**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).**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Nazwa projektu dokumentu: Projekt 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).** | | | | |
| **L.p.** | **Podmiot wnoszący uwagi** | **Jednostka redakcyjna, do której wnoszone są uwagi** | **Zgłoszone uwagi** | **Stanowisko MC/DC** |
|  | Biuro Bezpieczeństwa Narodowego | Uwaga ogólna | BBN pozytywnie opiniuje projekt ustawy | **Uwaga uwzględniona** |
|  | Biuro Bezpieczeństwa Narodowego | Uwaga ogólna | Propozycja ustanowienia norm prawnych dla funkcjonowania centrów wymiany i analiz informacji (tzw. ISAC) i wpisania tych podmiotów w krajowy system cyberbezpieczeństwa zasługuje na akceptację. Współpraca podmiotów prywatnych z państwowymi przyczyni się do poprawy stanu cyberbezpieczeństwa. | **Uwaga uwzględniona** |
|  | Biuro Bezpieczeństwa Narodowego | Uwaga ogólna | Za zasadne należy uznać także przyznanie Kolegium do Spraw Cyberbezpieczeństwa kompetencji do dokonywania oceny ryzyka dostawców sprzętu i oprogramowania (np. w odniesieniu do budowy sieci 5G w Polsce) pod katem zagrożenia dla bezpieczeństwa narodowego (nowy pkt 7 w art. 65 ust. 1 oraz art. 66a i 66b). W skład Kolegium wchodzą bowiem kluczowe organy administracji państwowej właściwe w zakresie bezpieczeństwa państwa i ich wspólne stanowisko w zakresie dopuszczenia na polski rynek określonego sprzętu i oprogramowania powinno być kluczowe. | **Wyjaśnienie**  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. |
|  | Biuro Bezpieczeństwa Narodowego | Uwaga ogólna | Należy zauważyć także, ze elementy wymienione w dodawanym art. 66 ust. 4 pkt 2 ustawy, które będą brane pod uwagę przy sporządzeniu takiej oceny w stosunku do dostawców pochodzących z państw spoza Unii  Europejskiej lub NATO są zgodne z *Zaleceniami Komisji (UE) 2019/534 z dnia 26 marca 2019 r. - Cyberbezpieczeństwo sieci 5G* (Dz. U. L 88 z 29.3.2019, s. 42). Komisja Europejskawskazuje, ze działania państw członkowskich UE majce na celu wyeliminowanie zagrożeńdla cyberbezpieczenstwa w sieciach 5G powinny uwzględniać czynniki techniczne orazczynniki innego rodzaju, takie jak m.in. ogólne ryzyko wywierania wpływu przez państwotrzecie, zwłaszcza w świetle funkcjonującego w nim modelu sprawowania rządów, brakporozumień między UE a danym państwem trzecim o wsp61pracy w zakresiecyberbezpieczeństwa, czy tez dotyczących ochrony danych osobowych oraz zwalczaniacyberprzestąpczosci. Wedlug pkt 2.37 *Unijnej skoordynowanej oceny ryzyka* z 9 pazdziemika2019 r. *(EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks)* ryzykaposzczególnych dostawców państwa UE mogą ocenić w oparciu o szereg czynników. Należybrać pod uwagę fakt, iż określony dostawca może podlegać silnym niekorzystnym wpływom państwa spoza UE, wynikającym z powiązania tego dostawcy z rządem takiego państwa np. z uwagi na jego strukturę własnościową. | **Wyjaśnienie**  Tak, taki był zamiar. |
|  | Biuro Bezpieczeństwa Narodowego | Uwaga ogólna | W ocenie Biura Bezpieczeństwa Narodowego uzasadnione jest również wyposażenie Pełnomocnika do spraw Cyberbezpieczeństwa w nowe narzędzie prawne jakim jest możliwość wydawania ostrzeżeń i poleceń zabezpieczających (projektowany art. 67a i następne ustawy o krajowym systemie cyberbezpieczeństwa). | **Wyjaśnienie**  Ostrzeżenie jako miękki środek będzie wydawał Pełnomocnik. |
|  | Rzecznik Małych i Średnich Przedsiębiorców | Uwaga ogólna | W związku z pracami nad projektem ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy - Prawo zamówień publicznych, w celu uniknięcia wprowadzenia sprzecznych uregulowań z dotyczącymi bezpieczeństwa sieci i usług, zawartymi w projekt ustawy - Prawo komunikacji elektronicznej, zwracam się z uprzejmą prośbą o określenie w sposób kompleksowy, jednoznaczny oraz spójny, w jednym akcie prawnym,  kwestii z zakresu: bezpieczeństwa sieci i usług oraz cyberbezpieczeństwa odnośnie mikro przedsiębiorców, małych i średnich przedsiębiorców z branży telekomunikacyjnej. | **Wyjaśnienie**  Kwestie dotyczące bezpieczeństwa sieci i usług komunikacji elektronicznej oraz cyberbezpieczeństwa docelowo znajdą się w jednym akcie prawnym – w ustawie o krajowym systemie cyberbezpieczeństwa. Przepisy dotyczące przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci i usług komunikacji elektronicznej zostaną dodane do uKSC za pomocą ustawy wprowadzającej PKE. |
|  | Rzecznik Małych i Średnich Przedsiębiorców | Uwaga ogólna | Jednocześnie zwracam się z uprzejmą prośbą o pilne uzupełnienie dostrzeżonych braków w Projekcie. Pragnę wskazać, ze przy opracowaniu Projektu pominięto istotne wymogi dotyczące tworzenia przepisów prawa wynikające z ustawy z dnia 6 marca 2018 r. - Prawo przedsiębiorców (Konstytucja Biznesu)":  Art. 66 ust 1 pkt 2, który stanowi, ze „Przed rozpoczęciem prac nad opracowaniem projektu aktu normatywnego określającego zasady podejmowania, wykonywania ub zakończenia działalności gospodarczej dokonuje się oceny przewidywanych skutków społeczno-gospodarczych, w tym oceny wpływu na mikroprzedsiębiorców, małych i średnich przedsiębiorców oraz analizy zgodności projektowanych regulacji z przepisami ustawy".  Ponadto zgodnie z art. 66 ust 2: „ Wyniki oceny i analiz, o których mowa w ust. 1, zamieszcza się w uzasadnieniu do projektu aktu normatywnego lub w ocenie skutków regulacji, *stanowiącej odrębną część uzasadnienia projektu aktu normatywnego ".* Konstytucja Biznesu ma charakter gwarancyjny dla ok. 6000 mikro przedsiębiorców, małych i średnich przedsiębiorców z branży telekomunikacyjnej.  W przypadku stwierdzenia wpływu projektu aktu normatywnego na najmniejsze firmy *„przy opracowaniu projektu aktu normatywnego dąży się do proporcjonalnego ograniczania* *obowiązków administracyjnych wobec tych przedsiębiorców albo uzasadnia brak możliwości zastosowania takich ograniczeń"* (art. 68 Prawa przedsiębiorców), co należy powiązać z zasadami proporcjonalności i adekwatności, a w szczególności należy: *„dążyć do nienakładania nowych obowiązków administracyjnych, a jeżeli nie jest to możliwe, dążyć do ich nakładania jedynie w stopniu koniecznym do osiągniecia ich celów"* (art. 67 pkt 1 Prawa przedsiębiorców). | **Uwaga uwzględniona**  **OSR został uzupełniony.** |
|  | Rzecznik Małych i Średnich Przedsiębiorców | Uwaga ogólna | Dodatkowo w art. 40 ust. 1 Europejskiego kodeksu łączności elektronicznej  wskazuje się, na konieczność uwzględniania we wprowadzanych uregulowaniach zasady proporcjonalności przez Państwa członkowskie w razie wystąpienia zagrożenia dla bezpieczeństwa sieci lub usług. Art. 40 ust. 2 EKLE stanowi, ze aby określić istotność wpływu danego incydentu związanego z bezpieczeństwem, uwzględnia się w szczególności następujące parametry, gdy są dostępne:  a) liczbę użytkowników, których dotyczy incydent związany  z bezpieczeństwem;  b) czas trwania incydentu związanego z bezpieczeństwem;  geograficzny zasięg obszaru dotkniętego incydentem związanym  z bezpieczeństwem;  d) zakres wpływu na funkcjonowanie sieci lub usługi;  e) zakres wpływu na działalność ekonomiczną i społeczną. | **Wyjaśnienie**  Przedsiębiorcy komunikacji elektronicznej zostaną zobowiązani do wdrożenia adekwatnych (proporcjonalnych) do oszacowanego ryzyka środków technicznych lub organizacyjnych mających zapewnić bezpieczeństwo sieci lub usług komunikacji elektronicznej. Przedsiębiorcy ci będą musieli obsługiwać incydent telekomunikacyjny (leży to w ich interesie) a zgłaszać do CSIRT Telco i CSIRT poziomu krajowego te incydenty telekomunikacyjne, które będą spełniać progi incydentu. |
|  | Rzecznik Małych i Średnich Przedsiębiorców | Uwaga ogólna | Dotychczas wprowadzane obowiązki w zakresie obowiązku sporządzania i posiadania planu działańw sytuacjach szczególnego zagrożenia nie obejmują mikroprzedsiębiorcow. Uregulowania te powinny zyskać rangę ustawową, ponieważ w obecnej wersji projektu zmiany ustawy o krajowym systemie cyberbezpieczeństwa brak jednoznacznego odniesienia dotyczącego konieczności kontynuacji tych wyłączeń wobec najmniejszych firm. Dodatkowego rozważenia wymagałaby możliwość objęcia tymi włączeniami małych i średnich przedsiębiorców oraz zastosowania ww. wyłączenia w powiązanych regulacjach dotyczących bezpieczeństwa sieci i usług. | **Uwaga bezprzedmiotowa**  Uwaga ta dotyczy projektowanej ustawy Prawo komunikacji elektronicznej, która reguluje te kwestie. |
|  | Rzecznik Małych i Średnich Przedsiębiorców | Uwaga ogólna | Nakłady związane z bezpieczeństwem sieci, usług i cyberbezpieczeństwem należą do istotnie obciążających najmniejsze krajowe firmy, które posiadają mniej rozbudowane struktury administracyjne niż międzynarodowe korporacje. Istnienie tych najmniejszych firm gwarantuje jednak istnienie realnej konkurencji na rynku usług komunikacji elektronicznej (w przeciwieństwie do większości państw europejskich, co przekłada się na niższe ceny i wyższą jakość usług oferowanym konsumentom. Jak stwierdzono w uzasadnieniu do samego projektu ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy - Prawo zamówień publicznych (UD68) (str. 33): *„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 ".*  W związku z powyższym wymagana jest modyfikacja stwierdzenia  na str. 44 uzasadnienia do projektu ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy - Prawo zamówień publicznych, że: „ *Zawarte w projekcie regulacje nie będą miały wpływu na działalność mikroprzedsiębiorców, małych i średnich przedsiębiorców* *zgodnie z art. 66 ust. 2 ustawy z dnia 6 marca 2018 r. - Prawo przedsiębiorców (Dz. U. 2019r. poz. 1292, z poźń. zm.)."* i wprowadzenie stosownych uzupełnień z rozważeniemmożliwych wyłączeń lub ograniczeń obowiązków nakładanych na najmniejsze firmy. | **Wyjaśnienie**  Przepisy prawa o których mowa w uwadze zostały przeniesione do ustawy wprowadzającej ustawę - Prawo Komunikacji Elektronicznej. |
|  | Prezes Urzędu Komunikacji Elektronicznej | Uwaga ogólna | W nawiązaniu do projektowanej regulacji, która m.in. dokonuje wdrożenia części przepisów dyrektywy 2018/1972 z dnia 11 grudnia 2018 r. ustanawiającej Europejski kodeks łączności elektronicznej (dalej: EKŁE), należy wskazać na przepisy art. 40 i 41 tej dyrektywy, określające zarówno obowiązki podmiotów udostępniających publiczne sieci łączności elektronicznej lub świadczących publicznie dostępne usługi łączności elektronicznej, jak i obowiązki właściwych organów krajowych w zakresie bezpieczeństwa sieci i usług. Obowiązki te dotyczą w szczególności:  • informowania właściwych organów innych państw członkowskich oraz ENISA w przypadku istotnych incydentów bezpieczeństwa,  • podawania informacji o incydencie do wiadomości publicznej, jeśli będzie leżało to w interesie publicznym,  • przekazywania rocznego sprawozdania podsumowującego otrzymane zgłoszenia i podjęte działania w związku z zaistniałymi incydentami do Komisji Europejskiej i ENISA.  W celu realizacji powyższych obowiązków niezbędne jest posiadanie przez właściwy organ krajowy informacji o incydentach związanych z bezpieczeństwem, które miały znaczący wpływ na funkcjonowanie sieci lub usług, przekazywanych przez podmioty udostępniające publiczne sieci łączności elektronicznej lub świadczące publicznie dostępne usługi łączności elektronicznej.  EKŁE nie wskazuje czy właściwym organem krajowym powinien być regulator rynku telekomunikacyjnego czy inny organ. Projekt ustawy - Prawo komunikacji elektronicznej (dalej: projekt Pke), przekazany w dniu 29 lipca br. do uzgodnień międzyresortowych, konsultacji publicznych i opiniowania przewidywał model, w którym rolę właściwego organu spełniał regulator rynku, a podmioty udostępniające publiczne sieci łączności elektronicznej lub świadczące publicznie dostępne usługi łączności elektronicznej przekazywały mu informacje niezbędne do realizacji nałożonych obowiązków.  Natomiast w przedstawionej do zaopiniowania nowelizacji zamieszczono szereg przepisów dotyczących przekazywania informacji o incydentach związanych z bezpieczeństwem, które miały znaczący wpływ na funkcjonowanie sieci lub usług (co najprawdopodobniej będzie wiązało się z usunięciem z projektu Pke m.in. art. 39, 42, 43 ust. 2 i 3 oraz art. 44). Zgodnie z przepisami ustawy o krajowym systemie cyberbezpieczeństwa (dalej: UKSC), w brzmieniu nadawanym projektowaną ustawą, głównymi podmiotami, do których będą wpływać informacje o incydentach są CSIRT TELCO (projektowany art. 20c ust. 3 UKSC) oraz CSIRT MON, CSIRT NASK i CSIRT GOV (projektowany art. 20c ust. 1 pkt 2 UKSC). Ponadto informacje mogą być uzupełniane na żądanie ww. CSIRT (projektowany art. 20d ust. 4 UKSC). Brak jest w tych przepisach obowiązku przekazywania informacji Prezesowi UKE; w projektowanym art. 34a UKSC wskazano jedynie, iż CSIRT współpracują z Prezesem UKE, a informacje o incydencie otrzymuje on wyłącznie na żądanie (w tym kontekście niejasna jest wytyczna do wydania rozporządzenia wskazana w projektowanym art. 20c ust. 4 UKSC).  Należy przy tym zaznaczyć, że część przepisów dotyczących obowiązków właściwego organu krajowego nadal pozostanie w projekcie Pke i będą to obowiązki Prezesa UKE (np. określone w art. 40 i 46 projektu Pke). Pojawia się zatem wątpliwość czy taki model transpozycji EKŁE do krajowego porządku prawnego zapewni możliwość właściwego wykonywania obowiązków przez Prezesa UKE. | **Wyjaśnienie**  Implementacja dyrektywy EKŁE zostanie zrealizowana poprzez projektowaną ustawę – Prawo Komunikacji Elektronicznej oraz dokonanie odpowiednich zmian w ustawie o krajowym systemie cyberbezpieczeństwa(kwestie dotyczące bezpieczeństwa sieci i usług oraz włączenie przedsiębiorców komunikacji elektronicznej do podmiotów ksc). Kwestia właściwej implementacji EKŁE jest zsynchronizowana. |
|  | Prezes Urzędu Komunikacji Elektronicznej | Uwaga ogólna | Należy poddać pod wątpliwość zasadność przeniesienia z projektu Pke do UKSC definicji pojęcia „bezpieczeństwo sieci i usług”, niezwiązanej z wprowadzanym projektowaną ustawą do UKSC pojęciem „incydent telekomunikacyjny” (w Pke definicję tę związano z pojęciem  incydentu bezpieczeństwa). Opcjonalnym rozwiązaniem jest zmiana zaproponowanej definicji incydentu telekomunikacyjnego w ten sposób by odpowiadał on definicji incydentu bezpieczeństwa z projektu PKE. Definicje incydentu bezpieczeństwa i bezpieczeństwa sieci i usług w projekcie Pke zostały zaprojektowane z uwzględnieniem definicji EKŁE (tak by były ze  sobą powiązane) i po długotrwałych dyskusjach, mających na celu harmonizację transpozycji narodowych tych pojęć, prowadzonych przez grupę roboczą do spraw art. 13 w ramach ENISA. Wprowadzenie nowego pojęcia „incydent telekomunikacyjny” niezgodnego z pojęciem „incydent bezpieczeństwa”, zaproponowanym w Pke, może spowodować nieprawidłową transpozycję EKŁE (problemy interpretacyjne, niewłaściwe raportowanie incydentów przez zobowiązane podmioty, utrudnienia we współpracy europejskiej w zakresie informowania o incydentach innych państw członkowskich i ENISA); | **Uwaga uwzględniona**  Te przepisy zostały przeniesione do przepisów wprowadzających Prawo Komunikacji Elektronicznej. |
|  | Prezes Urzędu Komunikacji Elektronicznej | Uwaga ogólna | Należy wskazać na brak jednoznacznie przypisanej właściwości CSIRT sektorowych i CSIRT Telco w odniesieniu do przedsiębiorców telekomunikacyjnych wchodzących w skład innych sektorów, np. sektora Infrastruktura Cyfrowa (dot. operatorów IXP). Ustawa wprowadza obowiązek utworzenia CSIRT sektorowego, więc dla tych przedsiębiorców telekomunikacyjnych będzie właściwy zarówno CSIRT IC, jak i CSIRT Telco. | **Uwaga nieuwzględniona**  CSIRT Telco będzie właściwy dla przedsiębiorców komunikacji elektronicznej w zakresie incydentów dotyczących bezpieczeństwa sieci i usług komunikacji elektronicznej. Innym zakresem będzie dotyczyć właściwość CSIRT sektorowego dla sektora infrastruktury cyfrowej. |
|  | Agencja Wywiadu | Uwaga ogólna | Ponadto, Agencja Wywiadu poddaje pod rozwagę ewentualne doprecyzowanie roli i funkcji CSIRT sektorowego. Należy bowiem zauważyć, że w świetle projektowanych przepisów CSIRT sektorowy nie ma możliwości zlecenia pełnienia swoich zadań podmiotom spoza administracji rządowej, np. spółkom z udziałem Skarbu Państwa. | **Uwaga nieuwzględniona**  CSIRT sektorowy ma być powołany przez organ właściwy dla danego sektora lub podsektora Ten organ będzie decydował która z jednostek przez niego nadzorowanych lub mu podlegająca będzie wykonywać zadania CSIRT sektorowego. Będzie miał także możliwość wyznaczenia innego podmiotu.  Innymi słowy to organ właściwy ma zdecydować który podmiot ma pełnić funkcję CSIRT sektorowego. Sam CSIRT nie powinien zlecać pełnienia swoich zadań innym podmiotom. Dla zapewnienia sprawności działania CSIRT ważne jest, aby zadania SOC i CERT były realizowane w ramach jednego podmiotu, a nie w modelu rozproszonym. |
|  | Prezes Urzędu Ochrony Danych Osobowych | Art. 1 pkt 5 | Z punktu widzenia unormowań *rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych* *i w sprawie swobodnego przepływu takich danych* *oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)* (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.1)), powoływanego dalej z zastosowaniem skrótu „RODO”, **doprecyzowania wymagają wprowadzane przez projekt ustawy nowelizującej – przepisy dotyczące danych kontaktowych**.  Skoro bowiem – stosownie do dyspozycji art. 5 ust. 1 lit. c RODO – dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych”), to – celem zagwarantowania zgodności z tą zasadą dotyczącą przetwarzania danych osobowych – zachodzi potrzeba wskazania  katalogu danych, które Projektodawca uznaje za „dane kontaktowe” osoby reprezentującej ISAC zamieszczone w wykazie ISAC [art. 4a ust. 3 pkt 2 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2020 r. poz. 1369). | **Uwaga uwzględniona**  Przepis zostanie został doprecyzowany. |
|  | Prezes Urzędu Ochrony Danych Osobowych | Art. 1 pkt 10 | Za wprowadzeniem do ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (przez odpowiednią zmianę tej ustawy przewidzianą w przepisach projektu ustawy nowelizującej) katalogu danych uznawanych przez Projektodawcę za „dane kontaktowe” przemawia przy tym okoliczność, iż w art. 14 ust. 6 pkt 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (w brzmieniu nadanym przez art. 1 pkt 10 projektu ustawy nowelizującej) pojęcie „danych kontaktowych” zostało potraktowane przez Projektodawcę jako pojęcie otwarte. Takie rozumienie pojęcia „danych kontaktowych”, na gruncie – przytaczanej wyżej – zasady minimalizacji danych, organ właściwy w sprawie ochrony danych osobowych uznaje za niewłaściwe i dlatego wskazuje potrzebę doprecyzowania przepisów dotyczących danych kontaktowych. Jeśli zaś zamiarem Projektodawcy jest wprowadzenie w poszczególnych przepisach ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa różnych katalogów danych składających się na pojęcie „danych kontaktowych” (w konkretnym przepisie tej ustawy), to takie rozwiązanie musi również znaleźć odzwierciedlenie w projekcie ustawy nowelizującej. | **Uwaga uwzględniona**  Przepis został doprecyzowany |
|  | Prezes Urzędu Ochrony Danych Osobowych | Art. 1 pkt 14 | **Doprecyzowania wymaga sformułowanie „dane kontaktowe” osób**  **z poszczególnych podmiotów publicznych w województwie, wskazanych przez kierownictwo tych podmiotów, do współpracy z właściwymi CSIRT MON, CSIRT NASK lub CSIRT GOV** (art. 24a pkt 2 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa | **Uwaga uwzględniona**  Przepis został doprecyzowany. |
|  | Komisja Nadzoru Finansowego | Art. 2 pkt 8f | 8f) bezpieczeństwo sieci i usług -– zdolność sieci telekomunikacyjnych lub usług komunikacji elektronicznej do odpierania ~~wszelkich~~ działań naruszających dostępność, autentyczność, integralność lub poufność:  (…)  Użycie słowa ***wszelkich*** (za słownikiem PWN: *wszelki – każdy, jaki tylko istnieje,* *każdy bez wyjątku, każdy możliwy*) jest w opinii KNF zbyt daleko idące, ponieważ powoduje, że w takim rozumieniu żadna  sieć i usługi nie byłyby uznane za bezpieczne. Proponujemy wykreślenie słowa ***wszelkich***, co byłoby zgodne z terminem przywołanym w uzasadnieniu projektu do zmiany ustawy (str. 35). | **Uwaga nieuwzględniona.**  Przepis nie mówi o tym, że sieci mają być odporne na wszelkie działania tylko, że mają mieć zdolność do odpierania. Nie jest zamiarem projektodawcy, żeby stworzyć sieci lub usługi, w których nigdy nie dojdzie do negatywnego zdarzenia, bo jest to niemożliwe. Celem jest nałożenie obowiązków stosowania metod i narzędzi służących do odpierania tych zdarzeń. |
|  | Najwyższa Izba Kontroli | Art. 4 | Proponuję dodać do art. 4 ustawy o KSC Państwowe Gospodarstwo Wodne Wody Polskie, które jest państwową osobą prawną jak Narodowy Fundusz Ochrony Środowiska i Gospodarki Wodnej. PGW WP utworzone zostało z dniem 1 stycznia 2018 r. | **Uwaga uwzględniona** |
| 1. . | Biuro Bezpieczeństwa Narodowego | Art. 4a | Wymaga dopracowania pod względem prawnym i legislacyjnym. w szczególności:  1) należałoby wskazać, iż ISAC „funkcjonuje" w ramach krajowego systemu  cyberbezpieczeństwa, zamiast „może funkcjonować". ISAC może być utworzony (fakultatywnie, bo nie przewiduje się obowiązku działania), ale gdy już powstanie powinien obligatoryjnie funkcjonować w krajowym systemie cyberbezpieczeństwa;  2) czy nie byłoby wskazane określenie w przepisach ustawy formy prawnej, w jakiej funkcjonuje ISAC: czy podmioty te tworzone są na podstawie umowy między przedsiębiorcami? Jak i kto je tworzy? Z omawianego projektu ustawy wynika, ze wpisanie do wykazu ISAC i wykreślenie z tego wykazu oraz zmiana danych wykazie ISAC jest czynnością materialno-techniczną. Zatem wpis do wykazu nie tworzy tego podmiotu i *de facto* nie ma znaczenia dla jego statusu;  3) nie jest jasne dlaczego w art. 4a ust. 3 pkt 3-5 dopuszcza się fakultatywność posiadania przez ISAC siedziby i adresu, NIP oraz numeru w rejestrze. | **Uwaga nieuwzględniona**  Utworzenie ISAC jest inicjatywą dobrowolną. Ustawa celowo nie nakłada wiele obowiązków na ISAC aby były łatwe do utworzenia i dodania w ramach KSC. Podkreślić należy, że do tej pory można było tworzyć ISAC w różnych formach prawnych – ustawa daje tylko możliwość dodania ISAC do KSC.  Wykaz ISAC ma zawierać dane w tym numer rejestru (np. numer KRS), jeżeli został nadany. |
|  | Komisja Nadzoru Finansowego | Art. 4a ust 4 | **Propozycja zmiany:**  Wpisanie do wykazu ISAC i wykreślenie z tego wykazu następuje na  wniosek podmiotu prowadzącego ISAC po uzyskaniu pozytywnej opinii CSIRT MON, CSIRT NASK lub CSIRT GOV oraz **organu właściwego dla sektora, w którym będzie działał ISAC.**  **Uzasadnienie:**  Uwzględnienie przez ministra właściwego do spraw informatyzacji opinii organu właściwego wyspecjalizowanego w funkcjonowaniu sektora, w którym planuje działać ISAC. Ponadto konieczne jest zdefiniowanie przez Ustawodawcę kryteriów oceny dokonywanej przez zespoły CSIRT i OW. Zgodnie z zaproponowanymi zmianami do Ustawy informacje przedstawione przez podmiot ubiegający się o statut ISAC zawierają jedynie dane teleadresowe co nie daje podstaw do wydania pozytywnej opinii przez CISRTy oraz OW. | **Uwaga częściowo uwzględniona**  ISAC mogą działać na rzecz podmiotów z różnych sektorów jak również podmiotów spoza krajowego systemu cyberbezpieczeństwa. W nowej wersji projektu zrezygnowano z opiniowania ISAC przez CSIRT poziomu krajowego natomiast będą opiniować wszystkie organy właściwe do spraw cyberbezpieczeństwa. |
|  | Komisja Nadzoru Finansowego | Art. 4a ust. 9 | **Propozycja zmiany:**  ISAC współpracują z CSIRT MON, CSIRT NASK, CSIRT GOV **i CSIRT sektorowymi oraz organem właściwym dla danego sektora, a także** przedkładają ministrowi właściwemu do spraw informatyzacji w terminie do dnia 31 marca każdego roku sprawozdanie z realizacji zadań za poprzedni rok kalendarzowy.  **Uzasadnienie:**  Uzasadnione wydaje się rozszerzenie katalogu podmiotów, z którymi możliwa będzie współpraca ISAC w ramach krajowego systemu cyberbezpieczeństwa. | **Uwaga uwzględniona**  **P**rzepis został zmieniony. |
|  | Komisja Nadzoru Finansowego | Art. 14 ust. 6 | **Propozycja zmiany:**  Podmiot niebędący operatorem usługi kluczowej, prowadzący SOC udostępnia na swojej stronie internetowej co najmniej następujące informacje na temat swojej działalności:  1) nazwa SOC i posiadanych przez SOC kompetencji;  2) zakres właściwości, w tym:  a) oferowany rodzaj wsparcia,  b) zasady współpracy i wymiany informacji,  c) politykę komunikacji i uwierzytelniania informacji;  3) oferowane usługi, w tym politykę obsługi incydentów i koordynacji  incydentów;  4) dane kontaktowe, w tym:  a) adres ze wskazaniem strefy czasowej,  b) numer telefonu, adres poczty elektronicznej oraz wskazanie innych dostępnych środków komunikacji z SOC,  c) dane o wykorzystywanych kluczach publicznych i sposobach szyfrowania komunikacji z SOC,  d) sposoby kontaktu z SOC, w tym sposób zgłaszania incydentów.  **Uzasadnienie:**  Ta regulacja jest sprzeczna z podstawowymi zasadami ochrony informacji wrażliwych. W opinii UKNF, Ustawa powinna wręcz  zakazywać podmiotom świadczącym usługi SOC udostępnianie na stronie internetowej tak szerokiego katalogu informacji, oraz obligować OUK do wprowadzenia do umów zawieranych z takimi podmiotami obowiązku ochrony informacji oraz zachowania pełnego NDA. Informacje o tym, który operator SOC świadczy usługi dla OUK w prostej drodze prowadzi do wykorzystania tych informacji jako wektora ataków, ukierunkowanego w pierwszej kolejności na SOC, a na dalszym etapie na OUK. W sytuacji, w której SOC będzie świadczył swoje usługi więcej niż jednemu OUK (istnieje również możliwość, że będą to OUK z różnych sektorów gospodarki)  generuje to w opinii UKNF wysokie ryzyko ukierunkowania działań  cyberprzestępczych na te podmioty. | **Uwaga częściowo uwzględniona**  Projekt nawiązuje do praktyki rynkowej – udostępniania informacji według wzoru dokumentu RFC 2350. Sformułowanie *zakres właściwości* zostało zastąpione sformułowaniem *zakres obszaru działania.* |
|  | Najwyższa Izba Kontroli | Pkt 12 - art. 20a ust. 3, art. 20 c ust. 1 pkt 1 | Dopisać – „ustawa z dnia ... - Prawo komunikacji elektronicznej". | **Uwaga uwzględniona** |
|  | Najwyższa Izba Kontroli | pkt 15 - art. 26 ust.2, ust. 3 pkt 21; pkt 16 - art.32 ust. 4; pkt 26 - art. 46 ust. 2b oraz pkt 29 - art. 66c ust.1 | Zostało wprowadzone pojęcie „podmiot krajowego systemu cyberbezpieczeństwa", które to podmioty wymienione są w art. 4 ustawy o krajowym systemie cyberbezpieczeństwa (zwana dalej „ustawa o KSC").  Projektodawca w ww. przepisach nie odnosi się konkretnie, których podmiotów - wymienionych w art. 4 ustawy **o** KSC – dotyczą te przepisy. Czy dotyczy to wszystkich wymienionych w art. 4 ustawy o KSC czy tez niektóre podmioty powinny zostać wyłączone?  Ponadto np. z pkt 15 - art. 26 ust.2 i ust. 3 pkt 21; pkt 16 -  art. 32 ust. 4 niniejszego projektu CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT sektorowy i CSIRT Telco, które są podmiotami objętymi krajowym systemem cyberbezpieczeństwa, wynika jakby nie byty one tymi podmiotami. Natomiast w pkt 30 - art. 67a ust. 4 pkt 1 odniesiono się do konkretnych punktów w art. 4 ustawy o KSC.  W świetle powyższego należy się zastanowić, czy może zastosować we wszystkich przepisach, do których jest odniesienie do podmiotów objętych krajowym systemem cyberbezpieczeństwa zasadę, ze przywoływany jest art. 4 ze stosownymi punktami. Należy również rozważyć wprowadzenia zamiast pojęcia „podmiot krajowego systemu cyberbezpieczeństwa" pojęcie „podmiot objęty krajowym systemem cyberbezpieczeństwa", co byłoby zgodne z art. 4 ustawy o KSC. | **Wyjaśnienie**  Użyte sformułowanie *podmiot krajowego systemu cyberbezpieczeństwa*  odnosi się do katalogu podmiotów określonego w art. 4. |
|  | Najwyższa Izba Kontroli |  | W pkt 15 lit. d - należy dodać art. 42 ust. 8 - pkt 23 niniejszego projektu i zamiast lit. d) w tym punkcie utworzyć nowy punkt, bowiem odnosi się nie tylko do art. 26, albo wyłączyć z pkt 15 lit. d art, 49 ust. 3 pkt 2 i po pkt 26 utworzyć nowy punkt. | **Uwaga uwzględniona** |
|  | Najwyższa Izba Kontroli | Art. 1 pkt 24 lit c - art. 44 ust. 6 i art. 2 PZP | W danych promulgacyjnych dopisać Dz. U. z 2020 r. poz. 288 i 1492. | **Uwaga uwzględniona** |
|  | Prezes Urzędu Komunikacji Elektronicznej | Art. 20a | Niejasny jest cel przeniesienia przepisów art. 39 projektu Pke do projektowanego art. 20a UKSC. Przepisy te stanowią całość i są tematycznie związane z dalszymi przepisami projektu Pke, a w szczególności z art. 40 i 41 projektu Pke. | **Wyjaśnienie**  Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE.  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.  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. |
|  | Prezes Urzędu Komunikacji Elektronicznej | Art. 34a  Art. 20a  Art. 20c  Art. 46 | Proponuje się uzupełnienie projektu o wymóg niezwłocznego informowania Prezesa UKE o incydentach związanych z bezpieczeństwem, które miały znaczący wpływ na funkcjonowanie sieci lub usług – w taki sposób, aby było to dokonywane przez CSIRT TELCO albo przez podmioty zobowiązane równocześnie z poinformowaniem CSIRT TELCO. Proponuje się także dodanie przepisów obligujących podmioty zobowiązane do przekazywania informacji uzupełniających o incydentach na żądanie Prezesa UKE. Należy bowiem zaznaczyć, że zaproponowane rozwiązanie (projektowany art. 34a UKSC), polegające na przekazywaniu przez CSIRT'y Prezesowi UKE informacji o incydentach jedynie na jego żądanie, przy jednoczesnym pozostawieniu w projekcie Pke rozwiązań nakładających na Prezesa UKE obowiązek informowania innych państw członkowskich, Komisji Europejskiej i ENISA o incydentach (art. 46 projektu Pke), czyni obowiązek Prezesa UKE trudnym do wykonania lub wręcz niewykonalnym. Ponadto zaproponowane w projekcie UKSC rozwiązanie polegające na przeniesieniu z projektu Pke obowiązków przedsiębiorców komunikacji elektronicznej do podejmowania określonych środków i przekazywania informacji o incydentach telekomunikacyjnych (projektowane art. 20a i 20c UKSC) przy jednoczesnym pozostawieniu w projekcie Pke kompetencji Prezesa UKE do ich kontroli i penalizacji (art. 385 i art. 409 projektu Pke) czyni tę kompetencję Prezesa UKE wątpliwą pod względem efektywnej realizacji. | **Wyjaśnienie**  Procedura przekazywania informacji o incydencie telekomunikacyjnym zostanie ustalona przez CSIRT krajowe i CSIRT Telco oraz Prezesa UKE.  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. |
|  | Komisja Nadzoru Finansowego | Art. 41 pkt 4 | **Propozycja zmiany:**  dla sektora bankowego i infrastruktury rynków finansowych - **Komisja Nadzoru Finansowego;**  **Uzasadnienie:**  Organem właściwym dla sektora bankowego i infrastruktury rynków  finansowych powinna zostać **Komisja Nadzoru Finansowego. Zgodnie z art. 3 ust. 1 ustawy o nadzorze nad rynkiem finansowym „**Urząd Komisji *Nadzoru Finansowego*, zwany dalej "UrzędemKomisji", jest państwową osobą prawną,której zadaniem jest zapewnienie obsługiKomisji *Nadzoru Finansowego* iPrzewodniczącego Komisji *Nadzoru Finansowego”*. Organem uprawnionym dowykonywania władzy publicznej jest KNF,dlatego tylko KNF może być organem właściwym dla sektora bankowego i infrastruktury rynków finansowych. | **Uwaga uwzględniona.** |
|  | Komisja Nadzoru Finansowego | Art. 41 pkt 12  Propozycja KNF | **Propozycja zmiany:**  12) dla SOC wykonujących usługi na zlecenie operatora usług kluczowych - minister właściwy do spraw informatyzacji.  **Uzasadnienie:**  W opinii KNF to minister właściwy do spraw informatyzacji powinien zostać wskazany jako organ właściwy dla SOC świadczących usługi na zlecenie OUK. Koreluje to z dalszą propozycją zmiany art. 74 ust. 1a pkt. 4 (nakładanie kar). Brak określenia w art. 41 organu właściwego dla „zewnętrznych” SOC, działających na zlecenie OUK, może w pewnych warunkach generować problemy natury formalnej – opisane poniżej. Dodany do projektu art. 14a określa, że minister właściwy do spraw informatyzacji prowadzi wykaz SOC. Wpisanie do wykazu SOC i wykreślenie z tego wykazu, a także zmiana danych (choć w tym ostatnim przypadku nie ujęto tego wprost), następowałoby na wniosek organu właściwego do spraw cyberbezpieczeństwa po uzyskaniu informacji od OUK. Można  przyjąć, że wniosek składałby organ właściwy dla OUK, ponieważ to do niego OUK wysyła informację, zgodnie z art. 14 ust. 4.  Może pojawić się okoliczność, w której SOC będzie świadczył usługi dla kilku OUK z różnych sektorów, które będą podlegały pod różne organy właściwe. Wobec tego kolejny organ właściwy usiłowałby złożyć wniosek o wpisanie SOC, z którym OUK zawarł umowę, do wykazu SOC, choć ten już by w wykazie istniał. Problem ujawnia się także w kwestii nakładania kar na SOC przez organ właściwy (według właściwości dla OUK), uregulowanego w art. 74 ust. 1a projektu. Mogłoby to powodować, że różne organy właściwe mogłyby chcieć nakładać na SOC kary za te same nieprawidłowości.  Art. 4 pkt. 16 określa, że krajowy system cyberbezpieczeństwa obejmuje m.in. SOC. Dlatego art. 41 powinien wskazywać organ właściwy również dla SOC wykonujących usługi dla operatorów usług kluczowych. | **Uwaga uwzględniona** |
|  | Komisja Nadzoru Finansowego | Art. 42 ust. 1 pkt 7 | **Propozycja zmiany:**  7) wzywa na wniosek CSIRT NASK, CSIRT GOV, CSIRT MON lub **CSIRT sektorowego** operatorów usług kluczowych lub dostawców usług  cyfrowych do usunięcia w wyznaczonym terminie podatności, które doprowadziły lub mogły doprowadzić do incydentu poważnego, istotnego lub krytycznego;  **Uzasadnienie:**  Analogicznie do treści art. 42 ust. 1 pkt 5, KNF sugeruje dodanie również CSIRTsektorowego. Wynika to niejako z regulacji pkt. 5, w którym organ właściwy we współpracy również z CSIRT sektorowymi przygotowuje rekomendacje dot. cyberbezpieczeństwa, w tym wytyczne sektorowe dotyczące zgłaszania incydentów. | **Uwaga uwzględniona**  Przepis został zmieniony. |
|  | Komisja Nadzoru Finansowego | Art. 44 ust 1 pkt 5 | **Propozycja zmiany:**  Współpraca z CSIRT MON, CSIRT NASK i CSIRT GOV, **a także CSIRT sektorowymi oraz ISAC,** w zakresie wymiany informacji i reagowania na incydenty poważne i krytyczne oraz wymianę informacji o zagrożeniach.  **Uzasadnienie:**  Zasadne jest rozszerzenie podmiotów, z którymi może współpracować CSIRT sektorowy w ramach realizacji swoich zadań. | **Uwaga nieuwzględniona**  ISAC nie jest jednostką operacyjną. Nie będzie miał żadnych kompetencji w kontekście zgłaszania incydentów. |
|  | Urząd Zamówień Publicznych | Art. 44 ust. 6 | Niezależnie od uwag UZP dotyczących zmian projektowanych w ustawie Pzp, należy zwrócić uwagę na art. 1 pkt 24 lit. c projektu ustawy, w którym proponuje się dodanie m.in. ust. 6 do art. 44 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Projektowany przepis przewiduje, że w przypadku braku możliwości realizacji zadań CSIRT sektorowego w trybie określonym w ust. 1 lub ust. 5 art. 44, organ właściwy może, po zasięgnięciu opinii Pełnomocnika, powierzyć realizację zadań CSIRT sektorowego podmiotowi, o którym mowa w art. 4 ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych (Dz. U. poz. 2019), oraz określić szczegółowy zakres realizowanych przez niego zadań, biorąc pod uwagę: 1) wymóg posiadania przez ten podmiot przygotowania technicznego i przeszkolonego personelu oraz doświadczenia w zakresie reagowania na incydenty, analizowania incydentów poważnych, wyszukiwania powiązań pomiędzy incydentami oraz opracowywania wniosków z obsługi incydentu, a także mając na względzie; 2) konieczność współpracy tego podmiotu z właściwym CSIRT MON, CSIRT NASK i CSIRT GOV; 3) poziom cyberbezpieczeństwa i liczbę podmiotów w danym sektorze oraz incydenty, które w nim wystąpiły. W związku z powyższym, odpowiednio do intencji projektodawcy, wnoszę o uzupełnienie projektowanego przepisu o wymóg, aby powierzenie zadania, o którym w nim mowa, następowało w oparciu o przepisy Pzp, albo o odpowiednie uzupełnienie uzasadnienia projektu ustawy o wskazanie podstawy wyłączenia stosowania przepisów ustawy Pzp | **Wyjaśnienie**  Odesłanie do ustawy - Prawo zamówień publicznych dotyczy wskazania podmiotów, nie chodzi o stosowanie trybu powierzenia wykonania zadania publicznego. |
|  | Komisja Nadzoru Finansowego | Art. 44a ust. 4 pkt 5 | **Propozycja zmiany:**  współpraca z CSIRT MON, CSIRT NASK i CSIRT GOV**, a także CSIRT sektorowymi oraz ISAC,** w zakresie wymiany informacji i reagowania na incydenty telekomunikacyjne i krytyczne oraz wymianę informacji o zagrożeniach.  **Uzasadnienie:**  Zasadne jest rozszerzenie podmiotów, z którymi może współpracować CSIRT Telco (jako również „sektorowy”) w ramach realizacji swoich zadań. | **Uwaga nieuwzględniona**  ISAC nie jest jednostką operacyjną. Nie będzie miał żadnych kompetencji w kontekście zgłaszania incydentów.  Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o krajowym systemie cyberbezpieczeństwa poprzez ustawę wprowadzającą ustawę – Prawo Komunikacji Elektronicznej. |
|  | Agencja Wywiadu | Art. 66a | W odniesieniu do proponowanego brzmienia art. 66a ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, sam fakt wprowadzenia w ust. 1 tego przepisu możliwości sporządzenia przez Kolegium, na wniosek członka Kolegium, oceny ryzyka dostawcy sprzętu lub oprogramowania istotnego dla cyberbezpieczeństwa podmiotów krajowego systemu cyberbezpieczeństwa, należy ocenić pozytywnie i podkreślić, iż przyznanie ww. uprawnienia Kolegium jest zasadne. | **Wyjaśnienie**  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. |
|  | Agencja Wywiadu | Art. 66a | W odniesieniu do projektowanego art. 66a ww. ustawy Agencja Wywiadu zwraca także uwagę, iż w ww. przepisie nie został wskazany zakres czasowy w jakim Kolegium może sporządzić ocenę ryzyka dostawcy sprzętu lub oprogramowania istotnego dla cyberbezpieczeństwa podmiotów krajowego systemu cyberbezpieczeństwa. Jedyne ramy czasowe jakie ujęto w ww. przepisie odnoszą się do terminu (14 dni od publikacji komunikatu o sporządzonej ocenie) na odwołanie się dostawcy sprzętu lub oprogramowania, którego dotyczy ocena określająca wysokie ryzyko. Termin na rozpatrzenie odwołania przez Kolegium również został określony i ma wynosić 2 miesiące. | **Wyjaśnienie**  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. |
|  | Agencja Wywiadu | Art. 66a ust. 2 pkt 2 | W zawartym w projekcie brzmieniu art. 66a ust. 2 w pkt 2 ww. ustawy przewidziano, że wniosek o sporządzenie oceny ma zawierać wskazanie możliwych obszarów działalności, w których dostawca sprzętu lub oprogramowania może stanowić zagrożenie dla bezpieczeństwa narodowego. Należy jednak zaznaczyć, że na gruncie prawa krajowego, ani w systemie prawnym Unii Europejskiej nie istnieje definicja legalna pojęcia „bezpieczeństwo narodowe”. Przedmiotowe pojęcie występuje w art. 4 ust. 2 Traktatu o Unii Europejskiej, który stanowi, że *„Unia szanuje równość Państw Członkowskich wobec Traktatów, jak również ich tożsamość narodową, nierozerwalnie związaną z ich podstawowymi strukturami politycznymi i konstytucyjnymi, w tym* w *odniesieniu do samorządu regionalnego i lokalnego. Szanuje podstawowe funkcje państwa, zwłaszcza funkcje mające na celu zapewnienie jego integralności terytorialnej, utrzymanie porządku publicznego oraz ochronę bezpieczeństwa narodowego. W szczególności bezpieczeństwo narodowe pozostaje w zakresie wyłącznej odpowiedzialności każdego Państwa Członkowskiego.".*  Należy podkreślić, iż ostatnie zdanie przywołanej powyżej regulacji Traktatu budzi wiele kontrowersji, jeśli chodzi o zakres kompetencji wyłącznej Państw Członkowskich w odniesieniu do sfery bezpieczeństwa narodowego, w szczególności biorąc pod uwagę tendencję do „zawłaszczania” tych kompetencji przez Unię Europejską.  Mając powyższe na uwadze, zdaniem Agencji Wywiadu, należy rozważyć zastąpienie w proponowanym brzmienu art. 66a ust. 2 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa określenia „bezpieczeństwo narodowe" wyrażeniem „bezpieczeństwo wewnętrzne i zewnętrzne państwa, o których mowa w art. 1 i 2 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. 2020 poz. 27)". | **Uwaga nieuwzględniona**  Według powszechnego stanowiska doktryny pojęcie bezpieczeństwa narodowego obejmuje bezpieczeństwo wewnętrzne i zewnętrzne Państwa. |
|  | Agencja Wywiadu | Art. 66a ust. 4 pkt 2 | Ponadto, w ocenie Agencji Wywiadu, należy rozważyć czy w zawartym w projekcie brzmieniu art. 66a ust. 4 pkt 2 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa właściwe jest użycie sformułowania, „prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego (...)". Ww. kryterium jest wysoce nieprecyzyjne i może budzić wątpliwości w toku sporządzania oceny. W opinii Agencji Wywiadu zasadnym wydaje się zmiana tego określenia na bardziej konkretne i precyzyjnie określające relację dostawcy sprzętu lub oprogramowania z danym państwem.  W nawiązaniu do powyższego, w projektowanym brzmieniu art. 66a ust. 4 pkt 2 w lit c przywołanej wyżej ustawy, Agencja Wywiadu poddaje pod rozwagę możliwość doprecyzowania tego przepisu poprzez zastąpienie wyrazów „porozumień w zakresie ochrony danych miedzy UE i danym państwem" wyrazami „porozumień w zakresie ochrony danych osobowych między UE a państwami spoza UE". Zdaniem Agencji Wywiadu, zasadne byłoby również doprecyzowanie zawartego w projekcie brzmienia art. 66a ust. 4 pkt 2 ww. ustawy także lit. d poprzez wskazanie, iż w sporządzaniu oceny uwzględnia się, oprócz struktury własnościowej dostawcy sprzętu lub oprogramowania, także powiązania kapitałowe i organizacyjne tego dostawcy. | **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. |
|  | Prezes Urzędu Komunikacji Elektronicznej | Art. 66b ust. 1 pkt 1 | Zaproponowany w projektowanym art. 66b ust. 1 pkt 1 UKSC obowiązek niewprowadzania do użytkowania przez podmioty krajowego systemu cyberbezpieczeństwa, sprzętu, oprogramowania i usług od dostawcy, który uzyskał wysoką ocenę ryzyka, nie uwzględnia okresu eksploatacji sprzętu co może wpłynąć znacząco na obciążenia finansowe przedsiębiorców. | **Wyjaśnienie**  W zaproponowanych przepisach prawa nie ma mechanizmu nakazującego natychmiastowe wycofanie sprzętu lub oprogramowania wskazanego w ocenie ryzyka dostawców. Podmioty krajowego systemu cyberbezpieczeństwa, w tym operatorzy usług kluczowych, czy przedsiębiorcy telekomunikacyjni, zostaną zobowiązani do wycofania danego sprzętu lub oprogramowania w określonym czasie. W projekcie jest mowa o 7 latach - termin ten jest często uznawany za średni okres użytkowania sprzętu lub oprogramowania, czyli tzw. cykl życia urządzenia. Z uwagi na wskazanie tak długiego okresu na wdrożenie decyzji o ocenie ryzyka, nie są planowane rekompensaty dla operatorów z uwagi na konieczność wycofania sprzętu lub oprogramowania od dostawców uznanych za dostawców wysokiego ryzyka. |
|  | Agencja Wywiadu | Art. 66b ust. 1 pkt 2  Art. 66b ust. 2 | Ponadto, w ocenie Agencji Wywiadu, warte rozważenia byłoby również doprecyzowanie, czy w świetle projektowanego przepisu art. 66b ust. 1 pkt 2 oraz ust. 2 pkt 2 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, podmioty krajowego systemu cyberbezpieczeństwa będą mogły kontynuować użytkowanie dotychczas posiadanych egzemplarzy sprzętu, oprogramowania oraz usług wykorzystywanych przed opublikowaniem komunikatu o ocenie danego dostawcy, w przypadku gdy wskutek wystąpienia nowych okoliczności mogących mieć wpływ na ocenę ryzyka tego dostawcy, ocena ta zostanie zmieniona przez Kolegium z oceny określającej wysokie ryzyko ww. dostawcy na ocenę określającą umiarkowane ryzyko dostawcy (*vide* art. 66a ust. 9). | **Uwaga nieuwzględniona**  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego.  W takiej sytuacji, jak opisana w uwadze będzie miał zastosowanie art. 145 KPA.  Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. |
|  | Prezes Urzędu Ochrony Konkurencji i Konsumentów | Art. 66a-66c  Art. 1 pkt 29 Projektu | Należy zwrócić uwagę, iż przyznanie Kolegium ds. Cyberbezpieczeństwa (dalej jako: „**Kolegium”**) kompetencji do oceny stopnia ryzyka dla cyberbezpieczeństwa Państwa u dostawców sprzętu, oprogramowania czy usług przy wykorzystaniu nieostrych kryteriów klarowności (art. 1 pkt 29 Projektu) może prowadzić do powstania ograniczeń konkurencji na rynku usług telekomunikacyjnych w Polsce. W przypadku bowiem gdy ocena Kolegium wykaże wysokie ryzyko dla cyberbezpieczeństwa Państwa u konkretnego dostawcy, podmioty krajowego systemu cyberbezpieczeństwa nie będą mogły nabywać od takiego dostawcy sprzętu, oprogramowania czy też usług, zaś w ciągu 5 lat od ogłoszenia komunikatu o ocenie, będą musiały taki sprzęt, oprogramowanie czy też usługi wycofać z użytkowania, co de facto spowoduje wyeliminowanie danego przedsiębiorcy z rynku, a w konsekwencji wpłynie na poziom konkurencji w Polsce. Tym samym zwracam uwagę, iż zasadne wydaje się sformułowanie wyżej wskazanych kryteriów w sposób na tyle konkretny i przejrzysty aby wyeliminować potencjalne wątpliwości w wyżej wymienionym zakresie.  Należy przy tym zauważyć, że wpływ tego ograniczenia na konkurencję jest dziś trudny do oszacowania z uwagi na dynamikę tego rynku i stały rozwój technologiczny a także powstawanie nowych przedsiębiorców świadczących usługi z tego zakresu. | **Wyjaśnienie**  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. |
|  | Polski Komitet Normalizacyjny | Art. 67a ust. 4 pkt 5 | **Proponowana zmiana:**  „4. Ostrzeżenie i polecenie zabezpieczające może dotyczyć:  (..)  5) dostawców usług zaufania, o których mowa w art. 3 pkt 19 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz. Urz. UE L 257 z 28.08.2014, str. 73, z poźn. zm.) oraz dostawców środków identyfikacji elektronicznej, o których mowa w art. 3. pkt. 2 tego rozporządzenia.  Na bezpieczeństwo obrotu prawnego prowadzonego za pomocą środków komunikacji elektronicznej w coraz większej skali wpływ ma nie tylko poziom wiarygodności kwalifikowanych usług zaufania, ale także niekwalifikowanych usług zaufania. Te ostanie usługi, szczególnie o statusie zaawansowanym, mogą być również szeroko wykorzystywane jako alternatywa do usług kwalifikowanych i ich wpływ na obniżenie bezpieczeństwa krajowego systemu cyberbezpieczeństwa może być też być istotny. Dlatego warto przewidzieć prawną możliwość oddziaływania również na niekwalifikowane usługi zaufania.  Podobna argumentacja przemawia za objęciem omawianym przepisem dostawców środków identyfikacji elektronicznej, z której coraz częściej i to na dużą skalę będą korzystać dostawcy usług świadczonych drogą elektroniczną. | **Uwag uwzględniona** |
|  | Prezes Urzędu Komunikacji Elektronicznej | Art. 74 ust. 1a pkt 1 | Projektowany art. 74 ust. 1a pkt 1 UKSC – w odniesieniu do tego przepisu należy zauważyć, że w art. 41-44 UKSC określono kompetencje i uprawnienia organów właściwych w poszczególnych sektorach, wśród których są wymienione także monitorowanie stosowania przepisów ustawy przez operatorów usług kluczowych i dostawców usług cyfrowych oraz kontrola tych podmiotów. Z kolei w art. 53 -59 UKSC określone są zasady sprawowania nadzoru i kontroli operatorów usług kluczowych i dostawców usług cyfrowych przez organy właściwe w poszczególnych sektorach. Przepisy powyższe nie mają zastosowania do większości przedsiębiorców telekomunikacyjnych (załącznik nr 1 do ustawy nie wyodrębnia sektora telekomunikacyjnego) i nie stanowią podstawy do działania Prezesa UKE (nie jest on organem właściwym do spraw cyberbezpieczeństwa). Również przepisy Prawa telekomunikacyjnego i projektu Pke nie określają kompetencji nadzorczych i kontrolnych Prezesa UKE w obszarze cyberbezpieczeństwa. Ponadto, Prezes UKE nie dysponuje pracownikami posiadającymi wiedzę ekspercką w zakresie wymaganym od organów zajmujących się sprawami cyberbezpieczeństwa. Brak jest również podstaw do budowy takich zasobów kadrowych, skoro Prezes UKE nie jest organem właściwym do spraw cyberbezpieczeństwa. Wobec powyższego przewidziana w projektowanym art. 74 ust. 1a pkt 3 UKSC kompetencja Prezesa UKE do nakładania kar na przedsiębiorców komunikacji elektronicznej niestosujących się do zakazu wprowadzania do użytkowania sprzętu, oprogramowania i usług lub nakazu ich wycofania (projektowany art. 66b UKSC) byłaby bardzo trudna do realizacji i powinna być pozostawiona we właściwości ministra właściwego do spraw informatyzacji. Abstrahując od powyższego należy zauważyć, że projektowana regulacja jest niepełna, bo nie reguluje sytuacji, w której strona nie osiągnęła obrotu (przychodu) w poprzednim roku obrotowym lub nie można go ustalić, ani nie określa wysokości minimalnych kar (które jednak są przewidziane w projektowanym art. 73 ust. 4 UKSC dla pozostałych przypadków naruszeń). Brakuje także przepisów dających podstawę do wzywania strony do przedstawienia danych niezbędnych do określenia podstawy wymiaru kary pieniężnej. | **Uwaga częściowo uwzględniona**  Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o krajowego systemu cyberbezpieczeństwa poprzez ustawę wprowadzającą PKE.  Uzupełniono przepisy dot. nadzoru Prezesa UKE nad przedsiębiorcami komunikacji elektronicznej w kontekście przestrzegania wymagań z zakresu bezpieczeństwa sieci i usług. |
|  | Komisja Nadzoru Finansowego | Art. 73 ust. 1 | **Propozycja zmiany:**  „Można nałożyć karę pieniężną na operatora usługi kluczowej, który: (…)”.  **Uzasadnienie:**  **1) Uznaniowość karania**  Sformułowania użyte przez ustawodawcę w art. 73 ust. 1 i ust. 2, art. 73 ust. 5 i art. 74 ust. 1 UKSC („karze pieniężnej podlega”, organ właściwy „nakłada”) mogą prowadzić do wniosku, że nałożenie kary pieniężnej na podstawie powołanych przepisów ma charakter obligatoryjny. W przedmiotowym przypadku brak jest uzasadnienia dla obligatoryjności nakładania kary pieniężnej. W związku z powyższym zasadne jest zastąpienie sformułowania *„karze pieniężnej podlega”* na *„może nałożyć karę pieniężną”* orazzastąpienie sformułowania *„nakłada”* na *„może nałożyć”.* Dokonanie przedmiotowejzmiany pozwoli KNF na zastosowanieuznania administracyjnego w odniesieniu do każdego przypadku naruszenia przepisów prawa. Zmiany te są zgodne z Dyrektywą 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii.  Zgodnie z treścią art. 21 ww. Dyrektywy *„Państwa członkowskie ustanawiają przepisy dotyczące sankcji mających zastosowanie w przypadku naruszeń krajowych przepisów przyjętych na podstawie niniejszej dyrektywy i podejmują wszystkie niezbędne środki w celu zapewnienia ich wykonania. Przewidziane* *sankcje muszą być skuteczne, proporcjonalne i odstraszające. Państwa członkowskie powiadamiają Komisję o tych przepisach i środkach do dnia 9 maja 2018 r., a także powiadamiają ją niezwłocznie o wszelkich późniejszych zmianach, które ich dotyczą.”*  Przywołana Dyrektywa **nie wymaga** zatem  od Państw Członkowskich UE wprowadzenia obligatoryjności karania. Za brakiem obligatoryjności karania przemawia także uzasadnienie do UKSC. W uzasadnieniu do projektu ustawy wskazano bowiem, cyt.: *„W rozdziale 14 zawarto* *przepisy regulujące nakładanie* *administracyjnych kar pieniężnych. Przewiduje się, iż organ właściwy dla danego sektora* ***będzie mógł nałożyć*** *na operatorów usług kluczowych administracyjną karę pieniężną za brak realizacji obowiązków wynikających z ustawy. Przykładowo administracyjną karą pieniężną* ***będzie mógł zostać ukarany*** *operator usługi kluczowej, który nie wdrożył środków technicznych i operacyjnych, nie zgłasza incydentów poważnych, nie zapewnia ich obsługi, w tym nie współdziała w trakcie realizacji tych czynności z właściwym CSIRT.”* Intencją ustawodawcybyło zatem wprowadzenie uznaniaadministracyjnego w zakresie nakładaniakar pieniężnych. Proponowane zmiany w UKSC są podyktowane zapewnieniem spójności rozwiązań obowiązujących w różnych sektorach rynku finansowego. Zmiany przyczynią się do zwiększenia efektywności postępowań oraz są wyrazem pragmatycznego podejścia. Wymierzanie sankcji administracyjnej w ramach uznania administracyjnego jest właściwszą formą oddziaływania nadzorczego i powinno być przyjęte jako reguła w postępowaniu z podmiotami nadzorowanymi. Uznanie administracyjne pozwala na rozważenie, czy w danych okolicznościach sprawy zasadne i celowe jest sięgnięcie po środki o charakterze sankcyjnym, czy też cel nadzorczy może zostać osiągnięty przy użyciu innych, mniej dolegliwych dla podmiotów nadzorczych, środków nadzorczych o charakterze nie  sankcyjnym. Obligatoryjność stosowania sankcji administracyjnych powinna być wyjątkiem, zastrzeżonym dla przypadków, w których charakter naruszeń lub dobro, które ma być chronione, wymagają w każdym przypadku stwierdzenia naruszeń, zastosowania dolegliwych środków nadzorczych. Wprowadzenie uznania administracyjnego umożliwi Komisji stosowanie środka nadzorczego adekwatnego do stwierdzonego naruszenia.  **2) Wysokość kar pieniężnych**  W chwili obecnej kary zdefiniowane w UKSC (art. 73 ust. 3 i ust. 5 ww. ustawy) są rażąco niskie, nie mają charakteru odstraszającego i nie spełniają wymogów dyrektywy 2016/1148 z dnia 6 lipca 2016 r.  w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium  Unii (dalej: dyrektywa NIS) w zakresie działania prewencyjnego i represyjnego.  Artykuł 21 tej dyrektywy stanowi, że: *„Państwa członkowskie ustanawiają* *przepisy dotyczące sankcji mających* *zastosowanie w przypadku naruszeń krajowych przepisów przyjętych na podstawie niniejszej dyrektywy i podejmują* *wszystkie niezbędne środki w celu zapewnienia ich wykonania. Przewidziane sankcje muszą być skuteczne, proporcjonalne i odstraszające. Państwa członkowskie powiadamiają Komisję o tych* *przepisach i środkach do dnia 9 maja 2018 r., a także powiadamiają ją niezwłocznie o wszelkich późniejszych zmianach, które ich dotyczą”.*  Operatorem usługi kluczowej zgodnie z UKSC może być m. in. bank krajowy czy instytucja kredytowa, tj. podmioty profesjonalne o znaczących aktywach i przychodach. Kary zaproponowane w UKSC dla tych podmiotów są nieadekwatne do kar pieniężnych przewidzianych w innych ustawach regulujących funkcjonowanie tych podmiotów np. ustawa Prawo bankowe przewiduje karę pieniężną w maksymalnej wysokości do 10% wartości przychodów banku (co może sięgać nawet kilku czy kilkudziesięciu mln złotych). Kara pieniężna, aby móc pełnić swoje funkcje represyjne i prewencyjne, musi mieć charakter odstraszający. Celem zastosowania przez organ nadzoru kary pieniężnej jest przede wszystkim zapewnienie przestrzegania przez adresatów norm prawnych obowiązków w obszarach uznanych za szczególnie istotne przez ustawodawcę. Sankcja nie może być oderwana od stwierdzonych nieprawidłowości i ma pozostawać z nimi w ścisłym związku przyczynowo - skutkowym, tak by w pełni odzwierciedlała stopień naganności zachowania jednostki w stosowaniu obowiązującego prawa. Administracyjne kary pieniężne mają na celu mobilizowanie podmiotów do działania zgodnego z przepisami prawa. Kary te, stosowane z mocy prawa, mają przede wszystkim znaczenie prewencyjne. Przez zapowiedź negatywnych konsekwencji, jakie nastąpią w wypadku naruszenia obowiązków określonych w ustawie, motywują adresatów określonych tam norm, do wykonywania ustawowych obowiązków. Tym samym kara administracyjna nie jest wyłącznie represją za naruszenie prawa, ale przede wszystkim stanowi środek przymusu, który ma służyć zapewnieniu wykonywania obowiązków nałożonych przez obowiązujące przepisy prawa (wyrok Trybunału Konstytucyjnego z dnia 25marca 2010 r., sygn. akt P 9/08). Celem kary jest również zapobieżenie podobnym naruszeniom w przyszłości i efektywniejsze wykonywanie przez podmioty nadzorowane przepisów prawa. Warto również przytoczyć stanowisko Trybunału Konstytucyjnego, który w wyroku z dnia 1 marca 1994 r. (sygn. akt: U 7/93) wskazał, iż kary pieniężne są środkami służącymi mobilizowaniu podmiotów do terminowego i prawidłowego wykonywania obowiązków na rzecz państwa. Kara administracyjna ma charakter środka przymusu, służącego zapewnieniu realizacji wykonawczo-zarządzających zadań administracji, agregowanych przez pojęcie interesu publicznego (por. wyrok Trybunału Konstytucyjnego z dnia 31 marca 2008 r., sygn. akt: SK 75/06). Zatem kluczowym powinno być dostosowanie art. 73 ust. 3 i ust. 5 UKSC do wymogów dyrektywy NIS poprzez znaczne zwiększenie wysokości kar, które mogą zostać nałożone na operatora usług kluczowych, w ten sposób, aby spełniały one warunek „odstraszania” (mając na uwadze status podmiotów mogących pełnić funkcję operatora usług kluczowych). Tak niskie kary jak przewidziane w UKSC (w porównaniu do kar pieniężnych możliwych do nałożenia na podstawie innych ustaw), mogą prowadzić do sytuacji, w której bardziej opłacalne będzie dla podmiotu uiszczenie kary pieniężnej, niż przestrzeganie wymogów i obowiązków nałożonych UKSC.  Administracyjna kara pieniężna powinna być skutecznym środkiem do wymuszania na adresatach norm administracyjnych  określonych zachowań. W obecnym brzmieniu przepisów art. 73 ust. 3 i ust. 4 UKSC, tj. w sytuacji gdy w z jednej strony  Podsumowując, aby spełnić wymóg art. 21 Dyrektywy NIS uregulowane w przepisach UKSC maksymalne kary pieniężne powinny być rygorystyczne, a KNF powinien mieć możliwość nałożenia kary w ramach, lecz nie być do nałożenia kary bezwzględnie zobowiązanym (uznanie administracyjne). Taka nowa regulacja pozwoli, aby KNF skupił się na nakładaniu sankcji za istotne naruszenia prawa. | **Uwaga nieuwzględniona**  Ad. 1 Na podstawie art. 189f KPA organ może odstąpić od nałożenia administracyjnej kary pieniężnej.  Ad. 2 Uwaga wykracza poza zakres przedmiotowy objęty nowelizacją. |
|  | Komisja Nadzoru Finansowego | Art. 73 ust. 2 | **Propozycja zmiany:**  „Można nałożyć karę pieniężną na dostawcę usługi cyfrowej, który: (…)”.  **Uzasadnienie:**  Zmiana podyktowana utrzymania spójnego, fakultatywnego systemu sankcji. | **Uwaga nieuwzględniona**  Na podstawie art. 189f KPA organ może odstąpić od nałożenia administracyjnej kary pieniężnej. |
|  | Komisja Nadzoru Finansowego | Art. 73 ust. 5 zdanie 1 | **Propozycja zmiany:**  „Jeżeli w wyniku kontroli organ właściwy do spraw cyberbezpieczeństwa stwierdzi, że operator usługi kluczowej albo dostawca usługi cyfrowej uporczywie narusza przepisy ustawy, powodując:  1) bezpośrednie i poważne zagrożenie  cyberbezpieczeństwa dla obronności, bezpieczeństwa państwa, bezpieczeństwa i porządku publicznego lub życia i zdrowia ludzi,  2) zagrożenie wywołania poważnej szkody majątkowej lub poważnych  utrudnień w świadczeniu usług kluczowych - organ właściwy do spraw  cyberbezpieczeństwa może nałożyć karę w wysokości do 1 000 000 zł.”  **Uzasadnienie:**  Zmiana podyktowana utrzymania spójnego, fakultatywnego systemu sankcji. | **Uwaga nieuwzględniona**  Na podstawie art. 189f KPA organ może odstąpić od nałożenia administracyjnej kary pieniężnej. |
|  | Komisja Nadzoru Finansowego | Art. 74 ust. 1 | **Propozycja zmiany:**  „Karę pieniężną, o której mowa w art. 73, może nałożyć, w drodze decyzji, organ właściwy do spraw cyberbezpieczeństwa”  **Uzasadnienie:**  Zmiana podyktowana utrzymania spójnego, fakultatywnego systemu sankcji. | **Uwaga nieuwzględniona**  Na podstawie art. 189f KPA organ może odstąpić od nałożenia administracyjnej kary pieniężnej. |
|  | Komisja Nadzoru Finansowego | Art. 74 ust. 1a pkt 4 | **Propozycja zmiany:**  4) w przypadku podmiotów wpisanych do wykazu SOC, wykonujących usługi na zlecenie operatora usług kluczowych – minister właściwy do spraw informatyzacji.  **Uzasadnienie:**  Zmiana ma związek z wyżej proponowaną zmianą art. 41 pkt 12 (organy właściwe). Może pojawić się okoliczność, w której SOC będzie świadczył usługi dla kilku OUK z różnych sektorów, które będą podlegały pod różne organy właściwe. Wówczas ujawnia się problem w kwestii nakładania kar na SOC przez organ właściwy (jeśli miałby być to organ według właściwości dla OUK). Mogłoby to powodować, że różne organy właściwe mogłyby chcieć nakładać na SOC kary za te same nieprawidłowości.  KNF zwraca uwagę, że mogą się pojawić wątpliwości interpretacyjne co do użycia słowa ***wpisanych*** w przypadku, gdy podmiot nie jest (jeszcze) wpisany do wykazu SOC. | **Uwaga uwzględniona** |
|  | Urząd Zamówień Publicznych | Art. 96 ust. 2 pkt 3 PZP | W myśl projektowanego pkt 3 w art. 96 ust. 2 Pzp zamawiający może określić w ogłoszeniu o zamówieniu lub dokumentach zamówienia wymagania związane z realizacją zamówienia, które mogą dotyczyć w szczególności poziomu ryzyka, jaki stanowi dostawca sprzętu lub oprogramowania, stwierdzonego oceną, o której mowa w art. 66a ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2020 r. poz. 1369). Zaproponowana redakcja przepisu nie wydaje się dostatecznie czytelna. Przepis powinien być doprecyzowany w zakresie wskazania czego konkretnie mają dotyczyć wymagania związane z realizacją zamówienia, o których mowa projektowanym przepisie, a w szczególności w związku z jakimi okolicznościami ocena, o której mowa w art. 66a ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa ma być przeprowadzana trakcie realizacji zamówienia. | **Wyjaśnienie**  W toku prac legislacyjnych zrezygnowano z nowelizacji Prawa zamówień publicznych. |
|  | Urząd Zamówień Publicznych | Art. 109 ust. 1 pkt 11 PZP | Projekt dodaje pkt 11 w art. 109 ust. 1 Pzp, zgodnie z którym z postępowania o udzielenie zamówienia zamawiający może wykluczyć wykonawcę, 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. Jeżeli zamówienie jest zamówieniem w dziedzinach obronności i bezpieczeństwa proponowana fakultatywna podstawa wykluczenia odpowiada podstawie wykluczenia wykonawcy przewidzianej w art. 39 ust. 2 lit. e) dyrektywy 2009/81/WE, zgodnie z którym w przypadku zamówień udzielanych w dziedzinie obronności i bezpieczeństwa zamawiający może wykluczyć każdego wykonawcę, który na podstawie dowolnych środków dowodowych, w tym chronionych źródeł danych, został uznany za nieposiadającego wiarygodności niezbędnej do wykluczenia zagrożenia dla bezpieczeństwa państwa członkowskiego. Ten przepis dyrektywy 2009/81/WE został wdrożony w art. 405 ust. 2 pkt 3 Pzp. Zastosowanie szczególnych przesłanek wykluczenia jest możliwe również w oparciu o art. 393 ust. 1 Pzp w odniesieniu do zamówień sektorowych. | **Wyjaśnienie**  W toku prac legislacyjnych zrezygnowano z nowelizacji Prawa zamówień publicznych. |
|  | Urząd Zamówień Publicznych | Art. 110 ust. 2 PZP | Proponuję wykreślenie projektowanej zmiany w art. 110 ust. 2 Pzp. Przepis ten miałby umożliwiać wykonawcy, w związku z zaistnieniem w stosunku do niego podstawy wykluczenia określonej w projektowanym art. 109 ust. 1 pkt 11 Pzp, podjęcia działań naprawczych i zapobiegawczych w ramach procedury samooczyszczenia. Dodatkowo należy zwrócić uwagę, iż ocena, o której mowa w art. 66a ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, obejmuje m.in. analizę prawdopodobieństwa, 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. Okoliczności wskazane w lit. b, c i e są okolicznościami niezależnymi od wykonawcy, co wyklucza jak się wydaje, możliwość podjęcia przez wykonawcę skutecznych działań naprawczych oraz zapobiegawczych z przyczyn, które nie leżą po stronie wykonawcy. Wdrożenie tego przepisu mogłoby sprawiać, że możliwość skorzystania przez wykonawcę z procedury samooczyszczenia w odniesieniu do projektowanej podstawy wykluczenia stawałaby się czynnością pozorną. | **Wyjaśnienie**  W toku prac legislacyjnych zrezygnowano z nowelizacji Prawa zamówień publicznych. |
|  | NASK | OSR | Mając na uwadze stały wzrost liczby procesów oraz poszerzający się katalog działań skierowanych do podmiotów znajdujących się w obszarze odpowiedzialności CSIRT NASK, zachodzi konieczność zrewidowania kosztów funkcjonowania CSIRT NASK. Budżet przewidziany w Ustawie na  dotację podmiotową na rzecz NASK PIB już obecnie nie jest wystarczający do realizacji przez CSIRT NASK działań ustawowych. W związku z tym, konieczne jest jego zwiększenie, zgodnie z estymacją kosztów przekazaną w piśmie NASK PIB o nr ZZP.051.200034.2020.ASI [OSR-KSC-2021+] z dnia 2 lipca 2020 roku. Estymacja ta została przygotowana z uwzględnieniem doświadczeń ekspertów NASK PIB oraz danych finansowych NASK PIB dotyczących wydatków poniesionych na realizację zadań wynikających z Ustawy w latach 2018-2020.  Równocześnie podkreślam, że zaproponowane przez Ministerstwo zmiany w Ustawie jeszcze zwiększają zakres zadań CSIRT NASK (m.in. w zakresie zadań wykonywanych na rzecz Pełnomocnika oraz objęcia zakresem Ustawy sektora telekomunikacyjnego, co także zwiększa zakres działania CSIRT NASK). W związku z powyższym konieczne jest zwiększenie finansowania na potrzeby tych nowych działań CSIRT NASK.  Dodatkowo, NASK PIB buduje system S46 (system teleinformatyczny opisany w Ustawie w art. 46). Będzie to system kluczowy dla działania krajowego systemu cyberbezpieczeństwa, a NASK PIB przygotowuje się do jego utrzymania i rozwoju, co wymaga odpowiedniego finansowania. NASK PIB  pracuje także nad uruchomieniem Centrum Certyfikacji. | **Uwaga uwzględniona**  OSR został uzupełniony o koszty dla NASK. |