**Tabela rozbieżności uwag zgłoszonych w ramach procesu uzgodnień międzyresortowych**

**Projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy – Prawo zamówień publicznych (poprzedni tytuł: projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa, ustawy – Prawo telekomunikacyjne oraz ustawy – Ordynacja podatkowa (UD68).**

|  |  |  |  |
| --- | --- | --- | --- |
| **Podmiot wnoszący uwagi** | **Jednostka redakcyjna, do której wnoszone są uwagi** | **Zgłoszone uwagi** | **Stanowisko KPRM/DC** |
| **Ministerstwo Klimatu i Środowiska** | Uwaga ogólna,  art. 1 pkt 2 lit. b i  pkt 12 | W opinii Ministerstwa Klimatu i Środowiska nie jest zasadne, aby przepisy dotyczące sektora telekomunikacyjnego, regulujące obowiązki przedsiębiorców komunikacji elektronicznej znalazły się w nowelizacji do ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2020 r. poz. 1369), a w procedowanej również na poziomie uzgodnień międzyresortowych projektu ustawy Prawo komunikacji elektronicznej (UC45). Telekomunikacja i przedsiębiorcy komunikacji elektronicznej posiadają podobnie jak sektory wymienione w dyrektywie PE i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii własne przepisy sektorowe. Nie oznacza to, że ww. przepisy regulujące przykładowo ciągłość działania usługi kluczowej, zarządzanie ryzykiem, zarządzanie incydentami w sektorze energetyki, zdrowia, finansów będą każdorazowo wprowadzane do ustawy o krajowym systemie cyberbezpieczeństwa. Wprowadzenie przepisów materialnych dotyczących przedsiębiorców komunikacji elektronicznej, w tym definicji właściwych dla sektora komunikacji elektronicznej, z racji swojej hermetyczności spowoduje wątpliwości interpretacyjne, zawęży krąg potencjalnych operatorów usług kluczowych, których włączenie do Krajowego Systemu Cyberbezpieczeństwa byłoby zasadne z punktu widzenia utrzymania ciągłości świadczenia usług kluczowych dla sprawnego funkcjonowania państwa.  Warto podkreślić, że Ministerstwo Klimatu w toku konsultacji do projektu Prawo komunikacji elektronicznej (UC45) przedłożyło propozycję zmiany definicji systemu informacyjnego w ustawie o krajowym systemie cyberbezpieczeństwa, tak aby definicja była dostosowana do szerszego grona podmiotów, a więc z sektorów innych niż np. telekomunikacyjny lub sektor usług cyfrowych, szczególnie tych, w których systemy automatyki przemysłowej odgrywają istotną rolę w procesie świadczenia usługi kluczowej.  Przeniesienie dodanych definicji art. 2 pkt 8a-8g do projektu ustawy Prawo komunikacji elektronicznej (UC45).  Przeniesienie rozdziału 4a: Obowiązki przedsiębiorców komunikacji elektronicznej do projektu ustawy Prawo komunikacji elektronicznej (UC45). | **Uwaga częściowo uwzględniona**  Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowych.  EKŁE stanowi w art. 40 ust. 2, że przedsiębiorcy komunikacji elektronicznej mają zgłaszać incydenty do właściwych organów, które mogą być inne niż krajowe organy regulacyjne.  Usługi świadczone przez przedsiębiorców komunikacji elektronicznej mają kluczowe znaczenie dla niezakłóconego świadczenia usług przez operatorów usług kluczowych, dostawców usług cyfrowych czy też administrację publiczną czyli innych podmiotów krajowego systemu cyberbezpieczeństwa.  Prace legislacyjne związane z wprowadzeniem przepisów prawnych dot. obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci i usług oraz zgłaszania incydentów zostały przeniesione do przepisów wprowadzających Prawo Komunikacji Elektronicznej.  Obecna definicja systemu informacyjnego jest wystarczająca. |
| **Ministerstwo Klimatu i Środowiska** | Uwaga Ogólna  art. 1 pkt 29 - 32 | Proponuje się, aby przepisy dotyczące nowych instytucji prawnych, a więc oceny ryzyka dostawcy sprzętu lub oprogramowania istotnego dla cyberbezpieczeństwa, ostrzeżenia i polecenia zabezpieczające oraz nowe kompetencje przypisane w tym zakresie Kolegium ds. Cyberbezpieczeństwa i Pełnomocnika Rządu ds. Cyberbezpieczeństwa obowiązywały wyłącznie sektor komunikacji elektronicznej. Podkreślić bowiem należy, że opisana w projekcie ustawy konstrukcja oceny ryzyka dostawcy sprzętu lub oprogramowania istotnego dla cyberbezpieczeństwa, ostrzeżenia i polecenia zabezpieczające to elementy, które wykraczają poza cele i minimalne wymagania określone dyrektywą NIS i ustawę o krajowym systemie cyberbezpieczeństwa, będącą jej implementacją w polskim porządku prawnym. W dyrektywie i obowiązującej ustawie jest bowiem wyłącznie mowa o zarządzaniu ryzykiem systemów informacyjnych OUK służących do świadczenia usług kluczowych. Ponadto niektóre sektory, w tym sektor energetyczny zgodnie z art. 7 dyrektywy NIS muszą stosować sektorowe akty prawne, w przypadku gdy obejmują przepisy dotyczące zarządzania ryzykiem. „W przypadku gdy sektorowy akt prawny Unii wymaga od operatorów usług kluczowych lub dostawców usług cyfrowych, aby zapewniali bezpieczeństwo swoich sieci i systemów informatycznych albo zgłaszali incydenty, stosuje się przepisy tego sektorowego aktu prawnego Unii, pod warunkiem że takie wymogi są przynajmniej równoważne pod względem skutku z obowiązkami określonymi w niniejszej dyrektywie.”. W przypadku sektora energetycznego chodzi o następujące akty prawne: a) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/1938 z dnia 25 października 2017 r. dotyczące środków zapewniających bezpieczeństwo dostaw gazu ziemnego i uchylające rozporządzenie (UE) nr 994/2010 (Tekst mający znaczenie dla EOG). b) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/941 z dnia 5 czerwca 2019 r. w sprawie gotowości na wypadek zagrożeń w sektorze energii elektrycznej i uchylające dyrektywę 2005/89/WE (Tekst mający znaczenie dla EOG)  c) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/943 w sprawie wewnętrznego rynku energii elektrycznej (wersja przekształcona). Dodatkowo szczegółowe wymagania cyberbezpieczeństwa, w tym wymagania wynikające z dyrektyw o rynku energii elektrycznej mają być regulowane w kodeksach sieciowych, a więc w aktach wykonawczych UE wydawanych w drodze komitologii.  Jak wskazano w uzasadnieniu na s. 29 „Coraz większe znaczenie dla bezpieczeństwa usług kluczowych ma niezawodność usług telekomunikacyjnych. Stacjonarne sieci szerokopasmowe będą uzupełniane przez sieci mobilne nowej generacji (sieci 5G i kolejnych). Polska brała udział w opracowaniu unijnego zestawu narzędzi na potrzeby cyberbezpieczeństwa sieci 5G (zwanej dalej „5G Toolbox”), w którym zawarto środki na poziomie strategicznym i technicznym oraz  wskazano działania wspierające stosowanie tych środków dla ograniczenia ryzyk cyberbezpieczeństwa europejskich sieci 5G.”. Zarówno lektura Zalecenia Komisji (UE) 2019/534 z dnia 26 marca 2019 r. Cyberbezpieczeństwo sieci 5G, publikacji Grupy Współpracy 1/2020 „Cybersecurity of 5G networks EU Toolbox of risk mitigating measures” (wspomniany 5G Toolbox), publikacji Grupy Współpracy 1/2020 „Report on Member States’ Progress in Implementing the EU Toolbox on 5G Cybersecurity” wskazuje na zbieżność zadań z zakresu zarządzenia ryzykiem sprzętu i oprogramowania z propozycjami nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy – Prawo zamówień publicznych, z zastrzeżeniem, że rozwiązania, o których tam mowa, w tym mechanizmy zarządzania ryzykiem, są skierowane wobec przedsiębiorców komunikacji elektronicznej i usług przez nich realizowanych, a nie wszystkich podmiotów tworzących w Polsce krajowy system cyberbezpieczeństwa, w tym przedsiębiorców energetycznych, posiadających jak wskazano wyżej dodatkowe sektorowe przepisy z zakresu zarządzania ryzykiem. W świetle przedłożonego projektu ustawy podkreślić należy, że zgodnie z dotychczasowym kształtem ustawy w Kolegium nie zasiadają wszyscy ministrowie właściwi dla sektorów usług kluczowych, w tym minister właściwy ds. energii, a znajomość funkcjonowania systemów informacyjnych stosowanych w energetyce i transporcie (w większości systemów automatyki przemysłowej) wymaga najwyższych kompetencji z zakresu cyberbezpieczeństwa. Trudno też wyobrazić sytuację, że decyzje nt. zarządzania ryzykiem względem sprzętu i oprogramowania stosowanego w sektorze energetycznym podejmują ministrowie nadzorujący inne działy administracji rządowej, bez wiedzy ministra zarządzającego ryzykiem z zakresu cyberbezpieczeństwa nadzorowanego sektora. Uzupełnienie składu Kolegium ds.  cyberbezpieczeństwa o ministra właściwego ds. energii znalazło się w propozycji zmian w projekcie ustawy o efektywności energetycznej oraz niektórych innych ustaw (UC 41, dalej: uEE). Efektem włączenia ministra właściwego ds. energii do składu Kolegium będzie powstanie możliwości wyrażania opinii w kontekście kierunków i planów działania na rzecz przeciwdziałania zagrożeniom cyberbezpieczeństwa, opiniowania w sprawach rekomendacji dotyczących stosowania urządzeń informatycznych lub oprogramowania, a także określanie stanowiska ministra właściwego ds. energii w innych sprawach określonych w art. 65 UKSC. Przełoży się to na uwzględnianie w wielu aspektach dotyczących cyberbezpieczeństwa, potrzeb, opinii, sektora energetycznego, który z racji wyżej wskazanej odmienności nie zawsze może dostosować się do rozwiązań pasujących w innych sektorach. Propozycja z projektu uEE znalazła się w propozycji zmian do ww. ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy – Prawo zamówień publicznych.  W art. 66 w ust. 1 w pkt 4 w lit g kropkę zastępuje się przecinkiem i dodaje się lit h w brzmieniu:  „h) minister właściwy do spraw energii.”;  Proponowane brzmienie poniższych przepisów:  „Art. 66a. 1. Kolegium może sporządzić, na wniosek członka Kolegium, ocenę ryzyka dostawcy sprzętu lub oprogramowania istotnego dla cyberbezpieczeństwa podmiotów, o których mowa w art. 4 pkt 2a.” - (przy uwzględnieniu usunięcia  definicji bezpieczeństwo sieci i usług)  „3. Wniosek o sporządzenie oceny może określać:  2) kategorie przedsiębiorców komunikacji elektronicznej, które uwzględnia się przy sporządzeniu oceny dostawcy sprzętu lub oprogramowania.”  „Art. 66b. 1. W przypadku sporządzenia oceny ryzyka określającej wysokie ryzyko dostawcy sprzętu lub oprogramowania przedsiębiorcy komunikacji elektronicznej.”  „2. W przypadku sporządzenia oceny określającej umiarkowane ryzyko dostawcy sprzętu lub oprogramowania przedsiębiorcy komunikacji elektronicznej:”  „Art. 66c 1. W szczególnie uzasadnionych przypadkach Pełnomocnik może zobowiązać przedsiębiorcę komunikacji elektronicznej:”  „2. Plan i harmonogram podlega zatwierdzeniu przez Pełnomocnika po uzgodnieniu z Prezesem UKE.”  „Art. 67a. 1. Pełnomocnik może wydać:  1) ostrzeżenie - w przypadku uzyskania informacji o sytuacji szczególnego zagrożenia, o której mowa w art. 2 pkt. 65 ustawy z dnia …- Prawo komunikacji elektronicznej,”  „3. Pełnomocnik, przed wydaniem ostrzeżenia lub polecenia zabezpieczającego przeprowadza, we współpracy z Zespołem, analizę uzasadniającą jego wydanie, obejmującą:  1) istotność sytuacji szczególnego zagrożenia;”  „4. Ostrzeżenie i polecenie zabezpieczające może dotyczyć:  1) podmiotów, o których mowa w art. 4 pkt 2a.”  w Art. 73:  „14) ust. 2a wynosi:  a) w przypadku podmiotów określonych w art. 4 pkt 2a nie stosujących się do art. 66b ust. 1 w wysokości do 3% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego,  b) w przypadku podmiotów określonych w art. 4 pkt 2a nie stosujących się do art. 66b ust. 2 w wysokości do 1% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego,”  w Art. 74 ust. 1a:  „1a. Karę pieniężną określoną w art. 73 ust. 2a  nakłada w drodze decyzji:  1) w przypadku podmiotów określonych w art. 4 pkt 7-15 – organ nadzorujący;  2) w przypadku podmiotów określony w art. 4 pkt 2a – Prezes UKE;  3) w przypadku podmiotów wpisanych do wykazu SOC, wykonujących usługi na zlecenie operatora usług kluczowych – organy właściwe do spraw cyberbezpieczeństwa.” | **Uwaga nieuwzględniona**  Celem dyrektywy NIS jest wprowadzenie jednolitych ram cyberbezpieczeństwa w Unii Europejskiej. Dyrektywa określa minimalne warunki, które państwa członkowskie mają wprowadzić w krajowych porządkach prawnych. Państwa członkowskie mają swobodę w kształtowaniu krajowego systemu bezpieczeństwa.  Ponadto zgodnie z art. 1 ust. 6 dyrektywa NIS nie narusza działań Państw członkowskich mających na celu ochronę bezpieczeństwa narodowego, a do takich działań należy zaliczyć prowadzenie postępowania w sprawie uznania za dostawcę wysokiego ryzyka oraz wydawania ostrzeżeń i poleceń zabezpieczające.  Fakt, że Toolbox 5G (który nie jest aktem prawnym) dotyczy przedsiębiorców komunikacji elektronicznej nie przeszkadza w rozciągnięciu skutków nowych kompetencji ministra właściwego ds. informatyzacji oraz Kolegium na wszystkie podmioty krajowego systemu cyberbezpieczeństwa.  Postępowaniu w sprawie uznania za dostawcę wysokiego ryzyka powinni podlegać wszyscy dostawcy sprzętu lub oprogramowania dla podmiotów kluczowych dla społeczno-ekonomicznego bezpieczeństwa państwa i obywateli.  Celem ostrzeżenia i polecenia zabezpieczającego jest umożliwienie skutecznej reakcji na zagrożenie wystąpienia incydentu krytycznego (ostrzeżenie) lub na sam incydent krytyczny (polecenie zabezpieczające). Incydent krytyczny może dotyczyć wszystkich podmiotów krajowego systemu cyberbezpieczeństwa. Skutki incydentu krytycznego mogą mieć zasięg międzysektorowy. Stąd też ograniczenie możliwości stosowania ostrzeżeń i poleceń zabezpieczających tylko do przedsiębiorców komunikacji elektronicznej wpłynie negatywnie na bezpieczeństwo pozostałych podmiotów krajowego systemu cyberbezpieczeństwa.  Zharmonizowanie wymagań z sektorem telekomunikacji przyczyni się do znacznie skuteczniejszej ochrony usług kluczowych świadczonych przez podmioty z pozostałych 6 sektorów, które w zdecydowanej większości są zależne od niezakłóconych i bezpiecznych usług telekomunikacyjnych.  Obecne przepisy prawa (art. 66 ust. 5 pkt 2) umożliwiają, na zaproszenie Przewodniczącego Kolegium, udział w posiedzeniach Kolegium m. in. przedstawicieli organów właściwych ds. cyberbezpieczeństwa. |
| **Ministerstwo Klimatu i Środowiska** | Uwaga ogólna  art. 1 pkt 2 lit. a,  (dot. zmian  wprowadzanych w  nowym przepisie  art. 2 pkt 3e)  Uzasadnienie | Nie jest jasne jaka jest głębokość zmian proponowanych projektem przez Ministerstwo Cyfryzacji w zakresie certyfikacji cyberbezpieczeństwa. Z jednej strony słownik ustawy o krajowym systemie cyberbezpieczeństwa został poszerzony o definicję dostawcy sprzętu lub oprogramowania, które w swojej konstrukcji zawiera definicję produktów ICT, usług ICT i procesów ICT w rozumieniu przepisów Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie, Dz. Urz. UE L 151 z 7.6.2019, str. 15, dalej: CSA), dokonano zmiany nazwy agencji ENISA w świetle zmiany nazwy wprowadzonej tym rozporządzeniem. Zmieniono przepisy materialne dotyczące oceny ryzyka dostawców sprzętu lub oprogramowania. Z drugiej strony nowelizacja, zarówno w świetle przepisów materialnych, jak i uzasadnienia nie jest całkowitą implementacją przepisów tego rozporządzenia w polskim porządku prawnym. Podkreślić tutaj należy, że rozporządzenie mówi o konieczności powołania przez kraje członkowskie krajowych organów ds. certyfikacji cyberbezpieczeństwa, akredytowanie krajowych jednostek certyfikujących ds. cyberbezpieczeństwa, notyfikacji akredytowanych jednostek oceniających zgodność i egzekwowanie wymagań wobec tych jednostek. Konstrukcja proponowanych przepisów zakłada w art. 65 ust. 1 pkt 7 wyrażenie przez Kolegium opinii w sprawach wniosków CSIRT MON, CSIRT NASK lub CSIRT GOV w sprawie rekomendacji dotyczących stosowania urządzeń informatycznych lub oprogramowania, w nowym pkt 7 oceny ryzyka sprzętu i oprogramowania, a z kolei w nowym art. 66a. ust. 1 na wniosek członka Kolegium, oceny ryzyka dostawcy sprzętu lub oprogramowania istotnego dla cyberbezpieczeństwa podmiotów krajowego systemu cyberbezpieczeństwa. Taka konstrukcja budzi poważne wątpliwości interpretacyjne. Oznacza, że członkowie Kolegium, w randze co najmniej podsekretarza stanu dokonują samodzielnie oceny ryzyka sprzętu i oprogramowania, a na wniosek innego członka Kolegium oceny ryzyka dostawcy sprzętu lub oprogramowania istotnego dla cyberbezpieczeństwa podmiotów krajowego systemu cyberbezpieczeństwa. Zgodnie z przepisami ustawy obsługę Kolegium zapewnia ministerstwo obsługujące Pełnomocnika Rządu, w tym przypadku Ministerstwo Cyfryzacji. Pojawia się pytanie o zakres terminu obsługa, czy oznacza to, że pracownicy Ministerstwa Cyfryzacji zapewniają usługę laboratorium badawczego bądź funkcje jednostki certyfikującej pod kątem oceny ryzyka sprzętu i oprogramowania, czy też ministrowie bądź ich zastępcy realizują funkcje stricte techniczne w informatyce, dokonując niejako certyfikacji sprzętu i oprogramowania samodzielnie. Wymaga również wyjaśnienia czy w świetle tych przepisów i propozycji nowych przepisów, ministrowe wykonują funkcje krajowego organu/krajowych organów ds. certyfikacji cyberbezpieczeństwa. Użyte w uzasadnieniu do projektu sformułowanie, że Kolegium jest organem opiniodawczo-doradczym w sprawach planowania, nadzorowania i koordynowania działalności zespołów CSIRT jest sformułowaniem daleko idącym, bo choćby w zakresie oceny ryzyka sprzętu i oprogramowania zależności pomiędzy Kolegium a CSIRT nie wyczerpują znamiona nadzoru. Nasuwają się tym samym wątpliwości względem uzasadnienia na s. 45 czy „projektowana regulacja nie zawiera przepisów technicznych w rozumieniu rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. poz. 2039, z późn. zm.) i nie podlega notyfikacji Komisji Europejskiej.” Konieczne jest zatem uzupełnienie uzasadnienia  projektu ustawy nt. relacji propozycji ustawowej względem ww. CSA, a także co istotniejsze uzupełnienia przepisów materialnych i implementację rozporządzenia CSA. | **Uwaga nieuwzględniona**  Kolegium nie będzie wydawało certyfikatów w rozumieniu aktu o cyberbezpieczeństwie. Będzie odpowiedzialne za przygotowanie opinii w ramach postępowania o uznaniu za dostawcę wysokiego ryzyka w oparciu m.in. o badania sprzętu, o których mowa w art. 33 ustawy KSC.  Należy wskazać, że w ramach nowelizacji ustawy o KSC do projektu zostaną dodane przepisy dostosowujące polski porządek prawny do aktu o cyberbezpieczeństwa. Przepisy te zostaną zawarte w nowym rozdziale 11a. |
| **Ministerstwo Klimatu i Środowiska** | Uwaga ogólna | Oprócz wspomnianej w Uzasadnieniu konieczności powstania centrów wymiany informacji ISAC, jest także potrzeba stworzenia takiego centrum na poziomie administracji rządowej. Obecnie system jest rozproszony i brakuje tutaj spójnej struktury współpracy i wymiany informacji, której budowanie mogłoby być inicjowane przez Pełnomocnika. Jest możliwość wzmocnienia obecnych mechanizmów współpracy na poziomie organów właściwych zwłaszcza w zakresie przeprowadzenia konsultacji, analiz, przepływu informacji itd. Organy właściwe bezpośrednio inicjują działania, ale to może nie wystarczyć do zbudowania dobrego systemu na poziomie krajowym. | **Uwaga nieuwzględniona**  Koordynowanie działań i realizowanie polityki Rządu w zakresie zapewnienia cyberbezpieczeństwa jest zadaniem Pełnomocnika Rządu ds. cyberbezpieczeństwa. Jego obsługę zapewnia urząd, przy którym Pełnomocnik został powołany.  Zadaniem organów właściwych jest inicjowanie działań wzmacniających cyberbezpieczeństwo w nadzorowanych sektorach.  Nie ma analiz sugerujących konieczność utworzenia centrum typu ISAC na poziomie administracji rządowej. |
| **Ministerstwo Klimatu i Środowiska** | Uwaga ogólna | Nie ma informacji na podstawie jakich danych jest szacowany wpływ na sektor finansów. | **Uwaga nieuwzględniona**  Wyliczenia wpływu na sektor finansów publicznych zostały wyczerpująco przedstawione w OSR. Obejmują one w szczególności koszty powołania zespołów CSIRT sektorowych (w ramach których mieszczą się usługi CERT oraz SOC), koszty obsługi dodatkowych zadań przez ministra właściwego ds. informatyzacji oraz koszty zatrudnienia ekspertów o unikalnych kompetencjach z zakresu cyberbezpieczeństwa. |
| **Ministerstwo Infrastruktury** | Uwaga ogólna | W nawiązaniu do art. 5 ust. 4 „W przypadku gdy podmiot świadczy usługę kluczową w innych państwach członkowskich Unii Europejskiej, organ właściwy do spraw cyberbezpieczeństwa w toku postępowania administracyjnego, za pośrednictwem Pojedynczego Punktu Kontaktowego, prowadzi konsultacje z tymi państwami w celu ustalenia, czy ten podmiot został uznany w tych państwach za operatora usługi kluczowej oraz w kontekście stwierdzenia, że „Operatorem usługi kluczowej jest podmiot, o którym mowa w załączniku nr 1 do ustawy, posiadający jednostkę organizacyjną na terytorium Rzeczypospolitej Polskiej – art. 5 ust. 1 zgłaszam następujący problem: Z konsultacji z Pojedynczym Punktem Kontaktowym nie wynikają żadne decyzje. Ustawa nie wskazuje, jak należy postąpić wobec operatorów usług kluczowych posiadających na terenie Rzeczypospolitej Polskiej oddział będący w rozumieniu ustawy jednostką organizacyjną, a jednocześnie wyznaczonych w innym kraju UE na operatora. Ustawa powinna określić, czy organ właściwy ds. cyberbezpieczeństwa powinien również wyznaczyć tego operatora na terenie Rzeczypospolitej Polskiej oraz w jakim przypadku:   * jeżeli system informacyjny operatora wykorzystywany do świadczenia usługi kluczowej jest posadowiony i administrowany na terenie Rzeczypospolitej Polskiej, * jeżeli system informacyjny wykorzystywany do świadczenia usługi kluczowej nie jest posadowiony i administrowany na terenie Rzeczypospolitej Polskiej, * innym, niż w/w.   Brak takiej regulacji istotnie utrudnia podjęcie właściwej decyzji o wyznaczeniu podmiotu na operatora usługi kluczowej (zwanego dalej OUK) oraz ma negatywny wpływ na ocenę sposobu postępowania w realizacji zadań wynikających z Ustawy o Krajowym Systemie Cyberbezpieczeństwa (zwaną dalej UKSC) zarówno ze strony OUK jak i organu właściwego. | **Uwaga nieuwzględniona**  Uwaga nie dotyczy projektu nowelizacji o krajowym systemie cyberbezpieczeństwa.  Obecne przepisy pozwalają na przeprowadzenie postępowań administracyjnych wobec podmiotów zagranicznych świadczących usługę kluczową na terenie Polski, nawet jeśli nie mają siedziby na terenie państwa polskiego.  Pojedynczy Punkt Kontaktowy pośredniczy w komunikacji pomiędzy organami właściwymi zainteresowanych państw członkowskich. |
| **Ministerstwo Infrastruktury** | Uwaga ogólna | W projekcie ustawy o krajowym systemie cyberbezpieczeństwa wskazano konieczność utworzenia Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego działającego na poziomie sektora lub podsektora, ustanowionego przez organ właściwy do spraw cyberbezpieczeństwa dla danego sektora lub podsektora (zwanego dalej CSIRT sektorowy) oraz możliwość powołania centrum wymiany i analizy informacji na temat podatności, zagrożeń i incydentów funkcjonującego w celu wspierania podmiotów krajowego systemu cyberbezpieczeństwa (zwanego dalej ISAC). W praktyce może się okazać, że podmiot realizujący zadania CSIRT-u, będzie również ISAC w tym samym bądź innym (pod)sektorze, a więc będzie mógł obsługiwać również partnerów niebędących OUK. Co więcej, najprawdopodobniej do realizacji obydwu zadań będą wykorzystywane te same zasoby kadrowe, narzędziowe i sprzętowe. Stąd, w mojej ocenie, w ustawie należy określić zasady funkcjonowania takiego podmiotu, w sposób niepowodujący konfliktu zarówno na etapie realizacji zadań jako CSIRT i ISAC. | **Uwaga nieuwzględniona**  Zespół CSIRT sektorowy nie może obsługiwać podmiotów, które nie są operatorami usług kluczowych w danym sektorze lub podsektorze gospodarki, dla którego ten sektorowy CSIRT został ustanowiony.  ISAC nie jest jednostką operacyjną i nie przyjmuje zgłoszeń o incydentach. ISAC nie pełni roli w kontekście zgłaszania i obsługi incydentów – jest to zadanie zespołów CSIRT. |
| **Ministerstwo Infrastruktury** | Uwaga ogólna | Projekt ustawy przewiduje szereg zadań dla organów właściwych, z czego jednym z nich jest utworzenie CSIRT-u sektorowego, zgodnie z art. 3 ust. 1 w terminie 18 miesięcy od dnia wejścia w życie niniejszej ustawy. Mając na względzie obecnie panującą sytuację epidemiologiczną oraz związane z nią konsekwencje, realizacja zadania w wyznaczonym terminie może być istotnie utrudniona. Stąd proponuję wydłużenie terminu o 6-12 miesięcy. Nadto w projekcie ww. ustawy, jak również w Ocenie Skutków Regulacji brak jest precyzyjnego wskazania źródła sfinansowania kosztów organu właściwego do spraw cyberbezpieczeństwa na zapewnienie funkcjonowania CSIRT sektorowego. Środki na pokrycie skutków finansowych realizacji ww. zadania należałoby uwzględnić w rezerwie celowej budżetu państwa | **Uwaga nieuwzględniona**  Przepis został zmieniony. Finansowanie będzie realizowane w ramach rezerwy celowej na powstanie i funkcjonowanie CSIRT.  Wyliczenia w zakresie wpływu na sektor finansów publicznych zostały wyczerpująco przedstawione w OSR. Obejmują one koszty powołania i funkcjonowania zespołów CSIRT sektorowych.  Tworzenie sektorowych zespołów cyberbezpieczeństwa umożliwia aktualny art. 44. W związku z tym, że do tej pory (w ciągu 25 miesięcy od wejścia w życie ustawy) powstał tylko jeden sektorowy zespół cyberbezpieczeństwa istnieje potrzeba przyspieszenia tego procesu. |
| **Ministerstwo Infrastruktury** | Uwaga ogólna | Projekt ustawy nakłada obowiązek powołania zespołu pełniącego funkcję operacyjnego centrum bezpieczeństwa w danym podmiocie (zwanego dalej SOC) wewnątrz swojej struktury bądź zawiera umowę dotyczącą prowadzenia SOC na jego zlecenie z innym podmiotem zgodnie z art. 14 ust 2, oraz realizację zadań zgodnie z art. 14 ust 3. Projekt ustawy nie zakłada jasno czasu realizacji wymaganego zadania, co w konsekwencji może powodować opieszałość operatorów usług kluczowych. Zasadnym więc wydaje się wprowadzenie zakresu czasu na dostosowanie podmiotu do nowych wymagań. | **Uwaga nieuwzględniona**  Zespoły SOC są doprecyzowaniem aktualnie funkcjonującym wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo. Wobec tego nie ma potrzeby wskazywania czasu realizacji tego obowiązku ustawowego. |
| **Ministerstwo Infrastruktury** | Uwaga ogólna | Część OUK zarządza infrastrukturą krytyczną, o której mowa w ustawie z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2018 r. poz. 1401), natomiast zarówno przytoczona ustawa jak i UKSC nie daje organowi właściwemu możliwości pozyskania takich informacji. Brak tej wiedzy może mieć negatywny wpływ na realizacji zadań organ właściwy wobec danego OUK, wynikających z UKSC. Stąd wnoszę o wprowadzenie do UKSC przepisu uprawniającego organ właściwy do żądania od OUK informacji, a OUK do udzielenia informacji nt. posiadanej infrastruktury krytycznej, wykorzystywanej pośrednio lub bezpośrednio przez system informacyjny OUK do świadczenia usługi kluczowej. | **Uwaga nieuwzględniona**  Minister właściwy ds. transportu ma dostęp do informacji o systemach transportowych na podstawie ustawie o zarządzaniu kryzysowym. |
| **Ministerstwo Infrastruktury** | Uwaga ogólna | UKSC przewiduje realizację szeregu zadań oraz katalog kar za brak ich realizacji. O ile wysokość kar jest określona w zakresie, o tyle terminy realizacji poszczególnych zadań podlegających karze już nie. Nowelizacja nie wnosi w żadnym stopniu zmiany podejścia do karania OUK, niezależnie od panującej sytuacji np. ekonomicznej spowodowanej pandemią, która wedle powszechnie dostępnej wiedzy jest zmienna. Stąd proponuję wprowadzenie bardziej elastycznego mechanizmu naliczania kar. Mianowicie, w uzasadnionych przypadkach, na wniosek OUK, decyzją organu właściwego, naliczenie kary mogłoby ulec zawieszeniu na dany okres czasu (wynikający z ustawy), z zastrzeżeniem, że jeżeli w tym okresie uchybienia, za które naliczono kary nie zostaną usunięte/naprawione, to kara zostanie naliczona w wysokości nie mniejszej niż np. 50% górnej kwoty wynikającej z UKSC. Ocenia się, że taki mechanizm zadziała na OUK-i mobilizująco, co w konsekwencji doprowadzi do realizacji celu, którym nie jest naliczanie kar, a osiągnięcie przez OUK-i pełnej zdolności operacyjnej w zakresie cyberbezpieczeństwa. W tym miejscu warto też się zastanowić i ewentualnie wprowadzić odpowiednie zapisy do nowelizacji UKSC wychodzące nieco naprzeciw OUK-om (głównie dotyczy przedsiębiorstw), w sytuacji gdy kondycja danego OUK uległa istotnemu pogorszeniu (w stosunku do okresu, w którym realizował zadania, na podstawie których został wyznaczony na OUK), np. jest w upadłości, likwidacji lub nie realizuje swojej statutowej działalności. Rekomendowane jest w takiej sytuacji wprowadzenie, na określonych zasadach i w określonym czasie, możliwości częściowego albo całościowego zawieszenia obowiązku naliczania kary bądź spełniania wymagań dla OUK wynikających z UKSC. | **Uwaga nieuwzględniona**  Postępowanie dotyczące nakładania kar jest uregulowane w Kodeksie postępowania administracyjnego, nie ma potrzeby regulowania go w ustawie ksc. |
| **Ministerstwo Obrony Narodowej** | Uwaga ogólna | 1.Proponuje się ponownie przeanalizować potrzebę powoływania formalnych (ustawowych) struktur: ISAC, CSIRT TELCO, CSIRT SEKTOROWE, SOC, które to bez wprowadzenia w projekcie formalnej hierarchii oraz opisu jasno sprecyzowanych zależności, uprawnień i obowiązków w zakresie istniejących podmiotów mogą dodatkowo skomplikować i tak już mocno złożoną strukturę. Wprowadzenie do istniejącego systemu ww. podmiotów może spowodować dezorganizację istniejącego systemu i spowodować szereg problemów w jego funkcjonowaniu. Nie negując przyjętej przez wnioskodawcę koncepcji należy zauważyć, że bezpieczniejszym rozwiązaniem mogłoby być rozszerzenie kompetencji istniejących podmiotów (np. poprzez partnerstwo publiczno-prywatne) lub rozwijanie struktur istniejących instytucji. | **Uwaga nieuwzględniona**  Zaproponowane przepisy jasno określają zależności między nowo tworzonymi podmiotami a dotychczasowymi. |
| **Ministerstwo Sprawiedliwości** | Uwaga ogólna | Dodatkowo należy zauważyć, że przewidziane w projekcie przepisy nie tworzą kompletnej regulacji postępowania przed Pełnomocnikiem lub Kolegium (brak np. regulacji dotyczącej trybu odwoławczego). W związku z powyższym, by uniknąć niejasności przy interpretacji, wskazane jest odesłanie do przepisów ustawy – Kodeks postępowania administracyjnego, poprzez dodanie odpowiedniego przepisu, np.:„Art. 67d. W sprawach nieuregulowanych w ustawie do postępowania przed Pełnomocnikiem lub Kolegium stosuje się przepisy ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego.”.  Abstrahując od powyższego, należy zauważyć, że w kontekście zadań postawionych przez ustawodawcę organom ścigania i wymiaru sprawiedliwości, projekt pomija kwestię okresu przez jaki podmioty wchodzące w skład szeroko pojmowanego krajowego systemu cyberbezpieczeństwa powinny przechowywać dane o incydencie. Informacje te mają istotne znaczenie dowodowe w przypadku stwierdzenia, że z incydentem związane jest naruszenie normy prawnej. Zagadnienie to ściśle powiązane jest z zapewnieniem odpowiedniego poziomu cyberbezpieczeństwa w kraju. Dla jego urzeczywistnienia wymagane jest przy tym wprowadzenie również tego typu odpowiednich rozwiązań do projektu ustawy – Prawo komunikacji elektronicznej, które to rozwiązania umożliwiać będą zabezpieczanie i pozyskiwanie dla potrzeb postępowania karnego niezbędnych danych.  Dla wzrostu bezpieczeństwa w sieci i systemów informacyjnych, podniesienia efektywności zwalczania cyberprzestępczości, jak również ograniczenia zjawiska kradzieży tożsamości, celowe jest nałożenie na podmioty świadczące usługi drogą elektroniczną obowiązków w zakresie gromadzenia i przechowywania logów związanych ze świadczoną usługą. Obecnie podmioty te nie są ustawowo zobligowane do gromadzenia i przechowywania logów dostępowych użytkowników. W efekcie o rozmiarze pozyskania tego rodzaju danych, w tym o ich czasookresie, decyduje regulamin danego podmiotu. Brak sposobności pozyskania odpowiednich danych niejednokrotnie powoduje niemożność ustalenia kto korzystał z danej usługi (np. z konta poczty elektronicznej), a także znacząco utrudnia lub wręcz uniemożliwia w niektórych przypadkach skuteczne przeprowadzenie postępowań dotyczących uzyskania nieuprawnionego dostępu (włamanie do konta użytkownika). Mając powyższe na względzie, zasadne jest wprowadzenie obowiązku retencji danych (w tym logów) przez okres 12 miesięcy, tak jak to ma miejsce w przypadku danych telekomunikacyjnych.  Ponadto niezbędne jest normatywne określenie zakresu danych gromadzonych i udostępnianych jako „logi”. Znaczna część podmiotów świadczących usługi drogą elektroniczną, czy też banków nie gromadzi informacji o numerach portów. Z uwagi na to, że operatorzy bardzo szeroko wykorzystują system NAT, jeden publiczny adres IP może być przydzielony nawet kilkudziesięciu tysiącom użytkowników. Zabieg ten uniemożliwia ustalenie abonenta usługi.  Dla podniesienia poziomu cyberbezpieczeństwa niezbędne jest także nałożenie na podmioty świadczące usługi drogą elektroniczną obowiązku weryfikacji tożsamości podmiotów korzystających z oferowanych przez nich usług. Obecnie podmioty świadczące usługi drogą elektroniczną opierają się głównie na danych deklaratywnie podawanych przez użytkowników. Dane te nie wymagają sprawdzenia. Sprawia to, że cyberprzestępcy dbając o zachowanie swojej anonimowości, w celu rejestracji usług podają nieprawdziwe dane, często udając inne osoby.  Przedstawione wyżej postulaty odpowiadają rekomendacjom Rady do Spraw Cyfryzacji zawartym w uchwale nr 7 z dnia 14 kwietnia 2020 r. w sprawie działań mających na celu zapobieganie kradzieży tożsamości oraz wnioskom sformułowanym przez Międzyresortowy Zespół do Spraw Ataków Kaskadowych. | **Uwaga nieuwzględniona**  Kwestie retencji danych oraz zwalczania cyberprzestępczości nie są przedmiotem ustawy o krajowym systemie cyberbezpieczeństwa ani Prawa komunikacji elektronicznej.  Ewentualne zmiany mogłyby dotyczyć ustawy o świadczeniu usług drogą elektroniczną – w takim przypadku Ministerstwo Sprawiedliwości powinno zaproponować zmianę w aktualnych przepisach.  Natomiast w projekcie dokonano zmian w zakresie postępowań w sprawie oceny ryzyka oraz wydawania poleceń zabezpieczających. |
| **Ministerstwo Finansów** | Uwaga ogólna do OSR i uzasadnienia do ustawy | W OSR, jak również w uzasadnieniu, nie wskazano na możliwe skutki tej ustawy w zakresie:   1. wzrostu kosztów usług IT, bo koszty obsługi tej ustawy usługodawcy IT będą przenosić na odbiorców; 2. znikania dostawców usług gwarancyjnych i pogwarancyjnych - w przypadku, w którym zostaną zidentyfikowani, jako źródło zagrożenia, zostaną wyłączeni z systemu zamówień publicznych w Polsce; 3. wydłużenia procedur przetargowych na dostawy usług IT - dostawcy sprzętu lub oprogramowania będą mogli zostać poddani procedurze sprawdzającej pod kątem zagrożeń dla społeczno-ekonomicznego bezpieczeństwa państwa; 4. ograniczenia z korzystania z niektórych planowanych bądź użytkowanych produktów IT, oprogramowania i usług danego dostawcy sprzętu lub oprogramowania. | **Uwaga nieuwzględniona**  Celem nowelizacji jest ograniczenie użytkowania sprzętu, oprogramowania i usług od dostawców, którzy stanowią ryzyko dla bezpieczeństwa narodowego.  Zadaniem państwa jest zapewnienie, aby kluczowe usługi były świadczone w sposób niezakłócony, stąd też istotne jest, aby sprzęt lub oprogramowanie wykorzystywane w krytycznych dla państwa podmiotach pochodził wyłącznie od dostawców zaufanych. |
| **Ministerstwo Sprawiedliwości** | Art. 1 ust 1 pkt 4 | Zgodnie z projektowanym art. 1 ust. 1 pkt 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2020 r. poz. 1369), ustawa określa zadania i obowiązki przedsiębiorców komunikacji elektronicznej, o których mowa w ustawie z dnia ... – Prawo komunikacji elektronicznej (Dz. U. ...), w zakresie wymogów dotyczących bezpieczeństwa i zgłaszania incydentów. Należy zauważyć, że projekt zakłada wprowadzenie do ww. ustawy regulacji dotyczących obowiązków operatorów telekomunikacyjnych oraz dostawców usług zaufania z zakresu zapewnienia cyberbezpieczeństwa, co jest sprzeczne z dyrektywą Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. Urz. UE 2016 L 194/1, dalej „dyrektywa NIS”). Zgodnie z art. 1 ww. dyrektywy regulacje dotyczące bezpieczeństwa i zgłaszania incydentów nie mają zastosowania ani do przedsiębiorstw telekomunikacyjnych, które podlegają wymogom art. 13a i 13b dyrektywy 2002/21/WE Parlamentu Europejskiego i Rady z dnia 7 marca 2002 r. w sprawie wspólnych ram regulacyjnych sieci i usług łączności elektronicznej (Dz. Urz. WE 2002 L 108/33, dalej „dyrektywa ramowa”) ani do dostawców usług zaufania, którzy podlegają wymogom art. 19 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającej dyrektywę 1999/93/WE (Dz. Urz. UE 2014 L 257/73). W związku z tym właściwymi aktami prawnymi do regulacji ww. kwestii jest ustawa z dnia 16 lipca 2004 r.– Prawo telekomunikacyjne (Dz. U. z 2019 r. poz. 2460, z późn. zm.), a w przyszłości – projektowana ustawa – Prawo komunikacji elektronicznej, mająca implementować postanowienia Kodeksu Łączności Elektronicznej – dyrektywy Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiająca Europejski kodeks łączności elektronicznej (Dz. Urz. UE 2018 L 321/36, dalej „KŁE”). W związku z powyższym projektowany art. 1 ust. 1 pkt 4 ustawy o krajowym systemie cyberbezpieczeństwa nie powinien znaleźć się w projekcie. Konsekwencją usunięcia niniejszego przepisu z projektu jest konieczność wykreślenia projektowanego art. 2 pkt 3b, a także projektowanego art. 4 pkt 2a i 5a ustawy o krajowym systemie cyberbezpieczeństwa. | **Uwaga nieuwzględniona.**  Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowych.  EKŁE stanowi w art. 40 ust. 2, że przedsiębiorcy komunikacji elektronicznej mają zgłaszać incydenty do właściwych organów, które są inne niż krajowe organy regulacyjne.  Usługi świadczone przez przedsiębiorców komunikacji elektronicznej mają kluczowe znaczenie dla niezakłóconego świadczenia usług przez operatorów usług kluczowych, dostawców usług cyfrowych czy też przez administrację publiczną czyli innych podmiotów krajowego systemu cyberbezpieczeństwa.  Stąd też do ustawy o krajowym systemie cyberbezpieczeństwa zostały dodane obowiązki przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci i usług oraz zgłaszania incydentów. Pozostałe obowiązki przedsiębiorców pozostały w PKE.  Celem ostrzeżenia i polecenia zabezpieczającego jest umożliwienie skutecznej reakcji na zagrożenie wystąpienia incydentu krytycznego (ostrzeżenie) lub na sam incydent krytyczny (polecenie zabezpieczające). Incydent krytyczny może dotyczyć wszystkich podmiotów krajowego systemu cyberbezpieczeństwa. Skutki incydentu krytycznego mogą mieć zasięg międzysektorowy.  Art. 1 ust. 2 pkt 2 został doprecyzowany – do dostawców usług zaufania będą się stosować wyłącznie art. 67a-67c, które dotyczą ostrzeżenia i polecenia zabezpieczającego oraz art.73-74 dotyczące kar pieniężnych. |
| **Ministerstwo Obrony Narodowej** | Art. 1 ust 1 pkt 4  (art. 1 pkt 1 lit. 2 projektu) | Proponuje się nadanie następującego brzmienia art. 1 ust. 1 pkt 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (dalej: *ustawa o ksc*)**:**  *„4) zadania i obowiązki przedsiębiorców komunikacji elektronicznej, o których mowa w ustawie z dnia ... – Prawo komunikacji elektronicznej (Dz. U. ...), w zakresie wymogów dotyczących cyberbezpieczeństwa i zgłaszania incydentów;”.*  Zmiana określenia „bezpieczeństwa” na „cyberbezpieczeństwa”, pozwoli na doprecyzowanie zakresu przedmiotowego *ustawy o ksc*. Precyzyjne wskazanie zakresu wymogów jakim przedsiębiorcy komunikacji elektronicznej będą podlegali wykonując swoje zadania i obowiązki może mieć ogromne znaczenie dla ich realizacji. Odwołując się do określenia „cyberbezpieczeństwo”, które zostało zdefiniowane w *ustawie o ksc* jasno określa się jakiego obszaru mają dotyczyć wskazane w przepisie wymogi. | **Uwaga nieuwzględniona**  Ustawa wdraża przepisy art. 40 i 41 EKŁE, które dotyczą bezpieczeństwa sieci i usług. |
| **Ministerstwo Sprawiedliwości** | Art. 1 ust. 2 | W myśl art. 1 pkt 1 lit. b projektu w ustawie o krajowym systemie cyberbezpieczeństwa w art. 1 ust. 2 uchyla się pkt 1 i 2, zgodnie z którymi nie stosuje się do przedsiębiorców telekomunikacyjnych, o których mowa w ustawie – Prawo telekomunikacyjne, w zakresie wymogów dotyczących bezpieczeństwa i zgłaszania incydentów, a także do dostawców usług zaufania, którzy podlegają wymogom art. 19 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE. W związku z zastrzeżeniami sformułowanymi w pkt 1, przepisy art. 1 ust. 2 pkt 1 i 2 ustawy o krajowym systemie cyberbezpieczeństwa, przewidujące wyłączenie z zakresu podmiotowego ustawy operatorów telekomunikacyjnych oraz dostawców usług zaufania – powinny zostać zachowane. | **Uwaga nieuwzględniona.**  Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowych.  EKŁE stanowi w art. 40 ust. 2, że przedsiębiorcy komunikacji elektronicznej mają zgłaszać incydenty do właściwych organów, które są inne niż krajowe organy regulacyjne.  Usługi świadczone przez przedsiębiorców komunikacji elektronicznej mają kluczowe znaczenie dla niezakłóconego świadczenia usług przez operatorów usług kluczowych, dostawców usług cyfrowych czy też administrację publiczną czyli innych podmiotów krajowego systemu cyberbezpieczeństwa.  Prace legislacyjne związane z wprowadzeniem przepisów prawnych dot. obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci i usług oraz zgłaszania incydentów zostały przeniesione do przepisów wprowadzających Prawo Komunikacji Elektronicznej..  Celem ostrzeżenia i polecenia zabezpieczającego jest umożliwienie skutecznej reakcji na zagrożenie wystąpienia incydentu krytycznego (ostrzeżenie) lub na sam incydent krytyczny (polecenie zabezpieczające). Incydent krytyczny może dotyczyć wszystkich podmiotów krajowego systemu cyberbezpieczeństwa. Skutki incydentu krytycznego mogą mieć zasięg międzysektorowy.  Art. 1 ust. 2 pkt 2 został doprecyzowany – do dostawców usług zaufania będą się stosować wyłącznie art. 67a-67c, które dotyczą ostrzeżenia i polecenia zabezpieczającego oraz art.73-74 dotyczące kar pieniężnych . |
| **Ministerstwo Klimatu i Środowiska** | Art. 2 pkt 3d | **Proponowane brzmienie w art. 2 pkt 3d:**  „3d) SOC – Operacyjne Centrum Cyberbezpieczeństwa świadczące usługi na rzecz operatora usługi kluczowej lub innego podmiotu krajowego systemu cyberbezpieczeństwa;”  **Uzasadnienie:**  Definicja SOC nie zawiera elementów rozwijających ten skrót w języku polskim, a jedynie wskazuje na rodzaj zadań jakie wykonuje i jego funkcjonalność. Definicja powinna być skonstruowana w sposób analogiczny do tych zawartych w art. 2 pkt 1-3, oraz art. 2 pkt 3b-3c UKSC, gdzie oprócz określenia katalogu zadań lub rodzaju funkcji pełnionej w organizacji, zostały wskazane także rozwinięcia nazw w języku polskim. Brak jest w definicji odniesienia do możliwości oddelegowania części zadań do podmiotów zewnętrznych. Art. 2 pkt 3d – zawiera definicję SOC jako zespół pełniący funkcję operacyjnego centrum bezpieczeństwa w danym podmiocie. Pojęcie „bezpieczeństwa” jest bardzo szerokie i np. w różnych podmiotach można wskazać wiele obszarów działania składających się na „bezpieczeństwo”, w tym niezwiązanych z cyberbezpieczeństwem. W powszechnym rozumieniu SOC, jak również spotykanych w organizacjach posiadających SOC lub świadczących SOC, oznacza co do zasady tylko część zadań stricte operacyjnych związanych z Monitorowaniem i wykrywaniem incydentów, i ew. reagowaniem na incydenty. W dużej mierze SOC jest częścią większej, złożonej struktury, uwzględniającej również zadania CERT’owe. Powszechnie przyjmuje się, że takie połączenie posiadają zespoły CSIRT (Computer Security Incident Response Team) które ma swoje odzwierciedlenie w ustawie na poziomie krajowym i sektorowy oraz jest opisane w powszechnych standardach funkcjonujących w obszarze cybersecurity. | **Uwaga nieuwzględniona**  Definicja SOC odnosi się do wieloletniej praktyki rynkowej, a skrót jest powszechnie rozpoznawalny.  Wskazane w uwadze zakres działania SOC to nie tylko kwestie operacyjne czyli wykrywanie i reagowanie na incydenty lecz także zarządzanie jakością zabezpieczeń systemów, informacji powierzonych aktywów oraz aktualizowanie ryzyk, które mogą wpłynąć na reakcję na incydent.  SOC zarządza kwestiami bezpieczeństwa w tym bezpieczeństwa osobowego, eksploatacji i architektury systemów na podstawie wyników przeprowadzonego szacowania ryzyka przez operatora usługi kluczowej. |
| **Ministerstwo Sprawiedliwości** | Art. 2 pkt 8a | Projektowany art. 2 pkt 8a ustawy o krajowym systemie cyberbezpieczeństwa, wprowadza do ustawy definicję pojęcia incydent telekomunikacyjny rozumiany jako incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi komunikacji elektronicznej. Należy zauważyć, że wprowadzenie kolejnego rodzaju incydentu (incydentu telekomunikacyjnego) może doprowadzić do problemów z klasyfikacją incydentów, przy czym warto zaznaczyć, że nie wyodrębniono w projekcie specjalnych kategorii incydentów dla innych sektorów | **Uwaga nieuwzględniona**  Ustawa o krajowym systemie cyberbezpieczeństwa zawiera definicję incydentu poważnego, który dotyczy wyłącznie operatorów usług kluczowych. Operator zgłasza taki incydent w oparciu o określone w rozporządzeniu progi incydentu poważnego. Ponadto dostawcy usług cyfrowych zgłaszają incydenty istotne w oparciu o progi określone na poziomie europejskim.  Natomiast incydenty telekomunikacyjne będą zgłaszane przez przedsiębiorców komunikacji elektronicznej jeżeli incydent powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi komunikacji elektronicznej. Progi incydentów telekomunikacyjnych określi minister właściwy ds. informatyzacji. |
| **Ministerstwo Obrony Narodowej** | Art. 2 pkt 8f | **Art. 1 pkt 2 lit. b *projektu*** – dotyczący propozycji brzmienia art. 2 pkt 8f *ustawy o ksc* **–** ze względu na fakt, że pojęcie „bezpieczeństwo sieci i usług” zostało zdefiniowane w art. 2 pkt 4 *projektu ustawy* - *Prawo komunikacji elektronicznej* i jest ono tożsame z definicją zawartą w *projekcie* proponuje się rozważenie odwołania się do definicji zawartej w *ustawie* - *Prawo komunikacji elektronicznej.* | **Uwaga nieuwzględniona**  Definicja bezpieczeństwa sieci i usług z Prawa komunikacji elektronicznej zostanie przeniesiona do ustawy o krajowym systemie cyberbezpieczeństwa. |
| **Ministerstwo Sprawiedliwości** | Art. 2 pkt 8g | Projektowany art. 2 pkt 8g ustawy o krajowym systemie cyberbezpieczeństwa, wprowadza do ustawy definicję pojęcia sytuacji szczególnego zagrożenia rozumianą jako sytuacja, o której mowa w art. 2 pkt 65 ustawy z dnia … – Prawo komunikacji elektronicznej. Przepis ten jest zbędny, gdyż jest jednym z tych przepisów, które powinny znaleźć się jedynie w ustawie – Prawo komunikacji elektronicznej, jako definiujące obowiązki przedsiębiorców telekomunikacyjnych. | **Uwaga nieuwzględniona**  Prace legislacyjne związane z wprowadzeniem przepisów prawnych dot. obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci i usług oraz zgłaszania incydentów zostały przeniesione do przepisów wprowadzających Prawo Komunikacji Elektronicznej.. |
| **Ministerstwo Klimatu i Środowiska** | Art. 4a ust. 1 | ISAC powinien obejmować swoim zakresem sektor lub podsektor. Funkcjonowanie jednego ISACa dla całego krajowego systemu cyberbezpieczeństwa spowoduje szum informacyjny i jednocześnie wpłynie negatywnie na skuteczną wymianę informacji. Obecny zapis sugeruje, że w ramach krajowego systemu cyberbezpieczeństwa będzie funkcjonował jeden ISAC. Nie należy również zamykać katalogu wymienianych informacji.  **Proponowane brzmienie:**  „Art. 4a 1. W ramach krajowego systemu cyberbezpieczeństwa, w danym sektorze lub podsektorze, może funkcjonować ISAC, do którego zadań należy w szczególności wymiana informacji, dobrych praktyk i doświadczeń dotyczących zagrożeń cyberbezpieczeństwa, podatności oraz incydentów, a także innych informacji mogących mieć wpływ na cyberbezpieczeństwo.” | **Uwaga nieuwzględniona**  W technice legislacyjnej używa się liczby pojedynczej dla określenia podmiotów, które będą spełniać cechy określone w ustawie.  Katalog nie jest zamknięty, ponieważ przepis zawiera słowo „w szczególności”. |
| **Ministerstwo Klimatu i Środowiska** | Art. 8 pkt 5 lit. b | Proponowane brzmienie w art. 8 w pkt 5 lit. b: „b) przeprowadzanie aktualizacji oprogramowania z uwzględnieniem zaleceń producenta, poziomu krytyczności poszczególnych aktualizacji oraz możliwości przeprowadzenia tych aktualizacji w kontekście zachowania stabilności i ciągłości działania. Zaleca się każdorazowo przeprowadzić ocenę ryzyka oraz testy,”  Realizacja wskazanego przepisu wprost będzie trudna w zderzeniu z realiami. Producent z reguły zaleca aktualizację zawsze do najnowszej wersji. W praktyce dla kluczowych systemów często jest świadoma zwłoka administratorów wynikająca ze stosowanego best practices, żeby wersja była sprawdzona w realnych warunkach i ujawniły się potencjalne błędy. Nie eksperymentujemy na środowiskach produkcyjnych, które są kluczowe. Czasem podatności naprawiane przez aktualizację nie występują w danym środowisku lub są mitygowane w inny sposób, wówczas pilność aktualizacji nie jest krytyczna. Część aktualizacji wymusza również zmiany sprzętowe lub konfiguracyjne ze względów architektonicznych, co implikuje konieczność zmian w architekturze działania aplikacji lub urządzeń współpracujących. Generalnie – aktualizacje tak, ale z uwzględnieniem uwarunkowań. | **Uwaga nieuwzględniona**  Prowadzenie regularnych aktualizacji oprogramowania przygotowanych przez producenta danego oprogramowania przy wykorzystaniu zaleceń tegoż producenta jest nieodzownym elementem zarządzania ryzykiem. Brak szybkiej reakcji i aktualizacji oprogramowania zgodnie z zaleceniami jego producenta niesie dużo większe ryzyko, gdyż luka bezpieczeństwa może zostać wykorzystana przez podmioty trzecie w celu nieautoryzowanego dostępu do systemu. |
| **Rządowe Centrum Legislacji** | Art. 14 ust. 1 | W związku z projektowanymi zmianami, przeanalizowania wymagają przepisy wykonawcze wydane na podstawie upoważnień zawartych w art. 10 oraz art. 11 ustawy o KSC, zwłaszcza w kontekście wpływu projektowanych zmian na wytyczne dotyczące treści aktu. Należy wziąć pod uwagę, że zgodnie z projektowanym art. 14 ust. 1 ustawy 4 o KSC obowiązki, o których mowa w art. 10 i 11 tej ustawy będą realizowane w ramach SOC. Projektowana zmiana powoduje, że akty wykonawcze wydane na podstawie tych przepisów mogą zostać objęte dyspozycją § 32 i § 33 ZTP. | **Uwaga nieuwzględniona**  Upoważnienia ustawowe w art. 10 i 11 nie są nowelizowane. Zmiany w art. 14 ust. 1 nie wpływają na treść tych rozporządzeń. |
| **Ministerstwo Klimatu i Środowiska** | Art. 14 ust. 1 | Proponowane brzmienie w art. 14 ust. 1:  „art. 14. 1.Zadania operatora usługi kluczowej, o których mowa w art. 8 pkt 2 lit. e, art. 8 pkt 3-6, art. 9 w zakresie cyberbezpieczeństwa mogą być realizowane w ramach SOC.”  Zgodnie z nowym brzmieniem art. 14 ust. 1 zespół operacyjnego centrum bezpieczeństwa (SOC) ma odpowiadać m.in. za wdrożenie systemu zarządzania bezpieczeństwem oraz wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych (w tym bezpieczeństwo fizyczne i środowiskowe). Obarczanie SOC zadaniami innymi niż operacyjne, tj. odpowiedzialność za wdrożenie SZB odpowiedzialność za wdrożenie środków technicznych lub organizacyjnych zabezpieczających przez ryzykiem zmienia zasadniczo charakter zespołu z operacyjnego. W dużych firmach gdzie odpowiedzialność za obszar szeroko rozumianego bezpieczeństwa (compliance, zarządzanie, raportowanie, operacyjne) jest umiejscowiona strukturalnie w różnych pionach koncentracja w SOC więcej kompetencji niż operacyjne cyberbezpieczeństwo będzie trudne czy wręcz niemożliwe do zrealizowania. Proponuje się utrzymanie zapisów pierwotnego brzmienia ustawy, tj., że to operator usługi kluczowej wdraża system zarządzania bezpieczeństwem w systemie informacyjnym wykorzystywanym do świadczenia usługi kluczowej itp. | **Uwaga nieuwzględniona**  Zespoły SOC są doprecyzowaniem aktualnie funkcjonującym „wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo” oraz zastępuje określenie „podmioty świadczące usługi na rzecz cyberbezpieczeństwa”. SOC będą realizowały zadania, które obecnie są realizowane przez wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo lub podmioty świadczące usługi z zakresu cyberbezpieczeństwa, z którymi dany operator zawrze umowę na świadczenie tego typu usługi. |
| **Ministerstwo Klimatu i Środowiska** | Art. 14 ust. 2-4 | Dodanie w ust. 2 wymagania, by OUK zdefiniował wskaźniki jakościowe usług świadczonych przez SOC (oraz podmiot świadczący usługi) zapewniające ciągłe monitorowanie jakości świadczonych usług.  W art. 14 ust. 2-4 wydaje się zasadne, by ustawa wskazała obowiązek OUK, by ten zdefiniował i monitorował wskaźniki jakościowe oceniające jakość pracy działania SOC (np. w umowie jako tzw. KPIs) pozwalające na ciągłe monitorowanie jakości usług SOC lub podmiotów świadczących usługi w zakresie cyberbezpieczeństwa. Bardzo mało jest w obecnej ustawie wymagań co do relacji OUK – podmiot świadczący usługi w zakresie cyberbezpieczeństwa, a to przecież ten jest często rzeczywistym operatorem cyberbezpieczeństwa u OUK i nadzór nad nim ma kluczowe znaczenie. | **Uwaga nieuwzględniona**  W ramach zasady swobody umów operator usługi kluczowej może wprowadzić takie zapisy do umowy. Operator usługi sam decyduje o wyborze podmiotu prowadzącego SOC i może wybrać taki podmiot, który zgadza się na ciągłe monitorowanie jakości świadczonych usług. Nie ma potrzeby, aby ta kwestia była regulowana na poziomie ustawowym. |
| **Ministerstwo Klimatu i Środowiska** | Art. 14 ust. 3 (dodatkowy) | Proponuje się w art. 14 po ust. 2 dodać dodatkowy ust. 3, a następne przenumerować, w następującym brzmieniu:  „3. Minister właściwy do spraw informatyzacji, po zasięgnięciu opinii szefa Agencji Bezpieczeństwa Wewnętrznego, określi w drodze rozporządzenia warunki organizacyjne i techniczne dla podmiotów świadczących usługi SOC, z uwzględnieniem niezbędnych certyfikatów dających rękojmię ich bezpiecznego funkcjonowania w celu zapewnienia autentyczności, integralności, dostępności, poufności przetwarzanych informacji.”  Zgodnie z art. 14 ust. 2, OUK może zawrzeć z innym podmiotem umowę na mocy której podmiot ten będzie realizował zadania i świadczył usługi SOC. Nie zostało jednoznacznie wskazane, czy ten drugi podmiot musi być OUK. Jeżeli nie musi, to możliwość zawarcia umowy z podmiotem zewnętrznym świadczącym usługi SOC, bez wskazania minimalnych warunków organizacyjnych, technicznych oraz certyfikatów jakie podmiot ten musi spełniać i posiadać, wiąże się z bardzo dużym ryzykiem. Istnieje wtedy możliwość funkcjonowania takiego podmiotu, który bez doświadczenia i odpowiednich certyfikatów będzie miał dostęp do krytycznych informacji. Można rozważyć wprowadzenie wymogu dla podmiotów prowadzących SOC, z którymi OUK będą podpisywać umowy w zakresie świadczenia takiej usługi, dotyczącego posiadania „dokumentu potwierdzającego zdolność do ochrony informacji niejawnych”, innymi słowy będzie posiadać Świadectwo Bezpieczeństwa Przemysłowego, analogicznie jak SOC opisany w proponowanym art. 14a ust. 7 pkt 2. Usługa SOC jest również usługą krytyczną i podmiot niezaufany, niezweryfikowany pod kątem zdolności zapewnienia ochrony informacji niejawnych może stanowić istotne zagrożenie dla bezpieczeństwa świadczenia usługi kluczowej danego OUK i jego know-how. Powyższe ma szczególne znaczenie w przypadku gdy OUK jest jednocześnie operatorem Infrastruktury Krytycznej. Zmiana taka powinna w tym zakresie zostać objęta stosownym vacatio legis dla przeprowadzenia stosownej procedury Postępowania Bezpieczeństwa Przemysłowego. | **Uwaga nieuwzględniona**  Art. 14 ust. 3 wskazuje wprost, że SOC wprowadza zabezpieczenia zapewniające poufności, integralność, dostępność i autentyczność przetwarzanych informacji. Zabezpieczenia te wynikają z przeprowadzonego szacowania ryzyka. Przyjęte założenie jest oparte o koncepcję *risk based approach*. |
| **Ministerstwo Klimatu i Środowiska** | Art. 14 ust. 3 | Po akceptacji proponowanej wyżej zmiany będzie to art. 14 ust. 4  Proponowane brzmienie w art. 14 ust. 3:  „3. Operator usługi kluczowej, na podstawie przeprowadzonego szacowania ryzyka, wprowadza zabezpieczenia zapewniające poufność, integralność, dostępność i autentyczność przetwarzanych informacji, z uwzględnieniem bezpieczeństwa osobowego, eksploatacji i architektury systemów, w celu:”  W Art. 14 ust. 3 wydaje się zasadne doprecyzowanie co kryje się za obowiązkiem wprowadzenia, przede wszystkim gdzie SOC ma te zabezpieczenia wprowadzać, czy w ramach swojej struktury czy działań u OUK, tym bardziej że decyzje takie na poziomie podmiotów prawa handlowego mogą się wiązać podejmowaniem decyzji co do których sam SOC nie będzie miał stosowanych upoważnień. Ponadto, pojawia się tu też kwestia odpowiedzialności i tego, że to na operatorze usługi kluczowej spoczywa odpowiedzialność za właściwą realizację zapisów ustawy. | **Uwaga nieuwzględniona**  W dalszym ciągu to wyłącznie na operatorze usługi kluczowej spoczywa obowiązek realizacji przepisów prawa wynikających z ustawy o ksc. |
| **Ministerstwo Finansów, Funduszy i Polityki Regionalnej** | Art. 14a | Uregulować tryb i zasady oraz sposób występowania przez uprawnione organy z wnioskiem o dostęp do danych z wykazu SOC (zespołów pełniących funkcję operacyjnego centrum bezpieczeństwa w danym operatorze usługi kluczowej), a także ich udostępniania przez ministra właściwego ds. informatyzacji lub wprowadzić delegację do wydania aktu wykonawczego w tym zakresie. | **Uwaga nieuwzględniona**  Nie jest to konieczne, dotychczasowe praktyki udostępniania danych z wykazu operatorów usług kluczowych, które są wzorcem dla tego przepisu, sprawdzają się doskonale. |
| **Koordynator Służb Specjalnych** | Art. 14a ust. 9 | W projektowanym art. 14a ust. 9 ustawy *o krajowym systemie cyberbezpieczeństwa* wskazano, iż dane z wykazu SOC udostępnia się m.in. CSIRT GOV. Natomiast w ust. 10 pkt 5 przewidziano, iż ww. dane udostępnia się m. in. Agencji Bezpieczeństwa Wewnętrznego. Wskazać należy, iż przepis ten jest zbyt ogólny w zakresie, w jakim odnosi się on do sposobu udostępnienia danych, bowiem wskazano jedynie, iż odbywa się to „na wniosek” właściwej służby. Należałoby, zatem wprowadzić w przedmiotowym przepisie rozwiązania występujące w innych ustawach, np. w ustawie - *Prawo o ruchu drogowym*, gdzie w art. 80c uregulowano, iż dane zgromadzone w ewidencji udostępnienia się m.in. Agencji Bezpieczeństwa Wewnętrznego, natomiast w ust. 6 tego przepisu wskazano, że minister właściwy do spraw informatyzacji może wyrazić zgodę, w drodze decyzji, na udostępnienie danych zgromadzonych w ewidencji podmiotom, o których mowa w ust. 1, z uwzględnieniem ust. 6a, albo ich jednostkom organizacyjnym, za pomocą urządzeń teletransmisji danych, bez konieczności składania pisemnego wniosku, jeżeli spełniają łącznie następujące warunki:   1. posiadają urządzenia umożliwiające odnotowanie w systemie, kto, kiedy, w jakim celu oraz jakie dane uzyskał; 2. posiadają zabezpieczenia techniczne i organizacyjne uniemożliwiające wykorzystanie danych niezgodnie z celem ich uzyskania; 3. jest to uzasadnione specyfiką lub zakresem wykonywanych zadań albo prowadzonej działalności.   Ponadto, uwaga powyższa odnosi się także do projektowanego art. 20b ustawy *o krajowym systemie cyberbezpieczeństwa*, w myśl którego przedsiębiorca komunikacji elektronicznej „zapewnia dostęp” do informacji o rejestrowanych incydentach właściwemu CSIRT MON, CSIRT NASK lub CSIRT GOV w zakresie niezbędnym do realizacji jego zadań - nie określając w jaki sposób ma się odbywać ten dostęp. | **Uwaga nieuwzględniona**  Zespoły CSIRT poziomu krajowego w tym CSIRT GOV dysponują stałym dostępem do wykazu operatorów usług kluczowych. Nie stanowi przeszkód, aby wykaz SOC także był udostępniany w podobny sposób zespołom CSIRT poziomu krajowego. Natomiast Szef ABW podobnie jak Policja czy też Prokuratura czy sądy może zwrócić się do ministra właściwego ds. informatyzacji o dostęp do wykazu SOC w zakresie niezbędnym do realizacji jego ustawowych zadań. |
| **Ministerstwo Klimatu i Środowiska** | Art. 14a ust. 9 | Proponowane brzmienie w art. 14a ust. 9:  „9. Dane z wykazu SOC minister właściwy do spraw informatyzacji udostępnia organom właściwym ds. cyberbezpieczeństwa, CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT sektorowemu w zakresie sektora lub podsektora, dla którego został ustanowiony, a także operatorom usług kluczowych w zakresie ich dotyczącym.” Proponuje się uzupełnić ten artykuł albo dodać kolejny opisujący sposób udostępnienia danych z wykazu SOC podmiotom wskazanym w ust. 9. W proponowanym art. 14a ust. 9 znajduje się zapis mówiący o tym, że minister ds. informatyzacji udostępnia organowi właściwemu ds. cyberbezpieczeństwa dane z wykazu SOC. Po pierwsze, dlaczego zapis dot. organu właściwego jest w liczbie pojedynczej, a nie mnogiej skoro jest kilka organów właściwych. Ten sam sposób zapisu został użyty w przypadku OUK. Po drugie, nie ma wskazanej żadnej procedury udostępnienia wykazu. | **Uwaga nieuwzględniona**  Użycie liczby mnogiej oznaczałoby, że informacji można udzielić co najmniej dwóm lub więcej organom właściwym, a nie wolno jednemu organowi.  W art. 14a ust. 10 jest opisana procedura udzielenia informacji z wykazu. Jest to procedura identyczna z tą opisaną w art. 7 ust. 8 w kwestii dotyczącej udostępnienia informacji dotyczącej wykazu usług kluczowych. |
| **Ministerstwo Sprawiedliwości** | Art. 20a | Wątpliwości budzi dodanie do projektu rozdziału 4a dotyczącego obowiązków przedsiębiorców komunikacji elektronicznej. Jak była mowa w pkt 1 przedstawianych uwag do projektu, takie przepisy powinny się znaleźć w ustawie – Prawo komunikacji elektronicznej, w szczególności, że częściowo pokrywają się z projektowanymi regulacjami ustawy o krajowym systemie cyberbezpieczeństwa (por. art. 20a opiniowanego projektu z art. 39 projektu ustawy – Prawo komunikacji elektronicznej, art. 20e z art. 42 ust. 2 i 3 projektu ustawy – Prawo komunikacji elektronicznej, zaś art. 20f – z art. 44 ust. 1 projektu ustawy – Prawo komunikacji elektronicznej). Z kolei w projektowanym art. 20a ust. 4 ustawy o krajowym systemie cyberbezpieczeństwa znajduje się delegacja dla ministra właściwego do spraw informatyzacji identyczna jak delegacja z art. 39 projektu ustawy – Prawo komunikacji elektronicznej. Analogiczna sytuacja ma miejsce w przypadku art. 20c ust. 4 omawianego projektu i art. 42 ust. 2 projektu ustawy – Prawo komunikacji elektronicznej. Zatem ww. projektowane przepisy ustawy o krajowym systemie cyberbezpieczeństwa są zbędne. | **Uwaga nieuwzględniona.**  Kwestie dotyczące bezpieczeństwa sieci i usług oraz zgłaszania incydentów przez przedsiębiorców komunikacji elektronicznej znajdą się w ustawie o krajowym systemie cyberbezpieczeństwa.  Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowych.  EKŁE stanowi w art. 40 ust. 2, że przedsiębiorcy komunikacji elektronicznej mają zgłaszać incydenty do właściwych organów, które są inne niż krajowe organy regulacyjne.  Usługi świadczone przez przedsiębiorców komunikacji elektronicznej mają kluczowe znaczenie dla niezakłóconego świadczenia usług przez operatorów usług kluczowych, dostawców usług cyfrowych czy też administrację publiczną czyli innych podmiotów krajowego systemu cyberbezpieczeństwa.  Stąd też do ustawy o krajowym systemie cyberbezpieczeństwa zostały dodane obowiązki przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci i usług oraz zgłaszania incydentów. Pozostałe obowiązki przedsiębiorców pozostały w PKE. |
| **Ministerstwo Obrony Narodowej** | Art. 20a | **Art. 1 pkt 12 *projektu* -** w projektowanym rozdziale 4a *Obowiązki przedsiębiorców komunikacji elektronicznej* proponuje się następujące brzmienie art. 20a *ustawy o ksc:*  *„Art. 20a. Przedsiębiorca komunikacji elektronicznej, w celu zapewnienia cyberbezpieczeństwa jest zobowiązany do realizacji zadań i obowiązków określonych w art. 39 ust. 1-4 ustawy z dnia ... - Prawo komunikacji elektronicznej.”.*  Treści zawarte w projektowanym art. 20a *ustawy o ksc*, są tożsame z treściami zawartymi w art. 39 *projektu* *ustawy - Prawo komunikacji elektronicznej.* W związku z powyższym, w celu uniknięcia powtarzania przepisów zamieszczonych w obu projektach ustawy, a tym samym powstania dwóch identycznych delegacji ustawowych do wydania rozporządzenia ministra właściwego do spraw informatyzacji (zawartych odpowiednio w projektowanym art. 20a ust. 4 oraz art. 39 ust. 4 - *projektu ustawy Prawo komunikacji elektronicznej*) proponuje się rozważyć wprowadzenie odesłania | **Uwaga nieuwzględniona.**  Kwestie dotyczące bezpieczeństwa sieci i usług oraz zgłaszania incydentów przez przedsiębiorców komunikacji elektronicznej znajdą się w ustawie o krajowym systemie cyberbezpieczeństwa.  Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowych.  EKŁE stanowi w art. 40 ust. 2, że przedsiębiorcy komunikacji elektronicznej mają zgłaszać incydenty do właściwych organów, które są inne niż krajowe organy regulacyjne.  Usługi świadczone przez przedsiębiorców komunikacji elektronicznej mają kluczowe znaczenie dla niezakłóconego świadczenia usług przez operatorów usług kluczowych, dostawców usług cyfrowych czy też administrację publiczną czyli innych podmiotów krajowego systemu cyberbezpieczeństwa.  Stąd też do ustawy o krajowym systemie cyberbezpieczeństwa zostały dodane obowiązki przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci i usług oraz zgłaszania incydentów. Pozostałe obowiązki przedsiębiorców pozostały w PKE. |
| **Ministerstwo Rozwoju, Pracy i Technologii** | Art. 20f | Przyznając przedsiębiorcom telekomunikacyjnym nowe uprawnienia pozwalające na blokowanie komunikatów oraz ograniczenie albo przerwanie świadczenia usług telekomunikacyjnych, należy uwzględnić uzasadniony interes osób trzecich. Warto przede wszystkim zobligować przedsiębiorców telekomunikacyjnych do każdorazowego informowania nadawców komunikatu lub użytkowników usług o zastosowanej blokadzie oraz o podstawie prawnej, np. poprzez przekierowanie na stronę zawierającą stosowne informacje w tym zakresie. Taki komunikat zwrotny mógłby również wskazywać na prawo do zakwestionowania zastosowanego środka, np. w drodze swoistej skargi/reklamacji kierowanej do rozpatrzenia przez przedsiębiorcę komunikacyjnego (alternatywnie: bezpośrednio do regulatora). Ostateczną kontrolę nad ograniczaniem dostępu do informacji powinien sprawować sąd, czego projekt w obecnym kształcie nie przewiduje. | **Uwaga nieuwzględniona**  Podobny przepis funkcjonuje obecnie, jako art. 180 Prawa telekomunikacyjnego. Takie działanie możliwe jest w przypadku stwierdzenia zagrożenia dla bezpieczeństwa sieci i usług oraz tylko w zakresie niezbędnym dla zapobiegnięcia zagrożeniu i nie dłużej niż do czasu ustania przyczyny zagrożenia. Zastosowanie powyższego środka nie wyklucza zagwarantowania otwartego dostępu do Internetu. |
| **Rządowe Centrum Legislacji** | Rozdział 4a | W odniesieniu do dodawanego rozdziału 4a w ustawie o KSC określającego obowiązki przedsiębiorców komunikacji elektronicznej, należy wskazać, że ich deklarowane przez Projektodawcę przeniesienie do projektu ustawy – Prawo komunikacji elektronicznej, zasadne z uwagi na brzmienie § 2 ZTP i zakres przedmiotowy tego rozdziału, będzie wymagało ponownej analizy i oceny spójności tych regulacji na poziomie pojęciowymi konstrukcyjnym zarówno z projektowaną ustawą, jak i projektowaną ustawą – Prawo komunikacji elektronicznej. | **Uwaga nieuwzględniona.**  Prace legislacyjne związane z wprowadzeniem przepisów prawnych dot. obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci i usług oraz zgłaszania incydentów zostały przeniesione do przepisów wprowadzających Prawo Komunikacji Elektronicznej. Przepisy zostały poddane dodatkowej analizie pod kątem spójności z oboma aktami prawnymi. |
| **Koordynator Służb Specjalnych** | Art. 34a | Z projektowanych przepisów wynika, że przedsiębiorca komunikacji elektronicznej zgłasza incydenty do właściwego CSIRT-u poziomu krajowego oraz jednocześnie do CSIRT Telco. Ma tu miejsce analogiczna sytuacja, jak w przypadku wskazanym w uwadze nr II dotyczącej CSIRT-u sektorowego, dlatego też uwaga dotycząca braku określenia CSIRT-u, który w pełni odpowiedzialny jest za koordynację obsługi incydentu, zgłaszanego w tym przypadku przez przedsiębiorcę komunikacji elektronicznej, jest również aktualna w tym zakresie, a problem ten powinien zostać rozwiązany w sposób systemowy.  Ponadto, z przeprowadzonej analizy projektu ustawy wynika, iż na etapie zgłaszania incydentu przedsiębiorca komunikacji elektronicznej nie będzie miał obowiązku informowania Prezesa Urzędu Komunikacji Elektronicznej o wykryciu incydentu. Natomiast projektowany art. 34a ustawy *o krajowym systemie cyberbezpieczeństwa* stanowi, że podczas trwania incydentu telekomunikacyjnego CSIRT-y poziomu krajowego współpracują z Prezesem Urzędu Komunikacji Elektronicznej, z czego *de facto* wynika, iż podmiotem informującym Prezesa Urzędu Komunikacji Elektronicznej o incydencie danego typu będzie CSIRT, a nie podmiot, u którego incydent wystąpił. W związku z powyższym proponuję, aby do katalogu podmiotów informowanych podczas dokonywania zgłoszenia przez przedsiębiorcę komunikacji elektronicznej został dodany Prezes Urzędu Komunikacji Elektronicznej. | **Uwaga nieuwzględniona**  Incydenty zgłaszane przez przedsiębiorców komunikacji elektronicznej będą zgłaszane do CSIRTu Telco, który zapewni bezpośrednie wsparcie w reagowaniu na incydent telekomunikacyjny oraz równocześnie do właściwego CSIRT poziomu krajowego, który zapewni koordynację obsługi tego incydentu. Należy podkreślić, że CSIRT poziomu krajowego dysponuje najpełniejszą wiedzą o poziomie ryzyka w skali kraju, stąd też jest w stanie ocenić, czy dany incydent telekomunikacyjny jest jednocześnie incydentem krytycznym.  Prezes UKE nie ma kompetencji operacyjnych. CSIRT Telco oraz CSIRT poziomu krajowego będą przekazywać informacje Prezesowi UKE o incydentach telekomunikacyjnych, w celu wypełnienia obowiązku informowania organów innych państw o istotnych incydentach oraz obowiązku sprawozdawczego wobec m.in. ENISA |
| **Koordynator Służb Specjalnych** | Art. 34a ust. 3 | Kolejną kwestią, która budzi wątpliwość jest brzmienie projektowanego art. 34a ust. 3 ustawy *o krajowym systemie cyberbezpieczeństwa*, który nakłada na CSIRT-y poziomu krajowego oraz CSIRT Telco obowiązek przekazywania raz na pół roku sprawozdania dotyczącego liczby i rodzajów incydentów telekomunikacyjnych. W tej kwestii proponuję, aby obowiązek przygotowywania sprawozdań dotyczących liczby i rodzajów incydentów telekomunikacyjnych został nałożony na przedsiębiorców komunikacji elektronicznej, a nie CSIRT-y poziomu krajowego. Ponadto, w projektowanych regulacjach należy wskazać komu mają być przekazywane dane ze sprawozdania. Proponuje się zatem, aby ich odbiorcą był Prezes Urzędu Komunikacji Elektronicznej i minister właściwy do spraw informatyzacji, którzy zebrane dane powinni publikować na stronach podmiotowych Biuletynu Informacji Publicznej.  Dodatkowo zasadne wydaje się ujednolicenie częstotliwości przygotowywania sprawozdań, o których mowa w projektowanym art. 34a ust. 3 ustawy *o krajowym systemie cyberbezpieczeństwa*, poprzez określenie okresów sprawozdawczych w sposób analogiczny jak w obecnie obowiązujących art. 45 i 63 ustawy *o krajowym systemie cyberbezpieczeństwa* tj. raz do roku.  Warto również w tym miejscu nadmienić, iż projektowane regulacje, w zakresie dotyczącym przedsiębiorców komunikacji elektronicznej, powinny zostać skorelowane z regulacjami zawartymi w projekcie ustawy - *Prawo komunikacji elektronicznej*. Wskazać należy, iż projekt ustawy - *Prawo komunikacji elektronicznej* w wersji skierowanej do uzgodnień międzyresortowych również uwzględnia kwestie zgłaszania incydentów przez analogiczny krąg podmiotów, ale za pośrednictwem Prezesa Urzędu Komunikacji Elektronicznej. W związku powyższym koniecznym jest ujednolicenie obu projektów celem wprowadzania spójnych rozwiązań dotyczących tych samych podmiotów. | **Uwaga nieuwzględniona**  Prace legislacyjne związane z wprowadzeniem przepisów prawnych dot. obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci i usług oraz zgłaszania incydentów zostały przeniesione do przepisów wprowadzających Prawo Komunikacji Elektronicznej. |
| **Ministerstwo Klimatu i Środowiska** | Art. 44 ust. 1 | Proponowane brzmienia w art. 44 ust. 1:  „1. Organ właściwy do spraw cyberbezpieczeństwa zapewnia funkcjonowanie CSIRT sektorowego dla operatorów usług kluczowych w danym podsektorze, wymienionym w załączniku nr 1 do ustawy lub dla kilku podsektorów łącznie w ramach jednego sektora, do którego zadań należy m.in.:”  W art. 44 ust. 1 został zawarty zamknięty katalog zadań CSIRT sektorowego. Proponuje się rozszerzyć tę kwestię w celu pełniejszej realizacji zadań przez CSIRT sektorowy. CSIRT sektorowy, aby mógł spełniać pokładane w nim założenia powinien obejmować swoim działaniem odpowiednio zawężony obszar (podsektora wymienionego w załączniku nr 1 do ustawy lub kilku łącznie). Dla przykładu: obszar sektora Energii jest zbyt szeroki, gdyż obejmuje zarówno obszar wydobywania kopalin jak i produkcji energii oraz produkcji paliw ciekłych i gazowych, a przedsiębiorstwa działające w różnych podsektorach mają inną specyfikę działalności, używają różnego parku maszynowego, odmiennych technologii i mają w związku z tym inne problemy, zagrożenia i wynikające z tego odmienne oczekiwania względem CSIRT. | **Uwaga nieuwzględniona**  Jeżeli organ właściwy uzna, że potrzebne jest stworzenie kilku zespołów CSIRT sektorowych właściwych dla danych podsektorów w nadzorowanym sektorze gospodarki, to może je utworzyć w ramach dostępnych w regule wydatkowej środków finansowych. Ponadto organ właściwy musi wówczas określić szczegółowe warunki współpracy CSIRT sektorowych właściwych dla danego podsektora.  Natomiast kwestią zasadniczą jest przeanalizowanie wariantu kilku równorzędnych sobie zespołów CSIRT sektorowych (podsektorowych) funkcjonujących w ramach jednego sektora kluczowego. Analizy takie powinny wykazać, że wariant taki jest zasadny pod względem efektywności wybranego rozwiązania. Ponadto należy przeanalizować koszty funkcjonowania tak rozbudowanego systemu kilku sektorowych (podsektorowych) CSIRT w ramach jednego sektora. |
| **Ministerstwo Klimatu i Środowiska** | Art. 44 ust. 5-6 | Proponowane brzmienia w art. 44 ust. 5 - 6:  „5. Organ właściwy do spraw cyberbezpieczeństwa może powierzyć realizację całości lub części zadań CSIRT sektorowego:  - jednostkom podległym,  - jednostkom nadzorowanym lub  - podmiotom, o którym mowa w art. 4 ustawy z  dnia 11 września 2019 r. - Prawo zamówień publicznych (Dz. U. poz. 2019).  6. Przy wyborze odpowiedniego podmiotu, o który mowa w ust. 5, organ właściwy zasięga opinii Pełnomocnika oraz bierze pod uwagę m.in.:   1. posiadane przez ten podmiot przygotowanie techniczne i przeszkolony personel, a także doświadczenie w zakresie reagowania na incydenty, analizowania incydentów poważnych, wyszukiwania powiązań pomiędzy incydentami oraz opracowywania wniosków z obsługi incydentu, 2. udział i współpracę z innymi organizacjami mającymi na celu wymianę wiedzy i doświadczenia w zakresie cyberbezpieczeństwa, 3. konieczność współpracy tego podmiotu z właściwym CSIRT MON, CSIRT NASK i CSIRT GOV; 4. poziom cyberbezpieczeństwa i liczbę podmiotów w danym sektorze lub podsektorze oraz incydenty, które w nim wystąpiły.”   Wprowadzenie dwustopniowego wyboru podmiotu powierzenia funkcji CSIRT jest niezasadne (art. 44 ust. 5 i ust. 6). Organ właściwy przy wyborze podmiotu powinien kierować się przede wszystkim kwestiami obiektywnymi bezpośrednio związanymi z kwestiami cyberbezpieczeństwa takimi jak zaplecze techniczne i organizacyjne, posiadany przeszkolony i kompetentny personel oraz odpowiednie doświadczenie. Innymi słowy kluczowym powinno być to by CSIRT sektorowy prowadzony był przez podmiot przygotowany do tego od strony technicznej i organizacyjnej, a nie jakie powiązania posiada z organem nadzoru. Mając na uwadze powyższe organ nadzoru powinien mieć możliwość powołania CSIRT sektorowego i wyboru odpowiedniego podmiotu już w pierwszym kroku po odpowiedniej ocenie merytorycznej przygotowania takiego podmiotu i wzięciu pod uwagę konkretnych kryteriów oraz opinii Pełnomocnika. Proponowana zmiana wpłynie korzystnie na realny poziom bezpieczeństwa oraz wykonywane funkcje przez CSIRTy sektorowe. Zasadnym jest zatem włączenie podmiotów o których mowa w art. 4 ustawy Prawo Zamówień Publicznych do projektu ustawy oraz określić odpowiednie kryteria wyboru. | **Uwaga nieuwzględniona**  CSIRT sektorowy składa się z immanentnych zadań SOCowych oraz CERTowych. Nie ma możliwości outsourcowania części zadań CSIRT sektorowego. Najważniejsze jest osiągnięcie pełnej efektywności działań zespołu CSIRT i zintegrowanego działania jego struktur. |
| **Rządowe Centrum Legislacji** | Art. 44a pkt 4 | W zakresie zadań CSIRT Teleco, o których mowa w projektowanym art. 44a pkt 4 ustawy o KSC, konieczne jest ich ponowne przeanalizowanie, gdyż ten zakres pokrywa się częściowo z zakresem zadań ISAC. | **Uwaga nieuwzględniona.** ISAC nie są podmiotami o kompetencjach operacyjnych, zatem nie zajmują się reagowaniem na incydenty. CSIRT Telco jest podmiotem o kompetencjach identycznych do CSIRT sektorowego. Zatem łączy w sobie zarówno kompetencje analityczne (CERT) jak i operacyjne (SOC). Natomiast ISAC jest podmiotem mającym za zadanie wzmocnienie współpracy w zakresie wymiany informacji o podatnościach, zagrożeniach i dobrych praktykach. |
| **Koordynator Służb Specjalnych** | Art. 46 ust. 2 | **Funkcjonowanie systemu tzw. „S46”**  Zgodnie z obowiązującym brzmieniem art. 46 ustawy *o krajowym systemie cyberbezpieczeństwa* minister właściwy ds. informatyzacji zapewnia rozwój lub utrzymanie systemu teleinformatycznego wspierającego:  1) współpracę podmiotów wchodzących w skład krajowego systemu cyberbezpieczeństwa;  2) generowanie i przekazywanie rekomendacji dotyczących działań podnoszących poziom cyberbezpieczeństwa;  3) zgłaszanie i obsługę incydentów;  4) szacowanie ryzyka na poziomie krajowym;  5) ostrzeganie o zagrożeniach cyberbezpieczeństwa.  CSIRT MON, CSIRT NASK, CSIRT GOV, sektorowe zespoły cyberbezpieczeństwa i Prezes Urzędu Komunikacji Elektronicznej mogą korzystać z ww. systemu teleinformatycznego na podstawie porozumienia zawartego z ministrem właściwym do spraw informatyzacji.  Projektowana ustawa przewiduje nowelizację art. 46 ust. 2 ustawy *o krajowym systemie cyberbezpieczeństwa* polegającą na zmianie charakteru korzystania z przedmiotowego systemu. Obecnie obowiązujące przepisy stanowią, iż korzystanie z tego systemu jest fakultatywne, a zakres i warunki korzystania określa się w porozumieniu, zaś projektowane regulacje nakładają na CSIRT-y poziomu krajowego obowiązek korzystania z tego systemu, który ma również być dedykowany do zgłaszania i obsługi incydentów.  Biorąc pod uwagę zarówno obecny wczesny etap prac nad systemem oraz brak dotychczas przeprowadzonych testów, zarówno wydajnościowych jak i funkcjonalnych, czy też dotyczących bezpieczeństwa systemu, proponuje się odstąpienie od obowiązku korzystania z tego systemu. Dotychczasowe regulacje, zakładające przyłączanie podmiotów na podstawie porozumień, pozwolą na weryfikację przygotowanego rozwiązania przez CSIRT-y poziomu krajowego, a także ewentualne płynne przejście na nowy system zweryfikowany pod kątem funkcjonalności.  Należy również wskazać, iż w przypadku podmiotów pozostających we właściwości CSIRT GOV, (rządowa administracja centralna i podmioty znajdujące się w wykazie infrastruktury krytycznej), niezmiernie istotna jest kwestia ograniczenia dostępu do wiedzy o zgłaszanej podatności w tych podmiotach, przynajmniej do momentu neutralizacji zagrożenia. W związku z tym, wprowadzenie obowiązku zgłaszania wszystkich incydentów za pośrednictwem danego systemu możliwe wydaje się dopiero po dokonaniu pełnej weryfikacji funkcjonalności i bezpieczeństwa przedmiotowego systemu, jak również po przyznaniu odpowiednich poziomów dostępu i nadaniu uprawnień dla poszczególnych uczestników systemu. | **Uwaga nieuwzględniona.** System został uruchomiony z podstawową funkcjonalnością od 1 stycznia 2021. Wykorzystuje on efekty zakończonego projektu Narodowej Platformy Cyberbezpieczeństwa. Projekt przewiduje obligatoryjne korzystanie z systemu przez zespoły CSIRT poziomu krajowego, Pełnomocnika, Prezesa UKE, CSIRT sektorowe. Natomiast inne podmioty KSC będą mogły zostać podłączone do S46 po podpisaniu porozumienia z ministrem właściwym do spraw informatyzacji. |
| **Ministerstwo Obrony Narodowej** | Art. 51 pkt 8 | 1. Proponuje się uchylenie art. 51 pkt 8 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (dalej: *ustawa o ksc*) oraz dodanie art. 51a w brzmieniu:   *„Art. 51a. 1.* *W warunkach zewnętrznego zagrożenia bezpieczeństwa państwa i w czasie wojny, Prezes Rady Ministrów, na wniosek Ministra Obrony Narodowej, może podjąć decyzję  o powierzeniu temu ministrowi uprawnień do koordynacji działań podmiotów,* *o których mowa w art. 4, w zakresie cyberbezpieczeństwa. Koordynację tę Minister Obrony Narodowej realizuje we współpracy z ministrem właściwym do spraw wewnętrznych i z ministrem właściwym do spraw informatyzacji.*  *2. Koordynację działań, o której mowa w ust. 1, Minister Obrony Narodowej realizuje za pośrednictwem CSIRT MON.”.*  CSIRT MON nie posiada bezpośrednich uprawnień do kierowania działaniami związanymi  z przygotowaniem do koordynacji i obsługą incydentów przez CSiRT NASK i CSiRT GOV  w czasie bezpośrednio poprzedzającym stan wojenny oraz w stanie wojny (czas wojny). Rola koordynacyjna, przypisana Ministrowi Obrony Narodowej na mocy art. 51 pkt 8 ustawy o ksc, zgodnie z którym: „Minister Obrony Narodowej jest odpowiedzialny za koordynację, we współpracy z ministrem właściwym do spraw wewnętrznych i ministrem właściwym do spraw informatyzacji, realizacji zadań organów administracji rządowej i jednostek samorządu terytorialnego w czasie stanu wojennego dotyczących działań obronnych w przypadku zagrożenia cyberbezpieczeństwa” – nie zabezpiecza w pełni potrzeb w tym zakresie.   1. Mając na uwadze proponowaną w pkt 1 niniejszego pisma zmianę, należy rozważyć dodanie w art. 1 pkt 15 projektu lit. e, f, g, h (zmiana brzmienia art. 26 ust. 5, 6,7 oraz dodanie ust. 5a ustawy o ksc):   *„e) ust. 5 otrzymuje brzmienie:*  *„5. Do zadań CSIRT MON należy:*  *1) koordynacja obsługi incydentów zgłaszanych przez:*  *a) podmioty podległe Ministrowi Obrony Narodowej lub przez niego nadzorowane, w tym podmioty, których systemy teleinformatyczne lub sieci teleinformatyczne objęte są jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym,*  *b) przedsiębiorców o szczególnym znaczeniu gospodarczo-obronnym, w stosunku do których organem organizującym i nadzorującym wykonywanie zadań na rzecz obronności państwa w rozumieniu art. 5 pkt 3 ustawy z dnia 23 sierpnia 2001 r. o organizowaniu zadań na rzecz obronności państwa realizowanych przez przedsiębiorców (Dz. U. z 2020 r. poz. 1669) jest Minister Obrony Narodowej;*  *2) koordynacja, w imieniu Ministra Obrony Narodowej, realizacji zadań CSIRT NASK i CSIRT GOV związanych z obsługą incydentów w warunkach zewnętrznego zagrożenia bezpieczeństwa państwa i w czasie wojny, w tym działań, o których mowa w art. 27 ust. 1.”;*  *f) po ust. 5 dodaje się ust. 5a w brzmieniu:*  *„5a. W warunkach zewnętrznego zagrożenia bezpieczeństwa państwa i w czasie wojny, w celu realizacji zadania, o którym mowa w ust. 5 pkt 2, CSIRT MON:*  *1) kieruje działaniami CSIRT NASK i CSIRT GOV;*  *2) współpracuje i wymienia informacje z podległą Ministrowi Obrony Narodowej jednostką organizacyjną właściwą w sprawach bezpieczeństwa cyberprzestrzeni.”*  *g) w ust. 6 w pkt 3 kropkę zastępuje się średnikiem i dodaje pkt 4 i 5 w brzmieniu:*  *„4) realizacja, kierowanych przez CSIRT MON, zadań związanych z obsługą incydentów w warunkach zewnętrznego zagrożenia bezpieczeństwa państwa i w czasie wojny;*  *5) uczestnictwo w ćwiczeniach i szkoleniach organizowanych przez CSIRT MON, mających na celu przygotowanie podmiotów krajowego systemu cyberbezpieczeństwa na wypadek działania o którym mowa w ust. 5a.”;*  *h) ust. 7 otrzymuje brzmienie:*  *„7. Do zadań CSIRT GOV należy:*  *1) koordynacja obsługi incydentów zgłaszanych przez:*  *a) jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 1, 8 i 9 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych, z wyjątkiem wymienionych w ust. 5 i 6,*  *b) jednostki podległe Prezesowi Rady Ministrów lub przez niego nadzorowane,*  *c) Narodowy Bank Polski,*  *d) Bank Gospodarstwa Krajowego,*  *e) inne niż wymienione w lit. a-d oraz ust. 5 podmioty, których systemy teleinformatyczne lub sieci teleinformatyczne objęte są jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym,*  *f) podmioty, o których mowa w ust. 6, jeżeli incydent dotyczy systemów teleinformatycznych lub sieci teleinformatycznych objętych jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym;*  *2) realizacja, kierowanych przez CSIRT MON, zadań związanych z obsługą incydentów w warunkach zewnętrznego zagrożenia bezpieczeństwa państwa i w czasie wojny;*  *3) uczestnictwo w ćwiczeniach i szkoleniach organizowanych przez CSIRT MON, mających na celu przygotowanie podmiotów krajowego systemu cyberbezpieczeństwa na wypadek działania o którym mowa w ust. 5a.”;* | **Uwaga nieuwzględniona**  W ocenie autora uwag niezbędne jest doprecyzowanie w ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (KSC) uprawnień i obowiązków Ministra Obrony Narodowej przed formalnym wprowadzeniem stanu wojennego oraz stanu wojny. W związku z tym zaproponowano dodanie art. 51a oraz wprowadzenie stosownych zmian w przepisach określających zadania CSIRT GOV i CSIRT NASK. W proponowanym art. 51a ust. 1 użyto niejasnego określenia ,,uprawnień do koordynacji działań podmiotów, o których mowa w art. 4”. Wydaje się, że jest to pojęcie zbyt szerokie – KSC odnosi się do koordynacji obsługi incydentów, nie zaś koordynacji wszystkich działań podmiotów KSC. Podobnie, wątpliwości budzi pojęcie „w warunkach zewnętrznego zagrożenia państwa”. Trudno ustalić o jakie warunki chodzi. Podkreślić należy, że z tego samego powodu, na podstawie art. 2 ust. 1 ustawy z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (Dz. U. z 2017 r. poz. 1932) Prezydent może wprowadzić stan wojenny. Możliwość wprowadzenia stanu wojennego została uwzględniona w KSC przez określenie zadań dla Ministra Oborny Narodowej: kierowanie działaniami związanymi z obsługą incydentów w czasie stanu wojennego (art. 51 pkt 5) oraz koordynacja we współpracy z ministrem właściwym do spraw wewnętrznych i ministrem właściwym do spraw informatyzacji, realizacji zadań organów administracji rządowej i jednostek samorządu terytorialnego w czasie stanu wojennego dotyczących działań obronnych w przypadku zagrożenia cyberbezpieczeństwa (art. 51 pkt 8).  Zgodnie z art. 67 ust. 2 KSC Prezes Rady Ministrów wydaje wiążące wytyczne dla CSIRT MON, CSIRT GOV i CSIRT NASK w zakresie obsługi incydentów krytycznych, w tym wskazuje CSIRT odpowiedzialny za obsługę incydentu krytycznego. Zgodnie z definicją (art. 2 pkt 6 KSC) incydentem krytycznym jest incydent skutkujący znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi, klasyfikowany przez właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV. Zatem do oceny merytorycznej pozostaje czy ww. przepisy nie są wystarczające dla zapewniania cyberbezpieczeństwa przed wprowadzeniem stanu wojennego. Należy przy tym zwrócić uwagę na możliwe wystąpienie kolizji z uprawnieniami ABW, wynikających z art. 5 ust. 1 pkt 2a ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2020 r. poz. 27).  Określenie „w warunkach zewnętrznego zagrożenia państwa” jest tożsame z określeniem „w razie zewnętrznego zagrożenia państwa”, którego wystąpienie jest podstawą wprowadzenia stanu wojennego. Dlatego wątpliwości budzi powierzanie zadań Ministrowi Obrony Narodowej przez Prezesa Rady Ministrów w stanie zewnętrznego zagrożenia państwa i stanu wojny, bowiem stoi w sprzeczność z uprawnieniami Rady Ministrów wynikającymi z ustawy z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz z ustawy z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej (Dz. U. z 2019 r. poz. 1541).  Propozycja MON odnosi się do wszystkich podmiotów systemu cyberbezpieczeństwa, nie określając przy tym ich zadań. Należy przy tym zwrócić uwagę, że Minister Obrony Narodowej ma uprawnienia jedynie wobec Sił Zbrojnych oraz jednostek jemu podporządkowanych. |
| **Ministerstwo Klimatu i Środowiska** | Art. 53 ust. 1 pkt 1 | W art. 1 projektu proponuje się dodanie po pkt 26 nowego pkt 27 w następującym brzmieniu: „27) w art. 53 w ust. 1 uchyla się pkt 1.”  Dodanie przepisu zmieniającego art. 53 w zakresie nadzoru. Proponuje się usunięcie w art. 53 ust. 1 pkt 1 – tego typu nadzór będzie sprawowany przez organy właściwe, ponieważ SOC będzie częścią operatora usługi kluczowej, który tym samym będzie odpowiadał za realizację jego zadań i stosowanie przepisów UKSC. | **Uwaga nieuwzględniona**  SOC ustanowiony w ramach operatora usługi kluczowej podlegać będzie nadzorowi przez organ właściwy na podstawie art. 53 ust. 2 pkt 2 lit a nowelizowanej ustawy. |
| **Ministerstwo Klimatu i Środowiska** | Art. 55 pkt 1 | W art. 1 projektu proponuje się dodanie po nowym pkt 27 nowego pkt 28 w następującym brzmieniu: „28) w art. 55 pkt 1 otrzymuje brzmienie: „1) swobodnego wstępu i poruszania się po terenie podmiotu kontrolowanego bez obowiązku uzyskiwania przepustki, ale z zachowaniem zasad obowiązujących w kontrolowanym podmiocie;”  Dodanie w art. 1 nowego pkt 28 zmieniającego  art. 55 pkt 1 UKSC w zakresie dodania: Osoba prowadząca czynności kontrolne powinna posiadać nieskrępowany dostęp do całej infrastruktury odpowiadającej za cyberbezpieczeństwo przedmiotowej usługi, w tym dostęp fizyczny do właściwych obiektów i pomieszczeń. Jednakże wskazany zapis może być interpretowany jako ustawowe zwolnienie z zasad dostępu, np. do infrastruktury krytycznej z zachowaniem BHP np. na stacjach elektroenergetycznych.  Skutkiem może być narażenie na utratę zdrowia lub życia przez osobę prowadzącą czynności kontrolne oraz naruszenie przepisów innych ustaw. | **Uwaga nieuwzględniona**  Jest to wzorowane na art. 29 ust. 1 pkt 2a ustawy o Najwyższej Izbie Kontroli. |
| **Koordynator Służb Specjalnych** | Art. 66a | Jednocześnie w związku z wprowadzeniem projektowanego art. 66a ustawy *o krajowym systemie cyberbezpieczeństwa*, wydaje się, iż zaangażowanie Agencji Bezpieczeństwa Wewnętrznego w procedurę zbierania informacji kluczowych dla przeprowadzanej oceny ryzyka wymaga uprzednich zmian ustawowych obejmujących właściwość Agencji, określoną w art. 5 ustawy z dnia 24 maja 2002 r. *o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu*, analogicznie jak miało to miejsce w przypadku pkt 2a w art. 5 ust. 1 tej ustawy dodanym ustawą z dnia 10 czerwca 2016 r. *o działaniach antyterrorystycznych*. Należy bowiem wskazać, iż zgodnie z art. 21 ust. 1 ustawy *o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu* funkcjonariusze Agencji Bezpieczeństwa Wewnętrznego wykonują czynności operacyjno-rozpoznawcze i analityczno-informacyjne w celu uzyskiwania i przetwarzania informacji istotnych dla ochrony bezpieczeństwa państwa i jego porządku konstytucyjnego w granicach zadań, o których mowa w art. 5 ust. 1 ww. ustawy. Dodatkowym problemem praktycznym w tym kontekście pozostaje kwestia wykorzystania w ramach procedury oceny ryzyka analizy informacyjnej sporządzonej przez Agencję Bezpieczeństwa Wewnętrznego z wykorzystaniem informacji uzyskanych w drodze czynności operacyjno-rozpoznawczych i w związku z tym zaklasyfikowanych jako informacja niejawna. | **Uwaga nieuwzględniona**  Ocena ryzyka dostawcy sprzętu lub oprogramowania dotyczy m. in. Analizy potencjalnego zagrożenia dla bezpieczeństwa narodowego związanego z wykorzystywaniem danego sprzętu lub oprogramowania. Nie ma potrzeby zmiany ustawy o ABW oraz AW, gdyż funkcjonariusze ABW i AW będą realizowali czynności mające na celu ochronę bezpieczeństwa Państwa.  Materiały mające być wykorzystane w trakcie przygotowywania opinii Kolegium w ramach postępowania z art. 66a mogą być sporządzone w sposób zapewniający ochronę źródeł informacji. Ponadto postępowanie z informacjami niejawnymi już jest uregulowane w ustawie o ochronie informacji niejawnych. |
| **Ministerstwo Sprawiedliwości** | Art. 66a ust 2 i 3 | Zgodnie z projektowanym art. 66a ust. 2-3 ustawy o krajowym systemie cyberbezpieczeństwa wniosek o sporządzenie oceny ryzyka dostawcy sprzętu lub oprogramowania istotnego dla cyberbezpieczeństwa podmiotów krajowego systemu cyberbezpieczeństwa zawiera wskazanie danych identyfikujących dostawcę sprzętu lub oprogramowania, możliwych obszarów działalności, w których dostawca sprzętu lub oprogramowania może stanowić zagrożenie dla bezpieczeństwa narodowego. Wniosek ten może określać rodzaje sieci telekomunikacyjnych i systemów teleinformatycznych lub produktów, usług i procesów, o których mowa w art. 2 pkt 3e lub kategorie podmiotów wchodzących w skład krajowego systemu cyberbezpieczeństwa, które uwzględnia się przy sporządzeniu oceny sprzętu lub oprogramowania. Należy zauważyć, iż przy ocenie bezpieczeństwa sieci oraz usług powinien być przede wszystkim oceniany sprzęt, a nie przedsiębiorcy go dostarczający. Stąd należy zastąpić w powyższym przepisie odwołania do dostawcy, odwołaniami do sprzętu i oprogramowania. | **Uwaga nieuwzględniona**  Przepisy art. 66a-66c zostaną zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Przewodniczącego Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa).  Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka.  Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i pozatechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty pozatechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3. |
| **Ministerstwo Obrony Narodowej** | Art. 66a ust. 5 | **W art. 1 pkt 29 *projektu* -** projektowanemu art. 66a ust. 5 proponuje się nadać brzmienie:  *„5. Sporządzona przez Kolegium ocena ryzyka dostawcy sprzętu lub oprogramowania wskazuje:*   1. *wysokie ryzyko, jeżeli dostawca stanowi poważne zagrożenie cyberbezpieczeństwa państwa, a zmniejszenie poziomu tego ryzyka przez wdrożenie środków technicznych lub organizacyjnych nie jest możliwe,* 2. *umiarkowane ryzyko, jeżeli dostawca stanowi poważne zagrożenie dla cyberbezpieczeństwa państwa, a zmniejszenie tego ryzyka możliwe jest przez wdrożenie środków technicznych lub organizacyjnych, albo* 3. *brak zidentyfikowanego poziomu ryzyka, jeżeli nie stwierdzono zagrożenia dla cyberbezpieczeństwa państwa lub jego poziom jest znikomy.”*   Proponuje się wprowadzenie 3 poziomów ryzyka, gdyż z projektowanych przepisów nie wynika różnica pomiędzy niewielkim (lit. c), a znikomym (lit. d) zagrożeniem. Ponadto, w celu zachowania spójności z treścią art. 66b ust. 1 pkt 1 *projektu*, który odnosi się także do kwestii usług, a nie tylko dostaw sprzętu i oprogramowania, rozważenia wymaga uzupełnienie pojęcia w następujący sposób: „dostawcy sprzętu, oprogramowania lub usług”. | **Uwaga nieuwzględniona**  Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka.  Postępowanie administracyjne będzie prowadzone w drodze decyzji dostawcę sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, jeżeli z przeprowadzonego postępowania wynika, że dostawca ten stanowi poważne zagrożenie dla bezpieczeństwa narodowego.  Pojęcie dostawcy sprzętu lub oprogramowania zostało wystarczająco wyjaśnione w art. 66a – dostawca taki może dostarczać usługi ICT. |
| **Ministerstwo Rozwoju, Pracy i Technologii** | Art. 66a i 66b | Zgodnie z projektem przy ocenie ryzyka dostawcy dla cyberbezpieczeństwa będzie brana pod uwagę w szczególności okoliczność pozostawania pod wpływem państwa spoza UE lub NATO. Proponowane kryteria pomijają ocenę ryzyka dostawców z tych krajów należących do NATO, które nie posiadają porozumień z UE w zakresie ochrony danych osobowych, przyjmując jednocześnie, że kraje nienależące do NATO nie spełniają tych standardów. Projekt nie uwzględnia też kosztów, jakie będą musieli ponieść abonenci usług telekomunikacyjnych w związku z potencjalną koniecznością wymiany elementów obecnie działającej infrastruktury sieci 4G, które w dużej części zostały dostarczone przez dostawców z państw spoza NATO i UE. W przedłożonej regulacji nie oceniono czy wymiana sprzętu w tak krótkim czasie pozostaje w zasięgu możliwości finansowych i organizacyjnych tych firm. | **Uwaga nieuwzględniona**  Termin na wycofanie sprzętu lub oprogramowania od dostawców wysokiego ryzyka zostanie zmieniony z 5 na 7 lat. Termin 7 lat jest często uznawany za średni okres  użytkowania sprzętu lub oprogramowania, czyli tzw. cykl życia urządzenia.  Z uwagi na wskazanie tak długiego okresu na wdrożenie decyzji o ocenie ryzyka, nie są planowane rekompensaty dla operatorów z uwagi na konieczność wycofania sprzętu lub oprogramowania od dostawców uznanych za dostawców wysokiego ryzyka. Warto podkreślić, że każdy sprzęt lub oprogramowanie ma swój określony bezpieczny czas użytkowania. Często przywoływany jest argument, że operatorzy telekomunikacyjni w momencie wdrażania technologii sieci 5G (i kolejnych generacji) poniosą znaczne wydatki związane z ewentualnym zastąpieniem sprzętu lub oprogramowania pochodzącego od dostawców wysokiego ryzyka. Należy wskazać, że w obecnej chwili żaden z operatorów w Polsce nie zapewnia łączności 5 generacji przy wykorzystaniu wyłącznie docelowych urządzeń lub oprogramowania, lecz bazuje na istniejącej infrastrukturze wykorzystywanej m.in. do łączności 4G (jest to tzw. model non-stand alone). Obecna infrastruktura nie jest wystarczająca do wykorzystania w pełni możliwości oferowanych przez technologie sieci 5G, w tym ultra-szybkiej wymiany danych. Ponadto, obecna infrastruktura podlega procesowi zużycia i docelowo będzie zastępowana rozwiązaniami dedykowanymi dla sieci najnowszej generacji (tzw. model stand alone). Przedsiębiorcy telekomunikacyjni zatem muszą w swoich planach inwestycyjnych już teraz uwzględniać koszty nie tylko wymiany infrastruktury, która kończy swój okres bezpiecznego użytkowania, lecz także muszą mieć plan wdrożenia infrastruktury dedykowanej sieci 5G.    Decyzje o cenach usług, w tym abonamentów, podejmuje dany dostawca usług telekomunikacyjnych.  Kwestia oceny ryzyka dostawców, którzy mogą znajdować się znajdować pod kontrolą państwa spoza UE wynika wprost z wspólnie uzgodnionego 5G Toolbox. Część partnerów strategicznych Polski nie jest członkami struktur europejskich, lecz wchodzą w skład Sojuszu NATO, dlatego rozwinęliśmy wyłączenie spod oceny ryzyka dostawców także z państw NATO. |
| **Koordynator Służb Specjalnych** | Art. 66b  Art. 66c  Art. 67a | Mając na uwadze zadania realizowane przez Agencję Bezpieczeństwa Wewnętrznego, a w szczególności funkcjonujący w ramach jej struktury organizacyjnej Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego (CSIRT GOV), proponuje się wyłączenie Agencji Bezpieczeństwa Wewnętrznego z obowiązków wynikających z projektowanych art. 66b i 66c ustawy *o krajowym systemie cyberbezpieczeństwa* dotyczących sporządzenia oceny ryzyka określającej wysokie ryzyko dostawcy sprzętu lub oprogramowania oraz projektowanego art. 67a ustawy *o krajowym systemie cyberbezpieczeństwa* w zakresie skutków wydania ostrzeżenia lub polecenia zabezpieczającego przez Pełnomocnika. | **Uwaga nieuwzględniona**    Zarówno ABW jak i CSIRT GOV są podmiotami krajowego systemu cyberbezpieczeństwa. Dla skuteczności proponowanych przepisów nie są przewiduje się odstępstw.  CSIRT GOV jest od początku zaangażowany w procedury wynikające z wydawanie ostrzeżeń lub poleceń zabezpieczających. Zatem CSIRT GOV ma wpływ na treść, zakres podmiotowy ostrzeżeń i poleceń. |
| **Ministerstwo Rozwoju, Pracy i Technologii** | Art. 66b ust. 2 pkt. 2 | W przypadku kontynuowania użytkowania dotychczasowego sprzętu i oprogramowania nabytego od dostawcy umiarkowanego ryzyka powinna istnieć możliwość dostarczania aktualizacji bezpieczeństwa przez dotychczasowego dostawcę. Nie jest jasne, czy poprawki nie zostaną zakwalifikowane jako nowe oprogramowanie wprowadzone do użytkowania (pkt 1). Jeżeli natomiast nie przewiduje się możliwości korzystania z usług dostawcy w sprawach związanych z użytkowaniem dotychczasowego sprzętu i oprogramowania, należy wyjaśnić, w jaki sposób zapewnić ich dalsze utrzymanie i rozwój, aby wraz z upływem czasu nie stwarzały zagrożeń w obszarze cyberbezpieczeństwa. | **Uwaga nieuwzględniona**  Zrezygnowano z poziomu umiarkowanego. Z kolei decyzja o uznaniu za dostawcę wysokiego ryzyka nie powinna być przesłanką do zakończenia wsparcia eksploatacyjnego przez dostawcę tego sprzętu do momentu wycofania danego sprzętu lub oprogramowania z użytkowania. |
| **Ministerstwo Obrony Narodowej** | Art. 67a ust. 3 pkt 5 | **Art. 1 pkt 30 *projektu ksc*** – użyty w art. 67a ust. 3 pkt 5 wyraz „skuteczność” proponuje się zastąpić wyrazem „nieskuteczność”. Celowym wydaje się dokonywanie analizy nieskuteczności alternatywnych środków. | **Uwaga nieuwzględniona.** Należy właśnie dokonać analizy czy są inne skuteczne środki. Analizowanie nieskuteczności innych środków jest bezprzedmiotowe. |
| **Ministerstwo Sprawiedliwości** | Art. 67c ust. 1 | Zgodnie z projektowanym art. 67c ust. 1 ustawy o krajowym systemie cyberbezpieczeństwa, pełnomocnik wydaje polecenie zabezpieczające w drodze decyzji administracyjnej. Decyzja podlega natychmiastowemu wykonaniu. Wydaje się, że wskazana jest rezygnacja z rygoru natychmiastowej wykonalności decyzji z mocy prawa z uwagi na jej możliwe nieodwracalne skutki. Pozostaje przy tym możliwość nadania rygoru natychmiastowej wykonalności takiej decyzji na podstawie art. 108 § 1 ustawy – Kodeks postępowania administracyjnego. | **Uwaga nieuwzględniona.** Incydent krytyczny może skutkować znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi. Polecenie zabezpieczające, jest niezbędne do natychmiastowej reakcji, umożliwiającej ograniczenie lub zmitygowanie skutków incydentu. Dlatego musi mieć nadany rygor natychmiastowej wykonalności. |
| **Ministerstwo Klimatu i Środowiska** | Art. 93 ust. 6 pkt 4-10 | Koszty stworzenia nowych stanowisk pracy, zwiększenia finansowania obecnych oraz utworzenia CSIRT sektorowego dla sektora energii będą pokrywane z 47 części budżetowej – energia w kwocie łącznej **96,032 mln zł** w skali całego okresu finansowania **do 2027 r.**, z czego 84 552 tys. zł będą poświęcone utworzeniu i utrzymywaniu CSIRT sektorowego, a 11 480 tys. zł będzie przeznaczone na stworzenie nowych stanowisk pracy oraz zwiększenie finansowania obecnych.   |  |  |  | | --- | --- | --- | | Rok | Koszty nowych stanowisk pracy oraz zwiększenia finansowania obecnych [mln zł] | Koszty utworzenia i utrzymania CSIRT Energia [mln zł] | | 2021 | 1,64 | 0 | | 2022 | 1,64 | 15,842 | | 2023 | 1,64 | 13,742 | | 2024 | 1,64 | 13,742 | | 2025 | 1,64 | 13,742 | | 2026 | 1,64 | 13,742 | | 2027 | 1,64 | 13,742 |   Proponuje się w art. 1 projektu dodać nowy pkt 34  w brzmieniu:  „34) w art. 93 w ust. 6 pkt 4-10 otrzymują  brzmienie:  „4) w 2021 r. - 1 640 tys. zł;  5) w 2022 r. - 17 487 tys. zł;  6) w 2023 r. - 15 387 tys. zł;  7) w 2024 r. - 15 387 tys. zł;  8) w 2025 r. - 15 387 tys. zł;  9) w 2026 r. - 15 387 tys. zł;  10) w 2027 r. - 15 387 tys. zł.”” | **Uwaga nieuwzględniona**  Koszty funkcjonowania w tym koszty osobowe i utworzenia CSIRT sektorowego dla sektora energii zostały wystarczająco opisane w OSR i uwzględnione w ramach reguły wydatkowej. W ocenie KPRM wskazane przez Ministerstwo Klimatu i Środowiska koszty są znacznie przeszacowane oraz brak jest wyszczególnienia kosztów cząstkowych m. in. nie wykazano pochodzenia łącznych kosztów utworzenia CSIRT energia. Nie wiemy zatem na ile oszacowano koszty usług SOCowych a także usług CERTowych.. |
| **Rządowe Centrum Legislacji** | Rozdział 4a | W odniesieniu do dodawanego rozdziału 4a w ustawie o KSC określającego obowiązki przedsiębiorców komunikacji elektronicznej, należy wskazać, że ich deklarowane przez Projektodawcę przeniesienie do projektu ustawy – *Prawo komunikacji elektronicznej*, zasadne z uwagi na brzmienie § 2 ZTP i zakres przedmiotowy tego rozdziału, będzie wymagało ponownej analizy i oceny spójności tych regulacji na poziomie pojęciowym i konstrukcyjnym zarówno z projektowaną ustawą, jak i projektowaną ustawą – *Prawo komunikacji elektronicznej.* | **Uwaga nieuwzględniona**  Prace legislacyjne związane z wprowadzeniem przepisów prawnych dot. obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci i usług oraz zgłaszania incydentów zostały przeniesione do przepisów wprowadzających Prawo Komunikacji Elektronicznej. Przepisy te zostaną poddane analizie i ocenie spójności z oboma wzmiankowanymi aktami prawnymi. |
| **Ministerstwo Finansów** | OSR  Pkt 6 | W **pkt 6 OSR**, jak i w treści uzasadnienia, zawarto informację o tym, że wejście w życie projektowanej regulacji będzie stanowić podstawę do ubiegania się o dodatkowe środki z budżetu państwa na ten cel w części 27 - Informatyzacja. Łączne wydatki budżetu państwa w okresie 10 lat od wejścia w życie ww. projektu określono w wysokości 439,35 mln zł (w roku 2022 r, jako pierwszym 52,43 mln zł). Należy zauważyć, że w świetle panującej obecnie pandemii COVID-19 oraz trudnych do przewidzenia dalszych skutków społeczno-gospodarczych i finansowych z nią związanych, projektowane regulacje i wydatki winny znajdować swoje źródło finansowania w ramach dostępnego limitu wydatków danego dysponenta części budżetowej. Informacje zawarte w pkt 6 OSR w poz. „Źródła finansowania” powinny zostać zatem skorygowane (również w uzasadnieniu) poprzez wskazanie, że ujęte w projekcie wydatki zostaną sfinansowane w ramach limitu wydatków dysponenta części 27 – Informatyzacja i nie będą stanowiły podstawy do ubiegania się o dodatkowe środki na ten cel z budżetu państwa w roku bieżącym, jak i w kolejnych latach budżetowych. Należy przy tym pamiętać, że ostateczne decyzje o wyborze priorytetów, realizowanych zadań i poziomie ich finansowania w ramach wyznaczonego limitu wydatków leżą w gestii dysponenta danej części budżetowej.  Analogicznie jak powyższej, w pkt 6 OSR należy dodatkowo wskazać, iż ewentualne wydatki dla Ministerstwa Obrony Narodowej oraz Agencji Bezpieczeństwa Wewnętrznego, związane z wejściem w życie przedmiotowej ustawy, będą finansowane w ramach limitu wydatków części 29 – Obrona narodowa oraz części 57 – Agencja Bezpieczeństwa Wewnętrznego, ustalanych corocznie w ustawie budżetowej, i nie będą stanowiły podstawy do ubiegania się o dodatkowe środki na ten cel w roku bieżącym, jak i w kolejnych latach budżetowych.  Ponadto, należy w sposób transparentny przedstawić całkowite wydatki w podziale na zadania i poszczególne lata włącznie z określeniem dysponenta finansującego to zadanie (w jednej tabeli). Obecnie w OSR określone wydatki zaprezentowane są w sposób nieczytelny i trudno jest wyjść na kwotę ogółem, jak i w pojedynczych latach (ujętych także w projektowanym art. 4 ustawy). Zaś w OSR w *Dodatkowych informacjach, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń* przedstawiono kalkulację kosztów utworzenia trzech rodzajów CSIRT sektorowych (usługi tzw. CERTowe analityczne oraz SOCowe reagowania na incydenty). Według podanych informacji roczny koszt ww. CSIRT sektorowych kształtować się ma na poziomie 2.874.960 zł. Na potrzeby obliczeń założono wynagrodzenie rynkowe specjalistów w CSIRT w wysokości 18.000 zł brutto m/c. Należy zatem zwrócić uwagę na wysoki poziom wynagrodzeń, co budzi zastrzeżenia, i nie może uzyskać akceptacji. Kolejno wskazano, iż usługi SOCowe zakładają stopniowe budowanie trzech linii wsparcia (od 14 pracowników w pierwszym roku działania do 20 pracowników w trzecim) przy wynagrodzeniu miesięcznym na etat stanowisko operatora I linii 12.000 zł do eksperta III linii 20.000 zł. Z uwagi na to, iż organ właściwy (zgodnie z OSR pkt 4 wskazano 7 organów), może powołać CSIRT sektorowy, zespół ds. cyberbezpieczeństwa, dodatkowo ww. organ będzie mógł powierzyć realizację zadań CSIRT sektorowego, jednostkom podległym lub nadzorowanym. W związku z powyższym należy wskazać, w jakim urzędzie/jednostce będą zatrudnione ww. wskazane osoby realizujące przedmiotowe zadania. Dodatkowo należy przedstawić szczegółową kalkulację kosztów. Nie jest bowiem jasne w jaki sposób i w oparciu o jakie założenia zostały one oszacowane. Ustawodawca wskazuje, iż projekt wygeneruje konieczność zatrudnienia wysoko wykwalifikowanych specjalistów zajmujących się cyberbezpieczeństwem, a także przekwalifikowania dotychczas posiadanej kadry. Należy zatem przedstawić koszty wynagrodzeń osobowych dotychczasowej kadry zajmującej się zadaniami z zakresu cyberbezpieczeństwa w podziale na organy zatrudniające te osoby. | **Uwaga nieuwzględniona.**  Nie jest możliwa realizacja tego przedsięwzięcia bez zwiększenia limitów, gdyż jest to zadanie nowe i dodatkowe. |
| **Koordynator Oceny Skutków Regulacji** | OSR  Pkt 6  Pkt 7 | Niezbędne jest przeniesienie z opisu w pkt 6 OSR fragmentów odnoszących się do kosztów ponoszonych przez przedsiębiorców (np. w odniesieniu do SOC) – właściwym miejscem na ten opis jest pkt 7 OSR | **Uwaga nieuwzględniona**  Nie jest wskazane przenoszenie opisu kosztów przeznaczonych na usługi SOCowe do pkt 7, gdyż jak wskazano wyżej, wyliczenia kosztów w pkt 6 dotyczą powstania i funkcjonowania CSIRT sektorowych. W skład usług oferowanych przez CSIRT sektorowy wchodzą usługi tzw. CERTowe (analityczne) oraz SOCowe (reagowania na incydenty). |