 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. …) zarządza się, co następuje:

§ 1. Progi uznania incydentu za istotny według rodzaju zdarzenia w poszczególnych sektorach i podsektorach określonych w załączniku do ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, są określone w załączniku do rozporządzenia.

§ 2. Rozporządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

P R E Z E S R A D Y M I N I S T R Ó W

Załącznik
do rozporządzenia Rady Ministrów
z dnia
Dz. U. poz.

PROGI UZNANIA INCYDENTU ZA ISTOTNY

Sektor	**Podsektor**	**Zdarzenie**	**Próg**
Energia	Wydobywanie kopalin	Incydent dotyczący wydobywania gazu ziemnego	1. Czas trwania zakłócenia usługi kluczowej, dłuższy niż 72 godziny, 2. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują, straty finansowe przekraczające 250 tys. zł.
		Incydent dotyczący wydobywania ropy naftowej	1. Czas trwania zakłócenia usługi kluczowej, dłuższy niż 72 godziny, 2. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują, straty finansowe przekraczające 250 tys. zł.
		Incydent dotyczący wydobywania węgla brunatnego	1. Czas trwania zakłócenia usługi kluczowej, dłuższy niż 48 godziny, 2. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują, straty finansowe przekraczające 250 tys. zł.
		Incydent dotyczący wydobywania węgla kamiennego	1. Czas trwania zakłócenia usługi kluczowej, dłuższy niż 72 godziny, 2. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują,

			straty finansowe przekraczające 250 tys. zł.
		Incydent dotyczący wydobywania miedzi	1. Czas trwania zakłócenia usługi kluczowej, dłuższy niż 72 godziny, 2. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują, straty finansowe przekraczające 250 tys. zł.
	Energia elektryczna	Incydent dotyczący wytwarzania energii elektrycznej	1. Czas trwania zakłócenia usługi kluczowej, powyżej 15minut: a) równoczesne, 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
		Incydent dotyczący przesyłania energii elektrycznej	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują, 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 2017r. ustanawiającego wytyczne dotyczące pracy systemu przesyłowego energii elektrycznej (Dz. Urz. UE L 220
		Incydent dotyczący dystrybucji energii elektrycznej	1. liczba użytkowników dotkniętych zakłóceniem: powyżej 1000 odbiorców, 2. Czas trwania zakłócenia usługi kluczowej: utrata, na co najmniej 30 minut, zasilania odbiorców w wysokości powyżej 30 % rzeczywistego zapotrzebowania systemu
		Incydent dotyczący obrotu energią elektryczną	1. Czas trwania zakłócenia usługi kluczowej, dłuższy niż 72 godziny, 2. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują, straty finansowe przekraczające 250 tys. zł.
		Incydent dotyczący wykonywania zadań związanych z jednolitym łączeniem rynków dnia następnego lub dnia bieżącego	1. Czas trwania zakłócenia usługi kluczowej, dłuższy niż 72 godziny, 2. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują, straty finansowe przekraczające 250 tys. zł.
		Incydent dotyczący zmiany zużycia energii elektrycznej odbiorcy końcowego w stosunku do jego zwykłego lub bieżącego zużycia energii elektrycznej w odpowiedzi na sygnały rynkowe	1. Czas trwania zakłócenia usługi kluczowej, dłuższy niż 24 godziny, 2. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują, straty finansowe przekraczające 250 tys. zł.

		Incydent dotyczący łączenia wielkości mocy lub energii elektrycznej oferowanej przez odbiorców, wytwórców energii elektrycznej lub posiadaczy magazynów energii elektrycznej	1. Czas trwania zakłócenia usługi kluczowej: utrata na co najmniej 3 minuty zasilania odbiorców w wysokości powyżej 10% rzeczywistego zapotrzebowania systemu w okresie poprzedzającym incydent
		Incydent dotyczący zarządzania punktem ładowania i jego obsługi	1. Czas trwania zakłócenia usługi kluczowej: utrata, na co najmniej 30 minut, zasilania odbiorców w wysokości powyżej 30 % rzeczywistego zapotrzebowania systemu w okresie poprzedzającym incydent
		Incydent dotyczący magazynowania energii elektrycznej	1. Czas trwania zakłócenia usługi kluczowej; utrata, na co najmniej 3 minuty, zasilania odbiorców w wysokości powyżej 10% rzeczywistego zapotrzebowania systemu w okresie poprzedzającym incydent
		Incydent dotyczący przetwarzania energii elektrycznej	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: 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 2017r. ustanawiającego wytyczne dotyczące pracy systemu przesyłowego energii elektrycznej (Dz. Urz. UE L 220
	Ciepło	Incydent dotyczący wytwarzania ciepła	1. Czas trwania zakłócenia usługi kluczowej, incydent doprowadził do przerwania wytwarzania ciepła na okres dłuższy niż 24 godziny, 2. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują 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 ciepłem	1. Czas trwania zakłócenia usługi kluczowej, incydent doprowadził do przerwania wytwarzania ciepła na okres dłuższy niż 24 godziny, 2. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują 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 przesyłania ciepła	1. Czas trwania zakłócenia usługi kluczowej: incydent doprowadził do przerwania

			przesyłania lub dystrybucji ciepła na dłużej niż 24 godziny, 2. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: 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 dystrybucji ciepła	1. Czas trwania zakłócenia usługi kluczowej: incydent doprowadził do przerwania przesyłania lub dystrybucji ciepła na dłużej niż 24 godziny, 2. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: 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 wytwarzania paliw ciekłych	1. Czas trwania zakłócenia usługi kluczowej, incydent skutkuje zakłóceniem w produkcji lub rafinacji lub w funkcjonowaniu urządzeń przetwarzających lub magazynowaniu i przesyłaniu ropy naftowej, dłuższym niż 24 godziny
		Incydent dotyczący przesyłania ropy naftowej	1. Czas trwania zakłócenia usługi kluczowej, incydent skutkuje niemożliwością terminowego i w ilościach nominowanych dostarczania i przesyłu ropy naftowej,

			przez okres dłuższy niż 24 godziny, 2. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: niekontrolowany wyciek ropy naftowej lub innych substancji niebezpiecznych do atmosfery lub gruntu.
		Incydent dotyczący przesyłania paliw ciekłych	1. Czas trwania zakłócenia usługi kluczowej, incydent skutkuje niemożliwością terminowego i w ilościach nominowanych dostarczania i przesyłu ropy naftowej, przez okres dłuższy niż 24 godziny, 2. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: niekontrolowany wyciek ropy naftowej lub innych substancji niebezpiecznych do atmosfery lub gruntu.
		Incydent dotyczący magazynowania ropy naftowej	1. Czas trwania zakłócenia usługi kluczowej: incydent skutkuje zakłóceniem w produkcji lub rafinacji lub w funkcjonowaniu urządzeń przetwarzających lub magazynowaniu i przesyłaniu ropy naftowej, dłuższym niż 24 godziny, 2. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: 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.
		Incydent dotyczący przeładunku ropy naftowej	1. Czas trwania zakłócenia usługi kluczowej: incydent skutkuje zakłóceniem w produkcji lub rafinacji lub w funkcjonowaniu urządzeń przetwarzających lub magazynowaniu i przesyłaniu ropy naftowej, dłuższym niż 24 godziny, 2. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: 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.
		Incydent dotyczący magazynowania paliw ciekłych	1. Czas trwania zakłócenia usługi kluczowej: incydent skutkuje zakłóceniem w magazynowania paliw ciekłych, dłuższym niż 24 godziny, 2. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: 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 paliw ciekłych lub innych substancji niebezpiecznych do atmosfery lub gruntu.

		Incydent dotyczący przeładunku paliw ciekłych	1. Czas trwania zakłócenia usługi kluczowej: incydent skutkuje zakłóceniem w przeładunku paliw ciekłych, dłuższym niż 24 godziny, 2. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: 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 paliw ciekłych do atmosfery lub gruntu.
		Incydent dotyczący obrotu paliwami ciekłymi lub obrotu paliwami ciekłymi z zagranicą	1. Czas trwania zakłócenia usługi kluczowej: incydent dotyczący obrotu paliwami ciekłymi lub obrotu paliwami ciekłymi z zagranicą, dłuższy niż 24 godziny
		Incydent dotyczący wytwarzania paliw syntetycznych	1. Czas trwania zakłócenia usługi kluczowej: incydent skutkuje zakłóceniem w wytwarzaniu paliw syntetycznych, dłuższym niż 24 godzin, 2. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: 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 paliw syntetycznych do atmosfery lub gruntu.
		Incydent dotyczący zapewnienia strategicznych	1. Czas trwania zakłócenia usługi kluczowej: incydent

		rezerw produktów żywnościowych, medycznych i technicznych oraz zapasów paliw	skutkuje przerwaniem realizacji procesu udostępniania rezerw strategicznych lub uwalniania zapasów agencyjnych ropy naftowej, produktów naftowych i gazu ziemnego na czas dłuższy niż 4 godziny
	Gaz	Incydent dotyczący wytwarzania paliw gazowych	1. Czas trwania zakłócenia usługi kluczowej, incydent skutkuje niemożliwością prawidłowego dostarczania i przesyłu paliw gazowych w okresie co najmniej 24 godzin lub zakłóceniem w produkcji lub w funkcjonowaniu urządzeń przetwarzających lub magazynowaniu lub przesyłaniu paliw gazowych, przez okres dłuższy niż 24 godziny, 2. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: 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.
		Incydent dotyczący przesyłania paliw gazowych	1. Czas trwania zakłócenia usługi kluczowej, incydent skutkuje niemożliwością

			prawidłowego dostarczania i przesyłu paliw gazowych w okresie co najmniej 24 godzin lub zakłóceniem w produkcji lub w funkcjonowaniu urządzeń przetwarzających lub magazynowaniu lub przesyłaniu paliw gazowych, przez okres dłuższy niż 24 godziny, 2. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: a) nieplanowany wyciek paliw gazowych 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.
		Incydent dotyczący obrotu paliwami gazowymi i obrotu gazem ziemnym z zagranicą	1. Czas trwania zakłócenia usługi kluczowej, 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 24 godziny,

			2. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: 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.
		Incydent dotyczący przesyłania paliw gazowych	1. Czas trwania zakłócenia usługi kluczowej, 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 24 godziny, 2. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: 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.
		Incydent dotyczący dystrybucji paliw gazowych	1. Czas trwania zakłócenia usługi kluczowej, 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 24 godziny, 2. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: 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.

		Incydent dotyczący magazynowania paliw gazowych	1. Czas trwania zakłócenia usługi kluczowej, 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 24 godziny, 2. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: 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.
		Incydent dotyczący skraplania i regazyfikacji LNG oraz sprowadzania i wyładunku LNG	1. Czas trwania zakłócenia usługi kluczowej, incydent skutkuje niemożliwością prawidłowego skraplania i regazyfikacji LNG oraz sprowadzania i wyładunku LNG w okresie co najmniej 24 godzin lub zakłóceniem w funkcjonowaniu urządzeń przetwarzających lub magazynujących lub przesyłających LNG, przez

			okres dłuższy niż 24 godziny, 4) inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: 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.
		Incydent dotyczący rafinacji i przetwarzania gazu ziemnego	1. Czas trwania zakłócenia usługi kluczowej, 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 24 godziny, 2. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: 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.
	Wodór	Incydent dotyczący produkcji wodoru	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent skutkuje bezpośrednim niebezpieczeństwem spowodowania uszczerbku na zdrowiu lub mieniu
		Incydent dotyczący magazynowania wodoru	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent skutkuje bezpośrednim niebezpieczeństwem spowodowania uszczerbku na zdrowiu lub mieniu
		Incydent dotyczący przesyłania wodoru	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent skutkuje bezpośrednim niebezpieczeństwem spowodowania uszczerbku na zdrowiu lub mieniu
		Incydent dotyczący dystrybucji wodoru	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent skutkuje bezpośrednim niebezpieczeństwem

			spowodowania uszczerbku na zdrowiu lub mieniu
	Energetyka jądrowa	Incydent dotyczący unieszkodliwiania odpadów promieniotwórczych	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent skutkuje bezpośrednim niebezpieczeństwem spowodowania uszczerbku na zdrowiu lub długotrwałym skażeniem środowiska
		Incydent dotyczący składowania odpadów promieniotwórczych	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent skutkuje bezpośrednim niebezpieczeństwem spowodowania uszczerbku na zdrowiu lub długotrwałym skażeniem środowiska
		Incydent dotyczący wytwarzania energii elektrycznej lub cieplnej	1. Czas trwania zakłócenia usługi kluczowej, trwające powyżej 15minut: a) równoczesne, 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
Transport	Transport lotniczy	Incydent dotyczący transportu lotniczego pasażerskiego	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: 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. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: 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 działalności usługowej wspomagającej transport lotniczy przez zarządzającego lotniskiem	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: 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 nadanym przesyłce na czas dłuższy niż 2 godziny.
		Incydent dotyczący działalności usługowej wspomagającej transport lotniczy przez przedsiębiorcę, posiadającego status zarejestrowanego agenta	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: 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 nadanym przesyłce na czas dłuższy niż 2 godziny.
		Incydent dotyczący działalności usługowej wspomagającej transport lotniczy przez przedsiębiorcę, posiadającego status zarejestrowanego agenta obsługi naziemnej	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: 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 nadanym przesyłce na czas dłuższy niż 2 godziny.
		Incydent dotyczący działalności usługowej wspomagającej transport lotniczy przez instytucję zapewniającą służby żeglugi powietrznej	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: 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. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: 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 transportu kolejowego pasażerskiego	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: 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 dotyczący transportu kolejowego towarów	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: 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 transportu morskiego pasażerskiego	1. Czas trwania zakłócenia usługi kluczowej: incydent spowodował brak możliwości świadczenia usługi kluczowej przez czas dłuższy niż 12 godzin
		Incydent dotyczący transportu morskiego towarów	1. Czas trwania zakłócenia usługi kluczowej: incydent spowodował brak możliwości świadczenia usługi kluczowej przez czas dłuższy niż 12 godzin
		Incydent dotyczący transportu wodnego śródlądowego pasażerskiego	1. Czas trwania zakłócenia usługi kluczowej: incydent spowodował brak możliwości świadczenia usługi kluczowej przez czas dłuższy niż 12 godzin
		Incydent dotyczący transportu wodnego śródlądowego towarów	1. Czas trwania zakłócenia usługi kluczowej: incydent spowodował brak możliwości świadczenia

			usługi kluczowej przez czas dłuższy niż 24 godziny
		Incydent dotyczący zarządzania portem morskim	1. Czas trwania zakłócenia usługi kluczowej: incydent spowodował brak możliwości świadczenia usługi kluczowej przez czas dłuższy niż 12 godzin, 2. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent spowodował uszkodzenie systemów informacyjnych kluczowych dla funkcjonowania obiektu portowego, powodujące utrudnienia dla funkcjonowania portu.
		Incydent dotyczący obsługi transportu morskiego pasażerów i towarów	1. Czas trwania zakłócenia usługi kluczowej: incydent spowodował brak możliwości świadczenia usługi kluczowej przez czas dłuższy niż 12 godzin 2. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent spowodował uszkodzenie systemów informacyjnych kluczowych dla funkcjonowania obiektu portowego, powodujące utrudnienia dla funkcjonowania portu.
		Incydent dotyczący działalności usługowej wspomagającej transport morski	1. Czas trwania zakłócenia usługi kluczowej: incydent spowodował brak możliwości świadczenia usługi kluczowej przez czas dłuższy niż 12 godzin 2. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent spowodował

			uszkodzenie systemów informacyjnych kluczowych dla funkcjonowania obiektu portowego, powodujące utrudnienia dla funkcjonowania portu.
		Incydent dotyczący monitorowania ruchu statków	1. Czas trwania zakłócenia usługi kluczowej: incydent spowodował brak możliwości świadczenia usługi kluczowej przez czas dłuższy niż 1 godzinę, 2. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent spowodował uszkodzenie systemów informacyjnych kluczowych dla ruchu statków
	Transport publiczny	Incydent dotyczący transport publicznego	1. Czas trwania zakłócenia usługi kluczowej: incydent spowodował brak możliwości świadczenia usługi kluczowej przez czas dłuższy niż 12 godzin
	Transport drogowy	Incydent dotyczący zarządzania drogami	1. Czas trwania zakłócenia usługi kluczowej: incydent spowodował brak możliwości świadczenia usługi kluczowej przez czas dłuższy niż 12 godzin, 2. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: 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.

		Incydent dotyczący inteligentnych systemów transportowych	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: 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 przyjmowania wkładów pieniężnych płatnych na żądanie lub z nadejściem oznaczonego terminu oraz prowadzenie rachunków tych wkładów	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczył przyjmowania wkładów pieniężnych płatnych na żądanie lub z nadejściem oznaczonego terminu oraz prowadzenie rachunków tych wkładów
		Incydent dotyczący prowadzenia innych rachunków bankowych	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczył prowadzenia innych rachunków bankowych
		Incydent dotyczący udzielania kredytów	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczył udzielania kredytów
		Incydent dotyczący przeprowadzania bankowych rozliczeń pieniężnych	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczył

			przeprowadzania bankowych rozliczeń pieniężnych
		Incydent dotyczący udzielania pożyczek pieniężnych	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczył udzielania pożyczek pieniężnych
		Incydent dotyczący świadczenia usług płatniczych oraz wydawania pieniądza elektronicznego	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczący świadczenia usług płatniczych oraz wydawania pieniądza elektronicznego
		Incydent dotyczący świadczenia usług zaufania oraz wydawania środków identyfikacji elektronicznej w rozumieniu przepisów o usługach zaufania	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: Incydent dotyczący świadczenia usług zaufania oraz wydawania środków identyfikacji elektronicznej w rozumieniu przepisów o usługach zaufania
		Incydent dotyczący wykonywanie czynności, o których mowa w art. 3 ustawy z dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych w zakresie określonym w tym przepisie	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczący wykonywanie czynności, o których mowa w art. 3 ustawy z dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych w zakresie określonym w tym przepisie
		Incydent dotyczący prowadzenia rynku regulowanego lub innej działalności w zakresie organizowania obrotu instrumentami finansowymi oraz działalności związanej z tym obrotem	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczący prowadzenia rynku regulowanego lub innej działalności w zakresie organizowania obrotu instrumentami finansowymi

			oraz działalności związanej z tym obrotem
		Incydent dotyczący prowadzenia alternatywnego systemu obrotu (ASO)	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczący prowadzenia alternatywnego systemu obrotu (ASO)
		Incydent dotyczący prowadzenia platformy aukcyjnej	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczący prowadzenia platformy aukcyjnej
		Incydent dotyczący prowadzenia zorganizowanej platformy obrotu (OTF)	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczący prowadzenia zorganizowanej platformy obrotu (OTF)
		Incydent dotyczący prowadzenia działalności jako dostawca usług w zakresie udostępniania informacji.	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczący prowadzenia działalności jako dostawca usług w zakresie udostępniania informacji.
		Incydent dotyczący prowadzenia działalności polegającej na świadczeniu usług finansowania społecznościowego.	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczący prowadzenia działalności polegającej na świadczeniu usług finansowania społecznościowego.
		Incydent dotyczący organizowania obrotu towarami giełdowymi.	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczący

			organizowania obrotu towarami giełdowymi.
		Incydent dotyczący działania pomiędzy kontrahentami kontraktów będących w obrocie na co najmniej jednym rynku finansowym, polegające na staniu się nabywcą dla każdego sprzedawcy i sprzedawcą dla każdego nabywcy (CCP)	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczący działania pomiędzy kontrahentami kontraktów będących w obrocie na co najmniej jednym rynku finansowym, polegające na staniu się nabywcą dla każdego sprzedawcy i sprzedawcą dla każdego nabywcy (CCP)
		Incydent dotyczący zadania, o których mowa w art. 48 ust. 1 pkt 1-6, ust. 2 i ust. 3 pkt 2 i 3 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi(Dz. U. z 2024 r. poz. 722 z późn zm.).	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczący zadania, o których mowa w art. 48 ust. 1 pkt 1-6, ust. 2 i ust. 3 pkt 2 i 3 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi(Dz. U. z 2024 r. poz. 722 z późn zm.).
		Incydent dotyczący administrowania kluczowymi wskaźnikami referencyjnymi.	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczący administrowania kluczowymi wskaźnikami referencyjnymi.
		Incydent dotyczący prowadzenia systemu rozrachunku papierów wartościowych i świadczenie co najmniej jednej z następujących usług: pierwsza rejestracja papierów wartościowych w systemie zapisów księgowych lub zapewnianie i prowadzenie rachunków papierów wartościowych na	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczący prowadzenia systemu rozrachunku papierów wartościowych i świadczenie co najmniej jednej z następujących usług: pierwsza rejestracja papierów wartościowych w systemie zapisów

		najwyższym poziomie ewidencji	księgowych lub zapewnianie i prowadzenie rachunków papierów wartościowych na najwyższym poziomie ewidencji
		Incydent dotyczący prowadzenia poza rynkiem regulowanym wielostronnego systemu kojarzącego oferty kupna i sprzedaży instrumentów finansowych	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczący prowadzenia poza rynkiem regulowanym wielostronnego systemu kojarzącego oferty kupna i sprzedaży instrumentów finansowych
		Incydent dotyczący prowadzenia wielostronnego systemu kojarzącego w sposób uznaniowy składane przez podmioty trzecie oferty kupna i sprzedaży obligacji, strukturyzowanych produktów finansowych, uprawnień do emisji, instrumentów pochodnych lub produktów energetycznych będących przedmiotem obrotu hurtowego	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczący prowadzenia wielostronnego systemu kojarzącego w sposób uznaniowy składane przez podmioty trzecie oferty kupna i sprzedaży obligacji, strukturyzowanych produktów finansowych, uprawnień do emisji, instrumentów pochodnych lub produktów energetycznych będących przedmiotem obrotu hurtowego
		Incydent dotyczący prowadzenia giełdy towarowej.	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczący prowadzenia giełdy towarowej.
		Incydent dotyczący prowadzenia rynku regulowanego w rozumieniu przepisów ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi (Dz. U. z 2024 r. poz. 722 z	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczący prowadzenia rynku regulowanego w rozumieniu

		późn zm.), z uwzględnieniem ograniczeń z art. 5 ust. 2c ustawy z dnia 26 października 2000 r. o giełdach towarowych (Dz. U. z 2024 r, poz. 910 z późn. zm.)	przepisów ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi (Dz. U. z 2024 r. poz. 722 z późn zm.), z uwzględnieniem ograniczeń z art. 5 ust. 2c ustawy z dnia 26 października 2000 r. o giełdach towarowych (Dz. U. z 2024 r, poz. 910 z późn. zm.)
		Incydent dotyczący prowadzenia platformy aukcyjnej zgodnie z art. 5 ust. 2f ustawy z dnia 26 października 2000 r. o giełdach towarowych (Dz. U. z 2024 r. poz. 910, z późn. zm.)	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczący prowadzenia platformy aukcyjnej zgodnie z art. 5 ust. 2f ustawy z dnia 26 października 2000 r. o giełdach towarowych (Dz. U. z 2024 r. poz. 910, z późn. zm.)
		Incydent dotyczący prowadzenia zorganizowanej platformy obrotu zgodnie z art. 5 ust. 2h i ust. 2i ustawy z dnia 26 października 2000 r. o giełdach towarowych (Dz. U. z 2024 r, poz. 910 z późn. zm.)	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczący prowadzenia zorganizowanej platformy obrotu zgodnie z art. 5 ust. 2h i ust. 2i ustawy z dnia 26 października 2000 r. o giełdach towarowych (Dz. U. z 2024 r, poz. 910 z późn. zm.)
		Incydent dotyczący prowadzenia działalności polegającej na świadczeniu usług finansowania społecznościowego	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczący prowadzenia działalności polegającej na świadczeniu usług finansowania społecznościowego
		Incydent dotyczący dokonywania rozliczeń zgodnie z art. 5 ust. 3 ustawy z dnia 26	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują:

		października 2000 r. o giełdach towarowych (Dz. U. z 2024 r, poz. 910 z późn. zm.)	incydent dotyczący dokonywania rozliczeń zgodnie z art. 5 ust. 3 ustawy z dnia 26 października 2000 r. o giełdach towarowych (Dz. U. z 2024 r, poz. 910 z późn. zm.)
		Incydent dotyczący obsługi finansowej transakcji giełdowych oraz organizacja i prowadzenie rozliczeń transakcji giełdowych, a także zapewnienie przeprowadzania rozliczeń z tytułu transakcji giełdowych.	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczący obsługi finansowej transakcji giełdowych oraz organizacja i prowadzenie rozliczeń transakcji giełdowych, a także zapewnienie przeprowadzania rozliczeń z tytułu transakcji giełdowych.
		Incydent dotyczący organizacji i prowadzenie rozliczeń	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczący organizacji i prowadzenie rozliczeń
		Incydent dotyczący organizacji i prowadzenie rozrachunku transakcji	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent obejmuje 25% płatności (pod względem liczby transakcji) lub 5 mln euro realizowanych przez dany podmiot będący: a) instytucjąkredytową, o której mowa w art. 4 ust. 1 pkt 17 ustawy z dnia 29 sierpnia 1997 r. - Prawo bankowe (Dz. U. z 2017 r. poz. 1876, z późn. zm.1)), b) bankiem krajowym, o którym mowa w art. 4 ust. 1 pkt 1 ustawy z dnia 29 sierpnia 1997 r. - Prawo bankowe, c) oddziałem instytucji kredytowej, o którym mowa w art. 4 ust. 1 pkt 18 ustawy z dnia 29 sierpnia 1997 r. -

			Prawo bankowe, d) spółdzielczą kasą oszczędnościowo-kredytową w rozumieniu ustawy z dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych (Dz. U. z 2017 r. poz. 2065, z późn. zm.2)).
		Incydent dotyczący przetwarzania i rozliczania transakcji międzybankowych	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczący przetwarzania i rozliczania transakcji międzybankowych
Ochrona zdrowia	Udzielanie świadczeń zdrowotnych i zdrowie publiczne	Incydent dotyczący udzielania świadczenia opieki zdrowotnej przez podmiot leczniczy	1. Czas trwania zakłócenia usługi kluczowej: incydent doprowadził do braku dostępności usługi powyżej 24 godzin, 2. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: 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 świadczenia usługi: Szpitalnego Oddziału Ratunkowego, Centrum Urazowego lub Centrum Urazowego dla Dzieci.	1. Czas trwania zakłócenia usługi kluczowej: incydent doprowadził do braku dostępności usługi powyżej 1 godziny, 2. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: 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 kierowania jednostkami systemu Państwowego Ratownictwa Medycznego	1. Czas trwania zakłócenia usługi kluczowej: incydent doprowadził do braku dostępności usługi powyżej 1 godziny, 2. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: 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 wykonywania analiz medycznych	1. Czas trwania zakłócenia usługi kluczowej: incydent doprowadził do braku dostępności usługi powyżej 1 godziny, 2. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: 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. Czas trwania zakłócenia usługi kluczowej: incydent doprowadził do braku dostępności usługi powyżej 1 godziny, 2. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: a) incydent doprowadził do braku poufności danych przetwarzanych w usłudze lub b) incydent doprowadził do braku integralności danych przetwarzanych w usłudze.
		Incydent dotyczący utrzymania Systemu Wspomagania Dowodzenia Państwowego Ratownictwa Medycznego	1. Czas trwania zakłócenia usługi kluczowej: incydent doprowadził do braku dostępności usługi powyżej 1 godziny, 2. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: 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 pozyskiwania, gromadzenia, konserwacji, przechowywania i przekazywania krwi i jej składników	1. Czas trwania zakłócenia usługi kluczowej: incydent doprowadził do braku dostępności usługi powyżej 1 godziny,

			2. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: 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 zlecania przez świadczeniodawców podwykonawcom udzielania świadczeń opieki zdrowotnej w ramach umowy o udzielanie świadczeń opieki zdrowotnej	1. Czas trwania zakłócenia usługi kluczowej: incydent doprowadził do braku dostępności usługi powyżej 24 godzin, 2. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: 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, dystrybucja, obrót i magazynowanie substancji czynnych, produktów leczniczych i wyrobów medycznych	Incydent dotyczący prowadzenia rejestru produktów leczniczych, wyrobów medycznych i produktów biobójczych	1. Czas trwania zakłócenia usługi kluczowej: incydent doprowadził do braku dostępności usługi powyżej 1 godziny, 2. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: a) incydent doprowadził do braku poufności danych

			przetwarzanych w usłudze lub b) incydent doprowadził do braku integralności danych przetwarzanych w usłudze.
		Incydent dotyczący obsługi organów inspekcji farmaceutycznej	1. Czas trwania zakłócenia usługi kluczowej: incydent doprowadził do braku dostępności usługi powyżej 24 godzin, 2. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: 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 prowadzenia działalności badawczo-rozwojowej w zakresie produktów leczniczych	1. Czas trwania zakłócenia usługi kluczowej: incydent doprowadził do braku dostępności usługi powyżej 24 godzin, 2. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: 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 obrotu, dystrybucji, magazynowania produktów leczniczych	1. Czas trwania zakłócenia usługi kluczowej: incydent doprowadził do braku dostępności usługi powyżej 24 godzin, 2. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: 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 dopuszczenia do obrotu produktu leczniczego	1. Czas trwania zakłócenia usługi kluczowej: incydent doprowadził do braku dostępności usługi powyżej 24 godzin, 2. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: 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 wytwarzania lub Importu produktów leczniczych	1. Czas trwania zakłócenia usługi kluczowej: incydent doprowadził do braku dostępności usługi powyżej 24 godzin,

			2. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: 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 produkcji, obrotu i dystrybucji substancji czynnej	1. Czas trwania zakłócenia usługi kluczowej: incydent doprowadził do braku dostępności usługi powyżej 24 godzin, 2. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: 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 obrotu i dystrybucji produktów leczniczych	1. Czas trwania zakłócenia usługi kluczowej: incydent doprowadził do braku dostępności usługi powyżej 24 godzin, 2. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: 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 świadczenia opieki zdrowotnej	1. Czas trwania zakłócenia usługi kluczowej: incydent doprowadził do braku dostępności usługi powyżej 24 godzin, 2. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: 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 ujmowania wody	1. Liczba użytkowników dotkniętych zakłóceniem: incydent doprowadził do braku dostępności usługi dla co najmniej 100 000

			użytkowników przez czas dłuższy niż 8 godzin;
		Incydent dotyczący uzdatniania wody	1. Liczba użytkowników dotkniętych zakłóceniem: incydent doprowadził do braku dostępności usługi dla co najmniej 100 000 użytkowników przez czas dłuższy niż 8 godzin;
		Incydent dotyczący dostarczania wody	1. Liczba użytkowników dotkniętych zakłóceniem: incydent doprowadził do braku dostępności usługi dla co najmniej 100 000 użytkowników przez czas dłuższy niż 8 godzin;
Zbiorowe odprowadzanie ścieków		Incydent dotyczący odprowadzania ścieków	1. Czas trwania zakłócenia usługi kluczowej: incydent doprowadził do braku dostępności usługi dla co najmniej 100 000 RLM przez czas dłuższy niż 8 godzin
		Incydent dotyczący oczyszczania ścieków	1. Czas trwania zakłócenia usługi kluczowej: incydent doprowadził do braku dostępności usługi dla co najmniej 100 000 RLM przez czas dłuższy niż 8 godzin
Infrastruktura cyfrowa	Infrastruktura cyfrowa z wyłączeniem komunikacji elektronicznej	Incydent dotyczący wymiany ruchu internetowego	1. Czas trwania zakłócenia usługi kluczowej: nieplanowany brak dostępności usługi przez co najmniej 8 godzin
		Incydent dotyczący prowadzenia autorytatywnego serwera DNS	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: nieplanowany brak dostępności usługi powyżej 4 godzin lub nieautoryzowana zmiana w bazie danych autorytatywnego serwera DNS.

		Incydent dotyczący prowadzenia rejestru domeny najwyższego poziomu (TLD	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: a) nieplanowana utrata możliwości zarządzania wpisami przez co najmniej 72 godziny lub b) nieplanowany brak dostępności serwerów DNS domeny najwyższego poziomu (TLD) powyżej 1 godziny lub c) nieautoryzowana zmiana w bazie danych serwera DNS Rejestru TLD lub d) nieautoryzowana zmiana w bazie danych Rejestru TLD.
		Incydent dotyczący dostarczania usług chmurowych	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczący dostarczania usług chmurowych
		Incydent dotyczący dostarczania usług ośrodka przetwarzania danych	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczący dostarczania usług ośrodka przetwarzania danych
		Incydent dotyczący dostarczanie treści	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczący dostarczanie treści
		Incydent dotyczący dostarczanie usług zaufania	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczący dostarczanie usług zaufania
		Incydent dotyczący świadczenia usługi rejestracji nazw domen	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują:

			incydent dotyczący świadczenia usługi rejestracji nazw domen
	Komunikacja elektroniczna	Incydent dotyczący świadczenia usług telekomunikacyjnych	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczący świadczenia usług telekomunikacyjnych
		Incydent dotyczący świadczenia usług komunikacji interpersonalnej niewykorzystującej numerów	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczący świadczenia usług komunikacji interpersonalnej niewykorzystującej numerów
Administracja publiczna		Incydent dotyczący zapewnienia dostępu do służb ratowniczych Incydent dotyczący zapewnienia możliwości przekraczania granic RP Incydent dotyczący zapewnienia dostępu do rejestrów państwowych Incydent dotyczący zapewnienia dostępu do rejestrów publicznych uznanych za bardzo istotne Incydent dotyczący zapewnienia dostępu do systemu Informacyjnego Schengen Incydent dotyczący zapewnienia dostępu do usług udostępnianych poprzez portal w domenie gov.pl	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczący zapewnienia dostępu do służb ratowniczych, incydent dotyczący zapewnienia możliwości przekraczania granic RP, incydent dotyczący zapewnienia dostępu do rejestrów państwowych, incydent dotyczący zapewnienia dostępu do rejestrów publicznych uznanych za bardzo istotne, incydent dotyczący zapewnienia dostępu do systemu Informacyjnego Schengen, incydent dotyczący zapewnienia dostępu do usług udostępnianych poprzez portal w domenie gov.pl
		Incydent dotyczący prowadzenia badań naukowych i prac rozwojowych	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują:

		ukierunkowanych na ich wdrożenie i zastosowanie w praktyce	incydent dotyczący prowadzenia badań naukowych i prac rozwojowych ukierunkowanych na ich wdrożenie i zastosowanie w praktyce
		Incydent dotyczący realizacji zadań wskazanych w ustawie z dnia 14 marca 2003 r. o Banku Gospodarstwa Krajowego	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczący realizacji zadań wskazanych w ustawie z dnia 14 marca 2003 r. o Banku Gospodarstwa Krajowego
		Incydent dotyczący realizacji zadań wskazanych w ustawie z dnia 21 grudnia 2000 r. o dozorze technicznym	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczący realizacji zadań wskazanych w ustawie z dnia 21 grudnia 2000 r. o dozorze technicznym
		Incydent dotyczący realizacji zadań wskazanych w ustawie z dnia 8 grudnia 2006 r. o Polskiej Agencji Żeglugi Powietrznej	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczący realizacji zadań wskazanych w ustawie z dnia 8 grudnia 2006 r. o Polskiej Agencji Żeglugi Powietrznej
		Incydent dotyczący realizacji zadań przypisanych Polskiemu Centrum Akredytacji zawartych w ustawie z dnia 30 sierpnia 2002 r. o systemie oceny zgodności	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczący realizacji zadań przypisanych Polskiemu Centrum Akredytacji zawartych w ustawie z dnia 30 sierpnia 2002 r. o systemie oceny zgodności
		Incydent dotyczący realizacji zadań przypisanych Komisji	1. Inne czynniki charakterystyczne dla danego sektora lub

		Nadzoru Finansowego zawartych w ustawie dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym	podsektora, jeżeli występują: incydent dotyczący realizacji zadań przypisanych Komisji Nadzoru Finansowego zawartych w ustawie dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym
		Incydent dotyczący uzyskiwania i przekazywania odbiorcom rzetelnych, obiektywnych i wszechstronnych informacji z kraju i z zagranicy	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczący uzyskiwania i przekazywania odbiorcom rzetelnych, obiektywnych i wszechstronnych informacji z kraju i z zagranicy
		Incydent dotyczący kształtowania i ochrony zasobów wodnych, korzystanie z wód oraz zarządzanie zasobami wodnymi	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczący kształtowania i ochrony zasobów wodnych, korzystanie z wód oraz zarządzanie zasobami wodnymi
		Incydent dotyczący funkcjonowania systemu instytucji rozwoju	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczący funkcjonowania systemu instytucji rozwoju
		Incydent dotyczący ochrony środowiska i warunków korzystania z jego zasobów	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczący ochrony środowiska i warunków korzystania z jego zasobów
		Incydent dotyczący realizacji zadań przez Państwowy Fundusz Rehabilitacji Osób Niepełnosprawnych	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczący realizacji zadań przez Państwowy

			Fundusz Rehabilitacji Osób Niepełnosprawnych
		Incydent dotyczący unieszkodliwiania odpadów promieniotwórczych	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczący unieszkodliwiania odpadów promieniotwórczych
		Incydent dotyczący realizacji zadań o charakterze użyteczności publicznej, których celem jest bieżące i nieprzerwane zaspokajanie zbiorowych potrzeb ludności w drodze świadczenia usług powszechnie dostępnych	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczący realizacji zadań o charakterze użyteczności publicznej, których celem jest bieżące i nieprzerwane zaspokajanie zbiorowych potrzeb ludności w drodze świadczenia usług powszechnie dostępnych
		Incydent dotyczący utrzymania infrastruktury przeciwpowodziowej, budowli hydrotechnicznych i pozostałych obiektów o charakterze inżynierskim w należytym stanie technicznym	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczący utrzymania infrastruktury przeciwpowodziowej, budowli hydrotechnicznych i pozostałych obiektów o charakterze inżynierskim w należytym stanie technicznym
Przestrzeń kosmiczna		Incydent dotyczący systemu satelitarnego wspomagającego GPS	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczący systemu satelitarnego wspomagającego GPS
		Incydent dotyczący realizacji zadań wskazanych w art.3 ustawy z dnia 26 września 2014 r. o Polskiej Agencji Kosmicznej	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczący realizacji zadań wskazanych w art.3 ustawy z dnia 26 września

			2014 r. o Polskiej Agencji Kosmicznej
Produkcja, przetwarzanie i dystrybucja żywności		Incydent dotyczący produkcji, przetwarzania i dystrybucji żywności	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczący produkcji, przetwarzania i dystrybucji żywności
	Produkcja pasz	Incydent dotyczący produkcji pasz	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczący produkcji pasz
	Utylizacja	Incydent dotyczący utylizacji	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczący utylizacji
Zarządzanie usługami ICT		Incydent dotyczący dostawcy usług ICT	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczący dostawcy usług ICT
Produkcja, wytwarzanie i dystrybucja chemikaliów		Incydent dotyczący produkcji oraz wytwarzania i dystrybucji substancji lub mieszanin substancji chemicznych	1.Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczący produkcji oraz wytwarzania i dystrybucji substancji lub mieszanin substancji chemicznych
		Incydent dotyczący wytwarzania z substancji lub mieszanin wyrobów chemicznych	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczący wytwarzania z substancji lub mieszanin wyrobów chemicznych
Usługi pocztowe		Incydent dotyczący dystrybucji pocztowej i kurierskiej	1. Inne czynniki charakterystyczne dla danego sektora lub

			podsektora, jeżeli występują: incydent dotyczący dystrybucji pocztowej i kurierskiej
Gospodarowanie odpadami	Zbieranie odpadów	Incydent dotyczący zbierania odpadów	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczący zbierania odpadów
	Transport odpadów	Incydent dotyczący transportu odpadów	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczący transportu odpadów
	Przetwarzanie odpadów wraz z nadzorem nad wymienionymi działaniami, a także późniejsze postępowanie z miejscami unieszkodliwiania odpadów	Incydent dotyczący przetwarzania odpadów, wraz z nadzorem nad wymienionymi działaniami, a także późniejsze postępowanie z miejscami unieszkodliwiania odpadów	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczący przetwarzania odpadów, wraz z nadzorem nad wymienionymi działaniami, a także późniejsze postępowanie z miejscami unieszkodliwiania odpadów
	Działania wykonywane w charakterze sprzedawcy odpadów lub pośrednika w obrocie odpadami	Incydent dotyczący działania wykonywanego w charakterze sprzedawcy odpadów lub pośrednika w obrocie odpadami	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczący działania wykonywanego w charakterze sprzedawcy odpadów lub pośrednika w obrocie odpadami
Finanse publiczne		Incydent dotyczący wspierania zrównoważonego rozwoju społeczno-gospodarczego Polski.	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczący wspierania zrównoważonego rozwoju społeczno-gospodarczego Polski.

		Incydent dotyczący ustalania wierzytelności zleceń płatniczych	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczący ustalania wierzytelności zleceń płatniczych
		Incydent dotyczący nadzorowania systemu ubezpieczeń społecznych	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczący nadzorowania systemu ubezpieczeń społecznych
		Incydent dotyczący nadzorowania systemu ubezpieczeń społecznych rolników	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczący nadzorowania systemu ubezpieczeń społecznych rolników
		Incydent dotyczący produkcji krajowych dokumentów identyfikacyjnych	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczący produkcji krajowych dokumentów identyfikacyjnych
		Incydent dotyczący produkcji i personalizacji krajowych dokumentów komunikacyjnych	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczący produkcji i personalizacji krajowych dokumentów komunikacyjnych
		Incydent dotyczący świadczenia usług Teleinformatycznych na rzecz Ministerstwa Finansów	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczący świadczenia usług Teleinformatycznych na rzecz Ministerstwa Finansów

		Incydent dotyczący zadania dotyczącego informatyzacji w zakresie działów administracji rządowej budżet i finanse publiczne.	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczący zadania dotyczącego informatyzacji w zakresie działów administracji rządowej budżet i finanse publiczne.
		Incydent dotyczący obsługi płatności w złotych w systemie RTGS i płatności w euro w aplikacji	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczący obsługi płatności w złotych w systemie RTGS i płatności w euro w aplikacji
		Incydent dotyczący zaopatrywania banków w walutę polską	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczący zaopatrywania banków w walutę polską
		Incydent dotyczący prowadzenia gospodarki rezerwami dewizowymi	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczący prowadzenia gospodarki rezerwami dewizowymi
		Incydent dotyczący realizacji polityki pieniężnej i kursowej	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczący realizacji polityki pieniężnej i kursowej
		Incydent dotyczący obsługi posiadacza rachunku	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczący obsługi posiadacza rachunku
		Incydent dotyczący działania operacyjnego na	1. Inne czynniki charakterystyczne dla danego sektora lub

		rzecz utrzymania stabilności finansowej	podsektora, jeżeli występują: incydent dotyczący działania operacyjnego na rzecz utrzymania stabilności finansowej
		Incydent dotyczący wykonywania zadań agenta emisji papierów wartościowych oraz prowadzenia rejestru papierów wartościowych	1. Inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują: incydent dotyczący wykonywania zadań agenta emisji papierów wartościowych oraz prowadzenia rejestru papierów wartościowych

UZASADNIENIE

Projektowane rozporządzenie stanowi wykonanie upoważnienia ustawowego z art. 6zv ust. 4 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, zwanej dalej „ustawą" i określa progi uznania incydentu za istotny dla świadczenia usług kluczowych.

Przedmiotowy projekt rozporządzenia w zakresie swojej regulacji wdraża do polskiego porządku prawnego dyrektywę 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 333 z 27.12.2022 r. str. 164).

Rozporządzenie będzie wykorzystywane przez podmioty krytyczne w procesie zgłaszania i obsługi incydentu. Podmioty krytyczne identyfikując incydent i rejestrując go, będą dokonywali klasyfikacji incydentu na podstawie progów uznawania incydentu za istotny.

Progi uznania incydentu za istotny według zdarzenia w poszczególnych sektorach i podsektorach określonych w załączniku do ustawy uwzględniają liczbę użytkowników dotkniętych zakłóceniem, czas trwania zakłócenia usługi kluczowej, obszar geograficzny, którego dotyczy zakłócenie biorąc pod uwagę stopień odizolowania geograficznego, inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują - kierując się potrzebą zapewnienia ochrony przed zagrożeniami życia lub zdrowia ludzi, znacznymi stratami majątkowymi oraz zagrożeniem obniżenia jakości świadczonej usługi kluczowej.

Progi uznania incydentu za istotny według zdarzenia w poszczególnych sektorach i podsektorach został sporządzony w oparciu o usługi kluczowe wskazane przez organy właściwe organy do spraw podmiotów krytycznych. Wykaz usług kluczowych będzie wykorzystywany w procesie identyfikacji i uznawania operatora infrastruktury krytycznej w danym sektorze lub podsektorze, wymienionych w załączniku do ustawy, za podmiot krytyczny.

Proces zgłaszania incydentów opisany został art. 6zv ustawy, określając sposób zarządzania incydentem przez podmiot krytyczny.

Projektowane rozwiązania wejdą w życie po upływie 14 od dnia ogłoszenia

Projekt rozporządzenia nie podlega notyfikacji zgodnie z przepisami dotyczącymi funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych.

Projekt rozporządzenia nie jest sprzecznym 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.

Nazwa projektu Rozporządzenie Rady Ministrów w sprawie progów uznania incydentu za istotny **Ministerstwo wiodące i ministerstwa współpracujące** **Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu** **Kontakt do opiekuna merytorycznego projektu**	**Data sporządzenia** **Źródło:** **Nr w wykazie prac …….**

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym przewiduje wskazanie progów uznania incydentów za istotny przez podmioty krytyczne.

Podmioty krytyczne identyfikując incydent i rejestrując go, będą dokonywali klasyfikacji incydentu na podstawie progów uznawania incydentu za istotny.

Dlatego też w ustawie zawarto upoważnienie ustawowe, w którym Rada Ministrów określi, w drodze rozporządzenia progi uznania incydentu za istotny według zdarzenia w poszczególnych sektorach i podsektorach określonych w załączniku do ustawy uwzględniają liczbę użytkowników dotkniętych zakłóceniem, czas trwania zakłócenia usługi kluczowej, obszar geograficzny, którego dotyczy zakłócenie biorąc pod uwagę stopień odizolowania geograficznego, inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują - kierując się potrzebą zapewnienia ochrony przed zagrożeniami życia lub zdrowia ludzi, znacznymi stratami majątkowymi oraz zagrożeniem obniżenia jakości świadczonej usługi kluczowej.

2. Rekomendowane rozwiązanie, w tym planowane narzędzia interwencji, i oczekiwany efekt

Wydanie rozporządzenia stanowi wykonanie upoważnienia ustawowego z art. 6zv ust. 4 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, zwanej dalej „ustawą” i określa progi uznania incydentu za istotny dla świadczenia usług kluczowych.

Przedmiotowy projekt rozporządzenia w zakresie swojej regulacji wdraża do polskiego porządku prawnego dyrektywę 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 333 z 27.12.2022 r. str. 164).

Progi uznania incydentu za istotny według zdarzenia w poszczególnych sektorach i podsektorach został sporządzony w oparciu o usługi kluczowe wskazane przez organy właściwe organy do spraw podmiotów krytycznych.
Proces zgłaszania incydentów opisany został art. 6zv ustawy – określający sposób zarządzania incydentem przez podmiot krytyczny.

3. Jak problem został rozwiązany w innych krajach, w szczególności krajach członkowskich OECD/UE?

4. Podmioty, na które oddziałuje projekt

Grupa	Wielkość	Źródło danych	Oddziaływanie
(dodaj/usuń)			
(dodaj/usuń)			
(dodaj/usuń)			
(dodaj/usuń)			

(dodaj/usuń)			

5. Informacje na temat zakresu, czasu trwania i podsumowanie wyników 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												
budżet państwa												
JST												
pozostałe jednostki (oddzielnie)												
Wydatki ogółem												
budżet państwa												
JST												
pozostałe jednostki (oddzielnie)												
Saldo ogółem												
budżet państwa												
JST												
pozostałe jednostki (oddzielnie)												

Źródła finansowania	Rozporządzenie nie powoduje konieczności wydatkowania środków finansowych z budżet państwa.
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	Nie dotyczy

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							
	(dodaj/usuń)							
W ujęciu	duże przedsiębiorstwa							

niepieniężnym	sektor mikro-, małych i średnich przedsiębiorstw	
	rodzina, obywatele oraz gospodarstwa domowe	
	(dodaj/usuń)	
Niemierzalne	(dodaj/usuń)	
	(dodaj/usuń)	

Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	

8. Zmiana obciążeń regulacyjnych (w tym obowiązków informacyjnych) wynikających z projektu

X 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:	☐ zwiększenie liczby dokumentów ☐ zwiększenie liczby procedur ☐ wydłużenie czasu na załatwienie sprawy ☐ inne:
Wprowadzane obciążenia są przystosowane do ich elektronizacji.	☐ tak ☐ nie ☐ nie dotyczy

Komentarz:

9. Wpływ na rynek pracy

10. Wpływ na pozostałe obszary

☐ środowisko naturalne ☐ sytuacja i rozwój regionalny ☐ sądy powszechne, administracyjne lub wojskowe	☐ demografia ☐ mienie państwowe ☐ inne:	☐ informatyzacja ☐ zdrowie

Omówienie 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?
Nie dotyczy.
13. Załączniki (istotne dokumenty źródłowe, badania, analizy itp.)
Nie dotyczy.

Projekt

R O Z P O R Z Ą D Z E N I E

R A D Y M I N I S T R Ó W

z dnia

w sprawie wymogów dla osób lub podmiotów przeprowadzających audyt podmiotów krytycznych

Na podstawie art. 6zza ust. 10 ustawy o zarządzaniu kryzysowym zarządza się, co następuje:

§ 1. Rozporządzenie określa wymogi dla osób lub podmiotów przeprowadzających audyt, o którym mowa w art. 6zz ust. 1 ustawy, w tym:

1) zakres wiedzy specjalistycznej;
2) wymagane doświadczenie zawodowe w dziedzinie objętej audytem;
3) sposób potwierdzania spełnienia wymogów, o których mowa w pkt. 1 i 2.

§ 2. Wymogi, o których mowa w § 1, określa się odrębnie dla audytów przeprowadzanych w zakresach wskazanych w art. 6zz ust. 1 pkt 1–3 ustawy.

§ 3. 1. Audytor, o którym mowa w art. 6zza ust. 1 pkt 2 ustawy, posiada certyfikat potwierdzający kompetencje do przeprowadzania audytu w zakresie odpowiadającym jednemu lub więcej zakresom audytu wskazanym w art. 6zz ust. 1 pkt 1–3 ustawy.

2. Certyfikat, o którym mowa w ust. 1, potwierdza w szczególności kompetencje audytowe obejmujące:

1) planowanie i przygotowanie audytu;
2) przeprowadzanie czynności audytowych;
3) ocenę spełnienia wymagań;
4) formułowanie ustaleń i wniosków;
5) sporządzanie raportu z audytu.

3. Rodzaje certyfikatów określa załącznik do rozporządzenia.

§ 4. 1. Audytor, o którym mowa w art. 6zza ust. 1 pkt 2 ustawy, posiada wiedzę w zakresie:

1) sektora lub podsektora infrastruktury krytycznej właściwego dla usługi kluczowej, w szczególności w zakresie uwarunkowań technicznych, organizacyjnych, regulacyjnych oraz zagrożeń charakterystycznych dla świadczenia tej usługi;
2) norm oraz wytycznych do ich stosowania, stanowiących podstawę wdrażania rozwiązań organizacyjno-technicznych, o których mowa w art. 6zt ust. 1 pkt 2 ustawy, w tym norm oraz wytycznych do ich stosowania wskazanych w przepisach wydanych na podstawie art. 6zt ust. 5 ustawy oraz dokumentów normalizacyjnych, o których mowa w art. 6zt ust. 6 ustawy.

2. Audytor, o którym mowa w art. 6zza ust. 1 pkt 2 ustawy, posiada wiedzę specjalistyczną adekwatną do zakresu audytu, o którym mowa w art. 6zz ust. 1 ustawy.

3. W przypadku audytu w zakresie, o którym mowa w art. 6zz ust. 1 pkt 1 ustawy, audytor posiada wiedzę obejmującą w szczególności zagadnienia dotyczące:

1) zarządzania bezpieczeństwem informacji ukierunkowanego na zapewnienie poufności, integralności i dostępności informacji wykorzystywanych przy świadczeniu usługi kluczowej;
2) identyfikowania informacji istotnych dla realizacji usługi kluczowej oraz zagrożeń i ryzyk związanych z ich przetwarzaniem, przechowywaniem i przekazywaniem;
3) planowanie i ocenę rozwiązań organizacyjnych, technicznych i proceduralnych służących ochronie informacji przed nieuprawnionym dostępem, utratą lub naruszeniem integralności;
4) reagowania na zdarzenia naruszające bezpieczeństwo informacji oraz ograniczania ich skutków dla świadczenia usługi kluczowej;
5) oceny skuteczności przyjętych rozwiązań w zakresie bezpieczeństwa informacji, w tym ich spójności z innymi elementami systemu zarządzania bezpieczeństwem świadczenia usługi kluczowej.

4. W przypadku audytu w zakresie, o którym mowa w art. 6zz ust. 1 pkt 2 ustawy, audytor posiada wiedzę specjalistyczną obejmującą w szczególności zagadnienia dotyczące:

1) zarządzania ciągłością działania ukierunkowanego na zapewnienie zdolności do nieprzerwanego świadczenia usługi kluczowej albo jej odtworzenia po wystąpieniu zakłócenia;
2) identyfikowania zdarzeń mogących zakłócić realizację usługi kluczowej oraz ich wpływu na zdolność organizacji do jej świadczenia;

3) planowania oraz oceny rozwiązań organizacyjnych, technicznych i proceduralnych służących utrzymaniu lub odtworzeniu świadczenia usługi kluczowej;
4) opracowywania, utrzymywania i testowania planów ciągłości działania oraz procedur reagowania na zakłócenia;
5) oceny skuteczności przyjętych rozwiązań w zakresie ciągłości działania, w tym ich spójności z innymi elementami systemu zarządzania bezpieczeństwem świadczenia usługi kluczowej.

5. W przypadku audytu w zakresie, o którym mowa w art. 6zz ust. 1 pkt 3 ustawy, audytor posiada wiedzę specjalistyczną obejmującą w szczególności zagadnienia dotyczące:

1) zapewniania bezpieczeństwa fizycznego infrastruktury krytycznej, ukierunkowanego na ochronę obiektów, terenów oraz zasobów istotnych dla świadczenia usługi kluczowej przed działaniami nieuprawnionymi, sabotażem, ingerencją lub innymi zdarzeniami o charakterze celowym albo losowym;
2) identyfikowania zagrożeń dla bezpieczeństwa fizycznego oraz ich wpływu na możliwość świadczenia usługi kluczowej, z uwzględnieniem lokalizacji i charakterystyki infrastruktury objętej audytem oraz jej powiązań z innymi elementami infrastruktury krytycznej;
3) planowania oraz oceny rozwiązań organizacyjnych, proceduralnych i technicznych służących zapewnieniu bezpieczeństwa fizycznego;
4) zasad doboru, funkcjonowania oraz oceny skuteczności systemów zabezpieczeń technicznych stosowanych w celu zapewnienia bezpieczeństwa fizycznego, w tym systemów sygnalizacji włamania i napadu, systemów kontroli dostępu oraz systemów dozoru wizyjnego;
5) zasad projektowania, instalowania, konserwacji, odbiorów, eksploatacji oraz utrzymania systemów zabezpieczeń technicznych stosowanych w infrastrukturze krytycznej, w tym ich integracji z ochroną fizyczną oraz procedurami organizacyjnymi;
6) oceny zgodności zainstalowanych systemów zabezpieczeń technicznych z wymaganiami właściwych dla nich norm, w tym w zakresie spełnienia deklarowanego stopnia zabezpieczenia, odpowiadającego przyjętym założeniom projektowym i poziomowi ryzyka,
7) zasad reagowania na zdarzenia naruszające bezpieczeństwo fizyczne oraz zasad ograniczania ich skutków dla świadczenia usługi kluczowej;

8) zasad zapewnienia spójności oraz wzajemnego oddziaływania rozwiązań organizacyjnych, proceduralnych i technicznych w zakresie bezpieczeństwa fizycznego;
9) zasad oceny skuteczności przyjętych rozwiązań w zakresie bezpieczeństwa fizycznego, w tym ich spójności z innymi elementami systemu zarządzania bezpieczeństwem świadczenia usługi kluczowej.

6. Zakres wiedzy specjalistycznej wskazany w ust. 1–4 potwierdza się ukończeniem szkoleń lub kursów specjalistycznych przez co najmniej jednego z audytorów wchodzących w skład zespołu audytowego, o którym mowa w art. 6zza ust. 1 pkt 2 ustawy.

§ 5. 1. Audytor posiada doświadczenie zawodowe adekwatne do zakresu audytu, o którym mowa w art. 6zz ust. 1 pkt 1–3 ustawy.

2. W przypadku audytu w zakresie, o którym mowa w art. 6zz ust. 1 pkt 1 ustawy, audytor posiada co najmniej 3-letnie doświadczenie zawodowe w zakresie audytowania systemów zarządzania bezpieczeństwem informacji.

3. W przypadku audytu w zakresie, o którym mowa w art. 6zz ust. 1 pkt 2 ustawy, audytor posiada co najmniej 3-letnie doświadczenie zawodowe w zakresie audytowania systemów zarządzania ciągłością działania.

4. W przypadku audytu w zakresie, o którym mowa w art. 6zz ust. 1 pkt 3 ustawy, audytor spełnia wymagania w zakresie doświadczenia zawodowego, jeżeli spełnia jedną z następujących przesłanek:

1) posiada certyfikat, o którym mowa w pkt 1 załącznika nr 1, w zakresie odpowiadającym bezpieczeństwu fizycznemu, w tym ochronie fizycznej budynków i terenów należących do podmiotu krytycznego oraz zabezpieczeniom technicznym uwzględniającym kontrolę dostępu, oraz:
   a) posiada co najmniej 3-letnie doświadczenie zawodowe w zakresie audytowania lub oceny rozwiązań z obszaru bezpieczeństwa fizycznego, w tym systemów zabezpieczeń technicznych,
   b) ukończył kurs pracownika zabezpieczenia technicznego w wyspecjalizowanej w tym zakresie placówce kształcenia ustawicznego działającej w systemie oświaty,
   c) posiada dokument potwierdzający odbycie szkolenia aktualizującego w zakresie obowiązujących na dzień rozpoczęcia audytu wymagań prawno-normatywnych dotyczących systemów zabezpieczeń technicznych, wydany nie wcześniej niż 3 lata przed dniem rozpoczęcia audytu;

   albo

2) posiada certyfikat, o którym mowa w pkt. 2 załącznika nr 1, w zakresie odpowiadającym bezpieczeństwu fizycznemu, w tym ochronie fizycznej budynków i terenów należących do podmiotu krytycznego oraz zabezpieczeniom technicznym uwzględniającym kontrolę dostępu, a także co najmniej 2-letnie doświadczenie zawodowe w zakresie audytowania lub oceny rozwiązań z obszaru bezpieczeństwa fizycznego, w tym systemów zabezpieczeń technicznych

5. Za doświadczenie zawodowe, o którym mowa w ust. 2–4, uważa się udokumentowane wykonywanie, w okresie 3 lat przed dniem rozpoczęcia audytu:

1) co najmniej 3 audytów odpowiadających zakresem danemu obszarowi audytu; albo
2) czynności audytowych lub kontrolnych w wymiarze czasu pracy nie mniejszym niż ½ etatu, związanych w szczególności z audytami, oceną zgodności, kontrolą lub nadzorem nad systemami objętymi zakresem audytu.

§ 6. 1. Spełnienie wymogów, o których mowa w § 4 i § 5, audytor potwierdza poprzez przedstawienie dokumentów potwierdzających posiadanie wymaganej wiedzy specjalistycznej oraz doświadczenia zawodowego, adekwatnych do zakresu audytu, o którym mowa w art. 6zz ust. 1 pkt 1–3 ustawy.

2. Dokumentami, o których mowa w ust. 1, są w szczególności:

1) certyfikaty, o których mowa w załączniku nr 1 do rozporządzenia;
2) dokumenty potwierdzające ukończenie szkoleń lub kursów specjalistycznych, o których mowa w § 5 ust. 6;
3) wykaz czynności zawodowych wykonywanych przez audytora w okresie, o którym mowa w § 6, obejmujący w szczególności informacje o rodzaju realizowanych audytów, ocen lub innych czynności odpowiadających zakresem danemu obszarowi audytu;
4) dokumenty potwierdzające udział audytora w czynnościach, o których mowa w pkt 3, w szczególności raporty z audytów, protokoły, referencje, zaświadczenia lub oświadczenia podmiotów, na rzecz których czynności były wykonywane.

3. W przypadku gdy audyt jest przeprowadzany przez zespół audytorów, o którym mowa w art. 6zza ust. 1 pkt 2 ustawy, każdy z audytorów wchodzących w skład zespołu audytowego posiada certyfikat, o którym mowa w załączniku do rozporządzenia, adekwatny do zakresu audytu, a wymagania określone w § 4 i § 5 są spełnione w taki sposób, że co najmniej jeden z audytorów spełnia je w pełnym zakresie.

4. Podmiot krytyczny zapewnia możliwość weryfikacji dokumentów, o których mowa w ust. 2, przed rozpoczęciem audytu oraz przechowuje je przez okres umożliwiający ocenę spełnienia wymogów, o których mowa w § 4 i § 5.

§ 7. Rozporządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

PREZES RADY MINISTRÓW

Załącznik
do rozporządzenia Rady Ministrów
z dnia
Dz. U. poz.

WYKAZ CERTYFIKATÓW UPRAWNIAJĄCYCH DO PRZEPROWADZANIA AUDYTU

ZARZĄDZANIE BEZPIECZEŃSTWEM INFORMACJI

1) Certified Internal Auditor (CIA);
2) Certified Information System Auditor (CISA);
3) Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz.U. z 2017 r. poz. 1398 oraz z 2018 r. poz. 650 i 1338), w zakresie certyfikacji osób;
4) Certified Information Security Manager (CISM);
5) Certified in Risk and Information Systems Control (CRISC);
6) Certified in the Governance of Enterprise IT (CGEIT);
7) Certified Information Systems Security Professional (CISSP);
8) Systems Security Certified Practitioner (SSCP);
9) Certified Reliability Professional;
10) Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert.

ZARZĄDZANIE CIĄGŁOŚCIĄ DZIAŁANIA

1) Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób.

BEZPIECZEŃSTWO FIZYCZNE, W TYM OCHRONA FIZYCZNA BUDYNKÓW I TERENÓW NALEŻĄCYCH DO PODMIOTU KRYTYCZNEGO ORAZ ZABEZPIECZENIA TECHNICZNE, UWZGLĘDNIAJĄCE KONTROLĘ DOSTĘPU

1) Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz.U. z 2017 r. poz. 1398 oraz z 2018 r. poz. 650 i 1338), w zakresie certyfikacji osób;
2) Certyfikat audytora wiodącego systemów zabezpieczeń technicznych w odniesieniu do wymagań normy PN-EN ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz.U. z 2017 r. poz. 1398 oraz z 2018 r. poz. 650 i 1338), w zakresie certyfikacji osób.

UZASADNIENIE

Projektowane rozporządzenie stanowi wykonanie upoważnienia ustawowego z art. 6zza ust. 10 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, zwanej dalej „ustawą" i określa wymogi dla osób lub podmiotów przeprowadzających audyt podmiotów krytycznych, z uwzględnieniem zakresu wiedzy specjalistycznej wymaganej od osób lub podmiotów legitymujących się poszczególnymi certyfikatami oraz wymaganym doświadczeniem.

Przedmiotowy projekt rozporządzenia w zakresie swojej regulacji wdraża do polskiego porządku prawnego dyrektywę 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 333 z 27.12.2022 r. str. 164).

Rozporządzenie będzie wykorzystywane przez podmioty krytyczne w procesie walidacji zintegrowanego systemu zarządzania bezpieczeństwem świadczenia usługi kluczowej, w zakresie:

1) zarządzania bezpieczeństwem informacji;
2) zarządzania ciągłością działania usługi kluczowej;
3) zapewnienia bezpieczeństwa fizycznego, w tym ochrony fizycznej budynków i terenów należących do podmiotu krytycznego oraz zabezpieczeń technicznych, uwzględniających kontrolę dostępu.

Zakres audytu pokrywa się z wykazem norm, który będzie wydany na podstawie upoważnienia ustawowego z art. 6zt. ust. 5. – audyt stanowi domknięcie wdrożonej w ustawie koncepcji standaryzacji zintegrowanego systemu zarządzania bezpieczeństwem świadczenia usługi kluczowej.

Zgodnie z art. 6zt. ust. 2, rozwiązania organizacyjno-techniczne, o których mowa w art. 6zt ust. 1 pkt 2, powinny spełniać wymagania określone w normach, wskazanych w akcie wykonawczym wydanym na podstawie ust. 5.

Rozporządzenie wskazuje minimalne kwalifikacje i standardy zawodowe dla audytorów przeprowadzających audyty zintegrowanego systemu zarządzania bezpieczeństwem świadczenia usługi kluczowej w podmiotach krytycznych.
Regulacja ta ma na celu zapewnienie wysokiej jakości, wiarygodności i jednolitych standardów audytowania, które są niezbędne do weryfikacji rzeczywistego poziomu zabezpieczeń oraz odporności podmiotów kluczowych na zagrożenia o zróżnicowanym charakterze. Audytorzy, którzy uzyskają certyfikat, będą nie tylko przygotowani merytorycznie, ale zapewniają także realizację audytów z uwzględnieniem generalnych zasad:

- rzetelności
- uczciwości w przedstawianiu wyników
- należytej staranności
- poufności
- niezależności
- podejściu opartym na dowodach
- podejściu opartym na ryzyku

Wprowadzenie jednolitych wymagań merytorycznych opartych na normach lub innych standardach zachowujących kompatybilność z normami, z uwzględnieniem wiedzy specjalistycznej i doświadczenia, pozwala na efektywny nadzór działania systemu zarządzania bezpieczeństwem świadczenia usługi kluczowej, eliminację jego słabych punktów oraz sprzyja profesjonalizacji audytów, ograniczając ryzyko powierzchownych lub nierzetelnych ocen.

Wprowadzenie wykazu certyfikatów jest korzystne dla rynku. Promuje uznawane międzynarodowo certyfikaty, wpływa pozytywnie na jakość usług oferowanych przez polskie jednostki certyfikujące i

szkoleniowe, tworząc popyt na wysokiej jakości kształcenie specjalistów ds. bezpieczeństwa i odporności IK. Co więcej, dzięki wykazowi certyfikatów, znacząco zwiększa się konkurencyjność dla profesjonalnych audytorów i zmniejsza się bariera wejścia dla audytorów, którzy posiadają już wymagane certyfikaty uzyskane np. w innych krajach UE.

Istotną kwestią jest ograniczenie nadużyć i fikcyjnych audytów. Dzięki powiązaniu uprawnień audytorów z posiadaniem określonych certyfikatów oraz potwierdzonego doświadczenia:

- eliminowane są przypadki powierzania audytów osobom nieposiadającym odpowiednich kwalifikacji,
- ograniczane jest zjawisko „pozornych audytów" wykonywanych wyłącznie dla spełnienia formalnych obowiązków,
- ułatwiona zostaje kontrola i weryfikacja audytorów przez organy nadzoru (np. Rządowe Centrum Bezpieczeństwa, ABW, jednostki certyfikujące).

Wpływ regulacji na sektor publiczny i przedsiębiorców jest korzystny. Podmioty krytyczne, niezależnie od tego, czy są publiczne, czy prywatne, zyskują jasny katalog kwalifikacji wymaganych od audytorów. Przedsiębiorcy świadczący usługi audytorskie mogą dopasować swój rozwój kompetencyjny i zasoby kadrowe do precyzyjnych wymagań ustawowych - to bardzo ważne, albowiem w sektorze ochrony i bezpieczeństwa konkurencyjność usług nie może opierać się na kryteriach niemerytorycznych.

Regulacja nie powoduje nadmiernych kosztów, ponieważ większość certyfikatów wskazanych w projektowanym rozporządzeniu jest już wskazana w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu i funkcjonuje na rynku od wielu lat.

Podsumowując, projektowane rozporządzenie stanowi kluczowy instrument wykonawczy, który:

- zapewnia profesjonalizację audytów bezpieczeństwa,
- harmonizuje krajowy system weryfikacji odporności infrastruktury krytycznej z podejściem europejskim,
- przyczynia się do rzeczywistego wzrostu bezpieczeństwa, a nie tylko spełniania wymagań formalnych.

Projektowane rozporządzenie wejdzie w życie po upływie 14 od dnia ogłoszenia

Projekt rozporządzenia nie podlega notyfikacji zgodnie z przepisami dotyczącymi funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych.

Projekt rozporządzenia nie jest sprzeczny 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.

Nazwa projektu Rozporządzenie Rady Ministrów w sprawie wymogów dla osób lub podmiotów przeprowadzających audyt podmiotów krytycznych **Ministerstwo wiodące i ministerstwa współpracujące** **Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu** **Kontakt do opiekuna merytorycznego projektu**	**Data sporządzenia** **Źródło:** **Nr w wykazie prac …….**

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

Podejście do nadzoru i egzekwowania przepisów zawarte w Dyrektywie CER w sprawie odporności podmiotów krytycznych i uchylającej dyrektywę Rady 2008/114/WE wprost uwzględnia konieczność audytowania wdrożonych przez podmioty krytyczne rozwiązań organizacyjno-technicznych. Państwa członkowskie są zobligowane do takiej implementacji celów Dyrektywy CER, aby zobowiązać podmioty krytyczne do przeprowadzania audytów przez niezależnego i wykwalifikowanego audytora.

Audytowanie wdrożonych rozwiązań organizacyjno-technicznych domyka zawarty w projekcie ustawy o zarządzaniu kryzysowym zintegrowany system zarządzania bezpieczeństwem świadczenia usługi kluczowej, oparty na stosowaniu europejskich i międzynarodowych norm. Standaryzacja narzuca konieczność wyznaczenia wymagań dla audytorów, uwzględniających nie tylko ogólne zasady audytowania (rzetelność, uczciwość, staranność, poufność, niezależność, podejście oparte na ryzyku, podejście oparte na dowodach), ale w szczególności aspekty merytoryczne.

Dlatego też, mając na względzie efektywność procesu audytowania podmiotów krytycznych w zakresie zintegrowanego systemu zarządzania bezpieczeństwem świadczenia usługi kluczowej, zawarto w projekcie ustawy upoważnienie ustawowe, na podstawie którego Rada Ministrów określi, w drodze rozporządzenia, wymogi dla osób lub podmiotów przeprowadzających audyt podmiotów krytycznych, uwzględniając zakres wiedzy specjalistycznej wymaganej od osób lub podmiotów legitymujących się poszczególnymi certyfikatami oraz wymagane doświadczenie.

2. Rekomendowane rozwiązanie, w tym planowane narzędzia interwencji, i oczekiwany efekt

Wydanie rozporządzenia zawierającego wykaz certyfikatów uprawniających do przeprowadzenia audytów, uwzględniając zakres wiedzy specjalistycznej wymaganej od osób lub podmiotów legitymujących się poszczególnymi certyfikatami oraz wymagane doświadczenie.

Wprowadzenie jednolitych wymagań merytorycznych opartych na normach lub innych standardach zachowujących kompatybilność z normami, z uwzględnieniem wiedzy specjalistycznej i doświadczenia, pozwala na efektywny nadzór działania systemu zarządzania bezpieczeństwem świadczenia usługi kluczowej, eliminację jego słabych punktów oraz sprzyja profesjonalizacji audytów, ograniczając ryzyko powierzchownych lub nierzetelnych ocen.

Bardzo istotna kwestią, którą reguluje rozporządzenie, jest ograniczenie ryzyka nadużyć i fikcyjnych audytów. Dzięki powiązaniu uprawnień audytorów z posiadaniem określonych certyfikatów (z uwzględnieniem specjalistycznej wiedzy i doświadczenia) eliminowane będą przypadki powierzania audytów osobom nieposiadającym odpowiednich kwalifikacji. Co więcej ograniczane jest zjawisko audytów „pozornych", wykonywanych wyłącznie dla spełnienia formalnych obowiązków – certyfikowani audytorzy podlegają bowiem weryfikacji np. przez jednostki certyfikujące.

Dzięki rozporządzeniu podmioty krytyczne uzyskują jasne narzędzia do selekcji kompetentnych audytorów.

Regulacja nie powoduje nadmiernych kosztów, ponieważ większość certyfikatów wskazanych w projektowanym rozporządzeniu jest już wskazana w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu i funkcjonuje na rynku od wielu lat.

3. Jak problem został rozwiązany w innych krajach, w szczególności krajach członkowskich OECD/UE?

Dyrektywa CER w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE wprost wskazuje, że audytowanie środków stosowanych celem zwiększenia odporności podmiotów krytycznych powinno być uwzględniane w przepisach krajowych państw członkowskich.

4. Podmioty, na które oddziałuje projekt

Grupa	Wielkość	Źródło danych	Oddziaływanie
(dodaj/usuń)			
(dodaj/usuń)			
(dodaj/usuń)			
(dodaj/usuń)			
(dodaj/usuń)			

5. Informacje na temat zakresu, czasu trwania i podsumowanie wyników 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												
budżet państwa												
JST												
pozostałe jednostki (oddzielnie)												
Wydatki ogółem												
budżet państwa												
JST												
pozostałe jednostki (oddzielnie)												
Saldo ogółem												
budżet państwa												
JST												
pozostałe jednostki (oddzielnie)												

Źródła finansowania	Rozporządzenie nie powoduje konieczności wydatkowania środków finansowych z budżet państwa.
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	Nie dotyczy

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							
	(dodaj/usuń)							
W ujęciu niepieniężnym	duże przedsiębiorstwa							
	sektor mikro-, małych i średnich przedsiębiorstw							
	rodzina, obywatele oraz gospodarstwa domowe							
	(dodaj/usuń)							
Niemierzalne	(dodaj/usuń)							
	(dodaj/usuń)							

Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	

8. Zmiana obciążeń regulacyjnych (w tym obowiązków informacyjnych) wynikających z projektu

X 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:	☐ zwiększenie liczby dokumentów ☐ zwiększenie liczby procedur ☐ wydłużenie czasu na załatwienie sprawy ☐ inne:
Wprowadzane obciążenia są przystosowane do ich elektronizacji.	☐ tak ☐ nie ☐ nie dotyczy

Komentarz:

9. Wpływ na rynek pracy

10. Wpływ na pozostałe obszary

☐ środowisko naturalne ☐ sytuacja i rozwój regionalny ☐ sądy powszechne, administracyjne lub wojskowe	☐ demografia ☐ mienie państwowe ☐ inne:	☐ informatyzacja ☐ zdrowie

Omówienie 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?

Nie dotyczy.

13.Załączniki (istotne dokumenty źródłowe, badania, analizy itp.)

Nie dotyczy.

Projekt

R O Z P O R Z Ą D Z E N I E

P R E Z E S A R A D Y M I N I S T R Ó W

z dnia

w sprawie pełnomocnika do spraw ochrony infrastruktury krytycznej

Na podstawie art. 6 ust. 8 ustawy z dnia 18 marca 2010 r. o szczególnych uprawnieniach ministra właściwego do spraw aktywów państwowych oraz ich wykonywaniu w niektórych spółkach kapitałowych lub grupach kapitałowych prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych (Dz. U. z 2020 r. poz. 2173) zarządza się, co następuje:

§ 1. Rozporządzenie określa:

1) szczegółowy tryb powoływania i odwoływania pełnomocnika do spraw ochrony infrastruktury krytycznej;
2) sposób wykonywania przez pełnomocnika obowiązku monitorowania działalności spółki w zakresie, o którym mowa w art. 2 ust. 1 i 2 ustawy z dnia 18 marca 2010 r. o szczególnych uprawnieniach ministra właściwego do spraw aktywów państwowych oraz ich wykonywaniu w niektórych spółkach kapitałowych lub grupach kapitałowych prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych, zwanej dalej „ustawą”.

§ 2. Użyte w rozporządzeniu określenia oznaczają:

1) minister – ministra właściwego do spraw aktywów państwowych;
2) dyrektor Centrum – dyrektora Rządowego Centrum Bezpieczeństwa;
3) spółka – spółkę, o której mowa w art. 1 ust. 1 ustawy;
4) pełnomocniku – pełnomocnika do spraw ochrony infrastruktury krytycznej, o którym mowa w o którym mowa w art. 5 ust. 1 ustawy z dnia 18 marca 2010 r. o szczególnych uprawnieniach ministra właściwego do spraw aktywów państwowych oraz ich wykonywaniu w niektórych spółkach kapitałowych lub grupach kapitałowych prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych….

§ 3. 1. Zarząd spółki, w terminie 5 dni od dnia otrzymania powiadomienia, o którym mowa w art. 4 ust. 2 ustawy, wyznacza kandydata na pełnomocnika, zwanego dalej „kandydatem”.

2. Kandydat, w terminie 5 dni od dnia otrzymania informacji od zarządu spółki o wyznaczeniu, przedstawia temu zarządowi:

1) oświadczenie o wyrażeniu zgody na objęcie stanowiska pełnomocnika;
2) do wglądu, dokumenty potwierdzające spełnienie kryteriów, o których mowa w art. 5 ust. 3 pkt 1 i 3 ustawy;
3) oświadczenie, że korzysta z pełni praw cywilnych i obywatelskich;
4) informację:
   a) z Krajowego Rejestru Karnego o niekaralności za umyślne przestępstwo lub umyślne przestępstwo skarbowe,
   b) o obecnym zatrudnieniu wraz ze wskazaniem stanowiska służbowego,
   c) o dotychczasowym przebiegu pracy zawodowej oraz posiadanych kwalifikacjach i doświadczeniu zawodowym.

3. Zarząd spółki sporządza dwa egzemplarze wniosku o wyrażenie zgody na powołanie kandydata na stanowisko pełnomocnika i przesyła je, po jednym egzemplarzu, do ministra oraz do dyrektora Centrum, w terminie 5 dni od dnia złożenia przez kandydata dokumentów, o których mowa w ust. 2.

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

1) informacje o kandydacie, w tym:
   a) imię i nazwisko,
   b) miejsce zamieszkania,
   c) numer PESEL, a w przypadku braku numeru PESEL – serię i numer dokumentu stwierdzającego tożsamość,
   d) informację o obecnym zatrudnieniu wraz ze wskazaniem stanowiska służbowego,
   e) informację o dotychczasowym przebiegu pracy zawodowej oraz posiadanych kwalifikacjach i doświadczeniu zawodowym,
   f) numer telefonu służbowego oraz adres poczty elektronicznej;
2) projekt zakresu obowiązków kandydata;
3) oświadczenie zarządu spółki o spełnieniu przez kandydata warunków, o których mowa w art. 5 ust. 3 ustawy, wraz z kopiami dokumentów i informacji potwierdzających ich spełnienie, poświadczonymi przez osobę upoważnioną przez zarząd spółki za zgodność z oryginałem.

5. Do wniosku, o którym mowa w ust. 3, zarząd spółki dołącza schemat struktury organizacyjnej spółki, w którym uwzględniono pełnomocnika.

6. Minister przekazuje niezwłocznie kopię wniosku, o którym mowa w ust. 3, do wiadomości Szefowi Agencji Bezpieczeństwa Wewnętrznego. W przypadku zmiany w zakresie informacji, o których mowa w § 9, minister niezwłocznie informuje o tym Szefa Agencji Bezpieczeństwa Wewnętrznego.

§ 4. 1. Minister rozpatruje wniosek, o którym mowa w § 3 ust. 3, w terminie 10 dni od dnia jego otrzymania, w tym:

1) sprawdza kompletność wniosku pod względem formalnym;
2) analizuje informacje zawarte we wniosku;
3) przeprowadza rozmowę z kandydatem, w trakcie której sprawdza, czy kandydat daje rękojmię prawidłowego wykonywania obowiązków pełnomocnika.

2. Po rozpatrzeniu wniosku, o którym mowa w § 3 ust. 3, minister:

1) wyraża zgodę na powołanie kandydata na stanowisko pełnomocnika albo
2) nie wyraża zgody na powołanie kandydata na stanowisko pełnomocnika, zwracając się do zarządu spółki o wyznaczenie innego kandydata, w terminie 5 dni od dnia otrzymania informacji o niewyrażeniu zgody.

3. W przypadku gdy wniosek, o którym mowa w § 3 ust. 3, jest niekompletny:

1) minister zwraca wniosek zarządowi spółki w celu jego uzupełnienia;
2) zarząd spółki uzupełnia wniosek w zakresie wskazanym przez ministra oraz, nie później niż w terminie 5 dni od dnia otrzymania zwróconego wniosku, ponownie składa uzupełniony wniosek.

4. Do rozpatrzenia uzupełnionego wniosku stosuje się ust. 1, przy czym wniosek ten minister rozpatruje w terminie 5 dni od dnia jego otrzymania.

5. W przypadku niewyrażenia zgody na powołanie kandydata na stanowisko pełnomocnika minister przekazuje zarządowi spółki oraz dyrektorowi Centrum informacje o przyczynach niewyrażenia zgody.

6. Przepisy ust. 1–5 stosuje się odpowiednio do rozpatrywania wniosku, o którym mowa w § 3 ust. 3, przez dyrektora Centrum.

7. Zarząd spółki nie może ponownie zgłosić kandydata, na powołanie którego nie uzyskał zgody ministra lub dyrektora Centrum. Do ponownego wyznaczania kandydata stosuje się przepisy ust. 1–6 oraz § 3 ust. 2–6.

§ 5. 1. Po uzyskaniu zgody ministra oraz dyrektora Centrum na powołanie kandydata na stanowisko pełnomocnika zarząd spółki powołuje pełnomocnika w drodze uchwały.

2. Zarząd spółki, niezwłocznie po powołaniu pełnomocnika, przekazuje ministrowi oraz dyrektorowi Centrum kopie:

1) uchwały, o której mowa w ust. 1;
2) zakresu obowiązków pełnomocnika.

§ 6. 1. Pełnomocnika odwołuje zarząd spółki, w drodze uchwały, po uzyskaniu zgody ministra oraz dyrektora Centrum.

2. Zarząd spółki sporządza dwa egzemplarze wniosku o wyrażenie zgody na odwołanie pełnomocnika i przesyła je, po jednym egzemplarzu, odpowiednio do ministra oraz dyrektora Centrum. Przepis § 3 ust. 6 zdanie pierwsze stosuje się odpowiednio.

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

1) imię i nazwisko pełnomocnika;
2) wskazanie daty powołania pełnomocnika;
3) kopie zgód wydanych zgodnie z § 4 ust. 2 pkt 1, dotyczących pełnomocnika;
4) uzasadnienie wniosku obejmujące w szczególności wskazanie przyczyn uzasadniających odwołanie pełnomocnika.

4. W przypadku złożenia wniosku o wyrażenie zgody na odwołanie pełnomocnika zarząd spółki składa jednocześnie wniosek, o którym mowa w § 3 ust. 3, dotyczący wyrażenia zgody na powołanie nowego pełnomocnika, z wyjątkiem sytuacji, w której odwołanie pełnomocnika jest związane ze zniesieniem obowiązku utrzymywania takiego stanowiska w spółce.

5. Do rozpatrywania wniosku o wyrażenie zgody na powołanie nowego pełnomocnika stosuje się przepisy § 3 ust. 2–6 oraz § 4 ust. 1–6 i ust. 7 zdanie pierwsze.

§ 7. 1. Minister, w terminie 10 dni od dnia otrzymania wniosku, o którym mowa w § 6 ust. 2:

1) wyraża zgodę na odwołanie pełnomocnika albo
2) nie wyraża zgody na odwołanie pełnomocnika, przedstawiając zarządowi spółki pisemne uzasadnienie swojego stanowiska w tej sprawie w postaci papierowej.

2. Przepisy ust. 1 stosuje się odpowiednio do rozpatrywania wniosku, o którym mowa w § 6 ust. 2, przez dyrektora Centrum.

§ 8. W przypadku uzyskania zgody na odwołanie pełnomocnika zarząd spółki niezwłocznie po podjęciu uchwały, o której mowa w § 6 ust. 1, przekazuje jej kopie ministrowi oraz dyrektorowi Centrum.

§ 9. Spółka zapewnia pełnomocnikowi warunki organizacyjno-techniczne niezbędne do efektywnego wykonywania zadań.

§ 10. 1. Zarząd spółki zawiadamia pisemnie pełnomocnika, w postaci papierowej lub elektronicznej, o terminie, miejscu oraz porządku obrad posiedzenia zarządu, w przypadku planowanego rozpatrywania spraw, o których mowa w art. 2 ust. 1 ustawy, lub właściwego organu spółki w przypadku spraw, o których mowa w art. 2 ust. 2 ustawy, w terminie określonym w statucie, umowie spółki lub regulaminie organu spółki, jednak nie później niż na dwa dni przed dniem posiedzenia właściwego organu.

2. Do zawiadomienia, o którym mowa w ust. 1, zarząd spółki dołącza materiały i dokumenty dotyczące spraw, o których mowa odpowiednio w art. 2 ust. 1 i 2 ustawy.

3. Zarząd spółki udostępnia pełnomocnikowi pisemną informację w postaci papierowej o zamiarze dokonania przez spółkę czynności, o której mowa w art. 2 ust. 1 lub 2 ustawy, wraz z kopiami dokumentów dotyczących tej czynności lub zdarzenia, nie później niż na dwa dni przed planowanym dokonaniem czynności.

4. Pełnomocnik niezwłocznie, nie później jednak niż w terminie 14 dni od dnia posiedzenia organu spółki, odbycia zgromadzenia wspólników albo walnego zgromadzenia, przedstawia ministrowi informacje o sprawach, o których mowa odpowiednio w art. 2 ust. 1 i 2 ustawy, będących przedmiotem posiedzenia, zgromadzenia wspólników albo walnego zgromadzenia.

§ 11. 1. Pełnomocnik występuje do organów spółki z żądaniem udostępnienia dokumentów, informacji oraz wyjaśnień dotyczących spraw, o których mowa w art. 2 ust. 1 i 2 ustawy, w formie pisemnej w postaci papierowej.

2. Jeżeli jest to uzasadnione okolicznościami, pełnomocnik może wystąpić z żądaniem, o którym mowa w ust. 1, w formie ustnej.

3. W przypadku, o którym mowa w ust. 2, pełnomocnik, po wystąpieniu z żądaniem, w terminie nie dłuższym niż 3 dni, sporządza notatkę, w której wskazuje w szczególności:

1) okoliczności, o których mowa w ust. 2;
2) formę zgłoszonego żądania;
3) datę zgłoszenia żądania;

4) organ spółki, do którego wystąpił z żądaniem;

5) zakres dokumentów, informacji lub wyjaśnień objętych żądaniem.

4. Kopię notatki, o której mowa w ust. 3, pełnomocnik niezwłocznie przekazuje organowi, do którego wystąpił z żądaniem, oraz w przypadku, gdy żądanie zostało wystosowane do organu innego niż zarząd spółki – zarządowi spółki.

§ 12. 1. Informacje lub wyjaśnienia, przekazywane pełnomocnikowi w związku z żądaniem, o którym mowa w § 11 ust. 1, właściwy organ spółki przekazuje pełnomocnikowi w formie pisemnej w postaci papierowej lub elektronicznej.

2. Jeżeli jest to uzasadnione okolicznościami lub w przypadku, o którym mowa w § 11 ust. 2, organ, do którego pełnomocnik wystąpił z żądaniem, o którym mowa w § 12 ust. 1, może udzielić informacji lub wyjaśnień w formie ustnej.

§ 13. 1. Pełnomocnik sporządza notatkę z czynności związanych z wykonywaniem obowiązków, dotyczących spraw, o których mowa w art. 2 ust. 1 i 2 ustawy, dokonanych w formie ustnej, w szczególności w przypadku, o którym mowa w § 11 ust. 2, odpowiednio do charakteru tej czynności, w której zawiera informację o podjętych przez siebie działaniach.

2. W przypadku gdy notatka, o której mowa w ust. 1, została sporządzona w związku z informacjami lub wyjaśnieniami przekazanymi w formie ustnej, osoby, które udzieliły tych informacji lub wyjaśnień, są obowiązane do jej parafowania. W przypadku odmowy jej parafowania pełnomocnik zaznacza to w notatce wraz z podaniem daty i przyczyn tej odmowy.

§ 14. Pełnomocnik zabezpiecza i przechowuje dokumentację dotyczącą wszystkich czynności podejmowanych przez niego w związku z realizacją zadań, o których mowa w art. 5 ust. 2 ustawy.

§ 15. 1. Przepisy § 1-14 stosuje się odpowiednio do zastępcy pełnomocnika ochrony infrastruktury krytycznej, o którym mowa w art. 5 ust. 1 ustawy z dnia 18 marca 2010 r. o szczególnych uprawnieniach ministra właściwego do spraw aktywów państwowych oraz ich wykonywaniu w niektórych spółkach kapitałowych lub grupach kapitałowych prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych.

2. Zastępca pełnomocnika ochrony infrastruktury krytycznej realizuje zadania, o których mowa w § 11-14, w przypadku nieobecności lub czasowej niemożności wykonywania zadań przez pełnomocnika ochrony infrastruktury krytycznej.

§ 16. Rozporządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

PREZES RADY MINISTRÓW

UZASADNIENIE

W celu zapewnienia ciągłości procesów realizowanych przez Pełnomocnika do spraw ochrony infrastruktury krytycznej (dalej: „Pełnomocnik OIK"), proponuje się zobowiązanie zarządów spółek do powoływania zastępcy Pełnomocnika OIK. Projektowane przepisy zakładają, że tryb powoływania i odwoływania oraz kompetencje i obowiązki zastępcy Pełnomocnika OIK będą analogiczne do zadań realizowanych przez Pełnomocnika OIK, z zastrzeżeniem, że zastępca Pełnomocnika OIK będzie powoływany w terminie 60 dni od dnia otrzymania przez zarząd spółki informacji o ujęciu składników jej mienia w wykazie (Pełnomocnik OIK powoływany jest w terminie 30 dni). Taki stan rzeczy pozwoli na zapewnienie przez Pełnomocnika OIK odpowiedniego wsparcia zarządowi spółki w zakresie pozyskania odpowiedniego, spełniającego kryteria formalne, kandydata na to stanowisko. Kluczowym zadaniem zastępcy Pełnomocnika OIK będzie zapewnienie zastępstwa, ale także wsparcie procesów i zadań realizowanych w spółce z zakresu bezpieczeństwa infrastruktury krytycznej.

Obecnie, w przypadku nieobecności pełnomocnika w pracy spowodowanej urlopem, chorobą lub innymi losowymi okolicznościami, których nie sposób przewidzieć, zastępstwo zapewniane jest przez inne osoby najczęściej pracujące w pionie bezpieczeństwa, których kompetencje pozostają niezweryfikowane. Nieoficjalni zastępcy nie posiadają narzędzi pozwalających np. na uczestnictwo w posiedzeniach organów spółki dotyczących infrastruktury krytycznej oraz nie posiadają prawa do żądania od organów spółki udzielenia informacji oraz wyjaśnień, a tym samym nie zapewniają rzetelnego wykonywania obowiązków należących do Pełnomocnika OIK, a w konsekwencji nie dają rękojmi do prawidłowego realizowania przepisów ustawy. Z uwagi na fakt, że zgodnie z art. 5 ust 2 ustawy *o szczególnych uprawnieniach* Pełnomocnik OIK jest pracownikiem spółki, tj. podlega przepisom Kodeksu pracy wraz z wszelkimi wynikającymi z tego faktu prawami i obowiązkami, niezbędne jest, w ocenie Ministerstwa, stworzenie warunków do zapewnienia Pełnomocnikowi OIK stosownego zastępstwa oraz zapewnienie ciągłości realizacji zadań ustawowych Pełnomocnika OIK.

Proponowane zmiany pozwolą na zapewnienie ciągłości realizowanych procesów oraz pozytywnie wpłyną na realizację zadań Pełnomocnika OIK w zakresie zapewnienia bezpieczeństwa infrastruktury krytycznej.

Podobnie jak w obowiązującym rozporządzeniu, organem wyrażającym zgodę na powołanie i odwołanie pełnomocnika jest minister właściwy do spraw energii, który wyraża zgodę w porozumieniu z dyrektorem Rządowego Centrum Bezpieczeństwa.

Pozostałe przepisy, określające szczegółowy tryb powoływania i odwoływania pełnomocnika oraz sposób wykonywania przez niego obowiązków, stanowią powtórzenie przepisów zawartych w obecnie obowiązującym rozporządzeniu.

Przewiduje się, że regulacja wejdzie w życie po upływie 14 dni od dnia ogłoszenia.

Projekt rozporządzenia nie jest objęty prawem Unii Europejskiej.

Projekt 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. z 2002 r. poz. 2039, z późn. zm.), w związku z tym nie podlega procedurze notyfikacji.

Projektowane rozporządzenie nie wymaga przedstawienia instytucjom i organom Unii Europejskiej lub Europejskiemu Bankowi Centralnemu.

Zgodnie z art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248) oraz stosownie do § 52 uchwały Nr 190 Rady Ministrów z dnia 29 października 2013 r. – Regulamin pracy Rady Ministrów (M.P. z 2016 r. poz. 1006, z późn. zm.), projekt rozporządzenia został udostępniony w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji, w serwisie Rządowy Proces Legislacyjny.

Zawarte w projekcie regulacje nie będą miały wpływu na działalność mikroprzedsiębiorców, małych i średnich przedsiębiorców, zgodnie z ustawą z dnia 6 marca 2018 r. – Prawo przedsiębiorców (Dz. U. z 2021 r. poz. 162).

Nazwa projektu Rozporządzenie Prezesa Rady Ministrów w sprawie pełnomocnika do spraw ochrony infrastruktury krytycznej **Ministerstwo wiodące i ministerstwa współpracujące** Ministerstwo Aktywów Państwowych **Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu** **Kontakt do opiekuna merytorycznego projektu**	**Data sporządzenia** **Źródło:** **Nr w wykazie prac:**

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

Dostosowanie rozporządzenia do znowelizowanej ustawy z dnia 18 marca 2010 r. o szczególnych uprawnieniach ministra właściwego do spraw aktywów państwowych oraz ich wykonywaniu w niektórych spółkach kapitałowych lub grupach kapitałowych prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych (Dz. U. z 2020 r. poz. 2173), zwanej dalej „ustawą".

Zgodnie z art. 67 ustawy z dnia 23 stycznia 2020 r. o zmianie ustawy o działach administracji rządowej oraz niektórych innych ustaw (Dz. U. poz. 284), dokonano nowelizacji ustawy, polegającej między innymi na zmianie organu realizującego jej przepisy. Zadania i uprawnienia w zakresie realizacji ustawy, które do tej pory były w kompetencji ministra właściwego do spraw energii, przejął minister właściwy do spraw aktywów państwowych.

W obowiązującym obecnie rozporządzeniu, organem wyrażającym zgodę na powołanie i odwołanie pełnomocnika do spraw ochrony infrastruktury krytycznej jest minister właściwy do spraw energii, który wyraża zgodę w porozumieniu z dyrektorem Rządowego Centrum Bezpieczeństwa. Rozporządzenie wymaga dostosowania do znowelizowanej ustawy, poprzez zmianę organu mającego uprawnienia do wykonywania przepisów rozporządzenia.

2. Rekomendowane rozwiązanie, w tym planowane narzędzia interwencji, i oczekiwany efekt

Rekomendowanym rozwiązaniem jest wydanie nowego rozporządzenia Prezesa Rady Ministrów w sprawie pełnomocnika do spraw ochrony infrastruktury krytycznej, dostosowanego do znowelizowanej ustawy, poprzez zmianę organu realizującego przepisy rozporządzenia i zastąpienie wyrazów „minister właściwy do spraw energii" wyrazami „minister właściwy do spraw aktywów państwowych". Wydanie nowego rozporządzenia pozwoli uniknąć wątpliwości, który z organów posiada kompetencje w zakresie wyrażania zgody na powoływanie i odwoływanie pełnomocników do spraw ochrony infrastruktury krytycznej.

W porównaniu do obowiązującego rozporządzenia, projekt zakłada również:

1) określenie terminu, w jakim wyznaczony przez zarząd spółki kandydat powinien wyrazić zgodę na objęcie stanowiska pełnomocnika;
2) doprecyzowanie zakresu informacji z Krajowego Rejestru Karnego, jakie kandydat na pełnomocnika powinien przedstawić zarządowi spółki;
3) zmianę rozpoczęcia biegu terminu, jaki ma zarząd spółki na sporządzenie i przesłanie wniosku o wyrażenie zgody na powołanie kandydata na stanowisko pełnomocnika;
4) zobowiązanie zarządu spółki do przekazywania ministrowi właściwemu do spraw aktywów państwowych oraz dyrektorowi Rządowego Centrum Bezpieczeństwa kopii uchwały dotyczącej odwołania pełnomocnika do spraw ochrony infrastruktury krytycznej.

Pozostałe przepisy, określające szczegółowy tryb powoływania i odwoływania pełnomocnika do spraw ochrony infrastruktury krytycznej oraz sposób wykonywania przez niego obowiązków, stanowią powtórzenie przepisów zawartych w obecnie obowiązującym rozporządzeniu. Brak jest możliwości osiągnięcia celu wynikającego z projektu za pomocą środków innych niż wydanie nowego rozporządzenia.

3. Jak problem został rozwiązany w innych krajach, w szczególności krajach członkowskich OECD/UE?

Nie dotyczy.

4. Podmioty, na które oddziałuje projekt

Grupa	Wielkość	Źródło danych	Oddziaływanie
Minister właściwy do spraw aktywów państwowych	1		Wyrażanie zgody na powoływanie i odwoływanie pełnomocników do spraw ochrony infrastruktury krytycznej oraz zastępców pełnomocników
Dyrektor Rządowego Centrum Bezpieczeństwa	1		Wyrażanie zgody na powoływanie i odwoływanie pełnomocników do spraw ochrony infrastruktury krytycznej oraz zastępców pełnomocników
Szef Agencji Bezpieczeństwa Wewnętrznego	1		Otrzymywanie dokumentów z danymi dotyczącymi kandydatów na pełnomocników do spraw ochrony infrastruktury krytycznej lub zastępców pełnomocników oraz informacji o zmianie tych danych
Spółki kapitałowe lub grupy kapitałowe prowadzące działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych, których mienie zostało ujawnione w jednolitym wykazie obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej z podziałem na systemy		Jednolity wykaz obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej z podziałem na systemy	Powoływanie i odwoływanie pełnomocników do spraw ochrony infrastruktury krytycznej lub zastępców pełnomocników, zapewnienie pełnomocnikowi warunków organizacyjno-technicznych, informowanie pełnomocnika o planowanych i dokonanych czynnościach prawnych wobec mienia stanowiącego infrastrukturę krytyczną
Pełnomocnicy do spraw ochrony infrastruktury krytycznej oraz zastępcy pełnomocników		Dane własne	Monitorowanie działalności spółki w zakresie czynności prawnych podejmowanych wobec mienia stanowiącego infrastrukturę krytyczną

5. Informacje na temat zakresu, czasu trwania i podsumowanie wyników konsultacji

Projektowane rozporządzenie, z uwagi na brak oddziaływania jego przepisów na podmioty zewnętrzne, nie będzie podlegało konsultacjom publicznym.
Projekt rozporządzenia został udostępniony w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji, w serwisie Rządowy Proces Legislacyjny.

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												
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	Wejście w życie projektowanego rozporządzenia nie spowoduje dodatkowych skutków finansowych dla sektora finansów publicznych, w tym budżetu państwa i budżetów jednostek samorządu terytorialnego.											

7. Wpływ na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców oraz na rodzinę, obywateli, osoby starsze i niepełnosprawne 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	0	0	0	0	0	0	0
	sektor mikro-, małych i średnich przedsiębiorstw	0	0	0	0	0	0	0
	rodzina, obywatele oraz gospodarstwa domowe	0	0	0	0	0	0	0
W ujęciu niepieniężnym	duże przedsiębiorstwa							
	sektor mikro-, małych i średnich przedsiębiorstw							
	rodzina, obywatele, osoby starsze i niepełnosprawne oraz gospodarstwa domowe							
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	Wejście w życie rozporządzenia nie będzie miało wpływu na konkurencyjność gospodarki i przedsiębiorczość, w tym na funkcjonowanie przedsiębiorców (również mikroprzedsiębiorców) oraz na rodzinę, obywateli i gospodarstwa domowe.							

8. Zmiana obciążeń regulacyjnych (w tym obowiązków informacyjnych) wynikających z projektu	
☐ nie dotyczy	
	☐ tak ☐ nie ☒ nie dotyczy
☐ zmniejszenie liczby dokumentów ☐ zmniejszenie liczby procedur ☐ skrócenie czasu na załatwienie sprawy ☐ inne:	☐ zwiększenie liczby dokumentów ☐ zwiększenie liczby procedur ☐ wydłużenie czasu na załatwienie sprawy ☒ inne: doprecyzowanie terminów przekazania dokumentów, doprecyzowanie zakresu wymaganych dokumentów
Wprowadzane obciążenia są przystosowane do ich elektronizacji.	☐ tak ☐ nie ☒ nie dotyczy
Komentarz:	

9. Wpływ na rynek pracy
Brak wpływu.

10. Wpływ na pozostałe obszary		
☐ środowisko naturalne ☐ sytuacja i rozwój regionalny ☐ inne:	☐ demografia ☐ mienie państwowe	☐ informatyzacja ☐ zdrowie
Omówienie wpływu	Wejście w życie rozporządzenia nie będzie miało wpływu na pozostałe obszary, np. środowisko naturalne, sytuację i rozwój regionalny itd.	

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?
Nie przewiduje się przeprowadzania ewaluacji projektu ze względu na techniczny charakter zmian w nim zawartych.

13.Załączniki (istotne dokumenty źródłowe, badania, analizy itp.)
Brak.