**Zbiorcza tabela uwag na temat** **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).**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| lp. | **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 niewuzględniona**  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 | W proponowanym projekcie ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa i ustawy – Prawo zamówień publicznych, nie wprowadzono delegacji ustawowej do uregulowania niektórych przepisów aktami wykonawczymi. Bez doprecyzowania pewnych przepisów w rozporządzeniach, mogą one być zbyt ogólne i nieprecyzyjne. | **Uwaga uwzględniona**  Projekt został uzupełniony o szereg delegacji ustawowych dla ministra właściwego do spraw informatyzacji . |
|  | **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 Finansów** | Uwaga ogólna do uzasadnienia projektu ustawy | Wątpliwości budzi próba wprowadzenia do ustawy o krajowym systemie cyberbezpieczeństwa siatki pojęciowej z projektowanej dopiero ustawy - Prawo komunikacji elektronicznej, która - z uwagi na etap prac - nie ma realnych szans na wejście w życie przed datą wejścia opiniowanych przepisów. | **Wyjaśnienie**  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 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. |
|  | **Rządowe Centrum Legislacji** | Uwaga ogólna | Projekt ustawy wymaga uzupełnienia w zakresie zmian przepisów wynikających z dokonywanej nowelizacji, tj.:  1) z powodu zmiany katalogu podmiotów objętych krajowym systemem cyberbezpieczeństwa (projektowany art. 4 ustawy o KSC) zmiany wymaga również zakres działania poszczególnych CSIRT, o którym mowa w art. 26 ust. 5- 7 ustawy o KSC,  2) w związku z wprowadzeniem obowiązku prowadzenia przez wojewodę listy danych kontaktowych osób z poszczególnych podmiotów publicznych w województwie, wskazanych przez kierownictwo tych podmiotów, do współpracy z właściwymi CSIRT MON, CSIRT NASK lub CSIRT GOV, należy nałożyć na te podmioty obowiązek poinformowania właściwego wojewody o wyznaczeniu takiej osoby i o wszelkich zmianach w tym zakresie, stosowną regulację można wprowadzić do art. 21 ustawy o KSC,  3) w związku z zobowiązaniem nowego podmiotu, tj. SOC, do wykonywania obowiązków, o których mowa w art. 8-13 ustawy o KSC, konieczne jest dostosowanie środków komunikacji umożliwiających dokonywanie zgłoszeń i przekazywanie informacji, o których mowa w art. 26 pkt 15 oraz art. 31 ustawy o KSC udostępnianych przez CSIRT poziomu krajowego, aby umożliwić wykonanie ustawowych obowiązków przez nowy podmiot,  4) w związku z usunięciem określenia „*podmioty świadczące usługi z zakresu cyberbezpieczeństwa*” konieczne jest również uzupełnienie przepisów o zmianę tytułu rozdziału 11 ustawy o KSC oraz art. 53 ustawy o KSC – również w zakresie odesłania do art. 14 ust. 2 tej ustawy,  5) ze względu na zmiany w zakresie zadań Kolegium powinien ulec zmianie regulamin Kolegium – określany rozporządzeniem wydawanym przez Radę Ministrów na podstawie upoważnienia zawartego w art. 62 ust. 9 ustawy o KSC, rozważenia wymaga także, czy z uwagi na skutek, o którym mowa w § 32 ZTP, konieczne będzie utrzymanie w mocy przepisów wykonawczych wydanych na tej podstawie zgodnie z regulacją § 33 ZTP lub ustanowienie możliwości ich zmiany w okresie utrzymania w mocy (§ 34 ZTP). | **Uwaga częściowo uwzględniona**  Ad 1. Przepis został uzupełniony.  Ad. 2. Przepis został uzupełniony – dopisano obowiązek poinformowania wojewody o wyznaczeniu osoby do kontaktu.  Ad. 3. Zespoły SOC są doprecyzowaniem aktualnie funkcjonującym wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo. Wobec tego nie ma potrzeby określania dodatkowych kanałów komunikacji.  Ad. 4 Przepisy zostały uzupełnione.  Ad. 5 Regulamin Kolegium zostanie zmieniony. |
|  | **Rządowe Centrum Legislacji** | Uwaga ogólna | Projekt ustawy wymaga dostosowania do wymogów określonych w *Regulaminie pracy Rady Ministrów* oraz licznych korekt redakcyjnych i legislacyjnych. | **Uwaga uwzględniona**  Korekty redakcyjne i legislacyjne zostaną wprowadzone. |
|  | **Ministerstwo Zdrowia** | Uwaga ogólna | Wskazanie Centrum e-Zdrowia jako podmiotu odpowiedzialnego za pełnienie funkcji CSIRT sektorowego dla sektora ochrony zdrowia należałoby uszczegółowić kwestie dotyczące skutków finansowych regulacji oraz zapewnić w planie finansowym Centrum e-Zdrowia odpowiednie środki finansowe na realizację przedmiotowego zadania. Obecnie bowiem projekt ustawy, jak również uzasadnienie oraz Ocena Skutków Regulacji (OSR) nie zawierają szczegółowych regulacji dotyczących finansowania CSIRT sektorowych, jak też procedury występowania o uruchomienie środków finansowych dla poszczególnych sektorów. Mając powyższe na uwadze wydaje się zasadnym, aby przynajmniej w uzasadnieniu do projektu czy też w OSR zostały uwzględnione te zagadnienia. Jednocześnie wskazać należy, że Centrum e-Zdrowia jako operator usług kluczowych (w zakresie zarządzania danymi epidemiologicznymi oraz jako podmiot zajmujący się gromadzeniem i udostępnianiem Elektronicznej Dokumentacji Medycznej), a także realizujący kluczowe projekty informatyczne dla systemu ochrony zdrowia wydaje się być podmiotem najbardziej odpowiednim do pełnienia roli CSIRT sektorowego. Wymaga to jednakże zapewnienia niezbędnych środków finansowych. | **Wyjaśnienie**  W OSR są przewidziane środki na budowę CSIRT sektorowego w sektorze zdrowia. Ponadto proponowane przepisy wskazują, że organ właściwy wyznacza CSIRT sektorowy spośród jednostek podległych lub nadzorowanych. Wobec tego nie przeciwskazań, żeby Minister Zdrowia wyznaczył jako CSIRT sektorowy Centrum e-Zdrowia. |
|  | **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.  OSR został uzupełniony. |
|  | **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 . |
|  | **Rządowe Centrum Legislacji** | Art. 1 ust. 2 pkt 2 | W zakresie zmiany w art. 1 ustawy z dnia 5 lipca 2018 r. *o krajowym systemie cyberbezpieczeństwa* (Dz. U. z 2020 r. poz. 1369), zwanej dalej „*ustawą o KSC*” –po projektowanym usunięciu w art. 1 w ust. 2 pkt 2, wyłączającego spod działania przepisów ustawy o KSC dostawców usług zaufania, szerszej analizy Projektodawcy wymaga, czy w konsekwencji takiej zmiany przepisów jedynym skutkiem projektowanej zmiany będzie możliwość wykorzystania przez dostawców usług zaufania oceny ryzyka dokonywanej wobec dostawców sprzętu lub oprogramowania – na co wskazuje uzasadnienie projektu – czy też wobec usunięcia przedmiotowego wyłączenia oraz braku kryteriów podmiotowych dotyczących dostawców usług zaufania w ustawie z dnia 5 września 2016 r. *o usługach zaufania i identyfikacji elektronicznej* (Dz. U. z 2020 r. poz. 1173) potencjalni dostawcy usług zaufania staną się elementem krajowego systemu cyberbezpieczeństwa i będą objęci obowiązkami z niego wynikającymi, a w konsekwencji konieczne będą zmiany dostosowujące i uwzględniające nowy charakter tych podmiotów, w tym także stosowne przepisy przejściowe. | **Wyjaśnienie**  Dostawcy usług zaufania nie będą włączeni w skład krajowego systemu cyberbezpieczeństwa. Nie będą również w grupie podmiotów zobowiązanych do wycofania sprzętu lub oprogramowania dostawcy wysokiego ryzyka.  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 . |
|  | **Rządowe Centrum Legislacji** | Art. 2  Pkt 3b  Pkt 3c  Pkt 3e  Pkt 8f | W zakresie zmiany w art. 2 ustawy o KSC należy zauważyć, że:  1) projektowane definicje wymagają ponownej analizy w kontekście przepisów projektowanej ustawy – *Prawo komunikacji elektronicznej*,  2) w projektowanej definicji CSIRT Teleco (wprowadzanej w art. 2 pkt 3b ustawy o KSC) – analogicznie do definicji CSIRT GOV, CSIRT NASK i CSIRT MON konieczne jest doprecyzowanie, czy CSIRT Teleco działa na poziomie krajowym czy ma charakter sektorowy, zasadne byłoby również przeniesienie z dalszej części ustawy regulacji dotyczącej podmiotu zobowiązanego do prowadzenia CSIRT Teleco, celem zachowania spójności z pozostałymi definicjami CSIRT,  3) projektowana definicja ISAC (wprowadzana w art. 2 pkt 3c ustawy o KSC) odwołuje się jedynie do jego funkcji jako „*centrum wymiany i analizy informacji na temat podatności, zagrożeń i incydentów*”, w podobny sposób zdefiniowane zostały również jego zadania „*w szczególności wymiana informacji, dobrych praktyk i doświadczeń dotyczących zagrożeń cyberbezpieczeństwa, podatności oraz incydentów*” (dodawanym art. 4a ustawy o KSC). W świetle powyższego projektowane przepisy wymagają uzupełnienia, gdyż z ich obecnego brzmienia trudno jest wywnioskować, jaką rolę w krajowym systemie bezpieczeństwa mają odgrywać ISAC, jakie będą zasady i tryb wymiany informacji i dobrych praktyk dotyczących cyberbezpieczeństwa. Zasadne byłoby również doprecyzowanie, jakie typy podmiotów będą miały status ISAC oraz, analogicznie jak w przypadku CSIRT, przypisanie nazwy własnej temu podmiotowi, a nie jedynie posłużenie się akronimem,  4) projektowana definicja dostawcy sprzętu lub oprogramowana (dodawany pkt 3e w art. 2 ustawy o KSC) wymaga doprecyzowania, gdyż posłużenie się w niej skrótem „*w rozporządzeniu (WE) nr 765/2008*”, nie wprowadzonym we wcześniejszej części ustawy o KSC, nie pozwala na ustalenie, do jakich przepisów odwołuje się projektowana definicja. Ponadto, z punktu widzenia określoności przepisów prawa budzi wątpliwości technika legislacyjna, która we wprowadzeniu do wyliczenia posługuje się odesłaniem do bezpośrednio stosowanego aktu prawa unijnego, tj. rozporządzenia, a następnie doprecyzowując cechy podmiotów objętych tą definicją przez odesłanie do kolejnego aktu prawa unijnego i równorzędnie – aktu prawa polskiego. Podwójne, kaskadowe odesłanie w projektowanym przepisie powoduje trudności w ustaleniu zakresu podmiotowego pojęcia dostawcy sprzętu lub oprogramowania,  5) w odniesieniu do projektowanej definicji bezpieczeństwa sieci lub usług (dodawany pkt 8f w art. 2 ustawy o KSC) – nie jest jasna relacja tej definicji do definicji cyberbezpieczeństwa, o której mowa w art. 2 pkt 4 ustawy o KSC. Wyjaśnienia wymaga zwłaszcza, czy sieci telekomunikacyjne stanowią również systemy informacyjne, o których mowa w definicji cyberbezpieczeństwa oraz czy usługi oferowane w tych sieciach stanowią usługi oferowane przez systemy informacyjne w rozumieniu definicji cyberbezpieczeństwa. Jeżeli zakresy tych definicji się pokrywają – definicja bezpieczeństwa sieci i usług będzie wymagała przeredagowania. | **Uwaga częściowo uwzględniona**  Prace legislacyjne związane z wprowadzeniem przepisów prawnych dot. CSIRT-u Teleco oraz obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci i usług oraz zgłaszania incydentów zostały przeniesione do przepisów wprowadzających Prawo Komunikacji Elektronicznej. Przeprowadzono analizy pod kątem spójności z oboma aktami prawnymi. Ad. 2 W dalszym ciągu pozostają na poziomie krajowym tylko 3 zespoły CSIRT. Zespół CSIRT Telco będzie wspierał przedsiębiorców komunikacji elektronicznej w obsłudze incydentów telekomunikacyjnych. Ponadto będzie zapewniał współpracę z CSIRTami poziomu krajowego w zakresie wymiany informacji i reagowania na incydenty telekomunikacyjne i krytyczne.  Definicja CSIRT Telco została uzupełniona o wskazanie, że minister właściwy ds. informatyzacji zapewnia funkcjonowanie CSIRT Telco.  Ad. 3 Tworzenie ISAC jest inicjatywą oddolną i to od podmiotów tworzących ISAC należy określenie jakie informacje zbierają, analizują i komu przekazują. Zakres przekazywanych informacji, organizacja i struktura będą ustalane przez podmioty tworzące ISAC np. w formie regulaminu. Zaproponowane rozwiązanie mają ułatwić tworzenie ISAC w ramach krajowego systemu cyberbezpieczeństwa. Dlatego też nie reguluje się formy prawnej ISAC, ponieważ to mogą być fundacje, stowarzyszenia, przedsiębiorcy a nawet osoby fizyczne.  Zasady i tryb wymiany informacji między ISAC a podmiotami KSC zostaną ustalone w umowach pomiędzy ISAC a podmiotami zainteresowanymi współpracą, gdyż to od ich decyzji zależy czy chcą korzystać z usług ISAC.  Ad. 4 Poprawione zostanie odniesienie do rozporządzenia (WE) nr 765/2008.  Ad. 5  Przepis dot. definicji bezpieczeństwa sieci i usług zostanie dodany do ustawy o krajowym systemie cyberbezpieczeństwa poprzez ustawę wprowadzającą PKE. Definicja bezpieczeństwa sieci i usług odnosi się wyłącznie do przedsiębiorców komunikacji elektronicznej, którzy na mocy nowelizowanych przepisów ustawy ksc w zakresie bezpieczeństwa sieci i usług oraz zgłaszania i obsługi incydentów na poziomie krajowym włączeni do krajowego systemu cyberbezpieczeństwa. |
|  | **Ministerstwo Klimatu i Środowiska** | Art. 2 pkt 3c | **Proponowane brzmienie w art. 2 pkt 3c:** „3c) ISAC - centrum wymiany i analizy informacji na temat m.in. podatności, zagrożeń i incydentów, funkcjonujące w ramach sektora lub podsektora, w celu wspierania właściwych dla sektora lub podsektora podmiotów krajowego systemu cyberbezpieczeństwa;”  **Uzasadnienie:**  W propozycji definicji ISAC został ujęty wąski i zamknięty katalog działań ISAC skupiający się na wymianie i analizie informacji w 3 aspektach – podatności, zagrożeń i incydentów, natomiast nie ma tu mowy o wymianie informacji na temat np. dobrych praktyk. Zwłaszcza, że w art. 1 pkt 5 wprowadzającym art. 4a ust. 1 do UKSC czytamy, że „… może funkcjonować ISAC, do którego zadań należy w szczególności...”, zatem jest to otwarty katalog zadań. Forma ISAC przedstawiona w obecnej definicji nie wskazuje jednoznacznie jaki zakres podmiotowy obejmuje i może wskazywać na to, że będzie funkcjonował jeden ISAC dla wszystkich operatorów usług kluczowych i DUC. Z racji różnorodności sektorów i idących za tym różnych rodzajów informacji, które są istotne i niosą ze sobą wartość dodaną, zasadnym jest tworzenie takich rodzajów ISAC w ramach sektora lub podsektora. Informacje o np. incydentach czy podatnościach kluczowych w danym sektorze, dla innego sektora mogą być nieistotne. Może się to wiązać z powstaniem chaosu informacyjnego. | Uwaga częściowo uwzględniona  Dokonano uspójnienia i doprecyzowania katalogu zadań ISAC z art. 4a (obecnie 25a) i definicji art. 2 pkt 3c.  W technice legislacyjnej używa się liczby pojedynczej dla określenia podmiotów, które będą spełniać cechy określone w ustawie. |
|  | **Rządowe Centrum Legislacji** | Art. 2 pkt 3c  Art. 4a | W odniesieniu do projektowanego art. 4a ustawy o KSC w związku z definicją ISAC dodawaną w art. 2 ustawy o KSC (art. 2 pkt 3c) wymaga wyjaśnienia, jaki charakter będzie miał ten nowy podmiot krajowego systemu cyberbezpieczeństwa: na czyją rzecz będą podejmowane działania przez ten podmiot, czy będzie to podmiot publiczny czy prywatny, w jakim celu będzie prowadzony wykaz ISAC, jak będą wyglądały relacje pomiędzy ISAC a innymi podmiotami krajowego systemu cyberbezpieczeństwa, czy „*wymiana informacji i doświadczeń oraz dobrych praktyk*”, która ma należeć do zadań ISAC, będzie następowała pomiędzy podmiotami krajowego systemu cyberbezpieczeństwa czy także poza nimi. | **Wyjaśnienie**  Tworzenie ISAC jest inicjatywą oddolną i to od podmiotów tworzących ISAC należy określenie jakie informacje zbierają, analizują i komu przekazują. Zaproponowane rozwiązanie mają ułatwić tworzenie ISAC w ramach krajowego systemu cyberbezpieczeństwa. Dlatego też nie reguluje się formy prawnej ISAC, ponieważ to mogą być fundacje, stowarzyszenia, przedsiębiorcy a nawet osoby fizyczne.  Zasady i tryb wymiany informacji między ISAC a podmiotami KSC zostaną ustalone w umowach pomiędzy ISAC a podmiotami zainteresowanymi współpracą, gdyż to od ich decyzji zależy czy chcą korzystać z usług ISAC.  Wykaz ISAC jest konieczny, ponieważ ISAC będą mogły na podstawie oddzielnego porozumienia z ministrem właściwym ds. informatyzacji korzystać z systemu informacyjnego prowadzonego na podstawie art. 46 ustawy ksc.  Nie ma przeszkód, aby ISAC pozyskiwał informacje m. in. o podatnościach i dobrych praktykach od podmiotów zewnętrznych a następnie udostępniał w ramach swojej działalności podmiotom ksc. |
|  | **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. |
|  | **Rządowe Centrum Legislacji** | Art. 4 | W zakresie zmiany dokonywanej w art. 4 ustawy o KSC, dotyczącej katalogu podmiotów objętych krajowym systemem cyberbezpieczeństwa, należy zauważyć, że:  1) zakres wprowadzonego odesłania do art. 7 pkt 3-7 ustawy z dnia 20 lipca 2018 r. – *Prawo o szkolnictwie wyższym i nauce* (Dz. U. z 2020 r. poz. 85, z późn. zm.) obejmuje kategorie instytutów badawczych, które zostały już objęte krajowym systemem cyberbezpieczeństwa na mocy art. 4 pkt 8 ustawy o KSC,  2) posłużenie się wyrażeniem „*SOC*” w art. 4 pkt 16 zamiast określenia „*podmioty świadczące usługi na rzecz cyberbezpieczeństwa*” powoduje, że rozstrzygnięcia w przepisach przejściowych i dostosowujących wymaga dotychczasowa sytuacja podmiotów świadczących usługi na rzecz cyberbezpieczeństwa. | **Uwaga uwzględniona**  Ad 1 Uwaga przyjęta, zostanie wprowadzony zakres podmiotowy art. 7 pkt 3-7 ustawy z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce (Dz. U. z 2020 r. poz. 85, z późn. zm.).  Ad 2 Zespoły SOC są doprecyzowaniem aktualnie funkcjonującym „wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo” oraz zastępuje określenie „podmioty świadczące usługi na rzecz cyberbezpieczeństwa”. Został dodany przepis dostosowujący. |
|  | **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. 4a ust. 4 | W proponowanym zapisie art. 4a ust. 4 pojawia się informacja, że wpisanie do wykazu ISAC następuje po uzyskaniu pozytywnej opinii CSIRT MON, CSIRT NASK lub CSIRT GOV. Jednakże, nie ma wskazanego żadnego trybu wystąpienia o taką opinię, a po drugie nie ma jasnych kryteriów, na podstawie których CSIRT poziomu krajowego mógłby taką opinię wyrazić lub odmówić jej wyrażenia. Co więcej, czy bez wpisania do wykazu ISAC dany podmiot, mający zazwyczaj formę stowarzyszenia, nie będzie mógł działać? W tym kontekście należałoby również rozważyć procedurę odwoławczą od negatywnej opinii wydanej przez CSIRT poziomu krajowego, jak również kwestię podziału, do którego CSIRT poziomu krajowego powinny zwracać się ISAC zrzeszające np. OUK będących też operatorami infrastruktury krytycznej, jak również OUK nieposiadających infrastruktury krytycznej.  Konieczne jest doprecyzowanie proponowanego art. 4a ust. 4. Tak sztywna regulacja form ISACów nie jest celem ustawy o krajowym systemie cyberbezpieczeństwa. Co do zasady, ISAC jest inicjatywą oddolną w zależności od podsektora i nie powinna być regulowana odgórnie. | **Wyjaśnienie**  Przepis został zmieniony. Wpisanie ISAC do wykazu ISAC będą opiniowane przez wszystkie organy właściwe do spraw cyberbezpieczeństwa. Wynika to z faktu, że ISAC będą mogły działać na rzecz wielu podmiotów krajowego systemu cyberbezpieczeństwa.  Centra ISAC funkcjonujące w ramach ksc będą miały, za pomocą porozumienia zawartego z ministrem ds. informatyzacji, możliwość podłączenia się do systemu informacyjnego o którym mowa w art. 46 ustawy ksc. |
|  | **Koordynator Służb Specjalnych** | Art. 4a ust. 4 | **ISAC - centrum wymiany i analizy informacji na temat podatności, zagrożeń i incydentów**  Na wstępie wskazać należy, iż ISAC, w ramach krajowego systemu cyberbezpieczeństwa, ma pełnić rolę centrum wymiany i analizy informacji na temat podatności, zagrożeń i incydentów, funkcjonujące w celu wspierania podmiotów krajowego systemu cyberbezpieczeństwa (na co wskazuje definicja zawarta w projektowanym art. 2 pkt 3c ustawy *o krajowym systemie cyberbezpieczeństwa*). Dlatego też zasadna wydaje się rezygnacja z procedury opiniowania podmiotu, który ubiega się o wpisanie do wykazu ISAC, przez CSIRT-y poziomu krajowego. Wskazać należy, iż działalność ISAC nie będzie wiązała się z reagowaniem na incydenty bezpieczeństwa teleinformatycznego, dlatego też nie wydaje się zasadne opiniowanie takich podmiotów przez CSIRT-y poziomu krajowego.  W przypadku nieuwzględnienia powyższej uwagi pragnę podkreślić, że konieczne jest doprecyzowanie projektowanego art. 4a ust. 4 ustawy *o krajowym systemie cyberbezpieczeństwa* w zakresie dotyczącym opiniowania ISAC przez m.in. CSIRT GOV przed wpisaniem go przez ministra właściwego do spraw informatyzacji do „Wykazu ISAC” poprzez wskazanie:  1) zakresu zagadnień, które mają podlegać opiniowaniu przez CSIRT-y poziomu krajowego;  2) terminu na wydanie opinii;  3) formy prawnej, w jakiej należy wydać opinię;  4) skutków wydania opinii negatywnej;  5) czasu, po którym podmiot wnioskujący o wpisanie do wykazu ISAC może ponownie ubiegać się o wpisanie do przedmiotowego wykazu, w przypadku uzyskania opinii negatywnej.  Uzupełnienie przedmiotowego przepisu o ww. kwestie pozwoli na określenie trybu, w jakim ma odbywać się procedura opiniowania podmiotów ubiegających się o wpisanie do wykazu ISAC przez wszystkie CSIRT-y poziomu krajowego i umożliwi dokonanie realnej i wiarygodnej oceny takiego podmiotu. | **Uwaga częściowo uwzględniona**  Przepis został zmieniony. Wpisanie ISAC do wykazu ISAC będą opiniowane przez wszystkie organy właściwe do spraw cyberbezpieczeństwa. Wynika to z faktu, że ISAC będą mogły działać na rzecz wielu podmiotów krajowego systemu cyberbezpieczeństwa.  Centra ISAC funkcjonujące w ramach ksc będą miały, za pomocą porozumienia zawartego z ministrem ds. informatyzacji, możliwość podłączenia się do systemu informacyjnego o którym mowa w art. 46 ustawy ksc.  Działalność ISAC nie będzie operacyjna. |
|  | **Koordynator Służb Specjalnych** | Art. 4a (dodanie ust. 5) | Proponuję dodanie w projektowanym art. 4a po ust. 4 ustawy *o krajowym systemie cyberbezpieczeństwa* kolejnej jednostki redakcyjnej w brzmieniu: „4a. CSIRT MON lub CSIRT GOV mogą odstąpić od uzasadnienia opinii, o której mowa w ust. 4, w części lub w całości, jeżeli wymaga tego ważny interes bezpieczeństwa państwa”. Biorąc pod uwagę, iż istnieje szeroki katalog informacji jawnych istotnych z punktu widzenia bezpieczeństwa państwa, które można określić mianem informacji wrażliwych, należy umożliwić CSIRT GOV nieujawnianie ich w toku procedury opiniodawczej. Tego rodzaju informacje, jeżeli będą brane pod uwagę w toku rozstrzygania i opracowywania opinii, jak również będą stanowiły podstawę faktyczną wydanej opinii, nie powinny być ujawniane w uzasadnieniu do danej opinii. Nadto, ograniczenie jawności w postaci odstąpienia od uzasadnienia, dotyczące wyłącznie końcowej fazy procesu załatwiania sprawy, nie narusza powinności organu zgromadzenia w sprawie pełnego materiału dowodowego, dokumentującego ustalone w postępowaniu okoliczności faktyczne wykorzystane jako przesłanki dokonanego rozstrzygnięcia. | **Uwaga częściowo uwzględniona**  Przepis został zmieniony. Wpisanie ISAC do wykazu ISAC będą opiniowane przez wszystkie organy właściwe do spraw cyberbezpieczeństwa. Wynika to z faktu, że ISAC będą mogły działać na rzecz wielu podmiotów krajowego systemu cyberbezpieczeństwa.  Centra ISAC funkcjonujące w ramach ksc będą miały, za pomocą porozumienia zawartego z ministrem ds. informatyzacji, możliwość podłączenia się do systemu informacyjnego o którym mowa w art. 46 ustawy ksc.  Działalność ISAC nie będzie operacyjna. |
|  | **Ministerstwo Klimatu i Środowiska** | Art. 4a ust. 9 | Proponowane brzmienie w art. 4a ust. 9:  „9. ISAC współpracują z CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT sektorowymi i organami właściwymi.”  Proponuje się całkowite usunięcie przepisu dotyczącego przedkładania ministrowi ds. informatyzacji sprawozdań z realizacji zadań za poprzedni rok kalendarzowy. W konsekwencji zmiany art. 4a ust. 9 konieczne będzie uchylenie ust. 10.  ISACi powinny również współpracować z CSIRTami sektorowymi. Z racji podobieństw funkcjonalnych tych podmiotów oraz zbieżności w przetwarzanych informacjach powinna istnieć możliwość wymiany informacji. Ponadto, minister właściwy ds. informatyzacji nie nakłada na ISACi konkretnych zadań, ani nie akceptuje, jak również nie uzgadnia z nimi planów działalności na dany rok, więc bezzasadne jest obowiązkowe zdawanie sprawdzania. ISAC może funkcjonować jako niezależna spółka lub stowarzyszenie, w związku z tym powinien posiadać pewną suwerenność. Co więcej, nie można tutaj mówić również o sposobie rozliczalności, ponieważ zgodnie z ust. 10 planowanego art. 4a minister ds. informatyzacji powinien badać jedynie zgodność działalności ISAC z prawem i zasadami współpracy w ramach krajowego systemu cyberbezpieczeństwa. Ta ostatnia kwestia również jest dosyć nieostra, ponieważ jest to bardzo ogólne stwierdzenie | **Uwaga częściowo uwzględniona.**  Przepis zostanie rozdzielony na 2 jednostki redakcyjne.  W jednym zostanie rozszerzone, że  „9. ISAC współpracują z CSIRT MON, CSIRT NASK lub CSIRT GOV, CSIRT sektorowymi i organami właściwymi w szczególności w zakresie wymiany informacji, dobrych praktyk i doświadczeń dotyczących zagrożeń cyberbezpieczeństwa, podatności oraz incydentów”.  „10. ISAC przedkładają ministrowi właściwemu do spraw informatyzacji w terminie do dnia 31  marca każdego roku sprawozdanie z realizacji zadań za poprzedni rok kalendarzowy.”  Minister właściwy ds. informatyzacji na podstawie sprawozdań otrzymywanych corocznie od centrów ISAC jest w stanie ocenić, czy ich działalność jest zgodna z prawem oraz czy nie narusza zasad współpracy w ramach krajowego systemu cyberbezpieczeństwa. |
|  | **Ministerstwo Finansów Funduszy i Polityki Regionalnej** | art. 4a ust. 10 | Wyjaśnienia wymaga, czy minister może zarówno wystąpić o usunięcie nieprawidłowości do centrum wymiany i analizy informacji, jak i wykreślić je z urzędu z rejestru, czy mają to być odrębne działania. | **Wyjaśnienie**  Minister właściwy ds. informatyzacji będzie mógł na podstawie uzyskanych informacji wystąpić do ISAC o usunięcie stwierdzonych nieprawidłowości. Na podstawie rodzaju i stopnia wykazanych nieprawidłowości minister jeśli uzna, że nieprawidłowości w poważny sposób naruszają zasady współpracy w krajowym systemie cyberbezpieczeństwa lub przepisy prawa, może wykreślić ISAC z wykazu. Może również wystąpić taka sytuacja, że ISAC nie usunie nieprawidłowości, wskazanych przez ministra i minister będzie musiał wykreślić ISAC z wykazu. |
|  | **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. |
|  | **Koordynator Służb Specjalnych** | Art. 10 ust. 2 pkt 2 | W projektowanym art. 10 ust. 2 pkt 2 ustawy *o krajowym systemie cyberbezpieczeństwa* proponuje się rozszerzenie katalogu zdarzeń przed którymi należy chronić dokument o wyrażenie „uszkodzeniem”. Należy zwrócić uwagę, iż wprowadzenie dodatkowej przesłanki odnoszącej się do ochrony dokumentów przed przypadkowym zniszczeniem, utratą, nieuprawnionym dostępem, niewłaściwym użyciem lub utratą integralności w postaci ochrony również przed „uszkodzeniem” zapewni komplementarne podejście operatora usługi kluczowej do ochrony dokumentów. Ochrona przed uszkodzeniem powinna być rozumiana jako właściwy sposób postępowania z dokumentami, w tym ich przechowywania i rozliczania. | **Uwag uwzględniona**.  Przepis został uzupełniony. |
|  | **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 | Proponowane brzmienie w art. 14 ust. 2: „2. Operator usługi kluczowej powołuje SOC wewnątrz swojej struktury lub zawiera umowę dotyczącą realizacji całości lub części zadań SOC na jego zlecenie z innym podmiotem. SOC powołany przez operatora usługi kluczowej może realizować zadania, o których mowa w ust. 1, także na rzecz innych podmiotów.”  Aktualnie proponowana treść nowelizacji może być interpretowana jako wymagania albo całościowej realizacji zadań w zakresie cyberbezpieczeństwa własnymi siłami OUK albo zawarcia całościowej umowy realizacji tych zadań przez podmiot trzeci. W praktyce korzystne i możliwe (a często konieczne) jest tylko częściowe zlecenie tych zadań na zewnątrz. | **Wyjaśnienie**  Art. 14 ust. 2 należy czytać z ust. 4 pkt. 3. Operator usługi kluczowej może zawrzeć umowę z kilkoma podmiotami realizujących inne zadania o których mowa w art. 14 ust.1. |
|  | **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. |
|  | **Rządowe Centrum Legislacji** | Art. 14 Art. 14a | W związku z brzmieniem projektowanych art. 14 i art. 14a ustawy o KSC:   1. uzupełnienia o stosowne przepisy przejściowe i dostosowujące wymaga kwestia wykonania obowiązków, o których mowa w art. 8 do art. 13 ustawy o KSC w dotychczasowym brzmieniu. Z uwagi na zmianę podmiotu, który te obowiązki ma wykonać oraz regulację w zakresie terminu wykonania po raz pierwszy obowiązku informacyjnego, o którym mowa w projektowanym art. 14 ust. 4, rozstrzygnięcia wymaga w szczególności kwestia utrzymania w mocy dotychczasowych zgłoszeń, również ze względu na regulację art. 16 ustawy o KSC wskazującej wyraźnie terminy wykonania obowiązków przez operatora usług kluczowych, 2. wobec wprowadzenia obowiązku wpisu SOC do wykazu prowadzonego przez ministra właściwego do spraw informatyzacji wyjaśnienia wymaga, czy do wykazu SOC będą wpisane zespoły pełniące funkcję operacyjnego centrum bezpieczeństwa jedynie na rzecz innych podmiotów, czy także takie zespoły działające w wewnętrznych strukturach operatorów usług kluczowych. W przepisach przejściowych należy przewidzieć odpowiedni termin, w którym te podmioty powinny zostać zgłoszone do wykazu po raz pierwszy. | **Uwaga częściowo uwzględniona**  Zostaną dodane przepisy dostosowujące.  Dotychczas powołane w ramach OUK wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo stają się SOC powołanymi w ramach OUK.  Podmioty świadczące usługi z zakresu cyberbezpieczeństwa, z którym dotychczas OUK zawarł umowę stają się podmiotami prowadzącymi SOC na rzecz operatora usługi kluczowej.  W wykazie SOC będą zawarte dane wszystkich SOC, także powołanych w ramach OUK. Organy właściwe już teraz mają dane o podmiotach świadczących usługi z zakresu cyberbezpieczeństwa. Z chwilą wejścia w życie ustawy będą musiały złożyć wniosek o wpis do wykazu SOC. Z kolei operatorzy usług kluczowych, którzy po wejściu w życie nowelizacji zawrą umowę z podmiotem prowadzącym SOC będą musiały przekazać informacje o tej umowie do organu właściwego do spraw cyberbezpieczeństwa. |
|  | **Ministerstwo Klimatu i Środowiska** | Art. 14 ust. 5 | Brakuje wyrazu jest: „5. W przypadkach, kiedy jest to niezbędne dla zapewnienia cyberbezpieczeństwa,…” | **Uwaga uwzględniona.** |
|  | **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. 7 pkt 2 | **SOC oraz kwestie ochrony informacji niejawnych**  Przepis art. 14a ust. 2 ustawy *o krajowym systemie cyberbezpieczeństwa* zawiera wymóg posiadania przez zespół pełniący funkcję operacyjnego centrum bezpieczeństwa (SOC) dokumentu potwierdzającego zdolność do ochrony informacji niejawnych zgodnie z ustawą z dnia 5 sierpnia 2010 r. *o ochronie informacji niejawnych* (Dz. U z 2019 r. poz. 742), zwaną dalej „ustawą OIN”. Przepis ten budzi następujące wątpliwości:  1) ustawa OIN przewiduje, że dokumentem potwierdzającym zdolność przedsiębiorcy do ochrony informacji niejawnych o klauzuli „poufne” lub wyższej jest świadectwo bezpieczeństwa przemysłowego (art. 54 ust. 1 i 2 ustawy OIN). Dokument ten nie jest wydawany podmiotom innym niż przedsiębiorca w rozumieniu ustawy OIN - jeśli więc SOC miałby działać w ramach podmiotu niebędącego przedsiębiorcą, to nie mógłby posiadać takiego dokumentu. Ponadto świadectwo takie wydawane jest przedsiębiorcy, a nie jego części np. działającemu w jego ramach określonemu zespołowi;  2) świadectwo bezpieczeństwa przemysłowego ma zawsze określony stopień (jeden z trzech) i potwierdza zdolność do ochrony informacji niejawnych o określonej klauzuli tajności. Jeśli więc przedsiębiorca przedstawi np. świadectwo trzeciego stopnia potwierdzające jego zdolność do ochrony informacji niejawnych o klauzuli „poufne”, a zadania, które będzie musiał realizować wchodzący w jego skład SOC będą wymagały przetwarzania np. informacji niejawnych o klauzuli „tajne” we własnych obiektach przedsiębiorcy, to świadectwo, które umożliwi mu wpisanie do wykazu SOC będzie nieprzydatne. Dla realizacji tych zadań konieczne będzie bowiem uzyskanie świadectwa drugiego stopnia potwierdzającego zdolność przedsiębiorcy do ochrony informacji niejawnych o klauzuli „tajne”;  3) jeśli zadania, które ma wykonywać przedsiębiorca posiadający SOC będą jawne lub „zastrzeżone” to w ogóle nie będzie podstaw do uzyskania świadectwa.  Podsumowując, należy stwierdzić, że każda jednostka organizacyjna, w tym każdy przedsiębiorca, który ma przetwarzać informacje niejawne jest zobowiązany do stosowania przepisów ustawy OIN i wydanych na jej podstawie aktów wykonawczych. Wprowadzanie wymogów dotyczących ochrony informacji niejawnych do innych ustaw wydaje się bezcelowe i może prowadzić do błędnych interpretacji.  W związku z powyższym, proponuje się usunąć art. 14a ust. 7 pkt 2 z projektu, albo uzupełnić go w ten sposób, by zawierał, odnoszący się do przedsiębiorcy, wymóg przedstawienia świadectwa bezpieczeństwa przemysłowego odpowiedniego ze względu na klauzulę tajności oraz sposób przetwarzania informacji niejawnych, do których dostęp będzie wynikał z zadań realizowanych przez SOC tego przedsiębiorcy. | **Wyjaśnienie**  Opisywana kwestia dotyczy jedynie SOC nie będących częścią krajowego systemu cyberbezpieczeństwa lecz z uwagi na posiadany potencjał oraz deklarację współpracy z Państwem mogą zostać wpisane do wykazu SOC przez ministra właściwego do spraw informatyzacji i tym samym współuczestniczyć w rozwoju krajowego systemu cyberbezpieczeństwa. |
|  | **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 Finansów, Funduszy i Polityki Regionalnej** | art. 20c ust. 2,  art. 34a ust. 2 | Niezrozumiałe jest sformułowanie o "przekazywaniu zgłoszenia/informacji w postaci elektronicznej, a w przypadku braku możliwości - przy użyciu innych dostępnych środków komunikacji" - w pierwszej części jest mowa o postaci dokumentu, a nie o sposobie jego przesłania, zatem przepisy trzeba przeredagować (albo odnieść się tylko do sposobu przekazania, albo - do samej postaci dokumentu). | **Uwaga częściowo uwzględniona**  Kwestia dotycząca o formie przekazywania zgłoszenia incydentu i przekazywania informacji w formie elektronicznej zostanie poprawiona w ustawie wprowadzającej 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. |
|  | **Ministerstwo Klimatu i Środowiska** | Art. 22 ust. 1 pkt 2a | Pominięto wyraz „mowa”:  „2a) będący jednostką samorządu terytorialnego, niezależnie od obowiązku, o którym mowa w punkcie 2,…” | **Uwaga uwzględniona.** |
|  | **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. |
|  | **Rządowe Centrum Legislacji** | Art. 24a | W kontekście obowiązków nakładanych na wojewodów, w dodawanym art. 24a ustawy o KSC, konieczne jest rozstrzygnięcie, kiedy po raz pierwszy podmioty publiczne z terenu województwa mają przekazać do wojewody informacje dotyczące danych kontaktowych osób, które będą odpowiadały za kontakty z odpowiednim CSIRT, jak również kiedy po raz pierwszy właściwi wojewodowie przekażą marszałkom województwa, wójtom, burmistrzom i prezydentom miast informacje, o których mowa w projektowanym art. 24a ust. 3 ustawy o KSC. | **Uwaga częściowo uwzględniona**  Podmioty publiczne miały za zadanie wyznaczyć osobę odpowiedzialną za utrzymywanie kontaktów z zespołami CSIRT poziomu krajowego na podstawie obecnego art. 22 ust. 1 pkt 5. Obowiązek ten zostanie rozszerzony o wyznaczenie dwóch osób kontaktowych a także dodana zostanie kara za nie wyznaczenie tych osób.  Zostanie określony termin do kiedy JST przekażą dane kontaktowe osób wyznaczonych do wojewodów.  Informacje o których mowa w ust. 3 wojewodowie będą przekazywali JST w momencie otrzymania materiałów od Pełnomocnika lub zespołów CSIRT poziomu krajowego. Wskazany zakres informacji z uwagi na dynamikę procesów zachodzących w cyberbezpieczeństwie sprawia, że nie da się na sztywno określić terminu przekazywania ww. informacji. Będą one przekazywane, jeżeli wyniknie taka potrzeba. |
|  | **Koordynator Służb Specjalnych** | Art. 24a | **Wojewoda jako podmiot zapewniający wymianę informacji na temat zagrożeń cyberbezpieczeństwa, podatności oraz incydentów dotyczących podmiotów publicznych w województwie**  W projektowanym artykule 24a ustawy *o krajowym systemie cyberbezpieczeństwa* określono zadania wojewody w zakresie cyberbezpieczeństwa. Wśród tych zadań wskazano m. in.: zapewnienie wymiany informacji na temat zagrożeń cyberbezpieczeństwa, podatności oraz incydentów, prowadzenie listy danych kontaktowych osób wskazanych do współpracy z CSIRT-ami poziomu krajowego. Należy jednak zauważyć, że katalog podmiotów, wobec których wojewoda prowadzi wymianę informacji, o której mowa w projektowanym art. 24a ustawy *o krajowym systemie cyberbezpieczeństwa* jest zbyt szeroki, gdyż obejmuje on wszystkie podmioty publiczne w województwie. Wskazać w tym miejscu należy, iż w województwie mazowieckim podmiotami publicznymi będą zarówno jednostki samorządu terytorialnego, jak i urzędy centralne. Taki sposób określenia przedmiotowego katalogu będzie skutkował powieleniem zadań CSIRT-ów poziomu krajowego określonych w art. 26 ust. 3 ustawy *o krajowym systemie cyberbezpieczeństwa* w stosunku do podmiotów krajowego systemu cyberbezpieczeństwa. Dlatego też niezbędnym jest skorelowanie projektowanego art. 24a z obecnie obowiązującymi przepisami ustawy *o krajowym systemie cyberbezpieczeństwa.* | **Uwaga przyjęta**  **Art. 24a zostanie zawężony do jednostek samorządu terytorialnego.** |
|  | **Ministerstwo Sprawiedliwości** | Art. 24a pkt 1 i 2 | Zastrzeżenia budzi projektowany art. 24a pkt 1 i 2 ustawy o krajowym systemie cyberbezpieczeństwa, zgodnie z którym wojewoda zapewnia wymianę informacji na temat zagrożeń cyberbezpieczeństwa, podatności oraz incydentów dotyczących podmiotów publicznych w województwie, a także prowadzi listę danych kontaktowych osób z poszczególnych podmiotów publicznych w województwie, wskazanych przez kierownictwo tych podmiotów, do współpracy z właściwymi CSIRT MON, CSIRT NASK lub CSIRT GOV. W przepisie tym jest mowa o podmiotach publicznych przy jednoczesnym braku uszczegółowienia, iż chodzi o podmioty publiczne wymienione w art. 4 pkt 7-15 ustawy o krajowym systemie cyberbezpieczeństwa, tak jak to ma miejsce w pozostałych przepisach ustawy, co powoduje, że wszystkie podmioty publiczne, do których zastosowanie znajdują postanowienia ww. ustawy w tym także powszechne jednostki organizacyjne prokuratury, będą zobowiązane do przekazywania właściwym wojewodom informacji wskazanych w dodawanym art. 24a pkt 1 i 2. Takie rozwiązanie z punktu widzenia standardów i dobrych praktyk bezpieczeństwa informacji jest nie do zaakceptowania.  Należy przy tym zauważyć, że zgodnie z art. 21 ust. 1 ustawy o krajowym systemie cyberbezpieczeństwa podmiot publiczny, o którym mowa w art. 4 pkt 7-15 tej ustawy jest obowiązany do wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa, co w praktyce przekłada się na utworzenie kanału komunikacji z właściwym CSIRT, natomiast art. 22 ust. 1 pkt 2 ww. ustawy wprost nakazuje zgłaszanie incydentów przez podmiot publiczny bezpośrednio do właściwego CSIRT.  Mając zatem na uwadze powyższe, w projektowanym art. 24a pkt 1 i 2 ustawy o krajowym systemie cyberbezpieczeństwa sformułowanie „podmiotów publicznych” należy zastąpić sformułowaniem „jednostek samorządu terytorialnego”. | **Uwaga przyjęta**  **Art. 24a zostanie zawężony do jednostek samorządu terytorialnego.** |
|  | **Ministerstwo Finansów, Funduszy i Polityki Regionalnej** | Art. 24a pkt 3 | Błąd literowy - powinno być - przekazuje (...) prezydentom miast informacje (bez litery w); | **Uwaga uwzględniona** |
|  | **Rządowe Centrum Legislacji** | Art. 26 | W kontekście zmienionego katalogu podmiotów z art. 4 ustawy o KSC odpowiedniej zmiany wymaga art. 26 ustawy o KSC. Konieczne jest w szczególności rozstrzygnięcie, czy do właściwości, któregoś z CSIRT poziomu krajowego będą należały kwestie związane z przedsiębiorcami komunikacji elektronicznej czy wyłącznie właściwy w tym zakresie będzie CSIRT Teleco. | **Uwaga uwzględniona.**  Co do zasady CSIRT NASK, jednakże przepis zostanie doprecyzowany. |
|  | **Ministerstwo Finansów, Funduszy i Polityki Regionalnej** | art. 26 ust. 3 pkt 21 | Błąd redakcyjny - zapisy lit. c i d nie powinny być ujęte w pkt. 21 (brak ciągłości treściowej z pkt. 21 lit. a i b, natomiast powinny być wykazane jako kolejne jednostki redakcyjne w ramach ust. 3; | **Uwaga uwzględniona, przepis zostanie poprawiony** |
|  | **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 Finansów, Funduszy i Polityki Regionalnej** | Art. 36 ust. 6 | Należy doprecyzować nowe brzmienie art. 36 ust. 6 poprzez wpisanie "posiedzenia Zespołu" zamiast "jego posiedzenia"; | **Uwaga uwzględniona, przepis zostanie poprawiony.** |
|  | **Rządowe Centrum Legislacji** | Art. 44 | W zakresie zmiany art. 44 ustawy o KSC – projektowana zmiana w zakresie CSIRT sektorowego może wymagać rozstrzygnięcia w przepisach dostosowujących o statusie CSIRT KNF, o którym mowa w uzasadnieniu projektu (str. 26). Ponadto w zakresie dodawanych ust. 5 i 6 wyjaśnienia wymaga, czy odesłanie do art. 4 ustawy z dnia 11 września 2019 r. – *Prawo zamówień publicznych* (Dz. U. poz. 2019) powoduje jedynie wyznaczenie podmiotów, którym organ cyberbezpieczeństwa może powierzyć rolę CSIRT czy to odesłanie ma sugerować również zastosowanie trybu powierzenia wynikającego z przepisów tej ustawy. | **Uwaga uwzględniona**  Odnośnie CSIRT KNF – zostanie zaproponowany przepis dostosowujący.  Odesłanie do Prawa zamówień publicznych dotyczy wskazania podmiotów, nie chodzi o stosowanie trybu powierzenia wykonania zadania publicznego. |
|  | **Koordynator Służb Specjalnych** | Art. 44 ust. 1 | W projektowanym art. 44 ust. 1 ustawy *o krajowym systemie cyberbezpieczeństwa* projektodawca wskazał, że organ właściwy zapewnia funkcjonowanie CSIRT-u sektorowego, do którego zadań ma należeć:   1. przyjmowanie zgłoszeń o incydentach; 2. reagowanie na incydenty; 3. gromadzenie informacji o podatnościach i zagrożeniach, które mogą mieć negatywny wpływ na cyberbezpieczeństwo; 4. współpracę z operatorami usług kluczowych w zakresie wymiany dobrych praktyk oraz informacji o podatnościach i zagrożeniach, organizację i uczestniczenie w ćwiczeniach oraz wspieranie inicjatyw szkoleniowych.   Biorąc pod uwagę fakt, iż CSIRT sektorowy ma być odpowiedzialny za przyjmowanie zgłoszeń o incydentach i reagowanie na nie, należy doprecyzować, który CSIRT jest właściwy do podejmowania działań w zakresie zaistniałego incydentu. Zgodnie z art. 26 ust. 3 pkt 5 ustawy *o krajowym systemie cyberbezpieczeństwa*, obowiązek reagowania na zgłaszane incydenty należy również do CSIRT-ów poziomu krajowego. Faktem jest, iż zgodnie z pkt 10 ww. przepisu CSIRT-y poziomu krajowego zobligowane są do współpracy z sektorowymi zespołami cyberbezpieczeństwa w zakresie koordynowania obsługi incydentów poważnych, w tym dotyczących dwóch lub większej liczby państw członkowskich Unii Europejskiej i incydentów krytycznych oraz w zakresie wymiany informacji pozwalających przeciwdziałać zagrożeniom cyberbezpieczeństwa. Jednakże określenie, który CSIRT, czy to poziomu krajowego czy sektorowy (w przypadku gdy ten ostatni został powołany), jest właściwy do koordynacji incydentu, powinno zostać uregulowane na poziomie ustawowym. Taka regulacja pozwoli na uniknięcie wątpliwości interpretacyjnych i przyspieszy działania w przypadku wystąpienia incydentu. Kluczowe dla podmiotów zgłaszających jest bezpośrednie wskazanie, który z CSIRT-ów poziomu krajowego jest właściwy do koordynacji obsługi incydentu zgłaszanego przez ten podmiot. Pozostawienie przedmiotowej kwestii do uregulowania w drodze np. porozumień może spowodować mnożenie różnych wariantów postępowania i pojawianie się wątpliwości. Co więcej, należy dodatkowo wskazać, iż w przypadku, gdy podmiot znajduje się w wykazie infrastruktury krytycznej, wówczas obowiązki zgłaszania incydentów w stosunku do systemów teleinformatycznych wynikają z art. 32d ustawy z dnia 24 maja 2002 r. *o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu*.  Zgodnie z obecnym brzmieniem art. 11 ust. 1 ustawy *o krajowym systemie cyberbezpieczeństwa*, w przypadku wystąpienia incydentu poważnego, operator usługi kluczowej, m. in.:   1. zapewnia dostęp do informacji o rejestrowanych incydentach właściwemu CSIRT MON, CSIRT NASK lub CSIRT GOV w zakresie niezbędnym do realizacji jego zadań; 2. klasyfikuje incydent jako poważny na podstawie progów uznawania incydentu za poważny; 3. zgłasza incydent poważny niezwłocznie, nie później niż w ciągu 24 godzin od momentu jego wykrycia, do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOT; 4. współdziała podczas obsługi incydentu poważnego i incydentu krytycznego z właściwym CSIRT MON, CSIRT NASK łub CSIRT GOV, przekazując niezbędne dane, w tym dane osobowe.   Dodatkowo, zgodnie z ust. 3 przedmiotowego przepisu, w przypadku ustanowienia sektorowego zespołu cyberbezpieczeństwa operator usługi kluczowej niezależnie od zadań określonych w ust. 1:  1) przekazuje jednocześnie temu zespołowi w postaci elektronicznej zgłoszenie, o którym mowa ust. 1 pkt 4;  2) współdziała z tym zespołem na poziomie sektora lub podsektora podczas obsługi incydentu poważnego łub incydentu krytycznego, przekazując niezbędne dane, w tym dane osobowe.  Podsumowując, operator usługi kluczowej zobligowany jest zatem do współdziałania zarówno z CSIRT-em poziomu krajowego jak i CSIRT-em sektorowym. Obecnie brak jest regulacji wskazującej wprost, które rekomendacje mają być wdrożone przez podmiot w przypadku, gdy są one różne. W odniesieniu do powyższego, należy również mieć na uwadze, iż funkcjonariusz publiczny w przypadku niedopełnienia obowiązków może odpowiadać za czyn z art. 231 ustawy z dnia z dnia 6 czerwca 1997 r. - *Kodeks karny*. Przypadek taki może mieć miejsce w sytuacji, gdy instytucją zgłaszającą incydent jest podmiot publiczny, a właściwe działania nie zostaną podjęte. | **Uwaga częściowo uwzględniona**  W art. 26 ust. 3 pkt 5 – sformułowanie „reagowanie na incydenty” zostanie zastąpione sformułowaniem „koordynację reagowania na zgłoszone incydenty”. Dzięki temu będzie jasne, że CSIRT sektorowy reaguje na incydenty a CSIRT poziomu krajowego koordynuje reagowanie na incydenty. |
|  | **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 Finansów, Funduszy i Polityki Regionalnej** | Art. 44 w ust. 1 pkt. 4 i 5 | Błędy literowe, odpowiednio zamiast "organizację"; powinno być "organizacja", zamiast "wymianę" powinno być "wymiana", w dodawanym ust. 6 pkt 1, końcowy zapis "a także mając na względzie" nie ma kontynuacji i wydaje się zbędny; | **Uwaga uwzględniona** |
|  | **Ministerstwo Klimatu i Środowiska** | Art. 44 ust. 1 pkt 5 | Proponowane brzmienie w art. 44 w ust. 1 pkt 5:  „5) współpraca z CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT sektorowymi w zakresie wymiany informacji i reagowania na incydenty poważne i krytyczne oraz wymianę informacji o zagrożeniach.”  W zmienianym art. 44 ust. 1 pkt 5 jest mowa o współpracy CSIRT sektorowego z innymi CSIRT poziomu krajowego. Proponuje się dodanie zapisu o współpracy z innymi CSIRT sektorowymi, ponieważ część podatności czy zagrożeń może dotyczyć dwóch różnych sektorów. W takiej sytuacji nie ma zapisu pozwalającego na taką kooperację. | **Uwaga uwzględniona**  Proponowane brzmienie art. 44 ust. 1 uzupełniono o pkt 6 według którego CSIRT sektorowe będą mogły wymieniać się informacjami wyłącznie o podatnościach i zagrożeniach. |
|  | **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. |
|  | **Ministerstwo Finansów, Funduszy i Polityki Regionalnej** | Art. 44a w ust. 4 pkt 4 i 5 | Zawierają błędy literowe, odpowiednio zamiast "organizację"; powinno być "organizacja"; zamiast "wymianę" powinno być "wymiana"; | **Uwaga uwzględniona, przepis zostanie poprawiony.** |
|  | **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 Finansów, Funduszy i Polityki Regionalnej** | Art. 46 w ust. 2 | W dodawanym pkt 2b celową może być zmiana zapisu "inne niż wskazane w ust. 2" na "inne niż wskazane w ust. 2 i 2a", ponieważ - ust. 2a dotyczy CSIRT sektorowych i CSIRT Telco, które "korzystają" z systemu teleinformatycznego w zakresie swojej właściwości, natomiast ust. 2b dotyczy podmiotów, które "mogą korzystać" z systemu teleinformatycznego na podstawie porozumienia z właściwym ministrem. Zapis w pkt 2b wyłącza z konieczności uzyskania pozwolenia podmioty wskazane w ust. 2, natomiast nie wyłącza z tej konieczności podmiotów wskazanych w ust. 2a, które podobnie jak podmioty wskazane w ust. 2 „korzystają z systemu” z tym, że w węższym zakresie swojej właściwości; | **Uwaga uwzględniona** |
|  | **Ministerstwo Klimatu i Środowiska** | Art. 46 ust 2b | **Jeżeli nie zostało to uwzględnione to należy dodać do reguły budżetowej środki na przystąpienie CSIRT sektorowych do S46.**  Proponowane brzmienie w art. 46 ust. 2b:  „2b. Podmioty krajowego systemu cyberbezpieczeństwa, inne niż wskazane w ust. 2 i 2a, mogą korzystać z systemu teleinformatycznego, o którym mowa w ust. 1, na podstawie porozumienia zawartego z ministrem właściwym do spraw informatyzacji.”  Zmieniany art. 46 wskazuje w ust. 2a, że CSIRT sektorowe korzystają z systemu teleinformatycznego, o którym mowa w ust. 1, w zakresie swojej właściwości. Tym samym, CSIRT sektorowe zostały zobligowane do korzystania z S46 w ramach swojej działalności. Z racji tego, że ta usługa jest płatna czy w nowelizacji ustawy zostały przewidziane środki finansowe na przystąpienie do tego systemu?  Ust. 2b odnosi się do podmiotów krajowego systemu cyberbezpieczeństwa, innych niż wskazane w ust 2. – należy dodać również ust. 2a, ponieważ w tej konfiguracji zapisy ust. 2a i 2b się wykluczają. Wynika to z faktu, że ust. 2b wprowadza dobrowolność korzystania z S46, a 2a mówi o obligatoryjności. | **Uwaga częściowo uwzględniona**  Ustęp 2b zostanie uzupełniony zgodnie z propozycją. |
|  | **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. |
|  | **Rządowe Centrum Legislacji** | Art. 62 ust. 1 pkt 7 | W zakresie zmiany dokonywanej w art. 62 ustawy o KSC (dodawany pkt 7 w ust. 1) należy zwrócić uwagę, że Pełnomocnikowi Rządu do spraw Cyberbezpieczeństwa, którego głównym celem jest koordynowanie działań i realizacji polityki rządu w zakresie zapewnienia cyberbezpieczeństwa, powierzono wydawanie ostrzeżeń i poleceń zabezpieczających, zatem rolę władczą organu administracji publicznej. Takie samo zadanie powierzono, na mocy dodawanego punktu 8 w art. 65 ust. 1 ustawy o KSC, również Kolegium do spraw Cyberbezpieczeństwa, zwanego dalej „Kolegium”. Powierzenie organowi o charakterze koordynacyjnym i zakresie zadań zbliżonym do organów pomocniczych Rady Ministrów kompetencji władczych budzi wątpliwości, zwłaszcza wobec braku jasnych kryteriów dokonywania oceny i dookreślenia procedury w tym zakresie. | **Uwaga uwzględniona.**  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). |
|  | **Ministerstwo Klimatu i Środowiska** | Art. 65 ust. 1 pkt 7 | Proponowane brzmienie w art. 65 w ust. 1 pkt 7:  „7) ocena ryzyka dostawcy sprzętu lub oprogramowania:”  Zmiana w pkt 7 w zakresie zmiany spójnika „i” na „lub”. | **Uwaga uwzględniona**  Przepis zostanie poprawiony. |
|  | **Rządowe Centrum Legislacji** | Art. 66a | W zakresie dodawanego art. 66a ustawy o KSC należy wskazać, że projektowany przepis wymaga ponownej, gruntownej analizy i odpowiedniej zmiany. Projektowane przepisy przewidują sporządzanie przez Kolegium oceny dostawcy ryzyka sprzętu lub oprogramowania istotnego dla cyberbezpieczeństwa podmiotów krajowego systemu cyberbezpieczeństwa, która to analiza jest dokonywana na wniosek członka tego Kolegium. Ocena jest dokonywana bez udziału dostawcy sprzętu lub oprogramowania. Przepisy ani nie przewidują procedury dokonania tej oceny, ani nie odsyłają w tym zakresie do innych regulacji proceduralnych, w tym Kodeksu postępowania administracyjnego, co skutkuje powstaniem luk prawnych. W tym miejscu należy wskazać, iż oceny sprzętu lub oprogramowania na podstawie art. 33 ustawy o KSC mogą dokonywać CSIRT poziomu krajowego, zaś badanie to ma na celu „*identyfikację podatności, której wykorzystanie może zagrozić w szczególności integralności, poufności, rozliczalności, autentyczności lub dostępności przetwarzanych danych, które może mieć wpływ na bezpieczeństwo publiczne lub istotny interes bezpieczeństwa państwa*”.  Natomiast projektowana w dodawanym art. 66a ustawy o KSC procedura ma charakter oceny podmiotowej dostawcy usług lub oprogramowania, o której nie jest on informowany na etapie sporządzania oceny czy wniosku o ocenę składanego przez członka Kolegium. Zgodnie z projektowanym art. 66a ust. 4 ustawy o KSC, który we wprowadzeniu do wyliczenia posługuje się zwrotem „*w szczególności”*, projektowane przepisy nie przewidują zamkniętego katalogu przesłanek oceny dostawcy usług i oprogramowania, co może prowadzić do dokonywania tej oceny w sposób dowolny. Projektowane przepisy nie wskazują również, na podstawie jakich środków dowodowych będą weryfikowane przesłanki, o których mowa w art. 66a ust. 4 ustawy o KSC. Ponadto sposób dokonywania tej oceny również nie został wskazany w przedstawionym projekcie. Ponownej analizy wymaga także projektowana procedura informowania o wyniku rozstrzygnięcia oceny ryzyka. Zgodnie z projektowanymi przepisami po sporządzeniu oceny komunikat o poziomie oceny ryzyka dostawcy jest publikowany w Dzienniku Urzędowym RP „Monitor Polski” i dopiero po opublikowaniu dostawca ma możliwość odwołania się od oceny dokonanej przez Kolegium, przy czym termin na wniesienie odwołania wynosi 14 dni od dnia ogłoszenia, zaś termin na rozpatrzenie sprawy przez Kolegium wynosi dwa miesiące. Brak informacji o toczącym się postępowaniu, a także brak udziału dostawcy na pierwszym etapie postępowania przed Kolegium powoduje, że procedura odwoławcza przewidziana w projektowanych przepisach może spotkać się z zarzutem iluzoryczności. Dostawca, aby dowiedzieć się o ocenie, będzie zmuszony do codziennego monitorowania dzienników urzędowych, a każde przeoczenie komunikatu o negatywnej ocenie może skutkować brakiem faktycznej możliwości skutecznego zaskarżenia oceny w przewidzianym terminie. Przepisy w zaproponowanym kształcie mogą spotkać się z zarzutem naruszenia art. 78 Konstytucji RP. Ponadto ponownej analizy wymaga także projektowana procedura salwatoryjna dla dostawcy usług lub oprogramowania, którego ryzyko oceniono jako niskie lub umiarkowane (projektowany art. 66a ust. 7 ustawy o KSC). Zgodnie z brzmieniem tego przepisu dostawca, którego ryzyko oceniono na niskie lub umiarkowane może przedstawić Kolegium środki zaradcze lub plany naprawcze, które pozwolą zniwelować ryzyko w ocenie Kolegium. Projektodawca nie rozstrzyga, czy przedstawienie tych środków oznacza wniesienie sprzeciwu od oceny Kolegium, nie określa trybu ich przedstawiania, nie wskazuje także jakie środki zaradcze lub plany naprawcze mógłby podjąć ten podmiot celem zmiany oceny ryzyka dokonanej przez Kolegium. W dodawanym w art. 66a ust. 9 ustawy o KSC Projektodawca przewiduje, że ocena może zostać zmieniona, jeżeli zajdą uzasadnione okoliczności, ale jedynie na wniosek członka Kolegium. Powyższe może spotkać się z zarzutem nieproporcjonalności wobec skutków, jakie wywołuje ocena ryzyka dostawcy. Dodatkowo należy zauważyć, że Projektodawca nie wskazuje, jaki skutek, w stosunku do pierwotnej oceny ryzyka, miałaby spowodować jej zmiana – czy formalnoprawnie dochodziłoby do uchylenia komunikatu Pełnomocnika czy może do jego nowelizacji. | **Uwaga uwzględniona**  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.  Zwrot „w szczególności w ust. 4 zostanie wykreślony”. |
|  | **Koordynator Służb Specjalnych** | Art. 66a | **Ocena ryzyka dostawcy sprzętu i oprogramowania**  W projektowanym art. 66a ustawy *o krajowym systemie cyberbezpieczeństwa* został uregulowany nowy rodzaj postępowania mającego na celu ocenę ryzyka dostawcy sprzętu i oprogramowania istotnego dla cyberbezpieczeństwa podmiotów krajowego systemu cyberbezpieczeństwa. Elementami przedmiotowego postępowania są:  1) analiza zagrożeń bezpieczeństwa narodowego o charakterze ekonomicznym, kontrwywiadowczym i terrorystycznym oraz zagrożeń dla realizacji zobowiązań sojuszniczych i europejskich, jakie stanowi dostawca sprzętu i oprogramowania;  2) ocena prawdopodobieństwa, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej, uwzględniająca:   * stopień i rodzaj powiązań pomiędzy dostawcą sprzętu lub oprogramowania i tym państwem, * prawodawstwo tego państwa w zakresie ochrony praw obywatelskich i praw człowieka, * prawodawstwo w zakresie ochrony danych osobowych, zwłaszcza tam gdzie nie ma porozumień w zakresie ochrony danych między UE i danym krajem, * strukturę własnościową dostawcy sprzętu lub oprogramowania, * zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania;   3) liczba i rodzaje, jak również sposób i czas eliminowania wykrytych podatności oraz incydentów;  4) stopień, w jakim dostawca sprzętu lub oprogramowania sprawuje nadzór nad procesem wytwarzania i dostarczania sprzętu lub oprogramowania oraz ryzyka dla procesu wytwarzania i dostarczania sprzętu lub oprogramowania;  5) treść wydanych wcześniej rekomendacji (...) dotyczących sprzętu lub oprogramowania.  Należy również zwrócić uwagę na zakres informacji podlegających badaniu w jego toku — w szczególności analizę zagrożeń bezpieczeństwa narodowego o charakterze ekonomicznym, kontrwywiadowczym i terrorystycznym oraz zagrożeń dla realizacji zobowiązań sojuszniczych i europejskich, jakie stanowi dostawca sprzętu i oprogramowania. Zasadne wydaje się doprecyzowanie na poziomie ustawowym trybu ustalania i przekazywania tego stanowiska przez zespoły analityczne do Kolegium do spraw Cyberbezpieczeństwa oraz trybu ustalania stanowiska przez Kolegium.  Warto również w tym miejscu podkreślić, iż analiza dotycząca oceny ryzyka dostawcy sprzętu i oprogramowania istotnego dla cyberbezpieczeństwa podmiotów krajowego systemu cyberbezpieczeństwa ma obejmować także liczbę i rodzaje, jak również sposób i czas eliminowania wykrytych podatności oraz incydentów, nie wskazując jednocześnie w jaki sposób podmiot dokonujący analizy ma pozyskać takie dane.  Kolejną kwestią, dotyczącą projektowanego art. 66a ustawy *o krajowym systemie cyberbezpieczeństwa*, budzącą wątpliwości jest to, iż projektodawca w projektowanych przepisach posługuje się sformułowaniem „dostawca sprzętu lub oprogramowania”, nie wskazując kim on *de facto* jest. Dostawcą może nie być producent albo wytwórca oprogramowania czy urządzenia, a podmiot trzeci, pośredniczący w umowach kupna-sprzedaży, jak również może to być także przedstawiciel handlowy. W związku z powyższym należy doprecyzować projektowane regulacje poprzez wskazanie, czy ocena określająca wysokie ryzyko dostawcy sprzętu będzie miała również zastosowanie w stosunku do tego samego sprzętu, ale pozyskanego od innego podmiotu.  Dodatkowo, projekt ustawy nie przewiduje rozwiązania w przypadku, gdy ocena określająca wysokie ryzyko obejmie specyficzne urządzenia czy oprogramowanie, które jest unikatowe, a na rynku brak jest alternatywnych rozwiązań technicznych umożliwiających jego zastąpienie.  Wątpliwości budzi również kwestia, czy skutek oceny określającej wysokie ryzyko będzie obejmował też komponenty wchodzące w skład innych urządzeń np. serwerów. | **Uwaga częściowo uwzględniona**  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.  Pojęcie dostawcy sprzętu lub oprogramowania w art. 66a odnosi się do definicji zawartych w art. 2 dostawcy oraz produktów ICT, usług ICT, procesów ICT  Definicja dostawcy odnosi się do definicji producenta, upoważnionego dystrybutora, importera, dystrybutora według przepisów Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 765/2008 z dnia 9 lipca 2008 r. ustanawiające wymagania w zakresie akredytacji i nadzoru rynku odnoszące się do warunków wprowadzania produktów do obrotu i uchylające rozporządzenie (EWG) nr 339/93  Zgodnie z tym rozporządzeniem:   * „producent” to każda osoba fizyczna lub prawna, która wytwarza produkt lub która zleca zaprojektowanie lub wytworzenie produktu i oferuje ten produkt pod własną nazwą lub znakiem towarowym; * „upoważniony przedstawiciel” to osoba fizyczna lub prawna mająca siedzibę we Wspólnocie, posiadająca pisemne pełnomocnictwo od producenta do występowania w jego imieniu w zakresie określonych zadań w odniesieniu do obowiązków producentów wynikających z odpowiedniego prawodawstwa wspólnotowego; * „importer” to każda osoba fizyczna lub prawna, mająca siedzibę we Wspólnocie, wprowadzająca na rynek wspólnotowy produkt z kraju trzeciego; * „dystrybutor” to każda osoba fizyczna lub prawna w łańcuchu dostaw, inna niż producent lub importer, która udostępnia produkt na rynku.   Definicje produktów ICT, procesów ICT oraz usług ICT odwołują się do Aktu o cyberbezpieczeństwie.  Odwołanie się do tych definicji kompleksowo wskazuje, kto może być dostawcą sprzętu lub oprogramowania. |
|  | **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 Sprawiedliwości** | Art. 66a ust. 4 | W myśl projektowanego art. 66a ust. 4 ustawy o krajowym systemie cyberbezpieczeństwa, w sporządzaniu oceny przeprowadza się w szczególności analizę zagrożeń bezpieczeństwa narodowego o charakterze ekonomicznym, kontrwywiadowczym i terrorystycznym oraz zagrożeń dla realizacji zobowiązań sojuszniczych i europejskich, jakie stanowi dostawca sprzętu i oprogramowania; prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, uwzględniającą: stopień i rodzaj powiązań pomiędzy dostawcą sprzętu lub oprogramowania i tym państwem, prawodawstwo tego państwa w zakresie ochrony praw obywatelskich i praw człowieka, prawodawstwo w zakresie ochrony danych osobowych, zwłaszcza tam gdzie nie ma porozumień w zakresie ochrony danych między UE i danym państwem, strukturę własnościową dostawcy sprzętu lub oprogramowania, a także zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. W pierwszej kolejności należy wskazać, iż podobnie jak w przypadku uwagi zgłoszonej w pkt 7, odwołania zastosowane w projektowanym przepisie do dostawcy, należy zastąpić odwołaniami do sprzętu i oprogramowania. Ponadto projektowany przepis budzi wątpliwości, gdyż zastosowano w nim szereg nieostrych i niedookreślonych zwrotów, np. „wpływ”, „znajdować się pod wpływem”, „prawdopodobieństwo”, „zdolność ingerencji państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania” (za taką ingerencję można uznać np. działania organów podatkowych czy inspekcji sanitarnej). Dyskusyjne jest przy tym również podnoszenie kwestii oceny „prawodawstwa tego państwa w zakresie ochrony praw obywatelskich i praw człowieka” ze względu na ogólność, a co za tym idzie możliwość bardzo szerokiej interpretacji. Po drugie, jak powszechnie wiadomo – państwo może z jednej strony w aktach prawnych gwarantować wysoki poziom ochrony praw człowieka i praw obywatelskich, a jednocześnie nie zapewniać skutecznych mechanizmów ich ochrony.  Z kolei odnosząc się do kwestii weryfikacji dostawcy sprzętu i oprogramowania można sięgnąć do rozwiązań przyjętych w ustawie z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2019 r. poz. 742) dotyczących przedsiębiorców zamierzających ubiegać się albo ubiegających się o zawarcie umów związanych z dostępem do informacji niejawnych lub wykonujących takie umowy albo wykonujących na podstawie przepisów prawa zadania związane z dostępem do informacji niejawnych. Zgodnie z art. 57 ust. 2 ww. ustawy sprawdzenie przedsiębiorcy, w tym na podstawie danych zawartych w rejestrach, ewidencjach, kartotekach, także niedostępnych powszechnie, obejmuje strukturę kapitału oraz powiązania kapitałowe przedsiębiorcy, źródła pochodzenia środków finansowych i sytuację finansową, strukturę organizacyjną, system ochrony informacji niejawnych, w tym środki bezpieczeństwa fizycznego, wszystkie osoby wchodzące w skład organów zarządzających, kontrolnych oraz osoby działające z ich upoważnienia, a także w szczególnie uzasadnionych przypadkach osoby posiadające poświadczenia bezpieczeństwa. W związku z tym wydaje się, że skoro wyżej wskazany zakres weryfikacji został przez ustawodawcę uznany za wystarczający przy dopuszczeniu przedsiębiorców do dostępu do informacji niejawnych, w przypadku dostawców sprzętu i oprogramowania można postąpić analogicznie, uzupełniając jednak o badanie regulacji w zakresie ochrony danych osobowych, zwłaszcza tam gdzie nie ma porozumień w zakresie ochrony danych między UE i danym państwem.  W związku z powyższym projektowany art. 66a ust. 4 ustawy o krajowym systemie cyberbezpieczeństwa powinien otrzymać brzmienie: „W sporządzaniu oceny przeprowadza się w szczególności:  1) analizę zagrożeń bezpieczeństwa narodowego o charakterze ekonomicznym, kontrwywiadowczym i terrorystycznym oraz zagrożeń dla realizacji zobowiązań sojuszniczych i europejskich, jakie stanowi sprzęt i oprogramowanie;  2) sprawdzenie przedsiębiorcy, w tym na podstawie danych zawartych w rejestrach, ewidencjach, kartotekach, także niedostępnych powszechnie, które obejmuje:  a) strukturę kapitału oraz powiązania kapitałowe przedsiębiorcy, źródła pochodzenia środków finansowych i sytuację finansową,  b) strukturę organizacyjną,  c) prawodawstwo w zakresie ochrony danych osobowych, zwłaszcza tam gdzie nie ma porozumień w zakresie ochrony danych między UE i danym państwem,”.  Jednocześnie należy wspomnieć, że projektodawca nie przewidział w projekcie kwestii spełnienia przez sprzęt norm międzynarodowych (tworzonych przez ISO, ITU, IEC; przede wszystkim norm z serii ISO 27000 – obowiązujących w Polsce jako polskie normy PN-EN ISO/IEC 27001:2017-06) lub uznanych przez UE norm bezpieczeństwa informacji, lub przez UE tworzonych (przez europejskie organizacje normalizacyjne wymienione w załączniku I do rozporządzenia 1025/2012 w sprawie normalizacji europejskiej, tj. rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1025/2012 z dnia 25 października 2012 r. w sprawie normalizacji europejskiej, zmieniające dyrektywy Rady 89/686/EWG i 93/15/EWG oraz dyrektyw Parlamentu Europejskiego i Rady 94/9/WE, 94/25/WE, 95/16/WE, 97/23/WE, 98/34/WE, 2004/22/WE, 2007/23/WE, 2009/23/WE i 2009/105/WE oraz uchylające decyzję rady 87/95/EWG i decyzję parlamentu europejskiego i rady nr 1673/2006/WE z dnia 25 października 2012 r., Dz.Urz.UE. 2012 L 316/12), czy uzyskania odpowiednich certyfikatów. | **Uwaga częściowo uwzględniona**  Odwołania do kryterium oceny w ust. 4 Pkt 2 lit b zostanie wykreślone.  W kontekście kryterium „zdolność ingerencji państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania” mowa jest o możliwości wpływania rządu państwa pochodzenia dostawcy na swobodę prowadzenia działalności gospodarczej w tym m.in. odgórnego wskazywania miejsca, gdzie dany sprzęt może być produkowany.  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.  Badanie z art. 33 dotyczy identyfikacji podatności sprzętu lub technologii używanych przez podmioty krajowego systemu cyberbezpieczeństwa.  Ponadto ocenie będą podlegać także kwestie dotyczące tego, czy dany sprzęt lub oprogramowanie spełnia powszechnie uznane standardy międzynarodowe w tym wydane przez m.in. ISO, ETSI, czy GSMA. Należy także brać pod uwagę europejskie certyfikaty cyberbezpieczeństwa, które będą wydawane w oparciu o regulacje zawarte w Akcie o cyberbezpieczeństwie – na podstawie którego powstają Europejskie Ramy Certyfikacji Cyberbezpieczeństwa produktów usług i procesów.W tym m.in. celu w ramach Grupy Współpracy NIS z inicjatywy Niemiec i Polski powstała ekspercka pod-grupa, której celem jest opracowania projektu europejskiego programu badan i certyfikacji 5G. |
|  | **Ministerstwo Finansów** | Art. 66a ust. 4 | Błąd literowy – zamiast „W sporządzania oceny” powinno być „W trakcie sporządzania oceny…”, ust. 4 pkt 1 - zapis „dostawca sprzętu i oprogramowania”, wskazanym jest jego skorygowanie na „dostawca sprzętu lub oprogramowania”, zgodnie z pozostałymi zapisami art. 66 a, w których jest mowa o „dostawcy sprzętu lub oprogramowania”, w ust. 4 pkt 2 – zamiast „uwzględniającą” powinno być – „uwzględniając”, | **Uwaga uwzględniona** |
|  | **Ministerstwo Klimatu i Środowiska** | Art. 66a ust.4 | Brakuje wyrazu „procesie”:  „4. W procesie sporządzania oceny przeprowadza się w szczególności:” | **Uwaga uwzględniona**  Przepis zostanie zmieniony według propozycji MF. |
|  | **Ministerstwo Obrony Narodowej** | Art. 66a ust. 4  Pkt 1  Pkt 2  Pkt 2 lit. b i c | **W art. 1 pkt 29 *projektu* -** projektowanemu art. 66a ust. 4 *ustawy o ksc* proponuje się nadać następujące brzmienie:  *„4. W ramach sporządzania oceny przeprowadza się w szczególności analizę:*   1. *zagrożeń bezpieczeństwa państwa o charakterze ekonomicznym, wywiadowczym i terrorystycznym oraz zagrożeń dla realizacji zobowiązań sojuszniczych i europejskich, jakie stanowi dostawca sprzętu lub oprogramowania;* 2. *prawdopodobieństwa, czy dostawca sprzętu lub oprogramowania znajduje się pod kontrolą państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego wskazującą:* 3. *stopień i rodzaj powiązań pomiędzy dostawcą sprzętu lub oprogramowania i tym państwem,* 4. *prawodawstwo oraz stosowanie prawa przez to państwo w zakresie ochrony praw obywatelskich i praw człowieka,* 5. *prawodawstwo oraz stosowanie prawa w zakresie ochrony danych osobowych, zwłaszcza tam gdzie nie ma porozumień w zakresie ochrony danych między Unią Europejską i danym państwem,* 6. *strukturę własnościową dostawcy sprzętu lub oprogramowania,* 7. *zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy lub oprogramowania;* 8. *liczby i rodzajów oraz sposobu i czasu eliminowania wykrytych podatności i incydentów, jeśli wystąpiły;* 9. *stopnia, w jakim dostawca sprzętu lub oprogramowania sprawuje nadzór nad procesem wytwarzania i dostarczania sprzętu lub oprogramowania oraz ryzyka dla procesu wytwarzania i dostarczania sprzętu;* 10. *treści wydanych wcześniej rekomendacji, o których mowa w art. 33, dotyczących sprzętu lub oprogramowania danego dostawcy.”.*   Proponowane w projektowanym art. 66a ust. 4 zmiany dotyczą:   * art. 66a ust. 4 pkt 1 - zastąpienia wyrazu „kontrwywiadowczym” wyrazem „wywiadowczym” – zadania kontrwywiadu koncentrują się na neutralizowaniu działań obcych służb wywiadowczych, w związku z czym wyszczególnione w przepisie zagrożenie powinny stanowić ewentualne działania wywiadowcze (a nie kontrwywiadowcze); * art. 66a ust. 4 pkt 1 – łączący wyrazy *sprzętu i oprogramowania* spójnik „i” proponuje się zastąpić spójnikiem „lub”. Wskazane przedmioty (sprzęt, oprogramowanie) nie muszą występować w portfelu działalności dostawcy łącznie. W związku z powyższym proponuje się zastąpienie koniunkcji alternatywą łączną - powyższe koreluje np.: z wprowadzeniem do wyliczenia w ust. 4 pkt 2. 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 następującym brzmieniu: „dostawcy sprzętu, oprogramowania lub usług”; * art. 66a ust. 4 pkt 2 – wyrazy „pod wpływem” proponuje się zastąpić wyrazami „pod kontrolą”; * art. 66a ust. 4 pkt 2 lit. b i c – proponuje się dodanie także kwestii stosowania prawa; * korekt redakcyjnych.   Jednocześnie należy wskazać, że wątpliwości budzi ograniczenie kwestii zagrożeń do kontroli nad podmiotami krajów spoza UE lub nie będących w NATO. Wydaje się, że w zakresie cyberbezpieczeństwa powinny być brane pod uwagę wszelkie ryzyka dotyczące celowego ograniczenia stopnia bezpieczeństwa sprzętu lub oprogramowania niezależnie od źródła pochodzenia zagrożenia. W związku z tym rozważenia wymaga rozszerzenie kręgu podmiotowego w tym zakresie. | **Uwaga częściowo uwzględniona**  W dotychczasowymust 4 w pkt 1 słowo „kontrwywiadowczym” zostało zamieniona na „wywiadowczym”.  W dotychczasowym art. 66a ust. 4 pkt 1 przepis został poprawiony na „dostawcą sprzętu lub oprogramowania”.  W dotychczasowym art. 66a ust. 4 pkt 2 wyrazy „pod wpływem” zostały zamienione wyrazami „pod kontrolą”.  Projekt zostanie poprawiony pod kątem redakcyjnym.  Dotychczasowy art. 66a ust. 4 pkt 2 lit c został uzupełniony o kwestii stosowania regulacji dotyczących ochrony danych osobowych.  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**.** |
|  | **Ministerstwo Sprawiedliwości** | Art. 66a ust. 5 | Zgodnie z projektowanym art. 66a ust. 5 ustawy o krajowym systemie cyberbezpieczeństwa, sporządzona przez Kolegium ocena ryzyka dostawcy sprzętu lub oprogramowania określa: wysokie ryzyko, jeżeli dostawca sprzętu lub oprogramowania stanowi poważne zagrożenie dla cyberbezpieczeństwa państwa i zmniejszenie poziomu tego ryzyka przez wdrożenie środków technicznych lub organizacyjnych nie jest możliwe, albo umiarkowane ryzyko, jeżeli dostawca sprzętu lub oprogramowania stanowi poważne zagrożenie dla cyberbezpieczeństwa państwa a zmniejszenie poziomu tego ryzyka możliwe jest przez wdrożenie środków technicznych lub organizacyjnych, albo niskie ryzyko, jeżeli dostawca sprzętu lub oprogramowania stanowi niewielkie zagrożenie dla cyberbezpieczeństwa państwa, albo brak zidentyfikowanego poziomu ryzyka, jeżeli nie stwierdzono zagrożenia dla cyberbezpieczeństwa państwa lub jego poziom jest znikomy. Zaproponowane rozwiązanie należy uznać za wadliwe, ponieważ brak w nim zachowania stopniowania zagrożenia w przypadku umiarkowanego i wysokiego ryzyka (pomijając w tym miejscu kwestie semantyczne – wydaje się, że „umiarkowane ryzyko” od „poważnego” dzieli znacznie więcej niż „niskie” od „umiarkowanego”, a nadto zestawienie „umiarkowane ryzyko” i „poważne zagrożenie” nie prezentuje się najlepiej) – w obu wypadkach jest to „poważne” ryzyko. Oba omawiane stopnie ryzyka ma odróżniać „możliwość zmniejszenia poziomu ryzyka przez wdrożenie środków technicznych lub organizacyjnych” – w przypadku ryzyka poważnego, zdaniem projektodawcy, nie ma takiej możliwości. Trudno wskazać taką sytuację. Wydaje się, że w rzeczywistości taki stan może nigdy nie zaistnieć. Jedynym rozwiązaniem jest rezygnacja z tego warunku i zastosowanie stopniowana zagrożenia. Czyli przyjąć należy, że wysoki stopień ryzyka charakteryzuje się bardzo poważnym (czy wyjątkowym, szczególnym lub znaczącym) zagrożeniem, poważny stopień (zamiast umiarkowany) stopień ryzyka – poważnym zagrożeniem. | **Uwaga częściowo uwzględniona**  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. |
|  | **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 Obrony Narodowej** | Art. 66a ust. 6 | **Art. 1 pkt 29 *projektu*** - w projektowanym art. 66a ust. 6 wskazano, że sporządzona przez Kolegium ocena ryzyka dostawcy sprzętu lub oprogramowania ogłaszana jest w postaci komunikatu w Dzienniku Urzędowym „Monitor Polski”. Mając jednak na względzie, że niektóre informacje, w tym w szczególności stanowiące informacje pochodzące od służb kontrwywiadowczych lub wywiadowczych, będą miały charakter informacji niejawnych, proponuje się ww. przepisowi nadanie brzmienia:  *„6. Sporządzona przez Kolegium jawna część oceny ryzyka dostawcy sprzętu lub oprogramowania przekazywana jest Pełnomocnikowi, który ogłasza ją w postaci komunikatu w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski.””.* | **Uwaga częściowo uwzględniona.**  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie prowadzone przez ministra właściwego ds. informatyzacji. Ocena ryzyka będzie wydana w formie decyzji administracyjnej.  Zostanie dodany przepis umożliwiający częściowe ograniczenie uzasadnienia decyzji ze względu na interes bezpieczeństwa Państwa (zgodnie z art. 107 par. 5 Kpa). |
|  | **Ministerstwo Sprawiedliwości** | Art. 66a ust. 7 | W myśl projektowanego art. 66a ust. 7 ustawy o krajowym systemie cyberbezpieczeństwa, w przypadku określenia umiarkowanego lub niskiego ryzyka, dostawca sprzętu lub oprogramowania, którego dotyczy ta ocena dostawcy sprzętu lub oprogramowania, może przedstawić Kolegium środki zaradcze i plan naprawczy. W przypadku akceptacji tych środków zaradczych i planu naprawczego, Kolegium może zmienić ocenę. Opiniowany przepis należy uzupełnić o wskazanie przypadku określenia wysokiego ryzyka (co jest konsekwencją ewentualnej zmiany projektowanego art. 66a ust. 5 lit a) oraz zastąpienie sformułowania „Kolegium może zmienić ocenę” sformułowaniem „Kolegium zmienia ocenę”. W przypadku bowiem, gdy podmiot przedstawił Kolegium środki zaradcze i plan naprawczy, zmiana oceny powinna mieć charakter obligatoryjny. Ponadto należy usunąć powtórzone sformułowanie, tj. „dostawca sprzętu lub oprogramowania”. W ten sposób omawiany przepis uzyskałby następujące brzmienie: „W przypadku określenia wysokiego, umiarkowanego lub niskiego ryzyka, dostawca sprzętu lub oprogramowania, którego sprzętu lub oprogramowania dotyczy ta ocena, może przedstawić Kolegium środki zaradcze i plan naprawczy. W przypadku akceptacji tych środków zaradczych i planu naprawczego, Kolegium zmienia ocenę.”. | **Uwaga częściowo uwzględniona**  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.  Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Z tego też powodu nie będzie konieczne przygotowywanie planów naprawczych, gdyż decyzje administracyjne będą odnosiły się tylko do dostawców wysokiego ryzyka. W wyniku decyzji administracyjnej podmioty wskazane w art. 66b będą musiały wycofać sprzęt lub oprogramowania od dostawcy wysokiego ryzyka. |
|  | **Ministerstwo Klimatu i Środowiska** | Art. 66a ust. 8 | We wprowadzonym art. 66a ust. 8 jest mowa tylko o tym, że wyłącznie dostawca sprzętu lub oprogramowania, którego dotyczy ocena określająca wysokie ryzyko może odwołać się w terminie 14 dni od publikacji komunikatu o sporządzonej ocenie do Kolegium. Proponuje się zastosować procedurę administracyjną zgodną z KPA i umożliwiającą procedurę odwoławczą dla dostawców sprzętu lub oprogramowania, których dotyczy ocena określająca wysokie, umiarkowane i niskie ryzyko. Decyzja administracyjna powinna być wydana przez ministra właściwego ds. informatyzacji. | **Uwaga uwzględniona**  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie prowadzone przez ministra właściwego ds. informatyzacji. Ocena ryzyka będzie wydana w formie decyzji administracyjnej. |
|  | **Ministerstwo Sprawiedliwości** | Art. 66a ust. 8 | Zgodnie z projektowanym art. 66a ust. 8 ustawy o krajowym systemie cyberbezpieczeństwa, dostawca sprzętu lub oprogramowania którego dotyczy ocena określająca wysokie ryzyko może odwołać się w terminie 14 dni od publikacji komunikatu o sporządzonej ocenie do Kolegium. Kolegium rozpatruje odwołanie w ciągu 2 miesięcy od otrzymania. Wniesienie odwołania nie wstrzymują działania określone w art. 66b. W pierwszej kolejności należy wskazać, że projektowany przepis pozbawia prawa do weryfikacji decyzji organu I instancji części dostawców – prawo odwołania przyznano jedynie tym dostawcom sprzętu lub oprogramowania, których dotyczy ocena określająca wysokie ryzyko. Ponadto w treści przepisu mowa jest o odwołaniu, a faktycznie jest to wniosek o ponowne rozpatrzenie sprawy. Wymaga to wyraźnego wskazania, gdyż Kolegium nie znajduje się wśród organów wskazanych w art. 127 § 3 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (Dz. U. z 2020 r. poz. 256, 695 i 1298), tj. podmiotów, od których nie służy odwołanie, jednakże strona niezadowolona z decyzji może zwrócić się do tego organu z wnioskiem o ponowne rozpatrzenie sprawy, w związku z tym należy postulować umieszczenie stosownego odesłania do przepisów ustawy – Kodeks postępowania administracyjnego (zob. uwagi do art. 67 opiniowanego projektu). Ponadto wskazana jest rezygnacja z rygoru natychmiastowej wykonalności decyzji z mocy prawa z uwagi na jej nieodwracalne skutki przy uwzględnieniu, iż istnieje możliwość nadania takiego rygoru na podstawie 108 § 1 ustawy – Kodeks postępowania administracyjnego. | **Uwaga częściowo przyjęta**  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie prowadzone przez ministra właściwego ds. informatyzacji. Ocena ryzyka będzie wydana w formie decyzji administracyjnej.  Ponadto z uwagi decyzje administracyjne otrzymają rygor natychmiastowej wykonalności tak jak to jest teraz rozwiązane w art. 5 ust 7 ustawy o ksc, w którym jest mowa, o decyzji o uznaniu za operatora usługi kluczowej.  Podmioty krajowego systemu cyberbezpieczeństwa, operatorzy infrastruktury krytycznej, przedsiębiorcy o szczególnym znaczeniu gospodarczo obronnym, przedsiębiorcy telekomunikacyjni których będą dotyczyły skutki wydania decyzji o wysokim ryzyku będą miały 7 lat na wycofanie sprzętu, oprogramowania lub usług. Ze względu na charakter sprawy – zagrożenie dla bezpieczeństwa narodowego – decyzja ta będzie podlegała natychmiastowej wykonalności. |
|  | **Ministerstwo Rozwoju, Pracy i Technologii** | Art. 66a ust. 8 | Proponuje się wskazanie innego niż Kolegium organu odwoławczego. Dzięki temu dostawca otrzyma większą gwarancję, że jego sprawa zostanie gruntownie rozpatrzona po raz drugi przez niezależną od Kolegium instancję. | **Uwaga uwzględniona**  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie prowadzone przez ministra właściwego ds. informatyzacji. Ocena ryzyka będzie wydana w formie decyzji administracyjnej. Dostawcy będzie przysługiwać wniosek o ponowne rozpatrzenie sprawy i skarga do sądu administracyjnego na decyzję. |
|  | **Ministerstwo Sprawiedliwości** | Art. 66b | W myśl projektowanego art. 66b ustawy o krajowym systemie cyberbezpieczeństwa, w przypadku sporządzenia oceny ryzyka określającej wysokie ryzyko dostawcy sprzętu lub oprogramowania podmioty krajowego systemu cyberbezpieczeństwa nie wprowadzają do użytkowania sprzętu, oprogramowania i usług określonych w ocenie danego dostawcy sprzętu lub oprogramowania; wycofują z użytkowania sprzęt, oprogramowanie i usługi określone w ocenie danego dostawcy sprzętu lub oprogramowania nie później niż 5 lat od dnia ogłoszenia komunikatu o ocenie. W przypadku sporządzenia oceny określającej umiarkowane ryzyko dostawcy sprzętu lub oprogramowania podmioty krajowego systemu cyberbezpieczeństwa: nie wprowadzają do użytkowania sprzętu, oprogramowania i usług określonych w ocenie danego dostawcy sprzętu lub oprogramowania; mogą kontynuować użytkowanie dotychczas posiadanych egzemplarzy sprzętu, oprogramowania oraz rodzaju i liczby usług wykorzystywanych przed opublikowaniem komunikatu o ocenie danego dostawcy sprzętu lub oprogramowania.  Należy zauważyć, że w projektowanym art. 66b ww. ustawy brak jest przepisów dotyczących odszkodowań za zobowiązanie podmiotów krajowego systemu bezpieczeństwa, którego ryzyko oceniono jako wysokie do wycofania z użytkowania sprzętu, oprogramowanie i usługi określone w ocenie danego dostawcy sprzętu lub oprogramowania nie później niż 5 lat od dnia ogłoszenia komunikatu o ocenie. Odszkodowania takie powinny również przysługiwać podmiotom, które zostaną zobowiązane do niewprowadzania do użytkowania sprzętu, oprogramowania i usług określonych w ocenie danego dostawcy sprzętu lub oprogramowania w wypadku, gdy sprzęt ten, oprogramowanie lub usługi, zostały wykupione, ale nie zostały wprowadzone do eksploatacji (projektowany art. 67b ust. 1 pkt 1, art. 67b ust. 2 pkt 1). Uzasadnieniem konieczności wprowadzenia powyższego rozwiązania jest okoliczność, że w wyniku działania państwa zgodnie z prawem, polegającym na wydaniu nowej regulacji, podmioty te poniosą niezawinione przez nie straty finansowe związane z koniecznością zakupu nowego sprzętu, oprogramowania i usług. | **Uwaga częściowo uwzględniona**  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.  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 |
|  | **Ministerstwo Spraw Zagranicznych** | Art. 66b | Ponadto projekt ustawy stanowi, że w przypadku oceny określającej wysoki stopień ryzyka dostawcy podmioty krajowego systemu cyberbezpieczeństwa wycofują z użytkowania sprzęt, oprogramowanie i usługi określone w ocenie danego dostawcy sprzętu lub oprogramowania nie później niż 5 lat od dnia ogłoszenia komunikatu o ocenie. Mowa o tym jest w propozycji zapisu art. 66b. 1. 2) na str. 20 projektu oraz w uzasadnieniach na str. 32 i 42. Oceny długości okresu na wycofanie sprzętu, oprogramowania lub usługi nie należą do bezpośrednich kompetencji MSZ, ale warto zwrócić uwagę, że inne kraje członkowskie NATO czy UE - jak np. Wielka Brytania czy Francja szykują 7 letnie okresy przejściowe na wycofanie sprzętu (co jest uzasadnione m.in. czasem starzenia się i amortyzacji używanego obecnie sprzętu, o który oparte są działające sieci 4G i 3G). | **Uwaga uwzględniona**  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. |
|  | **Ministerstwo Rozwoju, Pracy i Technologii** | Art. 66b ust. 1 i 2 | W związku z powyższym, celem zapewnienia kompletności regulacji projektowanego art. 66b ust. 1 i 2, w ustawie Pzp proponuje się rozważenie, przy zachowaniu zgodności z dyrektywami UE, uwzględnienia poziomu ryzyka dostawcy sprzętu lub usług jako przesłankę odrzucenia oferty. Obecnie art. 226 ust. 1 pkt 17 ustawy PZP wskazuje, jako przesłankę odrzucenia oferty to, że obejmuje ona urządzenia informatyczne lub oprogramowanie wskazane w rekomendacji, o której mowa w art. 33 ust. 4 ustawy o krajowym systemie cyberbezpieczeństwa, stwierdzającej ich negatywny wpływ na bezpieczeństwo publiczne lub bezpieczeństwo narodowe. **Proponuje się zatem rozważenie zmodyfikowania ww. przesłanki odrzucenia oferty w sposób zapewniający spójność systemową proponowanych regulacji, tj. uwzględniając, że zakup sprzętu, oprogramowania lub usługi od dostawcy o ryzyku wysokim, czy nawet umiarkowanym, byłby sprzeczny z zasadą celowego i racjonalnego wydatkowania środków publicznych, gdyż taki sprzęt, oprogramowanie lub usługa nie mogłaby być, zgodnie z art. 66b ust. 1 i 2, wprowadzona do użytkowania.** W tym miejscu należy zauważyć, że odrzuceniu nie podlegałaby oferta wykonawcy w ogóle nie poddanego ocenie. W tym stanie rzeczy, zamawiający musiałby mieć jednak możliwość zweryfikowania tej okoliczności. Powyższe zaś skłania do zauważenia, że projektowane art. 66a-66c, jak i inne projektowane przepisy, zdają się nie wskazywać, na jakich zasadach informacja o dostawcy, którego ryzyko oceniono jako wysokie albo umiarkowane, miałaby zostać udostępniona zamawiającemu. | **Wyjaśnienie**  W ramach prac nad projektem ustawy zrezygnowano ze zmian w Prawie zamówień publicznych. Podmioty zobowiązane z mocy ustawy do wycofania sprzętu lub oprogramowania pochodzącego od dostawcy wysokiego ryzyka nie będą mogli zamawiać tego sprzętu lub oprogramowania od dostawcy wysokiego ryzyka poprzez zamówienia publiczne, jeżeli stosuje się do nich przepisy ustawy PZP. |
|  | **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 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. 66c | Kolejną kwestią, która budzi wątpliwości na gruncie projektowanego art. 66c ustawy *o krajowym systemie cyberbezpieczeństwa* jest procedura wycofywania sprzętu lub oprogramowania. Przedmiotowy przepis przewiduje, iż w szczególnie uzasadnionych przypadkach Pełnomocnik może zobowiązać podmiot krajowego systemu cyberbezpieczeństwa, do którego zastosowanie ma ocena, do sporządzenia i dostarczenia w ciągu 3 miesięcy planu i harmonogramu wycofania z użytkowania sprzętu, oprogramowania i usług dostawcy, w przypadku wydania oceny określającej wysokie ryzyko. Plan i harmonogram podlegać ma zatwierdzeniu przez Pełnomocnika po uzgodnieniu z organem właściwym do spraw cyberbezpieczeństwa. Organy właściwe do spraw cyberbezpieczeństwa zostały określone w art. 41 ustawy *o krajowym systemie cyberbezpieczeństwa* i obejmują jedynie organy właściwe dla poszczególnych sektorów i dostawców usług kluczowych. Natomiast w przypadku podmiotów publicznych, które również mogą być zobligowane do przedstawienia planu i harmonogramu wycofania sprzętu, oprogramowania i usług, ani obecnie obowiązujące przepisy ustawy *o krajowym systemie cyberbezpieczeństwa*, ani przedmiotowy projekt ustawy nie przewidują powołania organów właściwych do spraw cyberbezpieczeństwa. W związku z powyższym proponuje się doprecyzowanie projektowanych regulacji poprzez wskazanie podmiotu, z którym Pełnomocnik będzie uzgadniał plan i harmonogram wycofania sprzętu, oprogramowania i usług w przypadku podmiotów publicznych, w tym w szczególności jednostek samorządu terytorialnego. | **Uwaga uwzględniona**  Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Z tego też powodu nie będzie konieczne przygotowywanie planów naprawczych, gdyż decyzje administracyjne będą odnosiły się tylko do dostawców wysokiego ryzyka. |
|  | **Ministerstwo Finansów** | art. 66c ust. 2 | Niezrozumiałe jest pojęcie "organu właściwego dla danego sektora", niewystępujące w zmienianej ustawie. | **Uwaga uwzględniona**  Przepis zostanie poprawiony. |
|  | **Ministerstwo Spraw Zagranicznych** | Art. 66a-66c | I. Uwagi do projektu (str. 18/19) dotyczące punktu 29) po art. 66 dodaje się art. 66a-66c obecnie w brzmieniu:  „Art. 66a. […]  4. W sporządzania oceny przeprowadza się w szczególności:  1) analizę zagrożeń bezpieczeństwa narodowego o charakterze ekonomicznym, kontrwywiadowczym i terrorystycznym oraz zagrożeń dla realizacji zobowiązań sojuszniczych i europejskich, jakie stanowi dostawca sprzętu i oprogramowania;  2) prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, uwzględniającą:  a) stopień i rodzaj powiązań pomiędzy dostawcą sprzętu lub oprogramowania i tym państwem,  b) prawodawstwo tego państwa w zakresie ochrony praw obywatelskich i praw człowieka,  c) prawodawstwo w zakresie ochrony danych osobowych, zwłaszcza tam gdzie nie ma porozumień w zakresie ochrony danych między UE i danym państwem,  d) strukturę własnościową dostawcy sprzętu lub oprogramowania,  e) zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania”.  W pkt. 4. 1) proponuje się dodać słowo „obronnym" lub „wojskowym" po słowie „ekonomicznym", gdyż katalog zagrożeń wymieniony w przepisie nie przywołuje zagrożeń o charakterze obronnym/wojskowym.  W pkt. 4. 1) proponuje się dodać słowo „może" przed słowem „stanowić", gdyż zanim dostawca zostanie oceniony i otrzyma negatywną ocenę nie należy z góry ogłaszać, iż stanowi zagrożenie.  W pkt. 4. 2) po słowie „państwa” proponuje się dodać „szczególnie” – nie można wykluczyć, że sprawdzeniu poddana winna zostać firma zarejestrowana np. w jednym z krajów UE. W przypadku akceptacji tej uwagi adekwatną zmianę należy uwzględnić w uzasadnieniu na str. 41 projektu.  W pkt. 4. 2) e) proponuje się usunąć słowo "gospodarczej", gdyż istotne jest ingerowanie państwa w różne elementy działalności firmy - nie tylko w swobodę działalności gospodarczej.  Do rozważenia jest też zmiana kolejności propozycji liter a) do e) w pkt. 4. 2) na następującą: a) e) d) b) c), gdyż taka kolejność jest przejściem od zagrożeń ogólnych na poziomie państwa do bardziej szczególnych dotyczących jednostki. | **Uwaga częściowo uwzględniona**  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.  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.  Celem przedsiębiorcy jest prowadzenie działalności gospodarczej. Stąd też ocena ryzyka będzie obejmowała także analizę zdolności ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania.  Kolejność jest prawidłowa. |
|  | **Rządowe Centrum Legislacji** | Art. 66b-c | W zakresie projektowanych art. 66b-66c ustawy o KSC, z uwagi na fakt, że kreują one zakazy, które wpływają na ograniczenie wolności działalności gospodarczej, a ich skutki mogą prowadzić nawet do naruszenia istoty tej wolności, w świetle art. 22 Konstytucji RP, konieczna jest ich ocena z perspektywy ochrony interesu publicznego oraz zasady proporcjonalności, o której mowa w art. 31 ust. 3 Konstytucji RP. | **Uwaga uwzględniona.** Uzasadnienie projektu ustawy zostanie uzupełnione o test proporcjonalności.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie prowadzone przez ministra właściwego ds. informatyzacji. Ocena ryzyka będzie wydana w formie decyzji administracyjnej |
|  | **Koordynator Służb Specjalnych** | Art. 67a | **Wydawanie ostrzeżeń i poleceń zabezpieczających przez Pełnomocnika, po uzyskaniu opinii Kolegium ds. Cyberbezpieczeństwa**  Wydawanie ostrzeżeń na podstawie obecnych przepisów, zgodnie z art. 26 ust 3 ustawy *o krajowym systemie cyberbezpieczeństwa,* jest zastrzeżone wyłączenie dla CSIRT-ów ze względu na ich ściśle techniczne aspekty. Ostrzeżenia wydawane są jako reakcja na identyfikowane zagrożenia lub zagrożenia wynikające z analiz zgłaszanych incydentów, wobec czego kluczowym wyznacznikiem skuteczności ostrzeżenia jest stosunkowo szybka ścieżka ich wydawania i dystrybucji. Wydłużony czas opracowania może spowodować, iż ostrzeżenie będzie nieskuteczne ze względu na znaczne rozprzestrzenienie się zagrożenia lub też jego neutralizację przez inne działania.  W przedmiotowym zakresie projektowane przepisy stanowią, że wydanie ostrzeżenia czy polecenia zabezpieczającego ma poprzedzić przeprowadzenie, we współpracy z Zespołem do spraw Incydentów Krytycznych, analizy uzasadniającej ich wydanie. Analiza ma obejmować:  1) istotność zagrożenia cyberbezpieczeństwa;  2) prawdopodobieństwo wystąpienia incydentu krytycznego;  3) skutki finansowe, społeczne i prawne wydania ostrzeżenia łub polecenia zabezpieczającego;  4) skuteczność alternatywnych metod zapewnienia cyberbezpieczeństwa.  Odnosząc się do powyższego wypada zauważyć, że ocena skutków finansowych czy skuteczność alternatywnych metod zapewniania cyberbezpieczeństwa będzie trudna do przeprowadzenia. Ostrzeżenie lub polecenie podlega opiniowaniu przez Kolegium do spraw cyberbezpieczeństwa, które możliwe jest do pominięcia w nagłych przypadkach. Przewidziana została także konsultacja przeprowadzana przez Pełnomocnika z podmiotami, których ostrzeżenie lub polecenie ma dotyczyć. Biorąc zatem pod uwagę powyższą procedurę, a także np. tryb pracy Kolegium do spraw Cyberbezpieczeństwa, ewentualna ścieżka wydania takiego ostrzeżenia w projektowanym trybie będzie stosunkowo długa, a w efekcie może nie przynieść spodziewanego rezultatu.  Ostrzeżenie może dotyczyć *stricte* technicznych aspektów, m.in.:  1) polecenia zastosowania określonej poprawki bezpieczeństwa w sprzęcie lub oprogramowaniu posiadającym daną podatność;  2) nakazu szczególnej konfiguracji sprzętu lub oprogramowania, zabezpieczającej przed wykorzystaniem określonej podatności;  3) nakazu wprowadzenia reguły ruchu sieciowego zakazującego połączeń z określonymi adresami IP lub nazwami URL.  W związku z powyższym trzeba brać także pod uwagę ewentualne negatywne skutki dla systemów teleinformatycznych m. in. podmiotów prywatnych, np. dysfunkcję systemów i systemów powiązanych ze względu na zastosowaną poprawkę. Gestor systemu wraz z administratorami są w stanie ocenić wpływ wgrywanych poprawek na świadczoną usługę. Wydaje się zatem, że celowe byłoby wprowadzenie rozwiązania zbliżonego do regulacji w art. 32e ustawy z dnia 24 maja 2002 r. *o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu*, w ramach którego, w stosunku do wydanych rekomendacji podmioty mogą wnieść do Szefa Agencji Bezpieczeństwa Wewnętrznego zastrzeżenia do rekomendowanych sposobów podniesienia poziomu bezpieczeństwa systemów teleinformatycznych z uwagi na negatywny wpływ rekomendowanych działań na funkcjonalność systemu lub powstanie nowych podatności.  W kontekście ostrzeżeń i poleceń zabezpieczających wydawanych przez Pełnomocnika, polegających na zakazie korzystania z określonego sprzętu lub oprogramowania, nakazie wstrzymania dystrybucji lub zakazie instalacji określonej wersji oprogramowania, należy rozważyć rozszerzenie projektowanych regulacji o kwestie uwzględnienia skutków wydania takich ostrzeżeń i poleceń zabezpieczających. Projektowane przepisy przewidują dla podmiotów krajowego systemu cyberbezpieczeństwa okresy na dostosowanie się do skutków jakie wywołuje ocena ryzyka dostawcy sprzętu i oprogramowania. Takiego rozwiązania nie przewidziano jednak w przypadku ostrzeżeń i poleceń zabezpieczających; co więcej, nie wskazano jednocześnie sposobu w jaki podmioty mają wykonać obowiązki wynikające z ostrzeżeń i poleceń zabezpieczających, jeżeli ich realizacja może znacząco wpłynąć na zadania realizowane przez ten podmiot. Dodatkowo projektodawca przewiduje w projektowanym art. 73 ust. 1 pkt 14 ustawy *o krajowym systemie cyberbezpieczeństwa* karę pieniężną dla operatora usługi kluczowej, który nie zastosował się do polecenia zabezpieczającego, nie określając jednocześnie wysokości tej kary pieniężnej. W związku z powyższym zasadne wydaje się uzupełnienie i doprecyzowanie projektowanych regulacji o ww. kwestie. | **Uwaga częściowo przyjęta**  Przepisy art. 67a -67c zostaną zmienione. Ostrzeżenia w dalszym ciągu będzie wydawał Pełnomocnik. Natomiast polecenia zabezpieczające będą wydawane w formie decyzji administracyjnej przez ministra właściwego do spraw informatyzacji, co oznacza, że podmiot będzie mógł odwołać się od danej decyzji. Zatem także minister właściwy do spraw informatyzacji będzie podejmował decyzje o ewentualnych karach także w formie decyzji administracyjnej. Przepis art. 73 zostanie uzupełniony o wysokość kary za nie zastosowanie się do polecenia zabezpieczającego.  Zrezygnowano z opiniowania ostrzeżenia i polecenia zabezpieczającego przez Kolegium.  W myśl art. 26 ust. 3 pkt 4 zespoły CSIRT poziomu krajowego mogą wydać jedynie komunikaty o zidentyfikowanych zagrożeniach cyberbezpieczeństwa. Komunikat, o którym w art. 26 ust 3 pkt 4 nie może być ostrzeżeniem, gdyż ostrzeżenie będzie dotyczyło możliwości wystąpienia incydentu krytycznego. W ostrzeżeniu Pełnomocnik nie tylko wskaże potencjalne zagrożenie, ale również zaleci sposób ograniczenia ryzyka wystąpienia incydentu krytycznego.  Do tej pory ani Pełnomocnik ani zespoły CSIRT nie mogły wydawać ostrzeżeń w formie proponowanej w nowelizacji. Pełnomocnik może wydawać rekomendacje dla podmiotów krajowego systemu cyberbezpieczeństwa na podstawie art. 33 ustawy o ksc.  Ostrzeżenie wydawane przez Pełnomocnika wskaże rodzaj zagrożenia, które uprawdopodobni wystąpienie incydentu krytycznego. Ponadto w ostrzeżeniu wskazane zostanie zakres podmiotowy, czyli Pełnomocnik określi, które podmioty dane ostrzeżenie dotyczy. Ostrzeżenie będzie zawierało także listę zalecanych działań, które podmioty powinny wdrożyć w celu ograniczenia ryzyk związanych z prawdopodobieństwem wystąpienia incydentu krytycznego. Przykładem takich zaleceń jest np. zwrócenie uwagi na określony typ zachowań czy incydentów. Pełnomocnik będzie przeprowadzał nie rzadziej niż raz na rok przegląd wydanych ostrzeżeń w celu ustalenia czy spełniają ustawową przesłankę ich wydania.  Natomiast polecenie zabezpieczające odnosi się do sytuacji związanej z wystąpieniem incydentu krytycznego. Minister właściwy ds. informatyzacji w oparciu o informacje otrzymywane od m.in. zespoły CSIRT poziomu krajowego oraz ustalenia podjęte na Zespole ds. Incydentów Krytycznych będzie mógł podjąć decyzję o podjęciu konkretnych działań w związku z reagowaniem na incydent krytyczny. M. in. nakaz określonego zachowania przez podmioty, których dotyczy polecenie w tym np. zabezpieczenie określonych informacji czy zakaz instalacji określonej wersji oprogramowania.  Należy podkreślić, że szybkość reakcji w przypadku wystąpienia incydentu krytycznego jest kluczowa w procesie ograniczenia skutków tego incydentu. |
|  | **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 Sprawiedliwości** | Art. 67a | Zgodnie z projektowanym art. 67a ustawy o krajowym systemie cyberbezpieczeństwa, pełnomocnik może wydać ostrzeżenie – w przypadku uzyskania informacji o zagrożeniu cyberbezpieczeństwa, która uprawdopodobni możliwość wystąpienia incydentu krytycznego, polecenie zabezpieczające – w przypadku wystąpienia incydentu krytycznego – po zatwierdzeniu przez Kolegium. W szczególnie uzasadnionych przypadkach, na wniosek Zespołu, Pełnomocnik może wydać ostrzeżenie lub polecenie zabezpieczające, które nie zostało zatwierdzone przez Kolegium. Pełnomocnik niezwłocznie informuje Kolegium o zastosowanych ostrzeżeniach lub poleceniach zabezpieczających. Ogłoszone ostrzeżenia lub polecenia zabezpieczające wymagają zatwierdzenia przez Kolegium na najbliższym posiedzeniu. (…) W przypadku odmowy zatwierdzenia przez Kolegium Pełnomocnik odwołuje ostrzeżenie lub polecenie zabezpieczające w części lub w całości albo stosuje wydaje inne ostrzeżenie lub polecenie zabezpieczające.  Należy zauważyć, że zgodnie z projektowanym przepisem, Pełnomocnik może wydać ostrzeżenia i polecenia zabezpieczające we współdziałaniu z Kolegium. W tym wypadku zastosowanie powinny znaleźć przepisy art. 106 i art. 106a ustawy – Kodeks postępowania administracyjnego, regulujące kwestię współdziałania organów. W związku z powyższym konieczne jest przeprowadzenie następujących zmian w projektowanym art. 67a ustawy o krajowym systemie cyberbezpieczeństwa: „Art. 67a. 1. Pełnomocnik może wydać:  1) ostrzeżenie - w przypadku uzyskania informacji o zagrożeniu cyberbezpieczeństwa, która uprawdopodobni możliwość wystąpienia incydentu krytycznego,  2) polecenie zabezpieczające - w przypadku wystąpienia incydentu krytycznego  – po wyrażeniu opiniiprzez Kolegium.  (…) 8. W przypadku wyrażenia negatywnej opinii Kolegium Pełnomocnik odwołuje ostrzeżenie lub polecenie zabezpieczające w części lub w całości albo stosuje wydaje inne ostrzeżenie lub polecenie zabezpieczające.”. | **Wyjaśnienie**  Przepisy zostały zmienione. Polecenie zabezpieczające odnosi się do sytuacji związanej z wystąpieniem incydentu krytycznego. Minister właściwy ds. informatyzacji w oparciu o informacje otrzymywane od m.in. zespoły CSIRT poziomu krajowego oraz ustalenia podjęte na Zespole ds. Incydentów Krytycznych będzie mógł podjąć decyzję o podjęciu konkretnych działań w związku z reagowaniem na incydent krytyczny. M. in. Nakaz określonego zachowania przez podmioty, których dotyczy polecenie w tym np. zabezpieczenie określonych informacji czy zakaz instalacji określonej wersji oprogramowania.  Należy podkreślić, że szybkość reakcji w przypadku wystąpienia incydentu krytycznego jest kluczowa w procesie ograniczenia skutków tego incydentu. |
|  | **Rządowe Centrum Legislacji** | Art. 67a | W odniesieniu do projektowanych art. 67a i następnych ustawy o KSC określających procedurę wydawania i publikowania przez Pełnomocnika poleceń zabezpieczających i ostrzeżeń należy zauważyć, że Pełnomocnikowi zostały przyznane władcze kompetencje do wpływania na działanie nie tylko podmiotów krajowego systemu cyberbezpieczeństwa, ale także właścicieli lub posiadaczy samoistnych obiektów, instalacji lub urządzeń infrastruktury krytycznej, krajowych instytucji płatniczych czy przedsiębiorców oraz dostawców usług zaufania (dodawany art. 67a ust. 4 ustawy o KSC). Mimo, że Kolegium przyznano funkcję organu kontrolującego Pełnomocnika w zakresie wydawanych ostrzeżeń i poleceń zabezpieczających, to wątpliwości budzi przyznana w projektowanym art. 67a ust. 8 kompetencja do zastosowania innego ostrzeżenia lub polecenia zabezpieczającego przez Pełnomocnika w sytuacji, w której Kolegium odmówiło zatwierdzenia ostrzeżenia lub polecenia zabezpieczającego. Uprawnienie to nie zostało obwarowane żadnymi przesłankami i umożliwia dowolne rozstrzygnięcie Pełnomocnika we wskazanym zakresie. Ostrzeżenie zawiera również wskazania określonego działania, o których mowa w dodawanym art. 67b ust. 3 ustawy o KSC – w tym *„zakaz stosowania określonego sprzętu lub oprogramowania”* lub *„nakaz wprowadzenia reguł ruchu sieciowego zakazującego połączeń z określonym adresem IP lub nazwami URL”.* Wszystkie te środki należy poddać ponownej ocenie Projektodawcy z punktu widzenia ich proporcjonalności. Ostrzeżenie wydawane przez Pełnomocnika, podobnie jak ocena ryzyka dostawcy – jest publikowane w formie komunikatu w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski”. Jego charakter wskazuje, że stanowi rozstrzygnięcie o obowiązkach określonych w tym ostrzeżeniu podmiotów – a zatem ma  charakter decyzji, o której mowa w art. 78 Konstytucji RP. W świetle powyższego projektowane przepisy powinny zostać uzupełnione o stosowną procedurę odwoławczą. Należy również zwrócić uwagę, że zgodnie z projektowanym art. 67a ust. 6 ustawy o KSC Pełnomocnik publikuje w Dzienniku Urzędowym RP „Monitor Polski” komunikaty o wydanych i odwołanych ostrzeżeniach, ale mimo możliwości przedłużenia ostrzeżenia o kolejne dwa lata na podstawie dodawanego art. 67b ust. 2 ustawy o KSC przepisy projektu nie przewidują publikacji komunikatu o przedłużeniu ostrzeżenia. Podobne uwagi należy podnieść w stosunku do poleceń zabezpieczających wydawanych na podstawie projektowanego art. 67c ustawy o KSC. Ponownej analizy wymaga także projektowana procedura publikowania polecenia zabezpieczającego w Dzienniku Urzędowym „Monitor Polski”. Jako akt podlegający natychmiastowemu wykonaniu powinien być on doręczany do podmiotów objętych tym poleceniem. Tak zaprojektowana regulacja dotycząca ogłaszania polecenia zabezpieczającego w dzienniku urzędowym może uniemożliwić natychmiastową wykonalność, na którą wskazuje projektodawca w projektowanym art. 67c ust. 1 ani nie pozwoli na osiągniecie celu, o którym mowa w projektowanym art. 67c ust. 2 – czyli zapewnienia koordynacji na czas obsługi incydentu krytycznego. Podnieść należy, że wydanie polecenia zabezpieczającego „*na czas obsługi incydentu krytycznego, nie dłużej niż na dwa lata*” budzi wątpliwości w zakresie adekwatności i proporcjonalności stosowania tego nadzwyczajnego środka zabezpieczającego przez tak długi czas. Wyjaśnienia, chociażby w uzasadnieniu, wymaga, jaki jest średni czas obsługi incydentów krytycznych i jaką rolę w tej obsłudze ma pełnić Pełnomocnik. Podobnie jak w przypadku oceny ryzyka dostawcy, jak i ostrzeżenia nie została w przedstawionym projekcie uregulowana procedura odwoławcza, o której mowa w art. 78 Konstytucji RP. Procedura zaskarżenia rozstrzygnięć Pełnomocnika i Kolegium jest konieczna również z uwagi na zakres i wysokość administracyjnych kar pieniężnych przewidzianych za niezastosowanie się do polecenia zabezpieczającej (projektowany art. 73 ust. 1 pkt 14 ustawy o KSC) czy niedostosowanie się do obowiązków, o których mowa w projektowanym art. 66b projektu ustawy (projektowany art. 73 ust. 2a ustawy o KSC), które to kary mają sięgać nawet do 3% „*całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego*” (projektowany art. 73 ust. 3 pkt 14 ustawy o KSC). | **Uwaga uwzględniona**  Przepisy art. 67a -67c zostaną zmienione. Ostrzeżenia w dalszym ciągu będzie wydawał Pełnomocnik. Natomiast polecenia zabezpieczające będą wydawane w formie decyzji administracyjnej przez ministra wł. ds. informatyzacji, co oznacza, że podmiot będzie mógł odwołać się od danej decyzji (zgodnie z Kpa). Minister właściwy ds. informatyzacji będzie podejmował decyzje o ewentualnych karach także w formie decyzji administracyjnej. Przepis art. 73 zostanie uzupełniony o wysokość kary za nie zastosowanie się do polecenia zabezpieczającego.  Do tej pory ani Pełnomocnik ani zespoły CSIRT nie mogły wydawać ostrzeżeń w formie proponowanej w nowelizacji. Pełnomocnik może wydawać rekomendacje dla podmiotów krajowego systemu cyberbezpieczeństwa na podstawie art. 33 ustawy o ksc.  Ostrzeżenie wydawane przez Pełnomocnika wskaże rodzaj zagrożenia, które uprawdopodobni wystąpienie incydentu krytycznego. Ponadto w ostrzeżeniu wskazane zostanie zakres podmiotowy, czyli zostaną określone podmioty, których ostrzeżenie dotyczy. Ostrzeżenie będzie zawierało także listę zalecanych działań, które podmioty powinny wdrożyć w celu ograniczenia ryzyk związanych z prawdopodobieństwem wystąpienia incydentu krytycznego. Przykładem takich zaleceń jest np. zwrócenie uwagi na określony typ zachowań czy incydentów. Pełnomocnik będzie przeprowadzał nie rzadziej niż raz na rok przegląd wydanych ostrzeżeń w celu ustalenia czy spełniają ustawową przesłankę ich wydania.  Natomiast polecenie zabezpieczające odnosi się do sytuacji związanej z wystąpieniem incydentu krytycznego. Minister właściwy do spraw informatyzacji w oparciu o informacje otrzymywane od m.in. zespołów CSIRT poziomu krajowego oraz ustaleń Zespoły ds. Incydentów Krytycznych będzie mógł podjąć decyzję o podjęciu konkretnych działań w związku z reagowaniem na incydent krytyczny. M. in. Nakazać podjęcie określonego zachowania przez podmioty, których dotyczy polecenie w tym np. zabezpieczenie określonych informacji czy zakaz instalacji określonej wersji oprogramowania.  Należy podkreślić, że szybkość reakcji w przypadku wystąpienia incydentu krytycznego jest kluczowa w procesie ograniczenia skutków tego incydentu.  Informacja o wydaniu polecenia zabezpieczającego będzie publikowana w Dzienniku Urzędowym ministra właściwego do spraw informatyzacji. |
|  | **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 Finansów** | art. 67a ust. 4 pkt 4 | 4) krajowych instytucji płatniczych, o których mowa w art. 2 pkt 16 ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych (Dz. U. 2020 r. poz. 794). Nie jest uzasadnione, dlaczego wybiórczo akurat ci dostawcy usług płatniczych z katalogu określonego w art. 4 ustawy o usługach płatniczych, mają znaleźć się w katalogu podmiotów, które mogą dotyczyć ostrzeżenie i polecenie zabezpieczające. | **Wyjaśnienie**  Instytucje te z uwagi na ich ogromne znaczenie w systemie płatności elektronicznych (świadczenie usług dla ogromnej liczby klientów w skali kraju) powinny być objęte ostrzeżeniem i poleceniem zabezpieczającym. Doświadczenie incydentu z 2018 r. (SkyCash) jasno pokazuje, że skutki incydentu w tego typu podmiocie mogą mieć zasięg ponadregionalny a nawet krajowy. |
|  | **Ministerstwo Finansów** | art. 67a ust. 7 | Dlaczego pełnomocnik ds. cyberbezpieczeństwa nie może ogłosić treści ostrzeżenia i polecenia zabezpieczającego (zamiast wskazanych komunikatów), skoro i tak przepis ten zawiera odesłanie do art. 67b ust. 1 i art. 67c ust. 3, czyli treści ostrzeżenia oraz polecenia zabezpieczającego? | **Uwaga częściowo uwzględniona**  Przepis zostanie zmieniony, polecenie zabezpieczające i ostrzeżenie będą publikowane na stronie BIP ministra właściwego do spraw informatyzacji oraz na stronie internetowej. Informacja o poleceniu zabezpieczającym będzie również publikowane w Dzienniku Urzędowym ministra właściwego ds. informatyzacji. |
|  | **Ministerstwo Finansów** | Art. 67a ust. 8 | Wątpliwości budzi zapis odnośnie „stosowania” przez Pełnomocnika Rządu do spraw Cyberbezpieczeństwa „innego ostrzeżenia lub polecenia zabezpieczającego” w przypadku odmowy zatwierdzenia ostrzeżenia lub polecenia przez Kolegium. Projekt mówi o „wydawaniu” ostrzeżeń lub poleceń przez Pełnomocnika, dlatego w przypadku odmowy ich zatwierdzenia przez Kolegium zapis o „stosowaniu” innych ostrzeżeń lub poleceń jest wątpliwy. Jeżeli miałoby to dotyczyć wcześniej wydanych ostrzeżeń lub poleceń, to dotyczą one innych uprzednio zidentyfikowanych incydentów krytycznych, ponadto w przypadku braku ich odwołania nadal obowiązują. (Zgodnie z art. 67a ust. 1 i 2, wszystkie ostrzeżenia i polecenia zabezpieczające wydawane przez Pełnomocnika wymagają zatwierdzenia przez Kolegium), | **Uwaga częściowo uwzględniona**  Przepisy art. 67a -67c zostaną zmienione. Ostrzeżenia w dalszym ciągu będzie wydawał Pełnomocnik. Natomiast polecenia zabezpieczające będą wydawane w formie decyzji administracyjnej przez ministra wł. ds. informatyzacji, co oznacza, że podmiot będzie mógł odwołać się od danej decyzji (zgodnie z Kpa). Minister właściwy ds. informatyzacji będzie podejmował decyzje o ewentualnych karach także w formie decyzji administracyjnej. Przepis art. 73 zostanie uzupełniony o wysokość kary za nie zastosowanie się do polecenia zabezpieczającego.  Do tej pory ani Pełnomocnik ani zespoły CSIRT nie mogły wydawać ostrzeżeń w formie proponowanej w nowelizacji. Pełnomocnik może wydawać rekomendacje dla podmiotów krajowego systemu cyberbezpieczeństwa na podstawie art. 33 ustawy o ksc.  Ostrzeżenie wydawane przez Pełnomocnika wskaże rodzaj zagrożenia, które uprawdopodobni wystąpienie incydentu krytycznego. Ponadto w ostrzeżeniu wskazane zostanie zakres podmiotowy, czyli zostaną określone podmioty, których ostrzeżenie dotyczy. Ostrzeżenie będzie zawierało także listę zalecanych działań, które podmioty powinny wdrożyć w celu ograniczenia ryzyk związanych z prawdopodobieństwem wystąpienia incydentu krytycznego. Przykładem takich zaleceń jest np. zwrócenie uwagi na określony typ zachowań czy incydentów. Pełnomocnik będzie przeprowadzał nie rzadziej niż raz na rok przegląd wydanych ostrzeżeń w celu ustalenia czy spełniają ustawową przesłankę ich wydania.  Natomiast polecenie zabezpieczające odnosi się do sytuacji związanej z wystąpieniem incydentu krytycznego. Minister właściwy ds. informatyzacji w oparciu o informacje otrzymywane od m.in. zespołów CSIRT poziomu krajowego oraz ustaleń Zespoły ds. Incydentów Krytycznych będzie mógł podjąć decyzję o podjęciu konkretnych działań w związku z reagowaniem na incydent krytyczny. M. in. nakazać podjęcie określonego zachowania przez podmioty, których dotyczy polecenie w tym np. zabezpieczenie określonych informacji czy zakaz instalacji określonej wersji oprogramowania.  Należy podkreślić, że szybkość reakcji w przypadku wystąpienia incydentu krytycznego jest kluczowa w procesie ograniczenia skutków tego incydentu. |
|  | **Ministerstwo Rozwoju, Pracy i Technologii** | Art. 67b | Niejasny jest charakter aktu nazwanego w projekcie ustawy ostrzeżeniem (art. 67b). Nie jest to akt indywidualny i jednostkowy, jak polecenie zabezpieczające, które ma postać decyzji (art. 67c). Ostrzeżenie ma wszelkie cechy aktu normatywnego adresowanego do podmiotów zewnętrznych w stosunku do administracji, m.in. wskazuje rodzaje podmiotów, których dotyczy, obowiązuje nawet przez 2-4 lata i wskazuje określone, powinne zachowania. Mimo to ostrzeżenie nie mieści się w obecnym katalogu aktów normatywnych, a jego prawny charakter i skutki nie są jasne. | **Uwaga uwzględniona**  Przepis zostanie poprawiony.  Ostrzeżenie wydawane przez Pełnomocnika wskaże rodzaj zagrożenia, które uprawdopodobni wystąpienie incydentu krytycznego. Ponadto w ostrzeżeniu wskazane zostanie zakres podmiotowy, czyli Pełnomocnik określi, które podmioty dane ostrzeżenie dotyczy. Ostrzeżenie będzie zawierało także listę zalecanych działań, które podmioty powinny wdrożyć w celu ograniczenia ryzyk związanych z prawdopodobieństwem wystąpienia incydentu krytycznego. Przykładem takich zaleceń jest np. zwrócenie uwagi na określony typ zachowań czy incydentów. Pełnomocnik będzie przeprowadzał nie rzadziej niż raz na rok przegląd wydanych ostrzeżeń w celu ustalenia czy spełniają ustawową przesłankę ich wydania. |
|  | **Ministerstwo Finansów** | 67b ust. 2 | Wyjaśnienia wymaga, czym jest "stosowanie ostrzeżenia" przez wskazany okres. | **Wyjaśnienie**  Przepis zostanie zmieniony.  Ostrzeżenie wydawane przez Pełnomocnika wskaże rodzaj zagrożenia, które uprawdopodobni wystąpienie incydentu krytycznego. Ponadto w ostrzeżeniu wskazane zostanie zakres podmiotowy, czyli Pełnomocnik określi, które podmioty dane ostrzeżenie dotyczy. Ostrzeżenie będzie zawierało także listę zalecanych działań, które podmioty powinny wdrożyć w celu ograniczenia ryzyk związanych z prawdopodobieństwem wystąpienia incydentu krytycznego. Przykładem takich zaleceń jest np. zwrócenie uwagi na określony typ zachowań czy incydentów. Pełnomocnik będzie przeprowadzał nie rzadziej niż raz na rok przegląd wydanych ostrzeżeń w celu ustalenia czy spełniają ustawową przesłankę ich wydania. |
|  | **Ministerstwo Finansów** | Art. 67c | Wątpliwości budzi relacja ust. 1 i 3 pkt 3 - z jednej strony polecenie zabezpieczające ma mieć formę decyzji administracyjnej z nadanym rygorem natychmiastowej wykonalności, z drugiej - ma zawierać datę wejścia w życie. Niejasne jest też pojęcie użyte w art. 67c ust. 2 pkt 2 i rozwinięte w ust. 4: "wskazania określonego zachowania, które zmniejszy skutki incydentu lub zapobiegnie jego rozprzestrzenianiu się". | **Uwaga częściowo uwzględniona**  Przepis zostanie zmieniony, usunięte zostaną wyrazy „data wejścia w życie”. |
|  | **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 Finansów** | Art. 74 ust. 1a pkt 3 | Zamiast „określony” powinno być – „określonych”; | **Uwaga uwzględniona** |
|  | **Ministerstwo Sprawiedliwości** | Art. 74 ust. 1a pkt 3 | Zgodnie z projektowanym art. 74 ust. 1a pkt 3 ustawy o krajowym systemie cyberbezpieczeństwa, karę pieniężną, określoną w art. 73 ust. 2a, w odniesieniu do podmiotów wskazanych w art. 4 pkt 2a (tj. przedsiębiorców komunikacji elektronicznej), będzie nakładał w drodze decyzji administracyjnej Prezes Urzędu Komunikacji Elektronicznej. Na tle proponowanej regulacji rodzi się pytanie, czy od decyzji tego typu będzie służyło odwołanie do Sądu Okręgowego w Warszawie – Sądu Ochrony Konkurencji i Konsumentów, podobnie jak w przypadku niektórych decyzji Prezesa UKE o karach nakładanych w trybie projektowanej ustawy – Prawo komunikacji elektronicznej. Przedstawiony do zaopiniowania projekt o takim odwołaniu nie stanowi, tym niemniej w piśmie Ministra Cyfryzacji z dnia 7 września 2020 r. zapowiedziano odpowiednie dostosowanie projektu do projektowanej ustawy – Prawo komunikacji elektronicznej. O ile zaś zostanie dopuszczona możliwość złożenia do sądu odwołania od decyzji Prezesa UKE, o której mowa w projektowanym w art. 74 ust. 1a pkt 3 ustawy o krajowym systemie cyberbezpieczeństwa, to należy zwrócić uwagę, że konieczne będzie zapewnienie środków finansowych na etaty sędziowskie i urzędnicze dla Sądu Ochrony Konkurencji i Konsumentów (SOKiK). Naturalną konsekwencją poszerzenia katalogu decyzji zaskarżalnych do SOKiK stanie się bowiem wzrost obciążeń tego sądu, co najprawdopodobniej przełoży się także na sądy rozpoznające środki zaskarżenia od orzeczeń SOKiK (Sąd Apelacyjny w Warszawie, Sąd Najwyższy). | **Wyjaśnienie.** Skargę na decyzję administracją o nałożeniu kary będzie rozpatrywał Wojewódzki Sąd Administracyjny |
|  | **Ministerstwo Klimatu i Środowiska** | Art. 74 ust. 1a pkt 4 | W Art. 74 ust. 1a pkt 4 w przypadku podmiotów wpisanych do wykazu SOC, wykonujących usługi na zlecenie OUK – organy właściwe ds. cyberbezpieczeństwa . Odpowiedzialność za realizację zadań wskazanych w UKSC odpowiada operator usługi kluczowej. Ponadto, niejednokrotnie SOC będzie wchodził w strukturę wewnętrzną danego podmiotu, więc ewentualna kara będzie nałożona na spółkę, a nie na jej strukturę wewnętrzną. Natomiast w przypadku outsourceowania usług SOC, organ właściwy nie ma podstawy do nałożenia kary na podmiot, którego bezpośrednio nie nadzoruje. Z racji tego, proponuje się wykreślić pkt 4.  Proponuje się w art. 74 w ust. 1a wykreślić pkt 4. | **Uwaga uwzględniona**  Przepis art. 74 ust. 1a pkt 4 dotyczy nałożenia kary na zewnętrzny SOC, wykonujący usługi na rzecz operatora usługi kluczowej. Nie dotyczy on SOC ustanowionego w ramach struktury operatora usługi kluczowej.  Przepis zostanie zmieniony, minister właściwy do spraw informatyzacji będzie nakładał kary na podmioty świadczące usługi SOC, tak jak obecnie w art. 53 ust. 1 pkt 1 minister jest organem nadzorczym nad podmiotami świadczącymi usługi z zakresu cyberbezpieczeństwa. |
|  | **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 nieuzwględniona**  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** | Art. 4 ust. 2 projektu | Zamiast „naograniczaniu” powinno być – „na ograniczaniu”. | **Uwaga uwzględniona** |
|  | **Rządowe Centrum Legislacji** | Art. 96 PZP | W zakresie zmian projektowanych w ustawie z dnia 11 września 2019 r. – *Prawo zamówień publicznych* (Dz. U. poz. 2019), zwanej dalej „PZP”, wobec niedookreślonej procedury dokonywania oceny ryzyka dostawcy budzi wątpliwości wprowadzenie odesłania do tej oceny jako wymagania, które zamawiający może określić w ogłoszeniu o zamówieniu lub dokumentach zamówienia (zmiana w art. 96 PZP) oraz wprowadzenie wysokiego poziomu ryzyka zdefiniowanego na podstawie tej oceny jako przesłanki umożliwiającej fakultatywne wykluczenie wykonawcy z postępowania o udzielenie zamówienia publicznego na podstawie art. 109 PZP. | **Wyjaśnienie**  W toku prac legislacyjnych zrezygnowano z nowelizacji Prawa zamówień publicznych. |
|  | **Ministerstwo Obrony Narodowej** | Art. 96 PZP  Art. 96 ust. 2 pkt 3 PZP | **Art. 2 pkt 1 *projektu*** - rozważenia wymaga wykreślenie z *projektu* zmiany do art. 96 ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych (dalej Pzp). Treść art. 96 Pzp odnosi się zasadniczo do klauzul społecznych (społecznie zrównoważone zamówienia). Mając na względzie, że przedmiotowa zmiana nie wpływa na kwestie społeczne, a dotyczy stricte kwestii dotyczących bezpieczeństwa, wątpliwe jest ich regulowanie we wskazanej jednostce redakcyjnej ustawy. Zagadnieniem budzącym wątpliwości, a odnoszącym się do charakteru dokonywanej oceny, jest projektowane brzmienie art. 96 ust. 2 pkt 3 Pzp. Należy bowiem wskazać, że jeśli ustawa z ryzykiem niskim lub jego brakiem nie wiąże szczególnych zakazów w zakresie wprowadzenia do użytkowania sprzętu, oprogramowania lub usług dostawcy, z natury rzeczy, ze względu na nieproporcjonalność środków, niezasadne jest pozostawienie zamawiającemu dowolności w zakresie określania wymagań w zakresie ryzyka. Jednocześnie, mając na uwadze zakazy we wprowadzaniu sprzętu/oprogramowania/usług w przypadku określenia ryzyka umiarkowanego lub wysokiego zamawiający de facto nie posiada możliwości dokonywania wyboru w określeniu akceptowalnego ryzyka, ponieważ nabycie byłoby sprzeczne z *ustawą o ksc*. | **Wyjaśnienie**  W toku prac legislacyjnych zrezygnowano z nowelizacji Prawa zamówień publicznych. |
|  | **Ministerstwo Rozwoju, Pracy i Technologii** | Art. 96 ust. 2 pkt. 2 PZP | Zmieniany przepis ust. 2 określa przykładowe wymagania jakie zamawiający może postawić wykonawcy. Wymagania wskazane w ust. 2 muszą mieścić się w katalogu wymagań określonych w art. 96 ust. 1. Tym samym, przykładowe wymaganie musiałoby mieścić się w ramach wymagań obejmujących aspekty społeczne lub gospodarcze lub środowiskowe lub związane z innowacyjnością, zatrudnieniem lub zachowaniem poufnego charakteru informacji przekazywanych wykonawcy w toku realizacji zamówienia. Wątpliwości jednak budzi to, czy wymaganie dotyczące poziomu ryzyka, jaki stanowi dostawca sprzętu lub oprogramowania mieści się w zakresie generalnych wymagań określonych w art. 96 ust. 1. w konsekwencji czy regulacja pozostawać będzie w zgodzie z dyrektywą Parlamentu Europejskiego i Rady 2014/24/UE z dnia 26 lutego 2014 r. w sprawie zamówień publicznych, uchylającą dyrektywę 2004/18/WE (Dz.Urz.UE.L Nr 94, str. 65). Jednocześnie należy zauważyć, że dodanie w art. 96 ust. 2 pkt 2, który jest regulacją fakultatywną i daje zamawiającemu jedynie możliwość wymagania od zamawiającego określonej oceny ryzyka (umiarkowanej, niskiej, braku ryzyka), należy uznać za rozwiązanie nie w pełni realizujące swoją rolę w kontekście projektowanego art. 66b ust. 2, który zabrania wprowadzenia do użytkowania sprzętu, oprogramowania i usług, jeżeli poziom ryzyka dostawcy jest umiarkowany. Postawienie takiego wymagania byłoby możliwie jedynie w zakresie niskiego ryzyka lub braku ryzyka dostawcy. Niemniej jednak, zaproponowane wymaganie nawet przy zawężeniu wymagania do ryzyka niskiego lub braku ryzyka dostawcy, budzi wskazane wyżej wątpliwości co do zgodności z przepisami UE. Dodatkowo, regulacja może nie spełnić swojego celu, czyli zachęcenia zamawiających, czy też dania im wyraźnej podstawy, do stawiania takiego wymagania w postępowaniu o udzielenie zamówienia. Postawienie takiego wymagania może być bowiem dla zamawiającego trudne do zrealizowania z przyczyn praktycznych. Wprowadzana procedura oceny ryzyka dostawy sprzętu, oprogramowania lub usług nie daje możliwości wystąpienia o taką ocenę wykonawcy zamówienia publicznego (samozweryfikowania się). Zgodnie z art. 66a wniosek o sporządzenie oceny może złożyć wyłącznie członek Kolegium, co oznacza, że postawienie takiego wymagania może wyeliminować z postępowania o udzielenie zamówienia szereg wykonawców tylko z tego powodu, że nie będą oni mogli przedstawić niskiej oceny ryzyka albo oceny wskazującej na brak ryzyka dostawcy. | **Wyjaśnienie**  W toku prac legislacyjnych zrezygnowano z nowelizacji Prawa zamówień publicznych. |
|  | **Ministerstwo Obrony Narodowej** | Art. 109 ust. 1 pkt 11 PZP | **Art. 2 pkt 2 *projektu ksc*** (dotyczy art. 109 ust. 1 Pzp)- mając na względzie brak jednoznaczności przepisów dotyczących charakteru oceny (ocena podmiotowa/ocena przedmiotowa) należy wskazać, że wprowadzona w art. 2 pkt 2 regulacja rodzi wątpliwości w kontekście spójności z przepisami Pzp, jak i samej realizacji założonego celu regulacji.  W pierwszej kolejności należy wskazać, że dodany w art. 109 w ust. 1 Pzp pkt 11, wskazuje na możliwość wykluczenia wykonawcy, wobec którego, w ramach oceny o której mowa w art. 66a ust. 1 *ustawy o ksc*, stwierdzono „wysokie” ryzyko. Jednakże *ustawa o ksc* wprost określa także kategorię ryzyka „umiarkowanego”, które skutkuje również brakiem możliwości wprowadzenia do użytkowania sprzętu, oprogramowania i usług określonych w ocenie danego dostawcy sprzętu i oprogramowania. Mając powyższe na względzie w takiej sytuacji *de facto* nie będzie możliwe formalne wykluczenie wykonawcy, a jednocześnie wykonawca nie będzie miał możliwości realizacji zamówienia. W związku z tym przedmiotowa regulacja wydaje się być niepełna i umożliwiałaby udzielenie zamówienia wykonawcy, który nie będzie mógł go zrealizować.  Co istotne także wskazana przesłanka wykluczenia ma charakter fakultatywny, co wydaje się być niespójne z treścią art. 66b ust. 1 *ustawy o ksc*, który wprost wskazuje na obligatoryjność zakazu w zakresie wprowadzania do użytkowania sprzętu oferowanego przez dostawcę objętego ryzykiem „wysokim”. W związku z tym należy konstatować, że przedmiotowa przesłanka wykluczenia powinna mieć charakter obligatoryjny, a nie fakultatywny.  Ponadto w kontekście dokonywanych zmian należy wskazać, że Pzp wprowadza, oprócz wykonawcy, także inne kategorie, jak choćby podwykonawcy, czy podmioty udostępniające zasoby. O ile w przypadku podmiotów udostępniających zasoby Pzp zawiera stosowne regulacje obligujące do badania przesłanek wykluczenia, o tyle w przypadku podwykonawców brak jest obligatoryjnej weryfikacji przez zamawiającego tych przesłanek. W związku z tym oparcie się na przesłance wykluczenia może nie dać oczekiwanych rezultatów w postaci niedopuszczenia do udzielenia takiemu podmiotowi zamówienia, a przez to, w przypadku braku wyrażonej przez zamawiającego woli weryfikacji podwykonawców w kontekście przesłanek wykluczenia przedmiotowa regulacja nie wyeliminuje z postępowania o udzielenie zamówienia podwykonawców objętych ryzykiem „wysokim”.  Należy zauważyć, że w treści art. 66a ust. 5 *ustawy o ksc* wskazuje się na sporządzone na podstawie oceny, o której mowa w ust. 4, elementy oceny, które zasadniczo odnoszą się do podmiotu, a nie przedmiotu. Jednocześnie, mimo braku wskazania wprost w przywołanej wyżej ocenie, jak też procesie jej dokonywania (ust. 4), na podstawie art. 66b ust. 1 pkt 1 oraz ust. 2 pkt 1 *ustawy o ksc* określono dla ryzyka wysokiego i umiarkowanego konieczność wskazania konkretnego sprzętu, oprogramowania lub usług. Mając powyższe na względzie nie jest jasne, czy dokonywana ocena powinna odnosić się do przedmiotu, czy też do podmiotu. W ocenie resortu obrony narodowej kwestia ta jest istotna z punktu widzenia dokonywanych zmian w przepisach ustawy - Prawo zamówień publicznych (przesłanka wykluczenia wykonawcy/odrzucenia oferty i ich relacja). W związku z tym konieczne jest jednoznaczne określenie w art. 66a ust. 5 *ustawy o ksc*, czy elementem oceny jest konkretny przedmiot (sprzęt/oprogramowanie), czy też podmiot (przesłanka wykluczenia).  W związku z powyższym w przypadku, gdy ocena miałaby charakter przedmiotowy (odnosiłaby się do sprzętu, oprogramowania lub usług dostawcy) niezasadnym wydawałoby się wprowadzanie dodatkowej przesłanki wykluczenia, w sytuacji istnienia przesłanek odrzucenia oferty (art. 226 ust. 1 pkt 4 Pzp). Zgodnie z nią, w przypadku, gdy dany przedmiot (element oferty stanowiący sprzęt lub oprogramowanie od dostawcy objętego ryzykiem „wysokim”) nie może być wprowadzony do użytkowania (na marginesie należy wskazać, że w przypadku zamówień należałoby wskazać na brak możliwości dostawy lub świadczenia usług), co wiąże się z ustalonym w ocenie, ryzykiem umiarkowanym albo wysokim, oferta wykonawcy oferującego przedmiot objęty zakazem powinna zostać odrzucona, jako niezgodna z przepisami odrębnymi. Co istotne, taka konstrukcja umożliwiałaby, niezależnie od decyzji zamawiającego, na odrzucenie oferty wykonawcy, w sytuacji, gdy przedmiot objęty wynikającym ze stosownego ryzyka zakazem, wprowadzania lub użytkowania, dostarcza także podwykonawca. Podejście przedmiotowe daje zatem szerszą i obiektywną możliwość zagwarantowania bezpieczeństwa w odniesieniu do szerokiego zakresu podmiotowego. W tym kontekście należy zauważyć, że w przypadku przyjęcia konstrukcji opartej na wykluczeniu wykonawcy zamawiający, w sytuacji gdy przedmiot objęty zakazem byłby dostarczany przez podwykonawcę, nie mógłby go wykluczyć z tego tytułu, w sytuacji, gdy zamawiający nie zastrzegłby możliwości weryfikacji podmiotowej (zbadanie podstaw wykluczenia) w stosunku do podwykonawców.  Podsumowując, Pzp daje narzędzia do wykluczenia wykonawców (art. 108 i 109 Pzp), jak i odrzucenia ofert (art. 226 ust. 1 pkt 4 Pzp – zamawiający odrzuca ofertę jeżeli jest nieważna na podstawie odrębnych przepisów). Jednocześnie, co istotne, w zakresie ewentualnej oceny podstaw do odrzucenia oferty lub wykluczenia wykonawcy należy mieć na względzie niejednorodność po stronie podmiotowej wykonawcy, jak też możliwości dokonywania oceny (weryfikacji) tych podstaw przez zamawiającego. Biorąc powyższe pod uwagę proponuje się oparcie oceny na wskazaniu przedmiotowym (sprzęt, oprogramowanie, usługi), a nie na podejściu podmiotowym (jako przesłanka wykluczenia). Powyższe uwarunkowane jest jednak oceną przez Kolegium sprzętu/oprogramowania/usług, a nie jedynie ich dostawcy. W związku z tym ewentualne niedopuszczenie rozwiązań objętych ryzykiem wysokim i umiarkowanym oparte zostałoby na przesłance odrzucenia oferty, wynikającej z art. 226 ust. 1 pkt 4 Pzp co byłoby spójne z obligatoryjnością stosowania zakazów, o których mowa w art. 66b ust.1 ustawy o ksc. | **Wyjaśnienie**  W toku prac legislacyjnych zrezygnowano z nowelizacji Prawa zamówień publicznych. |
|  | **Ministerstwo Obrony Narodowej** | Art. 110 ust. 2 PZP | **Proponuje się usunięcie art. 2 pkt 3 *projektu*** (dotyczącego art. 110 ust. 2 Pzp) - mając na względzie charakter przesłanek i okoliczności (zasadniczo natury wywiadowczej/politycznej) będących podstawą do określenia stopnia ryzyka, nie jest zasadne, aby to zamawiający miał dokonywać dla danego zamówienia odrębnej oceny, w tym w szczególności na podstawie art. 109 ust. 1 pkt 11 Pzp. Należy wskazać, że zamawiający, nie posiadają wiedzy w tym zakresie, w związku z tym każdorazowo powinni opierać się na ocenie i kwalifikacji dokonanej przez Kolegium. Dowolność w zakresie określania, bądź nie stopnia ryzyka lub wskazywania (bądź nie wskazywania) przesłanki wykluczenia, w sytuacji, gdy dany podmiot/przedmiot znajduje się na liście podmiotów/przedmiotów, oprócz braku racjonalnego uzasadnienia dla możliwości dokonywania zmiany samodzielnie przez zamawiającego może stanowić istotne zagrożenie korupcyjne. W tym kontekście wydaje się, że wszelkie decyzje, w tym zmieniające ocenę ryzyka lub dopuszczające wykonawców (podwykonawców) lub produkty, powinny być dokonywane przez podmiot określający stopnie ryzyka (Kolegium). Należy przy tym wskazać, że projektowana ustawa wprost przewiduje okoliczności i procedurę w zakresie zmiany oceny ryzyka (umiarkowanego).W związku z tym powinna ona odnosić się także do kwestii udzielania, bądź nie tym podmiotom zamówień publicznych.  Dodatkowo należy także wskazać, że o ile drogą interpretacji możliwe byłoby wprowadzenie do użytkowania danego sprzętu/oprogramowania, jednak brak jest normy zwalniającej z drugiej konsekwencji określenia ryzyka to jest konieczności wycofania z użytkowania. Należy bowiem wskazać, że ewentualne odstąpienie przez zamawiającego od konsekwencji związanych danym stopniem ryzyka odnosi się do postępowania, a więc umożliwia dostarczenia sprzętu lub oprogramowania, o tyle brak jest regulacji wskazującej na brak stosowania pozostałych konsekwencji, określonych w projektowanych art. 66b ust. 1 pkt 2 oraz ust. 2 pkt *2 ustawy o ksc.* | **Wyjaśnienie**  W toku prac legislacyjnych zrezygnowano z nowelizacji Prawa zamówień publicznych. |
|  | **Ministerstwo Rozwoju, Pracy i Technologii** | Art. 109 PZP  Art. 110 PZP | W art. 109 (i zw. z nim art. 110) przewiduje się zmianę polegającą na dodaniu fakultatywnej przesłanki wykluczenia wykonawcy, - tj. wykluczenia wykonawcy, "który jest dostawcą sprzętu lub oprogramowania, wobec którego stwierdzono wysokie ryzyko, w ramach oceny, o której mowa w art. 66a ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.". Dyrektywa 2014/24/UE określa zamknięty katalog przesłanek wykluczenia wykonawcy z postępowania o udzielenie zamówienia publicznego, w którym projektowana przesłanka zdaje się nie mieścić. Tym samym, regulacja niesie ryzyko uznania jej za niezgodną z prawem UE. Jednocześnie, podobnie jak w przypadku zmienianego art. 96, dodawanie w art. 109 Pzp proponowanej fakultatywnej przesłanki wykluczenia z powodu wysokiego ryzyka dostawcy sprzętu lub oprogramowania, może być niewystarczające w zw. z brzmieniem projektowanego art. 66b ust. 1. Przepis ten bowiem nie tylko zakazuje użytkowania sprzętu, oprogramowania i usług nabytego od takiego dostawcy, ale wręcz nakazuje taki sprzęt z użytkowania wycofać. Wprowadzenie zatem do systemu prawa regulacji o treści określonej w art. 66b ust. 1, nakazywałoby zamawiającemu wyeliminowanie oferty dostawcy, którego ryzyko oceniono jako wysokie. Co więcej, konieczność wyeliminowania przez zamawiającego oferty dostawcy powstaje również w przypadku dostawcy, którego ryzyko oceniono jako umiarkowane, z uwagi na brzmienie projektowanego art. 66b ust. 2. Przepis ten podobnie jak ust. 1 zakazuje bowiem użytkowania sprzętu, oprogramowania i usług takiego dostawcy. | **Wyjaśnienie**  W toku prac legislacyjnych zrezygnowano z nowelizacji Prawa zamówień publicznych. |
|  | **Ministerstwo Nauki i Szkolnictwa Wyższego** | uzasadnienie | W celu zapewnienia spójności z terminologią stosowaną w ustawie z dnia 20 lipca 2018 r. - Prawo o szkolnictwie wyższym i nauce (Dz.U. 2020 r. poz. 85 z późn.zm.) **uprzejmie proszę o zastąpienie wyrażenia „uczelnie wyższe” słowem „uczelnie”.** | **Uwaga uwzględniona** |
|  | **Koordynator Oceny Skutków Regulacji** | Ocena Skutków Regulacji:  Pkt 2 | Ocena skutków regulacji wymaga uzupełnienia poprzez:  rozszerzenie opisu proponowanych rozwiązań (pkt 2 OSR). | **Uwaga uwzględniona** |
|  | **Ministerstwo Finansów** | OSR  pkt. 3 | "Jak problem został rozwiązany w innych krajach, w szczególności krajach członkowskich OECD/UE?" wpisano "Ze względu na charakter wprowadzanych zmian, nie dokonano analizy prawno-porównawczej w obrębie krajów OECD/EU." Nie jest jasne, jaki charakter wprowadzonych zmian spowodował, że nie dokonano analizy prawno-porównawczej w obrębie tych krajów? | **Uwaga uwzględniona** |
|  | **Koordynator Oceny Skutków Regulacji** | OSR  Pkt 4 | Podanie pełnego opisu wpływu regulacji na wybrane podmioty (pkt 4 OSR); | **Uwaga uwzględniona** |
|  | **Ministerstwo Finansów** | OSR  Pkt 4  Pkt 6 | Ministerstwo Finansów zauważa, iż w art. 22 ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa zostanie dodany pkt 2a, zgodnie z którym podmioty publiczne, będące jednostkami samorządu terytorialnego (JST), będą zgłaszały incydent, o którym mowa w ww. ustawie, także do wojewody. W związku z tym w **OSR** należałoby:   * **w pkt 4** – „Podmioty, na które oddziałuje projekt” - wskazać także JST; * **w pkt 6** – „Wpływ na sektor finansów publicznych” - określić, czy proponowane zapisy będą powodowały skutki finansowe dla JST. Jeżeli tak to zgodnie z art. 50 ust. 2 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych projekt ustawy skutkującej zmianą poziomu dochodów lub wydatków jednostek samorządu terytorialnego wymaga określenia wysokości skutków tych zmian, wskazania źródeł ich sfinansowania oraz zaopiniowania przez Komisję Wspólną Rządu i Samorządu Terytorialnego. | **Uwaga uwzględniona** |
|  | **Koordynator Oceny Skutków Regulacji** | OSR  pkt 5 | Podanie informacji nt. planowanego czasu trwania konsultacji publicznych oraz konkretnych podmiotów, do których projekt zostanie skierowany (pkt 5 OSR). | **Uwaga uwzględniona** |
|  | **Koordynator Oceny Skutków Regulacji** | OSR  Pkt 6 | Podanie pełnej metodyki szacunków wpływu regulacji na sektor finansów publicznych, w sposób umożliwiający weryfikację poprawności tych szacunków (pkt 6 OSR). Co do zasady, wymagane jest omówienie wszystkich kanałów wpływu na sektor finansów publicznych i oszacowanie wysokości kosztów z tym związanych- suma tak uzyskanych kwot powinna odpowiadać wysokości wydatków sektora finansów publicznych w tabeli w pkt 6 OSR dla odpowiedniego roku.  Konieczne jest przy tym uwzględnienie w szacunkach wszystkich kosztów dodatkowych zadań nałożonych na organy administracji i jednoznaczne określenie, czy wszystkie te koszty pokrywane będą z części 27 – Informatyzacja, nawet w sytuacji, gdy zadaniami obciążone zostaną podmioty nie podlegające ministrowi właściwemu ds. cyfryzacji | **Uwaga uwzględniona** |
|  | **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. |
|  | **Ministerstwo Klimatu i Środowiska** | OSR  Pkt 6 | Zdanie ostatnie przed tabelą usług - powinno być "z Fundacją Bezpieczna Cyberprzestrzeń" | **Uwaga uwzględniona** |
|  | **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). |
|  | **Koordynator Oceny Skutków Regulacji** | OSR  Pkt 7 | Podanie wyczerpującego opisu wpływu regulacji na przedsiębiorców – szczególnie w odniesieniu do nakładanych nowych kosztów (tworzenie SOC), jak i ryzyk związanych z koniecznością wymiany infrastruktury w przypadku niekorzystnej oceny Kolegium ds. Cyberbezpieczeństwa (pkt 7 OSR). Wyniki szacunków powinny zostać uwzględnione w odpowiedniej tabeli; | **Uwaga częściowo uwzględniona**  Należy zauważyć, że wprowadzany w projekcie ustawy termin SOC, zastępuje dotychczasowe pojęcie odnoszące się do wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo u operatorów usług kluczowych. Pojęcie to, jak i same struktury funkcjonują już od 2 lat i wynikają z wejścia w życie ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Operatorzy usług kluczowych byli i są zobowiązani do utworzenia w swoich strukturach takich struktur lub outsourcować usługi cyberbezpieczeństwa od podmiotów rynkowych. Zatem nie ma potrzeby dokonywania dodatkowych szacunków w odniesieniu do struktur, które już są obecne u operatorów usług kluczowych.  Natomiast, w odniesieniu zarzutu braku szacunków związanych z koniecznością wymiany infrastruktury w przypadku uznania dostawcy za dostawcę wysokiego ryzyka należy wyraźnie podkreślić, że projekt nie dyskryminuje jakichkolwiek podmiotów, tylko daje narzędzia do oceny ich ryzyka dla krajowego systemu cyberbezpieczeństwa.  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. Postępowanie będzie prowadzone w oparciu o wszechstronną analizę i weźmie pod uwagę czynniki zarówno techniczne, jak i poza techniczne. 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. |
|  | **Ministerstwo Rozwoju, Pracy i Technologii** | OSR  Pkt 7 | Zbyt powierzchownie przeprowadzono również ocenę wpływu na konkurencyjność gospodarki i przedsiębiorczość (pkt 7 OSR). Nie oszacowano ile mogłaby kosztować przedsiębiorców telekomunikacyjnych wymiana sprzętu nabytego od firm pochodzących spoza UE i NATO. Nie wyjaśniono też, w jaki sposób wysokie wydatki na wymianę sprzętu wpłyną na konkurencyjność polskich przedsiębiorstw telekomunikacyjnych na rynku UE oraz na strukturę ich wydatków (mogą np. zmniejszyć zdolność do ponoszenia nakładów inwestycyjnych w innych obszarach). | **Uwaga częściowo uwzględniona**  OSR zostanie uzupełniony o wpływ niepieniężny. |
|  | **Koordynator Oceny Skutków Regulacji** | OSR Pkt 8 | Szczegółowe omówienie poszczególnych zmian obciążeń regulacyjnych, wraz ze wskazaniem, czy jest to zmniejszenie, czy podwyższenie ww. obciążeń (pkt 8 OSR). | **Uwaga uwzględniona** |
|  | **Ministerstwo Rozwoju, Pracy i Technologii** | OSR  Pkt 8 | Wskazane jest uzupełnienie punktu 8 OSR o wyliczenie nowych obciążeń regulacyjnych, takich jak choćby obowiązki SOC określone w art. 14 ust. 3, obowiązki informacyjne podmiotu prowadzącego SOC uregulowane w art. 14 ust. 6, jak również wymóg przeprowadzania przez przedsiębiorcę telekomunikacyjnego oceny ryzyka wystąpienia sytuacji szczególnego zagrożenia oraz udokumentowania tej czynności (art. 20a ust. 2) i wprowadzenie mechanizmu blokowania komunikatów przez tychże przedsiębiorców (art. 20f). W przypadku tych środków, jak również innych rozwiązań ingerujących w zasady podejmowania i wykonywania działalności gospodarczej, takich jak choćby nowych zakazów dotyczących dostawców sprzętu i oprogramowania, w stosunku do których stwierdzono wysokie ryzyko, zasadne jest przeprowadzenie oceny zgodności z przepisami Prawa przedsiębiorców (PP), a w szczególności z zasadami proporcjonalności i adekwatności (art. 67 PP) i z powinnością ograniczania obowiązków administracyjnych wobec MŚP (art. 68 PP). Zgodnie z art. 66 ust. 1 pkt 2 in fine w zw. z ust. 2 PP wyniki takiej oceny zamieszcza się w uzasadnieniu do projektu aktu normatywnego lub w ocenie skutków regulacji. | **Wyjaśnienie**  Należy zauważyć, że wprowadzany w projekcie ustawy termin SOC, zastępuje dotychczasowe pojęcie odnoszące się do wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo u operatorów usług kluczowych. Pojęcie to, jak i same struktury funkcjonują już od 2 lat i wynikają z wejścia w życie ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Operatorzy usług kluczowych byli i są zobowiązani do utworzenia w swoich strukturach takich struktur lub outsourcować usługi cyberbezpieczeństwa od podmiotów rynkowych.  Przepisy rozdziału 4a wdrażające EKŁE zostały przeniesione do projektu przepisów wprowadzających Prawo Komunikacji Elektronicznej, które znowelizują ustawę o krajowym systemie cyberbezpieczeństwa.  Przedsiębiorcy telekomunikacyjni już na mocy obecnie obowiązujących przepisów Prawa telekomunikacyjnego są zobowiązani do sporządzania planu działania na wypadek sytuacji szczególnego zagrożenia.  Blokowanie komunikatów już jest obecnie w Prawie telekomunikacyjnym.  Procedura oceny ryzyka zostanie zmieniona i będzie się do niej stosować przepisy Kodeksu Postępowania administracyjnego.  Zostanie uzupełniony OSR o ocenę zgodności Przepisów z Prawem przedsiębiorców. |
|  | **Ministerstwo Obrony Narodowej** | OSR (str. 33) | **W *Uzasadnieniu projektu - Skutki gospodarcze*** – fragmentowi na str. 33 proponuje się nadać brzmienie:  *„Skutki gospodarcze*  *Celem krajowego systemu cyberbezpieczeństwa jest zapewnienie bezpieczeństwa w cyberprzestrzeni. Poprzez nałożenie dodatkowych obowiązków na przedsiębiorców komunikacji elektronicznej związanych z dbaniem o cyberbezpieczeństwo tworzone są warunki do prowadzenia niezakłóconej działalności gospodarczej przez przedsiębiorców. Należy jednak zauważyć, że wielu z nich już obecnie posiada operacyjne centra bezpieczeństwa, ponieważ podobny wymóg istnieje w obowiązującej wersji ustawy. Poza tym, podmiot inwestujący we własne cyberbezpieczeństwo zyskuje zaufanie osób trzecich i potencjalnych kontrahentów.*  *Dostosowanie się do nowych wymogów pozwoli przedsiębiorcom skuteczniej dbać o cyberbezpieczeństwo w swojej działalności, co przełoży się na bezpieczne prowadzenie biznesu i minimalizację ryzyka strat.”*  Stwierdzenie *„Poprzez nałożenie różnych obowiązków na przedsiębiorców będących podmiotami tego systemu ogranicza się konstytucyjną wolność gospodarczą. Zobowiązuje bowiem tych przedsiębiorców do dbania o cyberbezpieczeństwo. Po stronie przedsiębiorców powoduje to koszty związane z koniecznością dostosowania się do wymogów ustawy”* - budzi kontrowersje. Należy zauważyć, że dbanie o bezpieczeństwo państwa i jego zapewnienie, w tym w dziedzinie cyberbezpieczeństwa jest obowiązkiem wszystkich organów państwowych i podmiotów, również podmiotów gospodarczych. Zatem obciążenie przedsiębiorców komunikacji elektronicznej realizacją określonych obowiązków i zadań, których koszty ponoszone będą przez nich, nie powinno być odbierane jako ograniczanie wolności gospodarczej gwarantowanej w Konstytucji RP. Wręcz odwrotnie, włączenie przedsiębiorców komunikacji elektronicznej w krajowy system cyberbezpieczeństwa tworzy warunki do bezpiecznego i niezakłóconego rozwoju gospodarczego przedsiębiorcy oraz bezpiecznego korzystania z jego usług przez inne podmioty i obywateli. | **Uwaga częściowo uwzględniona**    Uzasadnienie zostało poddane ponownej analizie pod kątem stylistycznym. |
|  | **Ministerstwo Rozwoju, Pracy i Technologii** | OSR  Informacje o wprowadzanych obciążeniach niewymaganych przez UE | Wprawdzie w OSR w polu dot. informacji o wprowadzanych obciążeniach niewymaganych przez UE zaznaczono pole "nie dotyczy", a w samym projekcie ustawy nie podano informacji o tym, że ustawa implementuje prawo UE, jednak należy przypuszczać, iż część przepisów ustawy implementuje EKŁE (być może również dyrektywę NIS), o czym poinformowano w uzasadnieniu - jeśli tak jest, to projekt powinien zostać uzupełniony o tabelę zgodności i odwróconą tabelę zgodności. | **Wyjaśnienie**  Dyrektywa NIS została w całości wdrożona ustawą z 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.  Przepisy rozdziału 4a wdrażające EKŁE zostały przeniesione do przepisów wprowadzających Prawo Komunikacji Elektronicznej. |