**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).**

**Część I.**

|  |
| --- |
| **Liczba organizacji, które otrzymały zaproszenia:** |
| **Organizacje, które zgłosiły swoje uwagi:** Związek Banków Polskich, Santander, Narodowy Instytut Cyberbezpieczeństwa, Związek Pracodawców Mediów Elektronicznych i Telekomunikacji MEDIAKOM, Bank Handlowy, Q-PRO Jakub Stoparek, RFCell Technologies Sp. z.o.o., KGHM/Związek Pracodawców Polska Miedź, Stowarzyszenie Libertariańskie, SayF, Transition Software, Izba Gospodarcza Gazownictwa/Polska Spółka Gazownictwa Sp. z.o.o./PGNIG SA Oddział w Zielonej Górze, Izba Przemysłowo-Handlowa Polska-Azja, Huawei Polska, Business Centre Club, Digital Poland, Excogitate, Fundacja Bezpieczna Cyberprzestrzeń, Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji KIGEIT, Narodowy Bank Polski, Naczelna Organizacja Techniczna. Federacja Stowarzyszeń Naukowo-Technicznych, Polskie Centrum Badań i Certyfikacji, Polski Związek Pracodawców Przemysłu Farmaceutycznego, T-Mobile, Federacja Przedsiębiorców Polskich, 1Innosystems, Polska Izba Komunikacji Elektronicznej, Fabryka E-Biznesu, Krajowa Izba Gospodarki Cyfrowej DigiCom, Home.pl, Install Tech, Polska Izba Handlu, ISACA Warsaw Chapter, Krajowy Sekretariat Łączności NSZZ Solidarność, MJC Sp. z.o.o., IAB Polska, Federacja Konsumentów, Stowarzyszenie „Miasta w Internecie”, Stowarzyszenie Inżynierów Telekomunikacji, Uniwersytet Jagielloński Collegium Medicum, PKP Energetyka, Sektorowa Rada ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo, Polskie Towarzystwo Informatyczne, ISSA Polska, Związek Przedsiębiorców i Pracodawców, Krajowy Depozyt Papierów Wartościowych, Politechnika Wrocławska. Wrocławskie Centrum Sieciowo-Superkomputerowe, EXATEL, S4IT Michał Podgórski, Orange Polska, Polsko-Chińska Główna Izba Gospodarcza SinoCham, Aberit, Młodzieżowy Delegat RP przy NATO, ERSTAR, ETOB-RES, Fundacja Alatum, GBX Soft, Instytut Lema, Mobile Logic, Mobilne Miasto, Nanocoder, NeuroGames Lab, SmartWeb Media, TELDATA, TEP Doradztwo Biznesowe, TILT, Związek Cyfrowa Polska, Signum Edward Kuś Marcin Kuś, PKN Orlen, Skandynawsko-Polska Izba Gospodarcza, Liquid Systems, Instytut Staszica, Akademia Sztuki Wojennej, Krajowa Izba Komunikacji Ethernetowej, Qualitel Service, JARTEL, Izba Gospodarki Elektronicznej, Konfederacja Lewiatan |
| **Podmioty, które odpowiedziały na zaproszenie, ale nie zgłosiły uwag do projektu:** Porozumienie Zielonogórskie. Federacja Związków Pracodawców Ochrony Zdrowia |
| **Podmioty, które zrezygnowały z udziału w konsultacjach:** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Podmiot wnoszący uwagi** | **Jednostka redakcyjna, do której wnoszone są uwagi** | **Zgłoszone uwagi** | **Stanowisko KPRM/DC** |
|  | Związek Banków Polskich | Uwaga ogólna | ISAC powinien również wspomagać podmioty z danego sektora, sektorów lub podsektorów, niezależnie od wydania decyzji o uznaniu konkretnego podmiotu za operatora usługi kluczowej – zapewni to szczelność systemu. Szczególnym przypadkiem jest tutaj sektor bankowy, w którym bezpieczeństwo jednego banku zależy również od wielu innych podmiotów, w szczególności pozostałych banków, dostawców usług płatniczych, czy też izb rozliczeniowych. Zdaniem ENISA dla prawidłowego rozwoju cyberbezpieczeństwa niezbędna jest współpraca pomiędzy sektorem publicznym i prywatnym. W związku z tym ustawa powinna przyznawać ISAC kompetencje umożliwiające taką współpracę. | **Wyjaśnienie**  ISAC nie jest jednostką operacyjną, nie zajmuje się reagowaniem na incydenty. Nie ma przeszkód, żeby ISAC wspomagał inne podmioty spoza ksc. |
|  | Związek Banków Polskich | Uwaga ogólna | Za krytyczny należy uznać brak w ramach krajowego systemu cyberbezpieczeństwa dostawców usług płatniczych, krajowych instytucji płatniczych i izb rozliczeniowych, co powoduje stworzenie luki w systemie płatniczym kraju oraz oznacza faktyczną niemożność wykrywania, przeciwdziałania i zwalczania cyberincydentów w obszarze realizacji i rozliczeń transakcji płatniczych | **Uwaga nieuwzględniona**  Niemożliwe jest uwzględnienie dostawców usług płatniczych z powodu kolizji ustawowej. Działalność dostawców usług płatniczych regulują inne przepisy powstałe w oparciu o Dyrektywę Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE (PSD2) |
|  | Związek Banków Polskich | Uwaga ogólna | Za krytyczne należy uznać wprowadzenie podstawy prawnej do przetwarzania tajemnic prawnie chronionych oraz danych osobowych w celu skutecznego działania CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT sektorowych oraz ISAC | **Uwaga nieuwzględniona**  Obecnie funkcjonujące regulacje w wystarczającym stopniu pozwalają CSIRT-om na ich działania. Nie jest więc konieczna zmiana przepisów w tym zakresie. |
|  | Związek Banków Polskich | Uwaga ogólna | Za krytyczne należy uznać brak przepisów umożliwiających przetwarzanie prawnie chronionych pomiędzy OUK, DUC, przedsiębiorcami komunikacji elektronicznej oraz ISAC, co uniemożliwia sprawną wymianę informacji o incydentach w celu ich wykrywania, analizowania, zapobiegania i zwalczania – propozycja dodania nowego przepisu. | **Uwaga nieuwzględniona**  ISAC jest centrum wymiany informacji ale nie informacji prawnie chronionych. Chyba że podmioty tworzące ISAC umówią się, że będą sobie przekazywać tajemnicę przedsiębiorstwa. |
|  | Związek Banków Polskich | Uwaga ogólna | Za krytyczny należy uznać fakt, że sektor bankowy własnym kosztem wytworzył wiele systemów wspierających bezpieczeństwo banków oraz ich klientów. Istotne jest, aby wprowadzić możliwość wykorzystania ich w ramach krajowego systemu cyberbezpieczeństwa. Również obowiązki informacyjne o incydentach np. względem CSIRT MON, CSIRT NASK i CSIRT GOV mogłyby być realizowane z ich użyciem. Pozwoli to uniknąć dublowania czynności związanych z notyfikacją incydentów do wielu instytucji państwowych, np. KNF, PUODO, prokuratury, policji itp. W związku z powyższym proponujemy dodanie przepisu, który będzie dawał możliwość wykorzystywania sektorowych systemów IT z centralnym systemem do zgłaszania incydentów. ZBP uczestniczył projekcie NASK – Narodowej Platformie Cyberbezpieczeństwa, której osiągnięcia są wykorzystywane w tworzonym Systemie S46. Ten projekt i integracja systemu sektorowego (BRIBIT) z NPC potwierdził deklarowane korzyści z integracji, która umożliwi niezakłócony dwukierunkowy przepływ informacji pomiędzy operatorami usług kluczowych a Instytucjami wchodzącymi w skład krajowego systemu cyberbezpieczeństwa. | **Wyjaśnienie**  Centralnym systemem zarządzania cyberbezpieczeństwem w Polsce jest system utworzony na podstawie art. 46 ustawy ksc.  Do systemu będą mogli dołączyć użytkownicy np. operatorzy usług kluczowych czy dostawcy usług cyfrowych na podstawie porozumienia zawartego z ministrem właściwym ds. informatyzacji |
|  | Santander | Uwaga ogólna | Mamy CSIRT NASK do którego raportujemy incydenty poważne i to samo musimy raportować do powołanego CSIRT KNF sektorowego. Czy nie powinno być tak, że zgłaszamy do naszego sektorowego i tam informacja jest zarządzona a do obsługi incydentu zdarzenia wykorzystywany jest jeden, spójny system? | **Wyjaśnienie**  CSIRT poziomu krajowego koordynuje obsługę incydentów. CSIRT sektorowy zajmuje się bezpośrednim wsparciem operatora. |
|  | Santander | Uwaga ogólna | Czy zostaną zmodyfikowane Rozporządzenia do Ustawy, odzwierciedlające aktualny stan pracy zdalnej, poza wydzielonymi strefami bezpiecznymi w kontekście pandemii COVID-19 np. pracowników SOC czy Threat Intelligence? | **Wyjaśnienie**  Rozporządzenie to straci moc z chwilą wejścia w życie ustawy. Operator usługi kluczowej będzie wdrażał zabezpieczenia w oparciu o *risk based approach*, także dotyczące pracy zdalnej. |
|  | Narodowy Instytut Cyberbezpieczeństwa | Uwaga ogólna | Przedłożony projekt budzi pewne wątpliwości w zakresie zgodności z polskim systemem prawnym. Znaczna część proponowanych rozwiązań dotyczy kryteriów oceny stosowanych podczas postępowania, które prowadzone ma być przez Kolegium do Spraw Cyberbezpieczeństwa. Zakłada się brak obecności w jego trakcie ocenionego dostawcy sprzętu czy też oprogramowania. Pozostałe wątpliwości związane są z ochroną konkurencji, a także dalszym rozwojem sieci 5G w Polsce.  W proponowanej wersji projektu nie wskazano konkretnych kryteriów według których oceniany będzie dostawca sprzętu lub oprogramowania. Aby stworzyć sytuację pewności po stronie ocenianego, kryteria te powinny być jasno i precyzyjnie określone. W przeciwnym razie mamy do czynienia z oceną uznaniowa, nie zaś merytoryczną. Ponadto, cały proces odbywa się bez udziału stron postępowania. To również może wpłynąć na ocenę całego procesu i powinno zostać zmienione w ostatecznej wersji aktu. Warto zaznaczyć, że te kwestie mogą być argumentem dla niektórych ze stron postępowania do kwestionowania dokonanego wyboru. Oceniany bowiem powinien mieć zagwarantowane prawo do czynnego udziału w postępowaniu, które zaważyć może na przyszłości prowadzonej przez niego działalności gospodarczej. Biorąc pod uwagę skutki w postaci zakazu wprowadzania przez niego nowego sprzętu lub oprogramowania na rynek oraz usunięcia tego, który jest już na nim obecny, jeżeli taka decyzję podjęłoby Kolegium. To może mieć negatywny wpływ na wizerunek Polski wśród inwestorów z branż, z uwagi na niepewność środowiska biznesowego.  Niejasne pozostają także kryteria, które służyć będą do wyboru dostawcy sprzętu i oprogramowania sieci 5G, jak i określania przez Kolegium ich ryzyka. Dostawcy ci nie mają również możliwości odwołania się od wydanej decyzji o wyborze innego podmiotu niż Kolegium. To w praktyce może prowadzić do nadużyć oraz stawiać znak zapytania przy zgodności proponowanych przepisów z zasada równości wobec prawa. Wszyscy dostawcy powinni być traktowani w jednolity sposób, które będzie gwarantem wspomnianej wcześniej równości, a który wyrażony byłby właśnie poprzez określenie konkretnych kryteriów oceny. Te, które zostały wskazane w projekcie ustawy są bardzo szerokie i dotyczą głównie kwestii polityczno-gospodarczych. W postępowaniu oceniającym pomija się specyfikacje techniczne, które maja równorzędne, jeśli nie nawet większe, znaczenie w przypadku przedmiotowej regulacji i to głównie na nich powinien się opierać wybór dostawcy sprzętu bądź oprogramowania przez operatora sieci telekomunikacyjnej, a także sam proces oceny ryzyka prowadzonej przez Kolegium. Niezastosowanie kryterium technicznego może się negatywnie odbić na rozwoju technologii 5G w Polsce, ponieważ operatorzy będą mieć ograniczony wybór dostawców, z których będą mogli korzystać.  Opisane wątpliwości mogą mieć wpływ na rynek konkurencji w Polsce. Ograniczenie ilości podmiotów oferujących sprzęt bądź oprogramowanie spełniające należyte wymogi w zakresie cyberbezpieczeństwa w wyniku stosowania niejasnych bądź niepełnych kryteriów, może doprowadzić do załamania rynku, a także pogorszenia się sytuacji konsumenta. Odnosząc się do kwestii niejasnych kryteriów należy także zauważyć, że także konsumenci odczują wspomniane wcześniej skutki z uwagi na wyższe ceny usług, spowodowane mniejszą konkurencją na rynku i wyższymi kosztami operatorów. Pozostając w obszarze ochrony konkurencji należałoby także zastanowić się, czy kompetencje przyznane Kolegium do Spraw Cyberbezpieczeństwa nie pokrywają się z kompetencjami innego podmiotu nadzorującego rynek telekomunikacyjny, także w zakresie konkurencji.  Konsekwencją rozwiązań ujętych w projekcie ustawy jest opóźnienie wprowadzenia sieci 5G w Polsce. Z tym jest bezpośrednio związane ryzyko pozostania Polski w tyle w stosunku do pozostałych krajów europejskich pod względem tempa rozwoju 5G. Ma to znaczenie dla innych powiązanych sektorów gospodarki, takimi jak chociażby nowoczesny przemysł, medycyna, edukacja zdalna, czy nawet rolnictwo. Opóźnienie wpłynie także na możliwość utworzenia nowych miejsc pracy. Wspomniany wyżej wpływ na konkurencję może natomiast przyczynić się do zwiększonego wykluczenia społecznego, z uwagi na wyższe koszty usług dostępu do sieci 5G.  Rozwój siei 5G będzie mieć fundamentalny wpływ na rozwój polskiej gospodarki. Dlatego tez istotne jest, by nowa regulacja stwarzała ku temu dobre warunki. Podstawa przyjaznego środowiska dla rozwoju sieci 5G jest przede wszystkim konkretna, jasna i przejrzysta regulacja prawna. Regulacja ta powinna zawierać kryteria oceny ryzyka dostawcy sprzętu lub oprogramowania istotnego dla cyberbezpieczeństwa oparte na precyzyjnej specyfikacji technicznej tak, aby zaistniała pewność co do tego, jakie warunki należy spełnić, by móc funkcjonować na rynku. Ponadto, samo postępowanie oceniające powinno być bardziej przejrzyste i należałoby je poszerzyć o możliwość odwołania się dostawców od decyzji wydanej przez Kolegium do Spraw Cyberbezpieczeństwa do innego, niezależnego podmiotu. Aktualnie proponowana regulacja, która przewiduje odwołanie od decyzji wydanej przez Kolegium do tego samego gremium budzi wątpliwości co do szans na inną decyzję w ostatecznym rozstrzygnięciu. Stwarza to również możliwość pojawiania się nadużyć. | **Wyjaśnienie**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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 nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony zostł 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 został dołączony do ustawy jako załącznik nr 3. |
|  | Osoba fizyczna | Uwaga ogólna | W mojej opinii, w ustawie brakuje jasno zdefiniowanych odpowiedzialności dot. edukacji. Są zapisy mówiące o "budowaniu świadomości podmiotów systemu". Powinny być jasne zapisy mówiące o tym: kto i w jakim zakresie jest odpowiedzialny za edukację. Dotyczy to edukacji zarówno podmiotów publicznych, organów administracji jak i społeczeństwa. Szkolenia i promowanie dobrych praktyk będzie miało bezpośrednie przełożenie na wzrost cyberbezpieczeństwa. | **Uwaga nieuwzględniona, nie dotyczy nowelizacji** |
|  | Związek Pracodawców Mediów Elektronicznych i Telekomunikacji MEDIAKOM | Uwaga ogólna | Biorąc pod uwagę powyższe, oraz treść pisma zawiadamiającego o konsultacjach, z którego wynika, że PKE ma zostać uzupełnione o przepisy regulujące obowiązki przedsiębiorców w zakresie zapewnienia bezpieczeństwa ciągłości świadczenia usług komunikacji elektronicznej oraz dostarczania sieci telekomunikacyjnej poprzez włączenie obowiązków zawartych w konsultowanym projekcie do PKE, nie jest do końca jasne przyjęty sposób regulacji. Czy konsultowane przepisy mają znaleźć się w dwóch równoległych ustawach? Czy też mają one być wprowadzone do PKE i usunięte z konsultowanej ustawy?  Mediakom postuluje, by kwestie bezpieczeństwa sieci i usług uregulowane zostały w jednym akcie prawnym, tak by maksymalnie uprościć przyjęte rozwiązania i zapewnić czytelność i możliwą łatwość stosowania przez przedsiębiorców komunikacji elektronicznej. Zbędne jest też powielanie tożsamych przepisów w dwóch niezależnych ustawach. | **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 przez ustawę wprowadzającą PKE.  Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowym.  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. |
|  | Q-PRO Jakub Stoparek | Uwaga ogólna | W ostatnim czasie, dotarły do nas niepojące opinie umieszczane w prasie lub Internecie dotyczące nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa. Jako firma Q-PRO Jakub Stoparek, z branży telekomunikacyjnej będziemy świadczyć usługi dla wielu firm telekomunikacyjnych. Po przeczytaniu wielu artykułów na ten temat niepokoi nas projekt ustawy, który może mieć negatywny wpływ na naszą firmę i pokrewne branże.  Jesteśmy przekonani, że polski rynek jest rynkiem otwartym, przejrzystym, gdzie panuje równość i uczciwa konkurencja. Rozumiemy, że Rząd chce chronić cyberbezpieczeństwo kraju, ale obawiamy się, że wykluczenie niektórych dostawców usług telekomunikacyjnych przyniesie skutki odwrotne do zamierzonych i wpłynie negatywnie na zatrudnienie i rozwój branży. Wydaje się niezasadnym stosowanie kryterium wskazywania firm podwyższonego ryzyka na podstawie ich pochodzenia, gdyż nie mierzy on poziomu ryzyka dla cyberbezpieczeństwa naszego państwa. Logicznym rozwiązaniem byłoby wprowadzenie ściśle określonych technicznych wymogów dotyczących sprzętu w strategicznych sektorach, które powinny być spełnione przez wszystkich dostawców sprzętu niezależnie od kraju ich pochodzenia. Wydaje się, że takie rozwiązanie wpłynęłoby pozytywnie i kompleksowo na poziom cyberbezpieczeństwa. Mamy nadzieję, że liczne wątpliwości ujawnione na etapie konsultacji społecznych, pozwolą ministerstwu opracowanie projektu ustawy pozbawionego ryzyka negatywnego wpływu na branżę teleinformatyczną lub bezpośrednio na konsumentów. Dziękujemy za wysłuchanie naszych opinii. | **Uwaga nieuwzględniona**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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 nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | RFCell Technologies Sp. z.o.o. | Uwaga ogólna | W ostatnim czasie, dotarły do nas niepojące opinie umieszczane w prasie lub Internecie dotyczące nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa. Jako firma RFCell Technologies Sp. z.o.o**.** z branży telekomunikacyjnej będziemy świadczyć usługi dla wielu firm telekomunikacyjnych. Po przeczytaniu wielu artykułów na ten temat niepokoi nas projekt ustawy, który może mieć negatywny wpływ na naszą firmę i pokrewne branże.  Jesteśmy przekonani, że polski rynek jest rynkiem otwartym, przejrzystym, gdzie panuje równość i uczciwa konkurencja. Rozumiemy, że Rząd chce chronić cyberbezpieczeństwo kraju, ale obawiamy się, że wykluczenie niektórych dostawców usług telekomunikacyjnych przyniesie skutki odwrotne do zamierzonych i wpłynie negatywnie na zatrudnienie i rozwój branży. Wydaje się niezasadnym stosowanie kryterium wskazywania firm podwyższonego ryzyka na podstawie ich pochodzenia, gdyż nie mierzy on poziomu ryzyka dla cyberbezpieczeństwa naszego państwa. Logicznym rozwiązaniem byłoby wprowadzenie ściśle określonych technicznych wymogów dotyczących sprzętu w strategicznych sektorach, które powinny być spełnione przez wszystkich dostawców sprzętu niezależnie od kraju ich pochodzenia. Wydaje się, że takie rozwiązanie wpłynęłoby pozytywnie i kompleksowo na poziom cyberbezpieczeństwa. Mamy nadzieję, że liczne wątpliwości ujawnione na etapie konsultacji społecznych, pozwolą ministerstwu opracowanie projektu ustawy pozbawionego ryzyka negatywnego wpływu na branżę teleinformatyczną lub bezpośrednio na konsumentów. Dziękujemy za wysłuchanie naszych opinii. | **Uwaga nieuwzględniona**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | KGHM/Związek Pracodawców Polska Miedź | Uwaga ogólna | Związek Pracodawców Polska Miedź pozytywnie ocenia fakt, iż przygotowane przez Ministra Cyfryzacji zmiany zawarte w projekcie ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy – Prawo zamówień publicznych, mają na celu stworzenie podstaw prawno-instytucjonalne dla cyberbezpieczeństwa na poziomie krajowym. | **Wyjaśnienie**  Dziękujemy za pozytywne stanowisko. |
|  | Stowarzyszenie Libertariańskie | Uwaga ogólna | Rządowy projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy – Prawo zamówień publicznych przewiduje możliwość wydawania przez Pełnomocnika Rządu ds. Cyberbezpieczeństwa „poleceń zabezpieczających” nakazujących np. wprowadzenie „reguły ruchu sieciowego zakazującego połączeń z określonymi adresami IP lub nazwami URL” lub „zakaz korzystania z określonego sprzętu lub oprogramowania”. Polecenia te będą mogły być wydawane między innymi:  - przedsiębiorcom o szczególnym znaczeniu gospodarczo-obronnym, o których mowa w art. 3 ustawy z dnia z dnia 23 sierpnia 2001 r. o organizowaniu zadań na rzecz obronności państwa realizowanych przez przedsiębiorców, czyli na przykład przedsiębiorcom telekomunikacyjnym, takim jak: Orange Polska, T-Mobile Polska, Netia, Polkomtel, Telefonia Dialog, EmiTel, Exatel, Multimedia Polska, TTcomm, TK Telekom czy nadawcom takim jak Telewizja Polska i Polskie Radio;  - podmiotom, o których mowa w art. 4 pkt 1-16 ustawy o krajowym systemie cyberbezpieczeństwa, czyli na przykład dostawcom usług cyfrowych, przez które rozumie się internetowe platformy handlowe (wszelki handel i usługi z umowami zawieranymi na stronie internetowej, czyli również usługi hostingu), wyszukiwarki internetowe oraz usługi przetwarzania w chmurze;  - krajowym instytucjom płatniczym.  „Polecenia zabezpieczające” będą mogły być wydawane w przypadku wystąpienia „incydentu krytycznego”, czyli incydentu skutkującego „znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi”, klasyfikowanego przez właściwy Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego.  Da to możliwość nakazania zablokowania dostępu do dowolnego serwera, strony internetowej czy usługi, zarówno głównym operatorom telekomunikacyjnym, jak i dostawcom hostingu, operatorom płatności lub samym właścicielom stron czy usług. Decyzją urzędnika, od której nie będzie przysługiwać odwołanie do sądu, bo takiej procedury nie przewidziano. Wystarczy uznanie przez odpowiedni państwowy zespół, że wystąpił „incydent krytyczny”, gdy – na przykład – zagrożone zostały czyjeś interesy gospodarcze w wyniku ujawnienia jakichś niewygodnych informacji. Za niezastosowanie poleceń zabezpieczających ma grozić kara pieniężna, jeszcze nie wiadomo w jakiej wysokości, bo tu w projekcie wydaje się być luka.  Jest to zagrożenie dla wolności słowa i furtka do stosowania faktycznej cenzury w cyberprzestrzeni. Dla ochrony przed cyberatakami wystarczy jedynie instytucja ostrzeżeń.  W związku z powyższym apeluję o wykreślenie z projektu przepisów dotyczących „poleceń zabezpieczających”. | **Uwaga nieuwzględniona**  Projektowane przepisy dot. ostrzeżenia i polecenia zabezpieczającego nie mają na celu ograniczenia wolności słowa i dostępu do internetu.  Ich stosowanie jest ograniczone tylko do niektórych grup podmiotów z sektorów gospodarki kluczowych dla społeczno-ekonomicznego bezpieczeństwa państwa m.in. do operatorów usług kluczowych, administracji publicznej, czy przedsiębiorców telekomunikacyjnych. Co więcej, środki te mogą być aktywowane w sytuacji zagrażającej wystąpieniu incydentu krytycznego (ostrzeżenie) lub w trakcie jego trwania, w związku z potrzebą zapewnienia koordynacji i odpowiednio szybkiej reakcji na zażeganie sytuacji kryzysowej wywołanej cyberatakiem (polecenie zabezpieczające). |
|  | Izba Przemysłowo-Handlowa Polska-Azja | Uwaga ogólna | **Prace Legislacyjne**  Charakter proponowanym przez Resort zmianom nadały między innymi **ostatnie**  **ustalenia na poziomie europejskim**, a więc **Europejski Kodeks Łączności Elektronicznej oraz zalecenia Komisji Europejskiej, dotyczące bezpieczeństwa 5G.** Nowy projekt wdraża zalecenia i standardy opublikowane **w tak zwanym 5G Toolbox**, czyli **zestawie narzędzi** przygotowanych przez Komisję Europejską i Agencję Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA). Czy nasi Partnerzy w UE pracują nad podobnymi czy tożsamymi rozwiązaniami jakie zaproponował Resort Cyfryzacji w tym zakresie ?Przy wyborze dostawcy sprzętu i oprogramowania uwzględniane będą:  • analiza zagrożeń bezpieczeństwa narodowego o  charakterze **ekonomicznym, kontrwywiadowczym i terrorystycznym** oraz zagrożeń dla realizacji **zobowiązań sojuszniczych** i europejskich;  • prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się **pod wpływem państwa spoza UE lub NATO**,  • jaki jest stopień i rodzaj powiązań pomiędzy dostawcą i tym państwem, **jakie jest prawodawstwo** tego państwa w zakresie **ochrony praw obywatelskich i praw człowieka**,  • jakie w tym państwie istnieje **prawodawstwo w zakresie ochrony danych osobowych**,  • **strukturę własnościową** dostawcy sprzętu lub oprogramowania,  • **zdolność ingerencji państwa** spoza UE lub NATO w swobodę działalności gospodarczej dostawcy.  MC chce, by ustawa weszła w życie 21 grudnia br. ‒ tj. wraz z ustawą – Prawo komunikacji elektronicznej. W efekcie na prace wewnątrz Rządu i w Parlamencie pozostaje niewiele czasu na debatę i poważny proces legislacyjny.  **Rola i skład Kolegium ds. Cyberbezpieczeństwa**  Oceniające dostawców **Kolegium ds. Cyberbezpieczeństwa** powstało przy Radzie Ministrów na mocy ustawy KSC z 2018 r. **Przewodniczy mu premier**, a zasiadają w nim: pełnomocnik rządu ds. cyberbezpieczeństwa, szefowie resortów właściwych  do spraw wewnętrznych, informatyzacji, służb specjalnych, obrony narodowej i spraw  zagranicznych, a także szef Kancelarii Prezesa Rady Ministrów i szef Biura Bezpieczeństwa Narodowego.  **Przewodnictwo Premiera**  Uważam, że w tym rozwiązaniu kryją się duże ryzyka, bowiem będą przenosić każdą decyzję Kolegium od razu w przestrzeń dyplomatyczną i polityczną. Rozumiem, że taka przyjęta konstrukcja miała pokazywać wagę państwową  cyberbezpieczeństwa. Jednak w praktyce, tym bardziej, że po drugiej stronie procesu decyzyjnego będą stały często międzynarodowe konsorcja firm czy globalne firmy,  w efekcie będzie dochodzić do dodatkowych napięć, konsekwencji czy reakcji nie tylko po stronie właścicieli czy udziałowców firm, ale też polityki i dyplomacji ich Państw.  Dzisiaj, ze zrozumiałych względów, mówimy o koordynacji działań wynikających z naszego członkostwa w NATO czy UE, ale nie da się wykluczyć sytuacji, także znaczących, różnic interesów przy kolejnych decyzjach dotyczących już tylko firm  państw członkowskich NATO czy UE. W efekcie, każdy polski wybór techniki, technologii czy partnera może skutkować oskarżeniami o polityczną ingerencję bez dochowania zasad konkurencji i praw rynku i może tworzyć dodatkowy obszar konfliktu dla Premiera i Jego najbliższego otoczenia z zagranicznymi partnerami na innych płaszczyznach i w innych obszarach współpracy.  Zwracam uwagę na te kwestie tym bardziej że pod osobistym kierunkiem i głosem stanowiącym Premiera analizowane będą:  • jaki jest stopień i rodzaj powiązań pomiędzy dostawcą i tym państwem, **jakie jest prawodawstwo** tego państwa w zakresie **ochrony praw obywatelskich i praw człowieka**,  • jakie w tym państwie istnieje **prawodawstwo w zakresie ochrony danych osobowych**,  • **strukturę własnościową** dostawcy sprzętu lub oprogramowania,  • **zdolność ingerencji państwa** spoza UE lub NATO w swobodę działalności gospodarczej dostawcy.  **Odpowiedzi na te pytania, tak zredagowane będą miały określoną siłę w dyplomacji i polityce międzynarodowej, często zapewne także**  **stygmatyzującą międzynarodowych Partnerów.**  Tak Pan Premier i kierownictwo Państwa poprzez obecne możliwości (rozwiązania ustawowe, procesy przetargowe etc) ma skuteczny wpływ na proces decyzyjny.  Jeśli Pan Minister będzie zainteresowany, to przekażę kilka moich praktycznych doświadczeń w tym zakresie (na przykład realizacji umów offsetowych i konsekwencji przeniesienia relacji firmy atlantyckie czy europejskie-Państwo Polskie z poziomu rynkowo- operacyjnego na poziom dyplomacji i polityki).  Problem pominięcia ofert czy wykluczenia z przetargów może też wydarzyć się w przyszłości w relacjach z firmami z Krajów NATO czy UE. **Do tego jeszcze** **dochodzi konstrukcja rozpatrywania odwołań od decyzji. Planuje się,** **że odwołania będzie rozpatrywał ten sam skład decydentów co na 1 etapie** **postępowania.**  Podjęto, i słusznie, już ważne decyzje kierunkowe o tym, że **sieć 5G zbuduje w Polsce spółka POLSKIE 5G, w której dominującym podmiotem będzie Skarb Państwa i to Państwo w ramach tej spółki wybierze technologię i ewentualnych dostawców techniki i technologii. Proces ten ze względu na decyzje o udziale**  **kapitałowym i decyzjach personalnych będzie transparentnie monitorowany i zarządzany przez stosowne organa z kierownictwem Państwa na czele.**  **Doświadczenia Komitetu Offsetowego są jak najbardziej pozytywne**  **i nie wymagają bezpośredniego zaangażowania w proces decyzyjny w ocenie propozycji firm Premiera co grozi konsekwencjami napięć dyplomatycznych i politycznych.**  **Państwo poprzez spółkę POLSKIE 5G będzie decydowało, jakie rozwiązania technologiczne, techniczne i oprogramowanie przez jaką firmę dostarczone będą stosowane w Polsce**.  Polskie 5G *ma być właścicielem jednolitej infrastruktury dla pasma 700 a Skarb Państwa ma zapewnić pasmo 700 MHz oraz dostęp do infrastruktury pasywnej na własnych nieruchomościach, a wybrane współpracujące podmioty prywatne ewentualnie dla potanienia procesu istniejącą albo rozbudowywaną infrastrukturę pasywną i aktywną (aport lub długoletnie dzierżawy) oraz ewentualne środki finansowe.*  **Jakie wnioski Resort Cyfryzacji wyciągnął z wdrożonych już rozwiązań i podjętych decyzji przez Kraje UE i NATO? Jak widzi analizowane i dyskutowane propozycje rozwiązań zapewniających cyberbezpieczeństwo w innych Krajach UE i NATO? Na przykład Wielkiej Brytanii?**  Brytyjskie telekomy po 31 grudnia 2020 roku nie będą mogły kupować sprzętu 5G od pozaeuropejskiego dostawcy, a jeśli już takiego używają, muszą go usunąć ze swoich sieci do 2027 roku.  Izba Gmin podjęła decyzję o zakazie współpracy operatorów telekomunikacyjnych w Wielkiej Brytanii z jednym producentem przy rozbudowie sieci. Decyzja jest konsekwencją sankcji, które na tę firmę nałożyły władze amerykańskie. Oliver Dowden, sekretarz ds. cyfryzacji poinformował, że łączny koszt tego i wcześniejszego ograniczenia nałożonego na dotychczasowego dostawcę na początku roku, wyniesie **do 2 mld funtów**.  W związku z decyzją podjętą przez Izbę Gmin, po **31 grudnia tego roku** brytyjscy operatorzy nie będą mogli współpracować z tą firmą przy rozbudowie swojej infrastruktury sieciowej. Dodatkowo, **do 2027 roku muszą zdemontować wszystkie** **urządzenia sieciowe 5G tego producenta, jeśli takie już posiadają**. Ponieważ  **amerykańskie sankcje dotyczą tylko przyszłego sprzętu, brytyjski rząd poinformował, że nie ma wystarczającego uzasadnienia dla usuwania urządzeń 2G, 3G i 4G.** Najnowsze ograniczenie może mieć wpływ równieżna szerokopasmowe łącza stacjonarne. Rząd Wielkiej Brytanii chce, aby telekomycałkowicie zrezygnowały z kupowania sprzętu od tej firmy, także w przypadku łączyświatłowodowych. Według Ministra Dowdena ma się to stać w ciągu dwóch  lat. Dodatkowy czas ma zapobiec uzależnieniu się Wielkiej Brytanii od Nokii, jako jedynego dostawcy niektórych urządzeń.  **Budując sieci telekomunikacyjne operatorzy nie będą mogli się zaopatrywać u dostawców uznanych za firmy wysokiego lub umiarkowanego ryzyka.**  **Urządzenia i oprogramowanie kupione wcześniej od tych pierwszych trzeba będzie usunąć z sieci najpóźniej w ciągu pięciu lat.**  Ministerstwo w uzasadnieniu projektu przyznaje, że nakładając na firmy nowe obowiązki, „ogranicza się konstytucyjną wolność gospodarczą”, tłumacząc to celem, którym jest „zapewnienie bezpieczeństwa w cyberprzestrzeni”. Pański Resort cyfryzacji przyznaje, że dostosowanie się do wymogów ustawy oznacza koszty dla przedsiębiorców. W uzasadnieniu podkreśla jednak, że to inwestycja „we własne cyberbezpieczeństwo” pozwalająca „skuteczniej dbać o cyberbezpieczeństwo  w swojej działalności, co przełoży się na bezpieczne prowadzenie biznesu i minimalizację ryzyka strat”.  **Mam nadzieję, że Resort starannie rozpatrzył w tej sprawie możliwe roszczenia podmiotów rynkowych od Skarbu Państwa.**  Przypomnę, że jeszcze borykamy się z konsekwencjami decyzji z 2016 r. w obszarze energetyki wiatrowej, kiedy to decyzje podjęte na poziomie menedżerskim, a nie państwowym, doprowadziły do konieczności ugód i wymuszonych przejęć niezadowolonych z decyzji podmiotów prywatnych w tym także kapitału obcego z ewidentną stratą Skarbu Państwa.  **Europa może mieć wielką trudność w rezygnacji z dostaw**  **od pozaeuropejskiego dostawcy, gdyż podstawą budowy sieci 5G ma być starsza sieć 4G, tymczasem w 16 państwach europejskich sieci 4G/LTE w ponad 50 proc. zostały zbudowane z wykorzystaniem sprzętu pozaeuropejskich dostawców. W Polsce wskaźnik ten wynosi 60 proc.** Takieestymacje przedstawiła duńska firma Strand Consult, która przeanalizowała **i**nfrastrukturę sieci 4G u 102 operatorów obsługujących w sumie 673 mln **u** żytkowników telefonów komórkowych.Stuprocentowy udział pozaeuropejskiego sprzętu jest w Belgii, na Cyprze i WyspachOwczych.  **W Polsce jest to 60 proc. –** przy czym w sieci 4G Plusa nie ma wcale, w sieciach Orange i T-Mobile jego udział Strand ocenia na 70 proc., a w Playu – na 90 proc. (udział w proc. jest obliczony według liczby abonentów podłączonych do sieci zbudowanej ze sprzętu danego dostawcy). W Niemczech udział pozaeuropejskich  dostawców wynosi 57 proc., na Węgrzech 55 proc., w Wielkiej Brytanii 40 proc., a we Francji 25 proc. Najmniej – 6 proc. –pozaeuropejskiego sprzętu stosuje Słowacja.  **Według umiarkowanego scenariusza budowa 5G bez wiodącego do tej pory pozaeuropejskiego dostawcy miałaby europejskie telekomy kosztować dodatkowo 3 mld euro rocznie przez 10 lat – czyli prawie o jedną piątą zwiększyć nakłady na nową sieć. To koszt dla 27 państw UE oraz Wielkiej Brytanii, Norwegii, Szwajcarii i Islandii. Na Polskę przypada z tej sumy 120 mln euro rocznie. Optymistyczny scenariusz to 1,4 mld euro wydatków dla 31 państw, a pesymistyczny – 4,5 mld euro.**  Dostawcami na polskim rynku są chiński Huawei, szwedzki Ericsson i fińska Nokia. Szef działu analiz Haitong Banku Konrad Księżopolski wyliczył łączny koszt wymiany obecnie zainstalowanego w sieciach 4G/5G sprzętu pozaeuropejskiego dostawcy  na 2,5‒2,9 mld zł. Największa kwota ‒ 1,3‒1,5 mld zł ‒ przypada na Play, po ok. 0,55‒0,6 mld zł będzie to kosztowało Orange i T-Mobile, a 100‒200 mln zł ‒ Polkomtel. Wyliczenia mogą być obarczone „istotnym ryzykiem błędu” ze względu na bardzo ograniczony dostęp do danych i nie obejmują kosztów uruchomienia sieci 5G, a jedynie wymianę starego sprzętu. Dla porównania: w USA Huawei ma 3,3 tys. anten 4G. A według oficjalnych danych przytaczanych przez amerykańskie media usunięcie tego sprzętu będzie kosztować  1,9 mld USD czyli ponad 7 mld zł. W Polsce trzej operatorzy - T-Mobile, Orange i Play - korzystają w sumie z 20 tys. anten. Jedynym telekomem, który nie poniesie strat związanych z wejściem w życie tego prawa, jest Plus w zdecydowanej większości korzystający z anten szwedzkiego Ericssona. Orange i Play to pod względem liczby obsługiwanych kart SIM to **największe firmy telekomunikacyjne w Polsce**. Pierwsza na koniec czerwca br. zanotowała wzrost  o 3,5 proc. wobec ub.r. – do 15,49 mln kart. Play zaliczył zaś niewielki spadek o 0,1 proc. – do 14,98 mln. **Operatorzy staną więc przed niesamowicie trudnym wyborem**: wystąpić z roszczeniami wobec Państwa za nieplanowane dodatkowe koszty, czy najpierw budować nowoczesną sieć 5G, czy przeznaczać środki na odbudowę od podstaw istniejących sieci. A w końcu o przeniesieniu kosztów tej operacji na finalnego klienta.  Nawet z tych szacunków widać, że polski rynek operatorów znajdzie się w nowych warunkach zdolności konkurencyjnych, bo nie wszyscy operatorzy będą musieli wydąć dodatkowo podobne środki na wymianę używanego sprzętu.  **Dodatkowo nie znamy konsekwencji ograniczenia grona dostawców, czy nie zmniejszyłoby konkurencji i stanowiło bodziec do podwyżki cen sprzętu.**  **I przyznam, że nie podzielam w tej sprawie Pańskiego optymizmu:**  *„Nie myślimy o żadnych rekompensatach ani nie jesteśmy przekonani, że sprzęt uznany za bezpieczniejszy koniecznie będzie również droższy. Dostawcy konkurują ze sobą w skali globalnej, część operatorów też działa w takiej skali. Liczymy, że to wpłynie hamująco na ceny”.*  Moje wątpliwości budzi też założenie Resortu, że wymiana sprzętu pochodzącego od dostawcy wysokiego ryzyka i tak nastąpiłaby w procesie normalnego modernizowania sieci.  **W rezultacie, taka decyzja bez rekompensat dla operatorów i wydłużenia czasu wymiany sprzętu może istotnie spowolnić rozwój sieci nowej generacji. Niejasne także pozostają konsekwencje proponowanych zmian dla pozostałych poza telekomunikacją, a już wdrożonych w technologiach pozaeuropejskich**  **dostawców na przykład realizowanego przez PKP PLK Programu sterowania ruchem kolejowym. Czy zainstalowane w polskich transporcie, sterowaniu ruchem urządzenia także mają podlegać wymianie ?** PKP Polskie Linie Kolejowe od 2018 r. realizują projekt o nazwie: „Budowa infrastruktury systemu ERTMS/GSM-R na liniach kolejowych zarządzanych przezPKP PLK w ramach Narodowego Planu Wdrożenia ERTMS”. Do końca tej dekady systemy ERTMS (który składa się z systemu ETCS i GSM-R) mają być zbudowane  na tzw. sieci bazowej TEN-T. **Jakie będą konsekwencje dla modernizacji i inwestycji realizowanych** **na polskiej sieci kolejowej?**  A przypomnę uzasadnienie dla powtórzenia aukcji o pasmo częstotliwości dla 5G: „Intencją rządu jest jak najszybsze wprowadzenie do Polski komercyjnie funkcjonującej **sieci piątej generacji (5G)** i dotrzymanie terminów określonych  w Europejskiej Agendzie Cyfrowej. Dlatego mając na uwadze możliwe  konsekwencje, a także kwestie związane z bezpieczeństwem, podjęto decyzję o konieczności powtórzenia całego postępowania". **Jaka w nowej sytuacji jest więc prognoza uruchomienia 5 G w Polsce?** | **Wyjaśnienie**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | TEP | Uwaga ogólna | Szanowny Panie Ministrze,  odbywające się aktualnie konsultacje społeczne nad propozycją zmiany ustawy o krajowym systemie cyberbezpieczeństwa są korzystnym i potrzebnym procesem. Poprzez niniejsze pismo pragniemy wziąć udział w pracach nad nowymi przepisami, które są kluczowe zarówno dla branży, jak i dla polskich obywateli i przedsiębiorców. Cieszy nas, że rządzący chcą wysłuchać naszego głosu, który - w co głęboko wierzymy - będzie miał wpływ na ustanowienie możliwie najlepszych społecznie i gospodarczo przepisów, które będą zabezpieczały nasz wspólny narodowy interes. Jako jeden z podmiotów szczególnie zainteresowanych nowymi regulacjami chcieliśmy wyrazić swoje obawy w kilku kwestiach, takich jak choćby:  a) naruszanie przez projekt zasad uczciwej konkurencji i równego traktowania podmiotów;  b) wpływanie przez Kolegium w sposób niejasny i bez szczegółowych wytycznych (technicznych) na podmioty w branży;  c) pozbawienie prawa do odwołania od decyzji Kolegium w przypadku ocen określających średnie i niskie ryzyko;  d) Relatywnie krótki termin wycofania z rynku sprzętu, oprogramowania i usług w przypadku wydania niekorzystnej oceny przez Kolegium oraz wysokie koszty wycofywania z rynku sprzętu i oprogramowania. | **Uwaga częściowo uwzględniona** |
|  | KIKE | Uwaga ogólna | Biorąc pod uwagę możliwe ograniczenia w zakresie dostarczania sprzętu telekomunikacyjnego od określonych dostawców, wdrożona ustawa będzie miała niebagatelny wpływ nie tylko na działalność dostawców sprzętu, technologii i oprogramowania wykorzystywanego w sieciach telekomunikacyjnych, ale także na działalność samych operatorów telekomunikacyjnych zrzeszonych w Izbie.  Wymiar faktyczny nowych regulacji wpłynie na ciągłość działania dostawców sieci i usług łączności elektronicznej oraz na konkurencję na rynku telekomunikacyjnym, co może mieć także istotne przełożenie na sytuację i interesy konsumentów, będących ostatecznymi odbiorcami usług telekomunikacyjnych, jak również będzie wpływać na dalszy rozwój społeczeństwa cyfrowego, co jest jednym z priorytetów Unii Europejskiej. Skutki te niestety nie zostały w dostatecznym stopniu przeanalizowane ani w uzasadnieniu, ani w Ocenie Skutków Regulacji. | **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 przez ustawę wprowadzającą PKE.  Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowym.  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. |
|  | KIKE | Uwaga rozdziału 4a | Przechodząc szczegółowo do uwag, zdaniem KIKE ustawa o krajowym systemie cyberbezpieczeństwa (dalej KSC) w ogóle nie powinna mieć zastosowania do operatorów telekomunikacyjnych, szczególnie z segmentu małych i średnich przedsiębiorców.  Należy przypomnieć, iż KSC stanowi implementację dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. (dalej Dyrektywa). Również nowelizacja jest motywowana jej implementacją. Zgodnie z motywem (7) Dyrektywy, Obowiązki nakładane na operatorów usług kluczowych i dostawców usług cyfrowych nie powinny jednak mieć zastosowania do przedsiębiorstw udostępniających publiczne sieci łączności lub świadczących publicznie dostępne usługi łączności elektronicznej w rozumieniu dyrektywy 2002/21/WE Parlamentu Europejskiego i Rady, które podlegają szczegółowym wymogom w zakresie bezpieczeństwa i integralności ustanowionym w tej dyrektywie, ani nie powinny mieć zastosowania do dostawców usług zaufania w rozumieniu rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014, którzy podlegają wymogom w zakresie bezpieczeństwa określonym w tym rozporządzeniu.  Dyrektywa wprost wyłącza spod jej stosowania określonych przedsiębiorców, podlegających w zakresie cyberbezpieczeństwa innym regulacjom. Z tego względu podczas uchwalania KSC w 2018 roku, spod zakresu podmiotowego wyłączono przedsiębiorców telekomunikacyjnych, o których mowa w ustawie z dnia 16 lipca 2004 r. Prawo telekomunikacyjne, w zakresie wymogów dotyczących bezpieczeństwa i zgłaszania incydentów. Powyższe zostało podkreślone w uzasadnieniu do KSC, Wzorem podejścia przyjętego w dyrektywie 2016/1148 ustawa nie ma zastosowania wobec przedsiębiorców telekomunikacyjnych i dostawców usług zaufania, którzy zostali już objęci europejskimi i krajowymi wymaganiami sektorowymi z zakresu cyberbezpieczeństwa.  Dyrektywa w zakresie podmiotów wyłączonych spod jej stosowania nie uległa zmianie. Nie ma więc powodu ani podstawy, aby ponad 2 lata po uchwaleniu ustawy implementującej Dyrektywę zmienić zakres podmiotowy i objąć stosowaniem KSC przedsiębiorców, którzy dotychczas nie byli objęci regulacją. Zmiana terminologii – przedsiębiorcy telekomunikacyjnego na przedsiębiorcę komunikacji elektronicznej nie spowoduje, że podmioty te z dnia na dzień zmienią zakres swojej działalności, będą bardziej podatni na cyberzagrożenia i będą w stanie sprostać wymogom stawianym przez KSC.  Co więcej, obowiązki przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci i usług oraz zadań i obowiązków na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego są określone w dziale 1 rozdziale 5 projektowanej ustawy prawo komunikacji elektronicznej (projekt ustawy z dnia 29 lipca 2020 r. – dalej jako PKE). To przepisy PKE będą regulować, jakie obowiązki ciążą na przedsiębiorcach komunikacji elektronicznej.  Zgodnie z przepisami PKE (art. 39 i nast. PKE) przedsiębiorcy komunikacji elektronicznej będą zobowiązani m.in. do zgłaszania Prezesowi UKE informacji o wystąpieniu incydentu, kwalifikując go zgodnie z rozporządzeniem wykonawczym. Ponadto przedsiębiorca komunikacji elektronicznej zobowiązany będzie do systematycznego przeprowadzania oceny wystąpienia sytuacji szczególnego zagrożenia czy podejmowania środków technicznych i organizacyjnych zapewniających poziom bezpieczeństwa adekwatny do poziomu zidentyfikowanego ryzyka. Nie ma zatem powodu, aby obowiązki w zakresie bezpieczeństwa sieci i usług rozdrabniać na dwie regulacje – KSC i PKE. Dodatkowo wskazać należy, że PKE zawiera własną definicję incydentu bezpieczeństwa. Nie ma potrzeb, aby obok tego pojęcia wprowadzać pojęcie incydentu telekomunikacyjnego.  Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiająca Europejski kodeks łączności elektronicznej (dalej EKŁE), którą implementuje PKE, również nie przewiduje innych, szczególnych obowiązków w zakresie bezpieczeństwa sieci i usług niż te już zaprojektowane w PKE. W szczególności EKŁE nie nakazuje stosowania Dyrektywy do przedsiębiorców komunikacji elektronicznej czy też nie nakazuje jej stosowania w zakresie nieuregulowanym w EKŁE. Wszelkie odesłania do Dyrektywy zawarte w EKŁE dotyczą współpracy organów państwowych, a nie obowiązków poszczególnych przedsiębiorców komunikacji elektronicznej (patrz: motyw 98 EKŁE oraz art. 41 ust. 4 i 5 EKŁE). | **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 przez ustawę wprowadzającą PKE.  Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowym.  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. |
|  | KIKE | Uwaga ogólna | W zakresie nowych obowiązków niewynikających z PKE wskazać należy, że CSIRT MON, CSIRT NASK i CSIRT GOV w sektorze telekomunikacyjnym uzyskają nowe kompetencje kosztem uprawnień Prezesa UKE oraz CSIRT Telco. Incydenty telekomunikacyjne będą badane przez ww. CSIRT, co należy uznać za błędną regulację - w zakresie bezpieczeństwa usług komunikacji elektronicznej i sieci telekomunikacyjnych główną rolę powinny odgrywać wyspecjalizowane organy telekomunikacyjne. Art. 42 PKE będzie zobowiązywać przedsiębiorcę komunikacji elektronicznej do zgłaszania incydentu bezpieczeństwa Prezesowi UKE, wobec czego nie ma potrzeb, aby przedsiębiorca ten musiał dodatkowo zgłaszać wystąpienie incydentu telekomunikacyjnego do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV i obok tego do CSIRT Telco oraz współdziałać z nimi przy obsłudze incydentu (projektowany art. 20c ust. 1 i 3 KSC). Ocena Skutków Regulacji błędnie zakłada, że wobec przedsiębiorców telekomunikacyjnych nowelizacja będzie oddziaływać w ten sposób, iż będą oni *zobowiązani do zgłaszania incydentów do zespołów CSIRT, zamiast do UKE.* Obowiązek zgłoszenia incydentu do UKE wynikający z PKE będzie niezależny od obowiązku przewidzianego w KSC. Dodatkowo projektowany art. 26 KSC wyraźnie wskazuje na działania CSIRT MON, CSIRT NASK i CSIRT GOV przy badaniu m.in. incydentów telekomunikacyjnych oraz przygotowywaniu materiałów dla Pełnomocnika, gdzie wyklucza się zarówno Prezesa UKE jak i CSIRT Telco. Przedsiębiorcy telekomunikacyjni będą zatem zobowiązani zgłaszać ten sam incydent dwa razy – do Prezesa UKE (na podstawie PKE), oraz do zespołów CSIRT (na podstawie KSC). | **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 przez ustawę wprowadzającą PKE.  Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowym.  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. |
|  | KIKE | Uwaga do art. 20d | Na uwagę zasługuje również szczegółowe wyliczenie elementów zgłoszenia incydentu telekomunikacyjnego, zaproponowane w projektowanym art. 20d KSC. Takie określenie elementów zgłoszenia nie występuje ex lege w PKE i jest ono zbyt szczegółowe, a wręcz nadmierne (np. wpływ na usługi kluczowe innych podmiotów, czego przedsiębiorca komunikacji elektronicznej może nie wiedzieć). Taka szczegółowość utrudni przedsiębiorcom telekomunikacyjnym zgłaszanie incydentów i będzie wprowadzać ich w błąd – przedsiębiorcy do zgłaszania incydentów telekomunikacyjnych będą zobowiązani do stosowania art. 20d KSC, a do zgłaszania incydentów bezpieczeństwa na podstawie PKE zobowiązani będą do stosowania formularza określonego w rozporządzeniu wydanym na podstawie art. 42 ust. 2 pkt. 2) PKE.  Zdaje się, że przepisy z zakresu cyberbezpieczeństwa powinny być spójne, a uchwalenie takich samych obowiązków w dwóch odrębnych aktach prawnych i dołożenie kolejnych z tego samego zakresu, nie będzie sprzyjać spójności przepisów. | **Uwaga nieuwzględniona**  Podobna szczegółowość zgłoszenia występuje przy art. 12 KSC. |
|  | KIKE | Uwaga ogólna | Nowelizacja KSC rozszerza również kompetencje Kolegium. Zgodnie z art. 64 KSC Kolegium ma stanowić organ opiniodawczo-doradczy w sprawach cyberbezpieczeństwa. Zgodnie z projektowanymi przepisami art. 66a-66c KSC, Kolegium na wniosek jego członka może sporządzić ocenę ryzyka dostawcy sprzętu lub oprogramowania istotnego dla cyberbezpieczeństwa podmiotów krajowego systemu cyberbezpieczeństwa (czyli również sprzętu telekomunikacyjnego, zarówno wprowadzenia do użytkowania nowego jak i użytkowania starego), przekazywaną następnie Pełnomocnikowi, który ogłasza ją w postaci komunikatu w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski”. **Dostawca sprzętu podlegający ocenie nie ma realnej możliwości odwołania się od decyzji**. Po pierwsze, termin na ewentualne odwołanie od oceny określającej ryzyko jako wysokie, wynosi 14 dni od publikacji komunikatu. Oznacza to, że *de facto* dostawcy sprzętu będą musieli codziennie śledzić Dziennik Urzędowy w poszukiwaniu informacji, czy czasem nie zostali objęci oceną ryzyka, o której mowa w art. 66a KSC. Po drugie, ewentualne odwołanie wnoszone jest do tego samego organu, który wydał zaskarżaną ocenę. Mało prawdopodobne, aby Kolegium chciało dokonać samokontroli swojej oceny na korzyść odwołującego. Po trzecie, dostawca sprzętu w ogóle nie ma możliwości odwołania się od oceny Kolegium w przypadku, gdy ryzyko zostało ocenione jako umiarkowane lub niskie – w takiej sytuacji możliwe jest jedynie zgłoszenie środków zaradczych i planu naprawczego poniekąd przyjmując, że w takiej sytuacji ocena Kolegium nie podlega kontroli. | **Uwaga częściowo uwzględniona**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3.  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 przekazanym 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. |
|  | KIKE | Uwaga ogólna | Dalej, w przypadku oceny ryzyka określonego jako umiarkowane, podmioty krajowego systemu cyberbezpieczeństwa mogą kontynuować użytkowanie dotychczas posiadanych egzemplarzy sprzętu, oprogramowania oraz rodzaju i liczby usług wykorzystywanych przed opublikowaniem komunikatu o ocenie danego dostawcy sprzętu lub oprogramowania (projektowany art. 66b ust. 2 pkt 2) KSC). Oznacza to, że podmioty korzystające ze sprzętu/oprogramowania danego dostawcy (w tym zrzeszeni w KIKE przedsiębiorcy), nie będą mogły dokonywać ani upgrade’u, ani update’u wykorzystywanych urządzeń/oprogramowania, co ma bezpośredni, negatywny wpływ na cyberbezpieczeństwo i jest wprost sprzeczne z celami KSC. Wszelkie luki zwiększające podatność sprzętu/oprogramowania na cyberataki usuwane są najczęściej poprzez aktualizację sprzętu/oprogramowania. Wyłączenie takiej możliwości spowoduje zmniejszenie poziomu cyberbezpieczeństwa, co stoi w sprzeczności z ogólnym celem KSC. | **Wyjaśnienie**  Zrezygnowano z poziomów umiarkowany, niski, brak zidentyfikowanego ryzyka. |
|  | KIKE | Uwaga ogólna | Cała powyższa koncepcja przeczy charakterowi Kolegium, które – pomimo, że ma być organem opiniodawczo-doradczym – będzie na podstawie art. 66a KSC wydawać opinie wywołujące wprost określone w art. 66b KSC skutki prawne w sferze praw i obowiązków stron. Może to być m.in. zakaz wprowadzenia do użytkowania sprzętu określonego dostawcy czy obowiązek wycofania jego sprzętu/oprogramowania z rynku. Kolegium będzie mogło arbitralnie wywierać wpływ na danego dostawcę decydując o tym, czy jego sprzęt lub oprogramowanie będzie mogło być użytkowane w Polsce czy nie. Jest to uprawnienie leżące poza kompetencjami opiniodawczo-doradczymi. Nie ma przy tym obiektywnych przesłanek, jakimi ja kierować się Kolegium przy dokonywaniu oceny. | **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 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 nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. |
|  | KIKE | Uwaga ogólna | Projektowany art. 66a ust. 4 KSC przewiduje, że przy wydawaniu oceny Kolegium ma się kierować m.in. tym, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, uwzględniając jednocześnie:  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,  zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania.  Są to nieobiektywne przesłanki niemożliwe do zweryfikowania bez podejmowania nadzwyczajnych środków kontrolnych. Kolegium nie ma instrumentów prawnych ani faktycznych aby badać strukturę własnościową zagranicznego dostawcy sprzętu/oprogramowania czy zdolność ingerencji państwa w swobodę działalności gospodarczej tego dostawcy. Powyższe wymagałoby również wnikliwej analizy prawodawstwa tego państwa w zakresie ochrony praw człowieka i ochrony danych osobowych. W konsekwencji Kolegium będzie mogło arbitralnie decydować o wykluczeniu z rynku określonego dostawcy sprzętu lub oprogramowania, pod pretekstem konieczności zapewnienia cyberbezpieczeństwa, co w praktyce będzie nieweryfikowalne. | **Uwaga nieuwzględniona**  Kryteria oceny nawiązują do kryteriów określonych w Toolbox 5G. |
|  | KIKE | Uwaga ogólna | Nie jest zrozumiałe, dlaczego pod uwagę mają być brane indywidualne cechy dostawcy, a pomijane będą najistotniejsze z punktu widzenia cyberbezpieczeństwa aspekty informatyczno-technologiczne. W infrastrukturze wykorzystywane są również urządzenia pasywne, co do których z punktu widzenia cyberbezpieczeństwa bez znaczenia jest, od jakiego są dostawcy.  Konkludując, na podstawie opinii organu opiniodawczo-doradczego nie można zakazać korzystania z określonych urządzeń telekomunikacyjnych czy oprogramowania bez możliwości realnej obrony przed taką opinią przez zainteresowane podmioty, w tym przedsiębiorców telekomunikacyjnych, którzy będą zmuszeni ewentualnie ponieść koszt wymiany urządzeń dostawcy objętego oceną. | **Uwaga nieuwzględniona**  Kryteria oceny nawiązują do kryteriów określonych w Toolbox 5G. Zawierają aspekty techniczne i nietechniczne. |
|  | KIKE | Uwaga ogólna | Co ważne, przepisy projektowanych art. 66a-66c KSC nie mają oparcia w Dyrektywie. Procedura sprawdzająca dostawcę nie jest w niej przewidziana, a 5G toolbox przywołany w uzasadnieniu zawiera wytyczne wyłącznie w zakresie zapewnienia bezpieczeństwa przy wdrażaniu sieci 5G, a nie przy infrastrukturze jako takiej.  Zgodnie z motywem (50) Dyrektywy, Mimo iż producenci sprzętu i twórcy oprogramowania nie są operatorami usług kluczowych ani dostawcami usług cyfrowych, ich produkty zwiększają bezpieczeństwo sieci i systemów informatycznych. Odgrywają oni zatem ważną rolę w umożliwianiu operatorom usług kluczowych i dostawcom usług cyfrowych zabezpieczenia ich sieci i systemów informatycznych. Taki sprzęt i oprogramowanie są już objęte obowiązującymi przepisami dotyczącymi odpowiedzialności za produkt. Dyrektywa (którą, jak podkreślamy, ma implementować KSC) nie przewiduje dodatkowej odpowiedzialności dostawców sprzętu czy oprogramowania. W polskim porządku prawnym dostawcy sprzętu i programowania odpowiadają za dostarczany produkt na podstawie art. 4491 kodeksu cywilnego (odpowiedzialność za produkt niebezpieczny). | **Uwaga nieuwzględniona**  Dyrektywa NIS pozwala na przyjmowanie środków z zakresu bezpieczeństwa, jakie Państwa Członkowskie uznają za stosowne.  Art. 1 ust. 6 Dyrektywy NIS stanowi:  *6. Niniejsza dyrektywa pozostaje bez uszczerbku dla działań podejmowanych przez państwa członkowskie w celu zagwarantowania ich podstawowych funkcji państwowych, w szczególności w celu ochrony bezpieczeństwa narodowego – w tym działań na rzecz ochrony informacji, których ujawnienie państwa członkowskie uważają za sprzeczne z podstawowymi interesami swojego bezpieczeństwa – oraz w celu utrzymania porządku publicznego, w szczególności w celu umożliwienia prowadzenia postępowań przygotowawczych w sprawie przestępstw, ich wykrywania i ścigania.*  Odpowiedzialność z art. 4491 KC dotyczy odpowiedzialności cywilnej za produkt niebezpieczny. Jest to relacja prywatnoprawna między producentem a osobą poszkodowaną. Odpowiedzialność następuje dopiero po wyrządzeniu szkody. Natomiast projektowane przepisy dotyczą sfery *imperium* Państwa, prawa administracyjnego. Państwo może przyjmować regulacje dotyczące wykonywania działalności gospodarczej, w celu ograniczenia ryzyka wystąpienia szkody, która będzie zagrażała wspólnemu bezpieczeństwu. |
|  | KIKE | Uwaga ogólna | 5G toolbox przewiduje, iż państwa członkowskie powinny mieć możliwość zastosowania odpowiednich ograniczeń dla dostawców uznanych za stwarzających wysokie ryzyko, w tym niezbędnych wyłączeń w odniesieniu do kluczowych zasobów. Z powyższego wynika, że:   wobec dostawców uznanych za stwarzających wysokie ryzyko mogą być stosowane odpowiednie ograniczenia,   niezbędne wyłączenia mogą być zastosowane w odniesieniu do kluczowych zasobów,   5G toolbox nie rozróżnia, czy chodzi o dostawcę pochodzącego z Europejskiego Obszaru Gospodarczego czy z państwa trzeciego,  wobec czego (1) przesłanki i ograniczenia przewidziane w art. 66a-66b KSC są niewspółmierne, (2) nie ma wskazanych kluczowych zasobów, wobec których mogą być zastosowane wyłączenia o najdonioślejszych skutkach, (3) każdy dostawca powinien móc podlegać ocenie, również krajowy. W żadnym wypadku dokonując oceny Kolegium nie powinno kierować się przesłankami zaproponowanymi w projektowanym art. 66a ust. 4 KSC. Należy jeszcze podkreślić, że 5G toolbox stanowi tzw. soft law i nie jest instrumentem o takiej samej mocy prawnej jak inne akty prawne. Zgodnie z art. 288 Traktatu o Funkcjonowaniu Unii Europejskiej, źródłami prawa europejskiego są rozporządzenia, dyrektywy i decyzje oraz niemające wiążącej mocy zalecenia i opinie. Ustanawianie tak rygorystycznych, niewspółmiernych do celu i nieobiektywnych przesłanek nie może nastąpić w oparciu o soft law.  Powielenie odpowiedzialności dostawców sprzętu w przepisach KSC powinno być zatem niedopuszczalne, szczególnie, że przepisy KSC wprowadzają odpowiedzialność za hipotetyczne, a nie stwierdzone niebezpieczeństwo i to nawet nie tyle samego wykorzystywanego sprzętu/oprogramowania, co osoby dostawcy w oparciu o nieobiektywne przesłanki. Nie ma w polskim porządku prawnym przepisu, który zezwalałaby na represjonowanie przedsiębiorcy z uwagi na kapitał, który za danym przedsiębiorcą stoi w oderwaniu od jakości produkowanego sprzętu.  Jeśli przepisy KSC koniecznie mają regulować bezpieczeństwo sprzętu/oprogramowania, to powinny skupiać się na sprzęcie/oprogramowaniu jako takim (model sprzętu, wersja oprogramowania, itp.), w oderwaniu od podmiotu, który go dostarcza. Zaproponowane przesłanki mogą w konsekwencji doprowadzić do wykluczenia wszelkich dostawców sprzętu o kapitale spoza Unii Europejskiej.  Z uwagi na dalekoidące skutki regulacji, KIKE wykonało badania, obejmujące szczegółową analizę dot. wykorzystania sprzętu dostawców spoza UE. Wyniki załączonego do niniejszego stanowiska Badania o skali wykorzystania w sektorze telekomunikacyjnym sprzętu dostawców pochodzących spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego (dalej jako „Badanie”), potwierdziło, że czołowi producenci sprzętu elektronicznego, najczęściej wykorzystywanego do budowy sieci w Polsce, mają swoją siedzibę właśnie poza Unią Europejską lub Organizacją Traktatu Północnoatlantyckiego (NATO), co stwarza możliwość objęcia ich oceną ryzyka. Są to przede wszystkim:  i. Dasan (siedziba Seongnam, Korea Południowa),  ii. D-Link (Siedziba: Tajpej, Tajwan),  iii. Huawei (siedziba: Shenzhen, Chiny),  iv. TP-Link (siedziba: Shenzhen, Chiny),  v. ZTE (siedziba: Shenzhen, Chiny),  vi. ZyXEL (siedziba: Xinzhu, Tajwan).  Sprzęt producentów azjatyckich średnio stanowi ponad 80% ogólnie wykorzystywanego przez ISP sprzętu. Co ważne, ponad połowa ankietowanych ISP posiada sieć zbudowaną na asortymencie jednym dostawcy! Są to w największej mierze Huawei (45%), Dasan (21%) oraz ZTE (21%). Wykluczenie z rynku któregokolwiek z producentów azjatyckich może „pogrążyć” małego lub średniego operatora, który de facto zmuszony będzie wymienić wszystkie urządzenia na urządzenia innego producenta. Szacowane koszty takiej wymiany liczone są w milionach złotych. Na koszt taki składałyby się nie tylko wygenerowana liczba elektrośmieci (tj. liczba wycofanych urządzeń, w tym wydane abonentom routery czy dekodery, co dodatkowo porusza kwestię wpływu regulacji na ochronę środowiska), ale zakup nowych, często kilkukrotnie droższych urządzeń, wynagrodzenie dla osób mających wdrożyć zmiany – zapewnienie kompatybilności urządzeń, wymiana urządzeń w terenie, dostosowanie systemów informatycznych, itp.  Już tylko sami ankietowani mali i średni operatorzy telekomunikacyjni oszacowali koszt ewentualnej wymiany na ponad 160 mln zł, a część z nich wprost wskazywała, że konieczność wymiany urządzeń skutkowałaby bankructwem firmy. Średni koszt wymiany sprzętu przypadający na jednego ankietowanego wyniósłby 2,99 mln zł. Gdyby założyć, że tego rodzaju skutki i w takiej skali dotkną każdego, aktywnie działającego na rynku przedsiębiorcę telekomunikacyjnego (a trzeba dodać, że skala finansowego zaangażowania operatorów dużych będzie zapewne na znacznie wyższym poziomie), to przyjmując liczbę aktywnych w Polsce przedsiębiorców telekomunikacyjnych (tj. takich, którzy składają raporty o swojej infrastrukturze) , których wedle raportów UKE na koniec 2019 było 3000 , finansowy wpływ na rynek będzie ogromny, sięgając kwoty niemal 9 mld (8.970.000.000 zł). | **Wyjaśnienie**  Projekt nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa jest neutralny  technologicznie, co oznacza, że przepisy prawa dotyczące m.in. procedury oceny ryzyka  dostawców sprzętu lub oprogramowania, w tym samym stopniu dotyczą każdego dostawcy  sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa.  Projekt nie przewiduje automatycznego wykluczenia czy specjalnego traktowania żadnego z  dostawców. Ewentualne decyzje o wycofaniu konkretnego sprzętu lub oprogramowania z  użytkowania w podmiotach krajowego systemu cyberbezpieczeństwa będą poprzedzone  transparentną – prowadzoną zgodnie z przepisami Kodeksu postępowania administracyjnego – procedurą oceny ryzyka zakończoną decyzją administracyjną.  Dostawca sprzętu lub oprogramowania zostanie uznany za dostawcę wysokiego ryzyka, jeżeli z przeprowadzonego postępowania wyniknie, że stwarza poważne zagrożenie dla bezpieczeństwa narodowego. |
|  | KIKE | Uwaga ogólna | Dalszym skutkiem uchwalenia nowelizacji KSC będzie zaburzenie konkurencji. Po pierwsze, konsekwencją zmuszenia operatora do wycofania sprzętu dostawcy azjatyckiego i zastąpienia go sprzętem innego dostawcy, będzie konieczność przekalkulowania swojej oferty. To użytkownicy końcowi poniosą finansowe konsekwencje nowelizacji. Oferty operatorów staną się droższe i przez to będą mniej atrakcyjne dla użytkowników końcowych, a w konsekwencji przestaną być konkurencyjne. Po drugie, operator taki nie będzie ryzykować wymiany sprzętu na sprzęt dostawcy „zwiększonego ryzyka” (tj. spoza UE/NATO), co do którego w najbliższym czasie również może zapaść decyzja o wykluczeniu z rynku. Dostawcy spoza UE/NATO staną się tym samym stygmatyzowani i to w oderwaniu od jakichkolwiek aspektów technicznych. Nie będzie istotne, czy sprzęt danego dostawcy rzeczywiście jest bezpieczny czy nie, tylko czy jest to dostawca spoza, czy z obszaru UE/NATO.  Sami ankietowani wskazali, że 95% z nich wydało swoim abonentom w ramach umowy o świadczenie usług, urządzenie producenta spoza UE/NATO. Ankietowani zadeklarowali, że dotyczy to łącznie ok. 222.903 abonentów. Ewentualna konieczność wymiany tego sprzętu finansowo dotnie przede wszystkich tych ostatnich, poniosą oni bezpośrednie koszty wymiany urządzenia końcowego, oraz pośrednie koszty wymiany kompatybilnych z tymi urządzeniami urządzeń sieciowych operatora.  Nadmienić należy, że projektowana regulacja stawia pod znakiem zapytania celowość wszystkich projektów POPC (w tym podłączenie do sieci szerokopasmowych placówek oświatowych), w których sprzęt jakiegokolwiek z ww. dostawców został wykorzystany. Zgodnie z podsumowaniem I, II i III naboru , w ramach projektów POPC zasięgiem zostało objętych łącznie 1 891 254 gospodarstw domowych oraz 13 246 placówek oświatowych. Wedle informacji przekazywanych przez członków Izby, w znacznej mierze w takich projektach wykorzystywany był sprzęt ww. dostawców, co potwierdziło Badanie. Spośród operatorów realizujących POPC i OSE:   przy realizacji POPC (lub podobnego programu), 82% operatorów zadeklarowało wykorzystanie sprzętu producenta spoza UE/NATO, gdzie szacowana łączna cena zakupu takich urządzeń wyniosła ok. 49,34 mln zł,   przy realizacji OSE, 90% operatorów zadeklarowało wykorzystanie sprzętu producenta spoza UE/NATO, gdzie szacowana łączna cena zakupu takich urządzeń wyniosła prawie 1,5 mln zł.  Na zakup takich urządzeń wydane zostały środki publiczne w kwocie ponad 50 mln zł. Wykluczenie z rynku któregokolwiek z ww. dostawców spowoduje m.in. to, że placówki oświatowe (a więc podmioty z sektora finansów publicznych) korzystające ze sprzętu któregokolwiek z ww. dostawców, będą zmuszone do ich wymiany. Projektowana regulacja przyczyni się do stworzenia sytuacji konfliktogennych, gdyż pierwszymi podmiotami, do których będą kierowane roszczenia związane z koniecznością zmiany sprzętu, będą beneficjenci POPC – a więc w tym i zrzeszeni w KIKE przedsiębiorcy telekomunikacyjni. Co więcej, dalsze procedowanie zmian w przyjętym projekcie może doprowadzić do chaosu organizacyjnego i niewykonania projektu Ogólnopolskiej Sieci Edukacyjnej (OSE) a to z uwagi na to, że szerokie grono wykonawców korzysta właśnie ze sprzętu i oprogramowania dostawców spoza UE. Z punktu widzenia gospodarności – art. 44 ust. 3 pkt 1) ustawy o finansach publicznych, wydanie ponad 50 mln zł na zakup sprzętu, który następnie decyzją ustawodawcy najpewniej będzie musiał zostać wycofany z rynku, nie jest wydatkowaniem środków publicznych w sposób celowy i oszczędny. Urządzenia takie zostały zakupione właśnie z uwagi na ich konkurencyjną cenę i wówczas nie było powodów aby przypuszczać, że w najbliższym czasie będą zagrożone koniecznością wycofania z rynku. | **Wyjaśnienie**  Projekt nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa jest neutralny  technologicznie, co oznacza, że przepisy prawa dotyczące m.in. procedury oceny ryzyka  dostawców sprzętu lub oprogramowania, w tym samym stopniu dotyczą **każdego dostawcy**  **sprzętu lub oprogramowania** dla podmiotów krajowego systemu cyberbezpieczeństwa.  Projekt nie przewiduje automatycznego wykluczenia czy specjalnego traktowania żadnego z  dostawców. Ewentualne decyzje o wycofaniu konkretnego sprzętu lub oprogramowania z  użytkowania w podmiotach krajowego systemu cyberbezpieczeństwa będą poprzedzone  transparentną – prowadzoną zgodnie z przepisami Kodeksu postępowania administracyjnego – procedurą oceny ryzyka zakończoną decyzją administracyjną.  Dostawca sprzętu lub oprogramowania zostanie uznany za dostawcę wysokiego ryzyka, jeżeli z przeprowadzonego postępowania wyniknie, że stwarza poważne zagrożenie dla bezpieczeństwa narodowego. |
|  | KIKE | Uwaga ogólna | Ocena Skutków Regulacji nie bierze pod uwagę jeszcze innych, istotnych kwestii – ewentualnych kosztów i roszczeń związanych z koniecznością wymiany użytkowanych urządzeń, jeśli zgodnie z KSC przedsiębiorcy komunikacji elektronicznej będą zmuszeni je wymienić, a także skutków („czarny PR”) opublikowania w Dzienniku Urzędowym informacji Pełnomocnika zawierającej ocenę ryzyka dostawcy sprzętu lub oprogramowania istotnego dla cyberbezpieczeństwa podmiotów krajowego systemu cyberbezpieczeństwa.  Są to koszty i roszczenia na chwilę obecną trudne do przewidzenia i oszacowania z uwagi na to, iż przesłanki, którymi ma się kierować Kolegium są nieobiektywne i nie pozwalają na przewidzenie, jaki dostawca może zostać wykluczony z rynku. Ryzyko to jest jeszcze wyższe, jeśli weźmie się pod uwagę fakt, że zgodnie z treścią obecnie obowiązującej ustawy Kolegium jest organem de facto politycznym, a nie specjalistycznym. Wykluczenie może zatem objąć teoretycznie każdego dostawcę spoza EOG. Stawia to przedsiębiorców komunikacji elektronicznej w stanie niepewności. Co więcej, nie wiadomo jakie przedsiębiorcom komunikacji elektronicznej będą przysługiwać roszczenia i przeciwko komu, skoro zgodnie z kodeksem cywilnym, przy ocenianiu bezpieczeństwa produktu nie bierze się pod uwagę cech dostawcy (w szczególności tego czy jest to dostawca spoza EOG czy też nie) lecz wyłącznie cechy samego produktu (tj. niebezpieczny jest produkt niezapewniający bezpieczeństwa, jakiego można oczekiwać, uwzględniając normalne użycie produktu). | **Wyjaśnienie**  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. |
|  | KIKE | Uwaga ogólna | Z kolei opublikowanie w Dzienniku Urzędowym informacji o konkretnym dostawcy sprzętu/oprogramowania może doprowadzić do nieuczciwej walki konkurencyjnej pomiędzy przedsiębiorcami działającymi na tym samym rynku, z których część korzysta ze sprzętu znajdującego się w opublikowanej informacji. Nie trudno wyobrazić sobie sytuację, w której dojdzie do masowego rezygnowania z usług konkretnego przedsiębiorcy telekomunikacyjnego przez abonentów tylko dlatego, że dojdzie do swoistej stygmatyzacji takiego przedsiębiorcy | **Uwaga uwzględniona**  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. |
|  | KIKE | Uwaga ogólna | Mając na uwadze powyższe, KIKE rekomenduje:  1) pozostawienie wyłączenia wskazanego w art. 1 ust. 2 KSC tak, aby objąć wyłączeniem spod nowelizacji przedsiębiorców komunikacji elektronicznej, o których mowa w PKE. W konsekwencji część projektowanych przepisów (w szczególności art. 20a i nast. KSC) powinny zostać całkowicie usunięte. Uregulowanie tej samej materii w dwóch różnych aktach prawnych jest sprzeczne z zasadami legislacji i spowoduje wprowadzenie w błąd adresatów obowiązków. PKE będzie kompleksowo regulować obowiązki przedsiębiorców komunikacji elektronicznej w zakresie zgłaszania incydentów cyberbezpieczeństwa. Nie ma powodu, dla którego obowiązki te powinny być powielone i rozszerzone w osobnym akcie prawnym; | **Uwaga nieuwzględniona**  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. |
|  | KIKE | Uwaga ogólna | 2) zapewnienie przejrzystego postępowania w zakresie art. 66A-66C KSC w oparciu o obiektywne, konkretne i niebudzące wątpliwości kryteria, w szczególności kryteria informatyczno-technologiczne, które powinny być nadrzędne przy podejmowaniu decyzji o wyłączeniu z rynku danego sprzętu;  3) zapewnienie dostawcy sprzętu, którego dotyczy postępowanie, możliwości czynnego udziału w każdym stadium postępowania.  KIKE proponuje, aby wzorem postępowania przewidzianego w prawie przedsiębiorców, postępowanie mogło być przeprowadzone dopiero po uprzednim dokonaniu analizy prawdopodobieństwa naruszenia prawa w ramach wykonywania działalności gospodarczej (art. 47 ust. 1 prawa przedsiębiorców) oraz aby o zamiarze przeprowadzenia kontroli zawiadomić zainteresowany podmiot (art. 48 ust. 1 prawa przedsiębiorców). Umożliwi to podmiotowi zainteresowanemu możliwość wypowiadania się na bieżąco do uwag i spostrzeżeń Kolegium na każdym etapie postępowania i co ważne – zainteresowany podmiot będzie wiedzieć, że poddany zostaje kontroli;  4) zobowiązanie Kolegium do wydania decyzji administracyjnej w przedmiocie uznania danego dostawcy za stwarzającego ryzyko dla cyberbezpieczeństwa – niezależnie od tego, czy ryzyko zostanie ocenione jako wysokie, umiarkowane, czy niskie.  W każdym przypadku zainteresowany podmiot musi mieć możliwość obrony przed decyzją wywołującą tak dalekoidące skutki, co sprowadza się do rekomendacji opisanej w pkt. 5) poniżej;  5) zapewnienie dwuinstancyjności postępowania, oraz możliwość zaskarżenia decyzji organu dwuinstancyjnego do Sądu Administracyjnego.  Kolegium nie może być jedynym, nieomylnym organem, którego decyzje nie podlegają kontroli. Regulacja w obecnym kształcie jest sprzeczna z konstytucyjną zasadą dwuinstancyjności postępowania administracyjnego.  6) wprowadzenie procedury, że publikacja ogłoszenia w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski” można następować wyłącznie na podstawie ostatecznej decyzji, a ewentualne zaskarżenie decyzji do sądu administracyjnego wstrzymałoby publikację automatycznie.  Mając na względzie daleko idące skutki rozszerzenia kompetencji Kolegium i Pełnomocnika, KIKE rekomenduje, aby zmienić treść projektowanych przepisów zgodnie z powyższymi rekomendacjami, jako że w obecnej treści są one wysoce szkodliwe, sprzeczne z Dyrektywą i nierealizujące 5G toolbox. | **Uwaga częsciowo uwzględniona**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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 nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. |
|  | Huawei Polska | Uwaga ogólna | Zawartość projektu pozostaje w sprzeczności zarówno z polskim  prawem, jak i prawem Unii Europejskiej, w szczególności:  1. Kryteria oceny ryzyka dostawcy zdefiniowane w projekcie to czynniki zupełnie nietechniczne: w tym m.in. relacje między dostawcą a krajem macierzystym, przepisy dotyczące praw człowieka w kraju macierzystym, przepisy dotyczące ochrony danych  osobowych w kraju macierzystym, struktura własności dostawcy, zdolność ingerencji kraju macierzystego w działalność dostawcy, itp.  2. Projekt ustawy daje Kolegium ds. Cyberbezpieczeństwa prawo wyboru dostawców dla operatorów telekomunikacyjnych, a rynek komercyjny podlega silnym wpływom politycznym, co nie sprzyja zachowaniu konkurencji rynkowej.  3. Ustawa nie precyzuje jednolitych i przejrzystych kryteriów oceny technicznej i nie określa zakresu ocenianych urządzeń: nabywcy są zobowiązani do zaprzestania zakupów  wszystkich urządzeń od dostawców wysokiego / średniego ryzyka zidentyfikowanego przez rząd, a operatorzy są również zobowiązani do wycofania z użytkowania urządzeń dostawców wysokiego ryzyka w ciągu 5 lat.  4. Projekt dyskryminuje dostawców pochodzących spoza Unii Europejskiej oraz tych, którzy pochodzą z państw, które nie są członkami NATO.  Projekt nie ustanawia ujednoliconych i przejrzystych kryteriów oceny, oraz nie spełnia wymogów w zakresie cyberbezpieczeństwa, a co więcej, narusza wiele przepisów polskiego prawa:  1. zasady praworządności, proporcjonalności, wolnego i równego handlu, o których mowa w art. 2, art. 14, art. 32 Konstytucji RP.  2. prawa podmiotu do udziału w procesie oceny na podstawie art. 9 Kodeksu Postępowania Administracyjnego.  3. przepisy art. 24 Kodeksu Cywilnego o ochronie praw osobistych podmiotów cywilnych.  4. podstawowe zasady wolnej konkurencji i wolnego rynku w polskim Prawie Konkurencji.  Jednocześnie, Projekt ten narusza również zasady Unii Europejskiej oraz Handlu Międzynarodowego, w tym:  1. zasadę niedyskryminacji oraz równego traktowania określone w art. 18 „Traktatów o Funkcjonowaniu Unii Europejskiej”, oraz w art. 20 i art. 21 Karty Praw Podstawowych UE.  2. art. 2 „Traktatu Północnoatlantyckiego”, określającego zasadę równości.  3. zalecenia „Nie wykluczania żadnego konkretnego kraju czy dostawcy” określonego w Toolboxie 5G Unii Europejskiej.  4. zasady Światowej Organizacji Handlu (WTO) dotyczące zasady wzajemności oraz klauzuli największego uprzywilejowania.  Regulacje przedstawione w Projekcie Ustawy noszą znamiona dyskryminacji i wykraczają daleko poza ustalenia dokonane przez kraje członkowskie UE, a także inne kraje na świecie:   |  |  |  | | --- | --- | --- | |  | **Polska** | **Inne kraje UE (Niemcy, Szwecja, Finlandia itp.)** | |  | Dostawcy sprzętu | Operatorzy | | Zakres oceny | Wyłącznie tożsamość dostawcy | Kluczowe urządzenia 5G | | Kryteria oceny | Pod uwagę brane są wyłącznie  czynniki nietechniczne: relacje  między dostawcami a krajem  macierzystym, przepisy dotyczące  praw człowieka w kraju  macierzystym, przepisy dotyczące  ochrony danych osobowych w  kraju macierzystym, struktura  własności dostawcy i zdolność  ingerencji kraju macierzystego w  działalność dostawcy | 1. Zarządzanie operatorów w zakresie  cyberbezpieczeństwa.  regulacyjne dokonują przeglądu z  wyprzedzeniem, a później ew. nakładają  kary. Brak wykluczeń poszczególnych  dostawców a priori  2. Neutralność technologiczna: do oceny  ryzyka używane są weryfikowalne  standardy techniczne, takie jak  mechanizm  zapewniania  bezpieczeństwa urządzeń sieciowych  NESAS. | | Sposoby zarządzania | Zabrania się kupowania sprzętu i  oprogramowania od dostawców  wysokiego i średniego ryzyka. | Zarządzane są tylko krytyczne produkty  i określone wrażliwe obszary. | | Proces oceny | Bezpośrednie podejmowanie  decyzji przez Kolegium ds  Cyberbezpieczeństwa bez udziału  interesariuszy z branży | 1. Ocena sporządzona i decyzja  podejmowana przez operatorów. Ocena  może polegać na oświadczeniu  złożonym przez dostawcę i fakcie, że  kluczowe sprzęty dla bezpieczeństwa są  certyfikowane.  2. Instytuty regulacyjne nakładają  potencjalne karyna operatorów w  przypadku wykrycia ryzyk. |   Projekt, który dotyczy zagadnienia cyberbezpieczeństwa, został opracowany w sposób, który wyklucza konkretnego dostawcę. Jeżeli firma Huawei zostanie wykluczona z listy dostawców sprzętu ICT w Polsce, spowoduje to straty gospodarcze szacowane na dziesiątki miliardów euro dla całego społeczeństwa i wygeneruje koszty dla branży ICT w wysokości 8,5 miliarda euro. W znacznym stopniu wpłynie to również na zaufanie inwestycyjne operatorów, może zmniejszyć ich gotowość do zakupu pasma częstotliwości i tym samym zmniejszy dochody z rządowej aukcji o setki milionów euro. Przewiduje się od 3 do 5 lat opóźnienia rozwoju sieci 5G w Polsce i krajowego procesu cyfryzacji, oraz negatywny wpływ na PKB dla wszystkich powiązanych branż szacowany na 3%, natomiast ceny taryf telefonii komórkowej dla użytkowników mogą wzrosnąć od 1 do 3  razy. Projekt wpływa na środowisko inwestycyjne w Polsce i kształcenie talentów teleinformatycznych z najwyższej półki. Sama firma Huawei zatrudnia w Polsce ponad 3000 osób, zatem polska kolebka talentów ICT w Europie również ulegnie degradacji.  Projekt zahamuje rozwój 5G w Polsce, przez co zmniejszy się jej konkurencyjność jej gospodarki w erze cyfrowej. Jako technologia komunikacyjna nowej generacji o ultra-dużej przepustowości i ultra niskim opóźnieniu, 5G nie tylko zapewnia szybkie połączenia dla zwykłych obywateli, ale także umożliwia cyfrową rewolucję przemysłową tysięcy branż. A więc utrudnienie budowy sieci 5G spowoduje zahamowanie rozwoju polskiej gospodarki cyfrowej.  W związku z powyższym Polska, a nawet Unia Europejska, aktywnie wprowadza politykę promującą rozwój sieci komunikacyjnej 5G. Aby zapewnić harmonijny rozwój polskiej gospodarce ICT i stworzyć uczciwe i sprawiedliwe otoczenie rynkowe i przemysłowe,  chcielibyśmy poprosić Państwa o ponowną weryfikację Projektu Ustawy. Równocześnie, chcielibyśmy zarekomendować następujące rozwiązania:  **Opcja 1**  Realizacja ostatniego rozporządzenia (z dnia 29 czerwca) dotyczącego cyberbezpieczeństwa i usunięcie klauzuli opartych na przesłankach politycznych czy dyskryminacyjnych z obecnego Projektu Ustawy o KSC.  **Opcja 2**  1. Proces Uwzględnienie publicznych konsultacji i przeprowadzenie kompleksowej oceny (koszty, konkurencja, rozwój branży, ekonomia i praworządność);  2. Przedmiot oceny  a) Powinien uwzględniać: krytyczny sprzęt i oprogramowanie 5G, a nie dostawcę;  b) Powinien być oparty na faktach i obiektywnych kryteriach, a nie politycznych;  c) Powinien być podejmowany przez wyspecjalizowaną instytucję, a nie Kolegium ds. Cyberbezpieczeństwa.  3. Korzystnym byłoby przyjęcie globalnych standardów, które są przyjęte w takich krajach jak Niemcy czy Korea Południowa - np. uzyskanie certyfikacji NESAS od GSMA.  W trosce o zdrowy rozwój polskiej gospodarki cyfrowej mamy nadzieję i głęboko wierzymy, że niniejszy list dostarczy Panu rzetelną i bezstronną informację zwrotną. Jednocześnie, jako przedstawiciele Huawei, mamy nadzieję i prosimy o spotkanie z Panem Ministrem, w celu omówienia Pana potencjalnych wątpliwości oraz w celu poinformowania o naszych przyszłych planach współpracy w Polsce. Z chęcią wysłuchamy Pańskiej opinii w tej sprawie. | **Uwaga nieuwzględniona**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały 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 nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano 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 został dołączony do ustawy jako załącznik nr 3. |
|  | Huawei Polska | Uwaga ogólna | Na wstępie chcielibyśmy podkreślić, iż w pełni rozumiemy i popieramy cel, jaki przyświeca autorom projektowanej ustawy, a jakim jest zwiększenie bezpieczeństwa infrastruktury i usług telekomunikacyjnych/teleinformatycznych. Zapewnienie bezpieczeństwa produkowanej infrastruktury i dostarczanych usług telekomunikacyjnych jest również priorytetem naszej spółki. Ważne jednak, aby środki do tego celu były przejrzyste, proporcjonalne i w sposób równy traktowały wszystkich zainteresowanych. Z tej perspektywy nie możemy nie zauważyć, że niektóre istotne proponowane w projekcie rozwiązania są nieobiektywne i mogą skutkować dyskryminacją podmiotową opartą o kryteria niekoniecznie związane z cyberbezpieczeństwem. Powyższe nie jest wyłącznie naszą opinią, ale podzielane jest przez innych przedsiębiorców z szeroko rozumianej branży telekomunikacyjnej i teleinformatycznej oraz ekspertów ds. cyberbezpieczeństwa. W efekcie działania zaproponowanych mechanizmów ustawowych może dochodzić do wykluczenia z polskiego rynku niektórych podmiotów dostarczających sprzęt lub usługi elektroniczne, bez jednoczesnego zwiększenia bezpieczeństwa sieci telekomunikacyjnych, w szczególności sieci 5G, a w niektórych sytuacjach nawet ze skutkiem w postaci pogorszenia tego bezpieczeństwa.  W kontekście regulacji krajowych warto wziąć pod uwagę zdanie Rady Europejskiej, przedstawione na posiedzeniu w dniach 1-2 października 2020 r. (EUCO 13/20; CO EUR 10 CONCL 6). W punkcie 7 i 11 swojego stanowiska, Rada Europejska zatwierdziła konkluzje z dnia 9 czerwca 2020 r. w sprawie kształtowania cyfrowej przyszłości Europy. Apeluje do UE i państw członkowskich o wykorzystanie przyjętego w dniu 29 stycznia 2020 r. unijnego zestawu narzędzi na potrzeby cyberbezpieczeństwa sieci 5G (Toolbox). Wskazuje jednak, że:  • po pierwsze, ewentualne ograniczenia wobec dostawców wysokiego ryzyka, dotyczyć powinny tylko kluczowych aktywów określonych jako krytyczne i wrażliwe w unijnych skoordynowanych ocenach ryzyka;  • po drugie, Rada Europejska podkreśla, że potencjalni dostawcy 5G muszą być poddawani ocenie opartej na wspólnych obiektywnych kryteriach.  • po trzecie wreszcie, podkreśla, że UE pozostanie otwarta dla wszystkich przedsiębiorców przestrzegających europejskich norm i przepisów.  Przedstawiony przez Ministra Projekt, wprowadza mechanizm szacowania ryzyka dostawcy sprzętu lub oprogramowania istotnego dla cyberbezpieczeństwa podmiotów krajowego systemu cyberbezpieczeństwa (art. 1 punkt 29 Projektu). Oceny takiej miałoby dokonywać działające przy Radzie Ministrów Kolegium ds. Cyberbezpieczeństwa („Kolegium”). Jeśli tak przeprowadzona ocena wskazałaby wysokie ryzyko konkretnego dostawcy, podmioty krajowego systemu cyberbezpieczeństwa (w tym m.in., po wejściu w życie przewidzianej w Projekcie zmiany art. 4 ustawy z dnia 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa („KSC”), przedsiębiorcy telekomunikacyjni), nie mogłyby nabywać od takiego dostawcy sprzętu, oprogramowania czy też usług określonych w rozstrzygnięciu Kolegium, zaś w ciągu 5 lat od dnia ogłoszenia komunikatu o ocenie, musieliby taki sprzęt, oprogramowanie czy też usługi wycofać z użytkowania. Dostawca taki mógłby również zostać wykluczony z ubiegania się o zamówienia publiczne.  W hipotetycznym więc przypadku arbitralnego zakazania wykorzystywania w Polsce urządzeń i oprogramowania pochodzącego od podmiotów chińskich (np. Huawei lub ZTE), struktura krajowego rynku urządzeń radiowej sieci dostępowej zbliżyłaby się do ustabilizowanego duopolu. Realizacja takiego scenariusza z pewnością doprowadziłaby do wzrostu kosztów budowy sieci 5G w Polsce, opóźnienia w oddaniu jej do użytkowania, a w konsekwencji do wyższych cen dla abonentów. Dla poparcia tezy o szkodliwości sztucznego „przerzedzenia” polskiego rynku urządzeń radiowej sieci dostępowej wskazać można, iż Komisja Europejska nigdy nie wyraziłaby zgody na doprowadzenie do analogicznego skutku w wyniku fuzji lub przejęć przedsiębiorstw. W Wytycznych w sprawie oceny horyzontalnego połączenia przedsiębiorstw na mocy rozporządzenia Rady w sprawie kontroli koncentracji przedsiębiorstw (2004/C31/03) wskazała ona, że „połączenia na rynkach oligopolistycznych, powodujące wraz z obniżeniem presji konkurencyjnej pozostałych konkurentów wyeliminowanie istotnych ograniczeń związanych z konkurencją, które poprzednio nakładały na siebie łączące się strony, mogą również stworzyć istotną przeszkodę dla konkurencji, nawet jeśli istnieje niewielkie prawdopodobieństwo koordynacji pomiędzy członkami oligopolu. Rozporządzenie WE w sprawie kontroli łączenia przedsiębiorstw wyjaśnia, że wszystkie połączenia powodujące takie nieskoordynowane efekty zostaną również uznane za niezgodne ze wspólnym rynkiem”.  Zaniepokojeni możliwymi negatywnymi konsekwencjami przyjęcia Projektu w zaproponowanym brzmieniu, zarówno w stosunku do wszystkich przedsiębiorców działających w Polsce, jak i do polskich konsumentów (o czym szerzej mowa w załączonej do niniejszego stanowiska „Analizie planowanej nowelizacji ustawy z 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa i jej konsekwencji” przygotowanej przez Squire Patton Boggs na zlecenie Huawei Polska sp. z o.o. w dniu 2 października br. zwanej dalej ”Memorandum”) pragniemy wskazać poniżej najważniejsze uchybienia Projektu, których usunięcie powinno zostać dokonane w toku dalszych prac legislacyjnych: | **Wyjaśnienie**  **Zastosowane w ustawie procedury, w szczególności zastosowania przepisów kodeksu postępowania administracyjnego, gwarantuje prawa stron ewentualnego postępowania w sprawie o uznania za dostawcę wysokiego ryzyka. Ponadto wszelkie przesłanki uznania za dostawcę wysokiego ryzyka są takie same dla każdego potencjalnego przedsiębiorcy. Ponadto procedura ta będzie miała zastosowanie jedynie w przypadku poważnych zagrożeń dla bezpieczeństwa narodowego. Ponadto wprowadzane przepisy są zgodne z prawem europejskim.** |
|  | PIIT |  | Poniższe stanowisko przedstawia odniesienie do wszystkich kluczowych zidentyfikowanych obszarów projektu ustawy.  Odnotowujemy przedstawione w tym zakresie uzasadnienie dotyczące konieczności przyspieszenia prac z uwagi na implementację Europejskiego Kodeksu Łączności Elektronicznej (EKŁE) do krajowego porządku prawnego, jednak **w naszej ocenie prezentowany projekt ustawy zdecydowanie wykracza poza zakres niezbędny do implementacji przepisów unijnych**, a zatem trudno uznać ww. uzasadnienie za trafne. Projekt zmiany ustawy o krajowym systemie cyberbezpieczeństwa (KSC) przedstawia plany bardzo istotnych, fundamentalnych wręcz reform w obszarze bezpieczeństwa, które jednocześnie wykraczają dalece poza zakres niezbędny dla implementacji EKŁE.  Podkreślić należy, że **zakres przedłożonego do konsultacji projektu ustawy jest bardzo rozległy, a jego treść trudna w interpretacji, co dodatkowo potęguje skromna treść uzasadnienia, brak wcześniej dyskusji nad kształtem planowanych zmian z ich adresatami oraz nakładanie się przepisów na projektowane nowe Prawo Komunikacji Elektronicznej, i to na 3 miesiące przed jego planowanym wejściem w życie.**  Tym samym, przedmiotowy **projekt powinien być procedowany jako odrębna inicjatywa legislacyjna, w warunkach konstruktywnego dialogu z podmiotami, do których kierowane są tak daleko idące zmiany i nowe obowiązki.** W innym przypadku, z uwagi na pośpiech, jaki towarzyszy pracom nad PKE, kluczowa tematyka cyberbezpieczeństwa zostanie zatracona w masie innych przepisów i dogłębna debata, także na poziomie parlamentu nie będzie mogła się odbyć w sposób należny tak ważnym zmianom. Tymczasem, dla budowy systemu cyberbezpieczeństwa niezbędna jest dobra współpraca wszystkich podmiotów, która właśnie w ramach wspólnego dochodzenia do odpowiednich rozwiązań powinna być budowana.  **W zakresie planowanego wprowadzenia mechanizmów oceny dostawców, niezależnie od dalszych uwag szczegółowych, przede wszystkim uważamy, że faktycznie efektywnym narzędziem poprawy bezpieczeństwa będzie wprowadzenie i stosowanie mechanizmów certyfikacji, w szczególności opartych o unijny „Cybersecurity act”**. Obszar sieci 5G jest jednym z obszarów jakie zostały zidentyfikowane do takiej certyfikacji, która powinna być uniwersalna i wymagana na poziomie całej UE. Jedynie w ten sposób UE będzie w stanie w spójny i oparty na merytorycznych przesłankach badać i dopuszczać lub odrzucać sprzęt lub oprogramowanie, które nie spełniają wymagań bezpieczeństwa. Ewentualna ocena w oparciu o kryteria nietechniczne powinna być rozważana dopiero w drugim kroku po ustabilizowaniu i ocenie stosowania mechanizmów certyfikacyjnych.  Mając na uwadze powyższe, obok uwag szczegółowych (w dalszej części wystąpienia), **poniżej przedstawiamy nasze kluczowe postulaty oraz określenie ram nowelizacji.** Liczymy, że będą one podstawą do wspólnej dyskusji z Państwem, czy to podczas konferencji uzgodnieniowej, czy innej formule w ramach dialogu Projektodawcy z rynkiem.   1. **Dotychczasowe wyłączenie przedsiębiorców telekomunikacyjnych oraz dostawców usług zaufania  z zakresu obecnej regulacji ustawy KSC musi zostać utrzymane**, z uwagi na fakt, że nawet, jeśli zostałyby wprowadzone dla nich dodatkowe obowiązki, z pozostałego zakresu ustawy KSC implementującego bezpośrednio dyrektywę NIS przedsiębiorcy ci muszą pozostać wyłączeni. 2. **Na tym etapie należy zrezygnować z dodatkowej regulacji obowiązków przedsiębiorców komunikacji elektronicznej na gruncie ustawy KSC oraz włączenia tej kategorii przedsiębiorstw do krajowego systemu cyberbezpieczeństwa. Wdrożenie nowych obowiązków przedsiębiorców komunikacji elektronicznej jest niemożliwe w przewidzianym w projekcie ustawy terminie, a przedstawiony projekt przepisów jest jeszcze niedojrzały i wymaga dalszych istotnych prac, zarówno w zakresie samej koncepcji, jak i właściwego uzasadnienia i oceny skutków regulacji.**   Nie jest to niezbędne do wdrożenia z uwagi na transpozycję EKŁE, za takim rozwiązaniem nie przemawiają faktyczne potrzeby wskazane w uzasadnieniu, a wysoce problematyczny jest brak czasu na wdrożenie, dublowanie się obowiązków z tymi przewidzianymi już w PKE (także w zakresie cyberataków), niespójność i nierozłączność definicji incydentu, brak przepisów wykonawczych, czy nawet brak powołanego CSIRT Telco, wobec, którego miałaby być wykonywana część nowych obowiązków.  Część przepisów PKE została przepisana do ustawy KSC bez wyjaśnienia intencji czy demarkacji, czego skutkiem byłoby np. wprowadzenie dwóch identycznych upoważnień do wydania rozporządzenia przez Ministra Cyfryzacji dla rozporządzenia w zakresie środków technicznych i organizacyjnych, jak i rozporządzenia w sprawie progów incydentów. Jednocześnie, absolutną koniecznością jest utrzymanie jednego kanału zgłaszania incydentów ze spójną siatką pojęciową, przejrzystą procedurą, nawet, jeśli miałby on zostać rozszerzony o dodatkowe zagadnienia związane z cyberbezpieczeństwem. Za zupełnie niezasadne uważamy przy tym całkowite przeniesienie obowiązków w zakresie bezpieczeństwa i integralności sieci i usług telekomunikacyjnych, z PT/PKE do KSC. Zakres ten jest o wiele szerszy niż samo cyberbezpieczeństwo i nie znajdujemy podstaw do takiego działania. Zakładamy, że znajdujące się w OSR sformułowanie, że *przedsiębiorcy telekomunikacyjni będą zgłaszali incydenty do zespołów CSIRT poziomu krajowego oraz do CSIRT Telco, zamiast do regulatora* ma charakter omyłki lub braku odpowiedniego zrozumienia charakteru incydentów zgłaszanych do UKE, z których większość to naruszenia wynikające z przyczyn fizycznych awarii lub problemów w systemach, a nie cyberataków. To UKE jako organ wyspecjalizowany  w obszarze telekomunikacji jest właściwy od przyjmowania takich zgłoszeń oraz podejmowania  w związku z nimi dalszych działań, w tym informowania podmiotów krajowego systemu cyberbezpieczeństwa jeśli incydenty. Warto w tym kontekście przypomnieć, że samo Ministerstwo Cyfryzacji w uzasadnieniu do przyjętego ostatnio rozporządzenia do art. 175d PT wskazało na marginalny udział cyberataków: *Najczęstszymi przyczynami naruszeń były awarie sprzętu i oprogramowania (168 przypadków). Dewastacja infrastruktury spowodowała 16 naruszeń, przerwa w zasilaniu – 6, a błąd ludzki – 5. Marginalne były przyczyny spowodowane klęską żywiołową  i cyberatakiem.”.*   1. **Uwzględniając przedstawianą przez Ministerstwo Cyfryzacji ocenę o kluczowej roli sektora komunikacji elektronicznej dla spójności krajowego systemu cyberbezpieczeństwa uważamy, że do dyskusji o rozszerzeniu aktualnych obowiązków należy wrócić po wdrożeniu ustawy PKE oraz w ramach trwającej aktualnie dyskusji na temat rewizji dyrektywy NIS, której jednym z wątków jest właśnie włączenie przedsiębiorstw komunikacji elektronicznej do zakresu jej regulacji. Deklarujemy gotowość do udziału w takiej dyskusji** i wypracowaniu optymalnych i niezbędnych rozwiązań, w tym w zakresie ich spójności z obowiązującymi już regulacjami w zakresie obsługi i zgłaszania incydentów. Podobnie jak udało się to zrealizować w przypadku dyskutowanych i wydanych ostatnio rozporządzeń do art. 175d i 176a PT.   Aktualnie jednak to implementacja EKŁE do krajowego porządku prawnego, a następnie wdrożenie ustawy PKE są absolutnie priorytetowe i z uwagi na bardzo krótkie terminy wejścia w życie będą stanowiły ogromne wyzwanie dla przedsiębiorców. W świetle tak znaczącej rewolucji porządku prawnego w obszarze komunikacji elektronicznej, w  naszej ocenie konieczne jest urealnienie oczekiwań Projektodawcy w tym zakresie.   1. **Projekt ustawy może, więc zostać ograniczony do wprowadzenia mechanizmów oceny dostawców, który wynika wprost z unijnych dokumentów takich jak tzw. 5G Toolbox**. Projekt ten powinien być procedowany odrębnie od projektu PKE. Kluczową osią naszych postulatów jest doprecyzowanie przepisów w taki sposób, aby uwzględnienie ewentualnych rekomendacji Kolegium odbywało się z poszanowaniem naturalnych procesów rozwoju i utrzymania, m.in. w zakresie sieci telekomunikacyjnych, tak, aby ograniczyć potencjalnie istotne skutki dla możliwości zachowania ciągłości i jakości usług dla ich użytkowników. 2. **Procedura oceny powinna zostać wprowadzona zgodnie z zalecaniami Toolbox 5G,** tj. w przypadku oceny ryzyka, jako wysokiego oraz ewentualnych restrykcji nakładanych na danego dostawcę powinny one być ograniczone do kluczowych zasobów (key assets). Zakres kluczowych zasobów powinien zostać określony na podstawie raportu w sprawie unijnej skoordynowanej analizy ryzyka oraz zakresu kluczowej infrastruktury określanej przez operatorów na podstawie par. 2 pkt 2 rozporządzenia do art. 175d PT, tj. *elementów infrastruktury telekomunikacyjnej i systemów informatycznych, których naruszenie bezpieczeństwa lub integralności będzie miało istotny wpływ na funkcjonowanie sieci lub usług o znaczeniu kluczowym dla funkcjonowania przedsiębiorcy*. Potencjalnie możliwe byłoby na ich podstawie wydanie rozporządzenia określającego przekrojowo co jest rozumiane jako kluczowe zasoby na potrzeby oceny w zakresie 5G. Po drugie ocena powinna opierać się o jasne i precyzyjne kryteria. 3. Zauważamy również, że projekt ustawy może skutkować istotnym poziomem **ingerencji, również w działalność gospodarczą podmiotów prywatnych,** a także na świadczone przez nie usługi przy jednoczesnym dość ogólnym i w rzeczy samej, uznaniowym podejściu do określenia kryteriów opisu sytuacji, w jakich po odpowiednie narzędzia, w szczególności Pełnomocnik Rządu może sięgać. Stąd, w poniższym stanowisku przedstawiamy nasze propozycje modyfikacji przedłożonego projektu. 4. Projekt ustawy powinien również uwzględnić podmioty, które działają na szeroko rozumianym rynku komunikacji elektronicznej. Warto wskazać, iż rynek telekomunikacyjny obecnie definiowany jest jako rynek komunikacji elektronicznej, na którym sieci oraz usługi dostarczają nie tylko tradycyjnie postrzegani przedsiębiorcy telekomunikacyjni ale również inne podmioty dzisiaj funkcjonujący poza rynkiem telekomunikacyjnym. 5. Punktem wyjścia jest przyjęcie założenia, iż przyszłe usługi łączności elektronicznej są (lub będą) świadczone w układzie trójkąta charakterystycznego dla sieci 5G:     Dla tak sformułowanego trójkąta usług łączności elektronicznej, rozszerza się liczba podmiotów/funkcji realizowanych w ramach komunikacji. Usługi łączności elektronicznej to nie tylko połączenie głosowe, szybki dostęp do sieci Internet (enhanced mobile broadband) ale również:   * sieci dedykowane dla komunikacji masowej IoT np. LTE-M, NB-IoT (massive machine type communication), * sieci o wysokich parametrach jakościowych np. campus network (ultra-reliable and low latency communication).   Dodatkowo sieci te będą świadczyć usługi w ramach tzw. network slicing, dedykując odpowiednie parametry jakościowe dla określonych usług np. usługi bankowe mogą wymagać wydzielonego zasobu sieciowego o określonych parametrach bezpieczeństwa, tworząc rozwiązanie E2E w ramach network slicing.  Każdy podmiot, który bierze udział w realizacji komunikacji/przesyłaniu sygnałów jest podmiotem, który świadczy usługi łączności elektronicznej, czyli:   * „tradycyjni” przedsiębiorcy telekomunikacyjni; * dostawcy urządzeń końcowych oraz systemów operacyjnych biorący udział w transmisji; * dostawcy rozwiązań chmurowych (np. Paas, Iaas); * dostawcy sieci dla sieci prywatnych (niepublicznych) dla klientów B2B w ramach Przemysłu 4.0. (np. sieci campus network).   Wszystkie te podmioty (nie tylko tradycyjnie postrzegani przedsiębiorcy telekomunikacyjni) powinny realizować działania w zakresie cyberbezpieczeństwa, w zależności od zakresu świadczonych usług oraz posiadanych możliwości technicznych, operacyjnych. Pominięcie, któregoś z tych podmiotów będzie oznaczało, iż albo część usług komunikacji elektronicznej nie będzie spełniać wymagań w zakresie cyberbezpieczeństwa (np. sieci prywatne różnych sektorów gospodarki, dostawców urządzeń końcowych wraz z oprogramowaniem).  W tym zakresie niezbędne jest zweryfikowanie pojęć stosowanych w projekcie prawa komunikacji elektronicznej dotyczących przedsiębiorców świadczących usługi komunikacji elektronicznej oraz dostarczających sieci komunikacji elektronicznej, ponieważ projekt prawa komunikacji elektronicznej wprowadza tutaj odmienne podejście od tego, co jest w przypisach europejskich.  Przykładowo proponowane przepisy najprawdopodobniej nie będą dotyczyć:   * dostawców urządzeń końcowych oraz oprogramowania, biorących udział w transmisji i świadczeniu usług (np. masowa usługa RCS). Wynika to z przyjętej definicji sieci telekomunikacyjnej (w projekcie PKE), który wyłącza urządzenia końcowe (w domyśle wraz z oprogramowaniem) z pojęcia sieci telekomunikacyjnej. Jest to odmienne podejście od zastosowane EKŁE, gdzie pojęcie sieci łączności elektronicznej nie wyłącza urządzeń końcowych. * dostawców rozwiązań chmurowych (np. usługi Paas, Iaas), pomimo tego, iż biorą udział w transmisji sygnałów. Wynika to z przyjętej definicji usługi komunikacji elektronicznej (w projekcie PKE), wyłącza usługi, które głównie nie zajmują się transmisji sygnałów. Jest to odmienne podejście od zastosowane w EKŁE, gdzie pojęcie usług łączności elektronicznej obejmuje usługi, które częściowo (nie głównie, jak to jest w PKE), zajmują się transmisją sygnałów. * dostawcy sieci dla sieci prywatnych (niepublicznych) dla klientów B2B w ramach Przemysłu 4.0., pomimo tego, iż realizują sieci oraz usługi, które mają bardzo często charakter kluczowy dla bezpieczeństwa określonych branż. Wydaje się, że wynika to z przyjętej definicji przedsiębiorcy komunikacji elektronicznej (w projekcie PKE), która koncentruje się na dostarczaniu publicznych sieci telekomunikacyjnych. Jest to odmienne podejście od zastosowane w EKŁE, gdzie pojęcie dostarczania sieci łączności elektronicznej abstrahuje od charakteru sieci, czy ma ona charakter publiczny, bądź niepubliczny oraz obejmuje urządzenia końcowe, które są zainstalowane w maszynach. | **Uwaga częsciowo uwzględniona**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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 zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3.  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 przekazanym 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.  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**.** |
|  | Business Centre Club | Uwaga Ogólna | W ocenie BCC jednym z podstawowych problemów dla sektora telekomunikacyjnego jest brak przyjaznego otoczenia prawnego, pozwalającego na sprawne i efektywne inwestowanie w infrastrukturę telekomunikacyjną. O istnieniu tych barier Pan Minister ma wiedzę, BCC bowiem dostrzega i docenia podejmowane od ponad 10 lat inicjatywy mające na celu ich likwidację. Tymczasem Nowela nie tylko nakłada na sektor telekomunikacyjny nowe obowiązki w zakresie cyberbezpieczeństwa, ale przede wszystkim projektuje rozwiązania, które na przedsiębiorców branży telekomunikacyjnej będą wywierać ogromy wpływ. Nowela może spowodować dla operatorów telekomunikacyjnych konieczność poniesienia trudnych do oszacowania nakładów inwestycyjnych związanych ze skutkami oceny ryzyka dostawcy sprzętu lub oprogramowania, jak również wydanych poleceń zabezpieczających lub ostrzeżeń. Ocena Skutków Regulacji Noweli zupełnie pomija aspekt finansowy i wpływ proponowanych rozwiązań na budżety poszczególnych podmiotów gospodarczych. Tymczasem, nie ulega wątpliwości, że konieczność wycofania sprzętu lub oprogramowania danego dostawcy musi się wiązać z:   1. zakupieniem nowego sprzętu lub oprogramowania, 2. zutylizowaniem wycofanego sprzętu, 3. zawarciem nowych umów serwisowych i utrzymaniowych, 4. przeorganizowaniem struktury przedsiębiorstwa, w tym nabyciem nowych kompetencji przez osoby odpowiedzialne za obsługę nowego sprzętu lub oprogramowania, 5. przeprojektowaniem sieci celem dostosowania jej do nowego sprzętu i oprogramowania, w tym pozyskaniem nowych zgód w procesie inwestycyjnym,   co stanowić będzie istotne, nieprzewidziane w normalnym trybie działalności nakłady finansowe.  Sieci telekomunikacyjne to skomplikowane, składające się z wielu elementów przedsięwzięcia, które swoim zasięgiem pokrywają terytorium całego kraju. Zatem wycofanie sprzętu lub oprogramowania danego dostawcy będzie oznaczać dokonywanie modyfikacji w zakresie wszystkich tych elementów sieci. W konsekwencji Ocena Skutków Regulacji powinna jednoznacznie wskazywać na wpływ przepisów Noweli na gospodarkę krajową, w skali zarówno mikro, jak i makroekonomicznej.  Odnosząc się do kwestii dotyczących ryzyka i rozwiązań w zakresie cyberbezpieczeństwa, BCC wyraża stanowisko, że kompromisowym rowiązaniem może być wdrożenie neutralnych technologicznie kryteriów oceny , a przedmiotem oceny ryzyka może być sprzęt i oprogramowanie uznane za krytyczne z technicznego punktu widzenia. BCC pragnie zwrócić uwagę, że istnieją rozwiązania w postaci norm technicznych i certyfikacji, umożliwiające obiektywną ocenę bezpieczeństwa sprzętu i oprogramowania. Są to przykładowo ENISA, czyli unijne ramy certyfikacji cyberbezpieczeństwa oraz NESAS, czyli schemat kompleksowego audytu cyberbezpieczeństwa, wypracowany wspólnie przez 3GPP i GSMA.  W przypadku określenia wysokiego ryzyka sprzętu, oprogramowania i usług danego dostawcy, BCC wskazuje również na możliwość zastosowania podejścia geograficznego, czyli eliminacji danego sprzętu, oprogramowania czy usług z określonych obszarów, zdefiniowanych jako wrażliwe bądź krytyczne z punktu widzenia krajowego systemu bezpieczeństwa. Niniejsze podejście może stanowić *salomonowe* rozwiązanie, gwarantując wysoki poziom cyberbezpieczeństwa w wyżej wskazanych strefach, przy równoczesnym zapewnieniu ciągłości działania sieci komórkowych na obszarach nie będących strategicznymi z punktu widzenia krajowego systemu cyberbezpieczeństwa.  W świetle powyższych uwag, zwracamy się z uprzejmą prośbą do Pana Ministra o ponowną, szczegółową analizę rozwiązań proponowanych w Noweli, w kontekście ich proporcjonalności, analizy alternatywnych rozwiązań dostępnych w obszarze cyberbezpieczeństwa oraz skutków wdrożenia przepisów w proponowanym kształcie dla sektora telekomunikacji w Polsce. | **Wyjaśnienie**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3.  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 przekazanym 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. |
|  | Digital Poland | Uwaga Ogólna | ***Opis problemu***  Wedle rozdziału 4a KSC pt. „obowiązki przedsiębiorców komunikacji elektronicznej” integralną częścią krajowego systemu cyberbezpieczeństwa mają zostać „przedsiębiorcy komunikacji elektronicznej”. Art. 2 pkt 41 projektu Prawa Komunikacji Elektronicznej (dalej „PKE”) definiuje zbiór przedsiębiorców komunikacji elektronicznej jako przedsiębiorcy telekomunikacyjni **oraz** **podmioty świadczące usługę komunikacji interpersonalnej niewykorzystującej numerów** (w rozumieniu art. 2 pkt 77 projektu PKE, którego nie ma potrzeby w tym miejscu przytaczać). W zakres drugiego z wymienionych podzbiorów wchodzi właśnie dostarczanie usługi poczty elektronicznej czy czatów internetowych, bowiem tak właśnie rozumie tę usługę motyw 17 zd. 1 EKŁE: „*Usługi łączności interpersonalnej są to usługi, które umożliwiają interpersonalną i interaktywną wymianę informacji, obejmujące takie usługi, jak tradycyjne połączenia głosowe między dwiema osobami, lecz również wszystkie rodzaje poczty elektronicznej, usług przekazywania wiadomości lub czatów grupowych*”.  Podsumowując powyższych wątek definicyjny, wedle projektowanych przepisów **licznymi i bardzo kosztownymi obowiązkami w zakresie cyberbezpieczeństwa państwa winny zostać objęci również m.in dostawcy poczty elektronicznej.**  ***Brak uzasadnienia***  Dla nałożenia takich ciężarów i obowiązków, które w wymiarze ekonomicznym mogą unicestwić ten sektor, nie ma żadnego racjonalnego uzasadnienia, poczynając już od tego, że usługa poczty elektronicznej zasadniczo różni się od usługi telekomunikacyjnej. Owa różnica jest wyraźnie wyeksponowana w motywie 95 EKŁE:  *„Z uwagi na rosnące znaczenie usług łączności interpersonalnej niewykorzystujących numerów należy zapewnić aby podlegały one również odpowiednim wymogom bezpieczeństwa zgodnie z ich specyficznym charakterem i istotną rolą w gospodarce. Dostawcy usług powinni również zapewnić poziom bezpieczeństwa proporcjonalny do istniejącego ryzyka.* ***Ze względu na to, że dostawcy usługi interpersonalnej łączności niewykorzystujące numerów zazwyczaj nie sprawują rzeczywistej kontroli nad transmisją sygnałów w sieciach, stopień ryzyka w przypadku takich usług można uznać za niższy pod pewnymi względami niż w przypadku tradycyjnych usług łączności elektronicznej. Dlatego też, jeżeli tylko jest to uzasadnione aktualną oceną ryzyka dla bezpieczeństwa, środki podejmowane przez dostawców usługi interpersonalnej łączności niewykorzystujące numerów powinny być łagodniejsze*** *(*podkr. własne*)****.*** *Takie samo podejście powinno być stosowane odpowiednio do usług łączności interpersonalnej wykorzystującej numery, jeżeli dostawca nie sprawuje rzeczywistej kontroli nad transmisją sygnału”.*  Wskazany motyw nakazuje zatem różnicowanie sytuacji prawnej podmiotów w zależności od ich faktycznego wpływu na bezpieczeństwo sieci.  Poza sporem pozostaje, że dostawcy poczty elektronicznej nie sprawują faktycznej, realnej kontroli nad transmisją danych – inaczej niż przedsiębiorcy telekomunikacyjni, którzy dysponują infrastrukturą techniczną. Ci ostatni, właśnie dla zapewnienia możliwości nieprzerwanej łączności telekomunikacyjnej, już obecnie posiadają wszelkie środki gwarantujące bezpieczeństwo sieci.  Oczywiste różnice występują także na poziomie elementarnej charakterystyki obu usług. O ile niezagrożona ciągłość świadczeń telekomunikacyjnych leży w żywotnym interesie całego społeczeństwa (przykładowo, konieczne jest zapewnienie możliwości nawiązania kontaktu telefonicznego ze służbami ratowniczymi w dowolnym czasie), o tyle nie można tego samego powiedzieć o znaczeniu kontaktu emailowego. Jakkolwiek ten ostatni ułatwia życie i w znacznym stopniu wyparł choćby tradycyjną pocztę, to potencjalna szkodliwość mikroprzerw w dostawie tej usługi jest nieporównywalnie mniejsza.  Pojawia się także argument ekonomiczny. W przypadku, gdyby nowym obowiązkom mieli podlegać jedynie rodzimi (tj. polscy) dostawcy usług, pojawiłby się kolejny problem swoistej wewnętrznej dyskryminacji konkurencyjnej wobec globalnych dostawców takich usług, których pozycja rynkowa i tak jest już hegemoniczna. Mając to na uwadze oraz dodając zwiększone obciążenie finansowe w prowadzeniu takiej usługi, przyszłość takich serwisów ze strony rodzimych przedsiębiorców stanęłaby pod znakiem zapytania. | **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 przez ustawę wprowadzającą PKE.  Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowym.  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. |
|  | Huawei Polska | Uwaga ogólna | * + 1. Zasada proporcjonalności   W myśl sformułowanej w art. 31 ust. 3 Konstytucji RP zasady proporcjonalności, wynikającej z zasady demokratycznego państwa prawnego, ustawodawca powinien, spośród dostępnych środków wybrać najmniej uciążliwy dla podmiotów nim dotkniętych, bądź zapewnić by środek ten był stosowany wyłącznie w zakresie niezbędnym do osiągnięcia określonego celu. Mechanizm oceny ryzyka dostawcy, który nie bazuje na obiektywnych kryteriach, może zatem naruszać tę zasadę[[1]](#footnote-2). | **Uwaga nieuwzględniona**  Konstytucja pozwala na ograniczenie swobody prowadzenia działalności gospodarczej ze względu na ważny interes publiczny (art. 22 Konstytucji). Projekt jest proporcjonalny i adekwatny do celu, jakim jest zapewnienie bezpieczeństwa narodowego. |
|  | Huawei Polska | Uwaga ogólna | * + 1. Prawo do sądu   Projektowane rozwiązania w zakresie wyboru dostawcy sprzętu i oprogramowania sieci telekomunikacyjnych, w tym 5G pozwalają na arbitralne wykluczenie dostawców z udziału we wdrożeniu sieci telekomunikacyjnych, w tym 5G w oparciu o nieokreślone kryteria, które nie zawierają elementów analizy technicznej. Nie gwarantują również możliwości realnego odwołania od oceny Kolegium. Wobec tego pojawia się istotna wątpliwość, co do zgodności z konstytucyjną zasadą prawa do sądu (art. 45 Konstytucji RP)[[2]](#footnote-3). | **Uwaga częsciowo uwzględniona**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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). |
|  | Huawei Polska | Uwaga ogólna | * + 1. Ograniczenie konstytucyjnej swobody działalności gospodarczej   Zgodnie z art. 22 Konstytucji RP „*ograniczenie wolności działalności gospodarczej jest dopuszczalne tylko w drodze ustawy i tylko ze względu na ważny interes publiczny*”. Ustawodawca powinien każdorazowo wskazać „ważny interes publiczny” uzasadniający wprowadzanie jakiegokolwiek rodzaju ograniczeń. Tymczasem w uzasadnieniu Projektu temu jakże ważnemu zagadnieniu poświęcono zaledwie jedno zdanie, będące raczej stwierdzeniem faktu aniżeli jakąkolwiek analizą: „*Poprzez nałożenie różnych obowiązków na przedsiębiorców będących podmiotami tego systemu ogranicza się konstytucyjną wolność gospodarczą*” (s. 33 uzasadnienia Projektu). W takiej sytuacji należałoby oczekiwać pełnego i wyczerpującego uzasadnienia, dlaczego ochrona cyberbezpieczeństwa uzasadnia tak daleko idące ograniczenia prawa prowadzenia działalności gospodarczej. W szczególności należy oczekiwać, że projektodawca przedstawi argumenty (i) dlaczego i w jakim zakresie, dobru w postaci zapewnienia cyberbezpieczeństwa, mają ustąpić inne dobra, takie jak chociażby swoboda prowadzenia działalności gospodarczej i (ii) czy proponowany środek jest właściwy dla realizacji zamierzonego celu oraz proporcjonalny i nie wykracza poza ograniczenia konieczne do osiągnięcia celu. Tej analizy w uzasadnieniu Projektu brakuje (patrz zasada proporcjonalności wyrażona w art. 31 ust. 3 Konstytucji RP)[[3]](#footnote-4). | **Wyjaśnienie**  Konstytucja pozwala na ograniczenie swobody prowadzenia działalności gospodarczej ze względu na ważny interes publiczny (art. 22 Konstytucji). Projekt jest proporcjonalny i adekwatny do celu, jakim jest zapewnienie bezpieczeństwa narodowego. Zagadnienie zostało szczegółowo omówione w poprawionym uzasadnieniu. |
|  | Huawei Polska | Uwaga ogólna | * + 1. Brak zastosowania przepisów procedury administracyjnej   W projektowanych przepisach nie przewidziano prawa dostawcy do udziału w postępowaniu przed Kolegium. Należy zaznaczyć, iż z Projektu nie wynika w jakim trybie będzie prowadzone postępowanie przed Kolegium. Przede wszystkim brak jest odesłania do procedury administracyjnej, co narusza m.in. zasadę czynnego udziału stron w postępowaniu, w tym zasadę że przed wydaniem decyzji organ administracji obowiązany jest umożliwić stronom wypowiedzenie się co do zebranych dowodów i materiałów (str. 10 k.p.a.), zasadę pogłębiania zaufania uczestników postępowania do władzy publicznej (art. 8 k.p.a.) czy zasadę informowania stron postępowania przez organy administracji publicznej (art. 9 k.p.a.). | **Uwaga częściowo uwzględniona**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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). |
|  | Huawei Polska | Uwaga ogólna | Rozwiązania zawarte w Projekcie, które mogą nakazać operatorom telekomunikacyjnym rezygnację z dostaw wiodącego dostawcy sprzętu do budowy sieci 5G oraz wymianę infrastruktury już istniejącej, mogą skutkować daleko idącymi, negatywnymi skutkami społecznymi (takimi jak likwidacja miejsc pracy, obniżenie dostępności nowoczesnych usług, wzrost wykluczenia cyfrowego) oraz gospodarczymi (obniżenie konkurencyjności polskiej gospodarki, spadek zaufania inwestorów oraz ograniczenie konkurencji). | **Uwaga nieuwzględniona**  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 przekazanym 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. |
|  | Huawei Polska | Uwaga ogólna | Projekt nie wskazuje także potencjalnych konsekwencji finansowych, jakie zaproponowane w nim rozwiązania mogą za sobą pociągnąć. W szczególności wyliczone powinny zostać konsekwencje finansowe w postaci możliwości wzrostu cen usług telekomunikacyjnych dla obywateli oraz kosztów dla operatorów telekomunikacyjnych, albowiem tylko wtedy można będzie dokonać prawidłowej oceny skutków finansowych wprowadzonych ograniczeń. Obywatele i operatorzy telekomunikacyjni powinni wiedzieć jakie będą skutki finansowe i gospodarcze proponowanych regulacji. Tymczasem w uzasadnieniu Projektu na s. 33, w części poświęconej skutkom gospodarczym i finansowym, w ogóle nie ma o tym mowy. Wspomina się tylko o kosztach związanych z powoływaniem nowych struktur administracyjnych z zakresu cyberbezpieczeństwa (s. 49-52 uzasadnienia) i obowiązkach informacyjnych. Sugeruje się w ten sposób, że skutków takich nie będzie, co jest niezgodne z prawdą, albowiem wpływ taki może być liczony nawet w setkach milionów lub nawet miliardach złotych, zwłaszcza w przypadku konieczności usunięcia przez operatorów telekomunikacyjnych infrastruktury pochodzącej od określonego dostawcy. Brak analizy skutków gospodarczych i finansowych dla operatorów telekomunikacyjnych i obywateli stanowić może istotne naruszenie procesu legislacyjnego (§ 28 Regulamin Pracy Rady Ministrów, tj. M.P. z 2016 r. poz. 1006) i może stanowić o naruszeniu zasady demokratycznego państwa prawa (art. 2 Konstytucji RP). | **Uwaga nieuwzględniona**  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 przekazanym 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. |
|  | Huawei Polska | Uwaga ogólna | Istotnym argumentem, który należy podnieść, jest także kwestia niedopełnienia obowiązku notyfikacji Projektu Komisji Europejskiej, który to obowiązek nakłada na projektodawcę *Rozporządzenie Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych*[[4]](#footnote-5). Zgodnie z tym rozporządzeniem, projekty aktów prawnych zawierające przepisy techniczne powinny zostać notyfikowane Komisji Europejskiej, tak by ta mogła zgłosić do nich ewentualne uwagi i zmiany. Projektodawcy błędnie uznali, że Projekt nie zawiera przepisów technicznych i tym samym notyfikacji takiej nie dokonali[[5]](#footnote-6). | **Uwaga uwzględniona** |
|  | Huawei Polska | Uwaga ogólna | EKPC stwierdza, że: „Każda osoba fizyczna i prawna ma prawo do poszanowania swego mienia. Nikt nie może być pozbawiony swojej własności, chyba że w interesie publicznym i na warunkach przewidzianych przez ustawę oraz zgodnie z ogólnymi zasadami prawa międzynarodowego"[[6]](#footnote-7). W przypadku wejścia w życie Projektu, operatorzy telekomunikacyjni zostaną *de facto* wywłaszczeni z posiadanego sprzętu, w takim znaczeniu, iż będą oni zmuszeni do wycofania sprzętu, który wcześniej zakupili, mimo, iż gdyby nie projektowane rozwiązanie, mogliby z tego sprzętu korzystać w dalszym ciągu. | **Uwaga nieuwzględniona**  Projekt jest zgodny z EKPCz. |
|  | Huawei Polska | Uwaga ogólna | Każda ocena ryzyka lub decyzja o wprowadzeniu ograniczeń rynkowych i pozataryfowych barier w handlu na podstawie niejednoznacznych kryteriów (np. kraj pochodzenia dostawców zawarty w projekcie) i nietransparentne procedury administracyjne, są w naszej ocenie sprzeczne z podstawowymi zasadami równego traktowania i niedyskryminacji, które znajdują odzwierciedlenie w art. 18 (zakaz dyskryminacji ze względu na narodowość), art. 34 (zakaz ograniczeń ilościowych w przywozie oraz wszystkich środków o skutku równoważnym), zasada swobodnego przepływu towarów (art. 26, 28-37) czy zakaz ograniczeń swobody przedsiębiorczości (art. 49) TFUE.  Kluczową zasadą praworządności jest to, że prawo musi mieć zastosowanie do wszystkich i być stosowane jednakowo i w sposób konsekwentny. Jest to powtórzone w Karcie Praw Podstawowych Unii Europejskiej (art. 20), w której „każdy jest równy wobec prawa”. Karta (art. 21 ust. 2) zabrania „wszelkiej dyskryminacji ze względu na narodowość”. Trybunał Sprawiedliwości Unii Europejskiej zauważył, że „zakaz dyskryminacji (…) jest tylko konkretnym wyrazem ogólnej zasady równości, która wynika z podstawowych zasad prawa wspólnotowego, w myśl której porównywalne sytuacje nie mogą być traktowane w odmienny sposób, chyba że to rozróżnienie jest uzasadnione względami obiektywnymi”[[7]](#footnote-8). Jest zatem zgodne z zasadą praworządności, że wymogi bezpieczeństwa powinny być powszechnie stosowane do wszystkich dostawców, a nie dotyczyć wybranych dostawców lub dostawców z określonych krajów. | **Wyjaśnienie**  Projekt jest zgodny z prawem europejskim. |
|  | Huawei Polska | Uwaga ogólna | W sprawie C-331/88 Fedesa Trybunał Sprawiedliwości Unii Europejskiej stwierdził, iż ażeby zastosowany środek ograniczający swobodę prowadzenia działalności gospodarczej uznać za proporcjonalny musi on być (1) odpowiedni i niezbędny do osiągnięcia celu jaki przyświeca ustawodawcy (2) jeśli istnieje wybór pomiędzy kilkoma środkami, należy wybrać ten który jest najmniej uciążliwy oraz (3) niedogodności spowodowane przez ten środek nie mogą być nieproporcjonalne w stosunku do zamierzonych celów.  Wykluczanie sprzętu danego dostawcy, w oparciu o kryteria pochodzenia tego dostawcy (a nie obiektywne kryteria techniczne dotyczące określonego sprzętu) jest nadmiernym ograniczeniem swobody i środkiem nadmiernie uciążliwym w stosunku do celu, jakim jest zapewnienie cyberbezpieczeństwa sieci teleinformatycznych. | **Wyjaśnienie**  Projekt jest zgodny z prawem europejskim. |
|  | Huawei Polska | Uwaga ogólna | Dyrektywa Komisji 2002/77/WE z dnia 16 września 2002 r. w sprawie konkurencji na rynkach sieci i usług łączności elektronicznej („Dyrektywa o konkurencji”) zakazuje przyznawania wszelkich specjalnych praw w sektorze łączności elektronicznej. Mechanizm oceny dostawcy w kształcie zaproponowanym w Projekcie, bezpodstawnie przyznawałby prawa specjalne określonym kategoriom dostawców, odmawiając ich innym, co mogłoby stanowić naruszenie art. 2 Dyrektywy o konkurencji[[8]](#footnote-9). | **Wyjaśnienie**  Projekt jest zgodny z prawem europejskim. |
|  | Huawei Polska | Uwaga ogólna | Układ Ogólny w sprawie Taryf Celnych i Handlu (GATT) zawiera klauzulę największego uprzywilejowania. Członek WTO nie może dyskryminować indywidualnych partnerów handlowych, traktując niektóre kraje bardziej przychylnie niż inne. | **Wyjaśnienie**  Porozumienie o Wolnym Handlu GATT w art. XXI pozwala na stosowanie przez strony porozumienia wszelkich działań, jakie uważają one za niezbędne do ochrony swych żywotnych interesów bezpieczeństwa. Projektowane przepisy wpisują się wobec tego w środki opisane w art. XXI GATT. |
|  | Huawei Polska | Uwaga ogólna | Zasada krajowego traktowania GATT zobowiązuje członków WTO do traktowania „podobnych” produktów, usług i usługodawców zagranicznych i krajowych w równym stopniu. Zgodnie z nią, zagraniczne produkty, usługi lub usługodawcy nie mogą podlegać mniej korzystnym regulacjom niż „podobne” produkty, usługi lub usługodawcy krajowi (art. III GATT). Tymczasem, projektodawca koncentruje się na ocenie cech podmiotowych dotyczących dostawców, nie zaś na bezpieczeństwie sprzętu czy oprogramowania, jakie ten dostawca zapewnia. Jedną z istotnych cech branych pod uwagę przy szacowaniu ryzyka danego dostawcy jest kryterium pochodzenia tego dostawcy z danego kraju. Rodzi to ryzyko, że Polska naruszy umowy międzynarodowe, zakazujące dyskryminacji ze względu na pochodzenie[[9]](#footnote-10). | **Wyjaśnienie**  Porozumienie o Wolnym Handlu GATT w art. XXI pozwala na stosowanie przez strony porozumienia wszelkich działań, jakie uważają one za niezbędne do ochrony swych żywotnych interesów bezpieczeństwa. Projektowane przepisy wpisują się wobec tego w środki opisane w art. XXI GATT. |
|  | Huawei Polska | Uwaga ogólna | Przyjęcie prawodawstwa, które pozwoli na wykluczenie z polskiego rynku podmiotów reprezentujących kapitał zagraniczny, narusza zobowiązania Polski na mocy umów dwustronnych z innymi państwami. Na przykład, jeżeli dostawca z państwa trzeciego będzie wykluczony na podstawie niejasnych kryteriów, to może skutkować uznaniem za naruszenie przez Polskę obowiązku równego i sprawiedliwego traktowania na terytorium Polski na mocy porozumień dwustronnych łączących Polskę i Chiny[[10]](#footnote-11). | **Wyjaśnienie**  Projekt jest zgodny z prawem międzynarodowym. |
|  | Huawei Polska | Uwaga ogólna | Postanowienia Projektu, w przypadku ich wejścia w życie mogą doprowadzić do wykluczenia z rynku dostaw sprzętu do budowy sieci telekomunikacyjnych 5G pochodzącego od niektórych dostawców. Środki przewidziane przez Projekt są nieproporcjonalne do celu jaki przyświecał projektodawcom, wprowadzają nadmierne ograniczenia swobody prowadzenia działalności gospodarczej i czynią to w oparciu o kryteria oceny, które mogą być uznane za dyskryminującej, subiektywne i niemierzalne. Dodatkowo, środki takie mogą naruszać szereg innych przepisów obowiązującego prawa (patrz pkt I powyżej). | **Wyjaśnienie**  Przepisy zaproponowane w projekcie są proporcjonalne do celu. |
|  | Huawei Polska | Uwaga ogólna | Wykluczenie z rynku jednego z wiodących dostawców technologii 5G, jak również konieczność ogromnych zmian w ramach sieci komórkowych; wprowadzenie sieci 5G w Polsce może się opóźnić o okres 3-5 lat; | **Uwaga nieuwzględniona**  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 przekazanym 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.  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. |
|  | Huawei Polska | Uwaga ogólna | Z powodu braku konkurencji cena sprzętu bez wiodącego dostawcy rozwiązań 5G wzrośnie o przynajmniej 30%, a koszty usług telekomunikacyjnych mogą wzrosnąć nawet 3-krotnie; | **Uwaga nieuwzględniona**  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 przekazanym 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.  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. |
|  | Huawei Polska | Uwaga ogólna | Według prezentowanych na rynku analiz, koszt wymiany infrastruktury przez operatorów może sięgać 3 mld złotych (podawane też wyższe kwoty)[[11]](#footnote-12). Może to w konsekwencji rodzić odpowiedzialność odszkodowawczą po stronie Skarbu Państwa. | **Uwaga nieuzwględniona, patrz stanowisko do uwagi 53.** |
|  | Huawei Polska | Uwaga ogólna | Istnieje ograniczona liczba dostawców elementów sieci 5G w Polsce i na świecie. W sytuacji, gdy jeden z dostawców zostanie wykluczony, ograniczy to innowacyjność, opóźni wprowadzenie technologii 5G oraz znacząco zmniejszy konkurencję na rynku. W konsekwencji może to spowodować wzrost cen dla konsumentów. | **Uwaga nieuwzględniona**  Projekt nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa jest neutralny  technologicznie, co oznacza, że przepisy prawa dotyczące m.in. procedury oceny ryzyka  dostawców sprzętu lub oprogramowania, w tym samym stopniu dotyczą każdego dostawcy  sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa.  Projekt nie przewiduje automatycznego wykluczenia czy specjalnego traktowania żadnego z  dostawców. Ewentualne decyzje o wycofaniu konkretnego sprzętu lub oprogramowania z  użytkowania w podmiotach krajowego systemu cyberbezpieczeństwa będą poprzedzone  transparentną – prowadzoną zgodnie z przepisami Kodeksu postępowania administracyjnego – procedurą oceny ryzyka zakończoną decyzją administracyjną.  Co istotne, analizy duńskiej firmy konsultingowej Strand Consult wskazują, że ewentualne  wykluczenie niektórych dostawców nie wpłynie znacząco na koszt budowy sieci 5G. Podaje  się przykład zakupu w Stanach Zjednoczonych przez Nokię w 2016 r. firmy Alcatel Lucent.  Mimo tego, że rynek dostawców zmalał z trzech dużych dostawców do dwóch dużych i  jednego mniejszego, paradoksalnie, zamiast podwyżki i monopolizacji, doprowadziło to  zmniejszenia kosztów sprzętu telekomunikacyjnego. Należy również dodać, że każdy  operator telekomunikacyjny ma własną strategię pozyskiwania unikalnego sprzętu  dostosowanego do jego potrzeb. Niektórzy z klientów operatorów telekomunikacyjnych  oczekują usług telekomunikacyjnych opartych o sprzęt pochodzący od zaufanych  dostawców, ponieważ wcześniej zmagali się ze skutkami ataków hakerskich ze strony  państwa pochodzenia jednego z dostawców. Dlatego też, operatorzy starają się dostosować  do potrzeb swoich klientów. |
|  | Huawei Polska | Uwaga ogólna | Argument bezpieczeństwa narodowego i cyberbezpieczeństwa sieci teleinformatycznych nie powinien być nadużywany. Nadal zastosowanie powinny mieć zasady proporcjonalności, obiektywności, przejrzystości i minimalnej ingerencji. | **Uwaga nieuwzględniona**  Państwo musi dbać o swoje bezpieczeństwo narodowe. Projekt spełnia wymogi proporcjonalności opisane w Konstytucji. |
|  | Huawei Polska | Uwaga ogólna | Opóźnienia w rozwoju i implementacji technologii 5G mogą utrudnić osiągnięcie przez Polskę korzyści z tytułu rozwoju tej technologii; korzyści te szacowane są na 10-13 mld euro[[12]](#footnote-13). | **Uwaga nieuwzględniona**  Koszty zagrożeń bezpieczeństwa narodowego mogą być większe niż korzyści z korzystania z niebezpiecznych rozwiązań technologicznych. |
|  | Huawei Polska | Uwaga ogólna | Przyjęcie przepisów zaproponowanych w Projekcie może mieć negatywny wpływ na gotowość podmiotów do składania ofert na spektrum 5G. | **Uwaga nieuzwględniona,** patrz stanowisko do uwagi 53. |
|  | Huawei Polska | Uwaga ogólna | Ograniczenie operatorów w zakresie możliwości wyboru dostawcy opóźni uruchomienie sieci 5G w Polsce od 3 do 5 lat, co może przełożyć się na utratę konkurencyjności polskiej gospodarki. | **Uwaga nieuwzględniona,** patrz stanowisko do uwagi 55. |
|  | Huawei Polska | Uwaga ogólna | Przedsiębiorcy, których swoboda prowadzenia działalności gospodarczej została ograniczona mogą wystąpić z roszczeniami odszkodowawczymi wobec polskiego rządu. | **Uwaga niezuwględniona**  Konstytucja pozwala na ograniczenie swobody prowadzenia działalności gospodarczej ze względu na ważny interes publiczny (art. 22 Konstytucji). Projekt jest proporcjonalny i adekwatny do celu, jakim jest zapewnienie bezpieczeństwa narodowego**.**  Dalej patrz stanowisko do uwagi 53. |
|  | Huawei Polska | Uwaga ogólna | Opóźnienie wdrożenia technologii 5G może wywrzeć negatywny wpływ na prawie 570 tys. nowych miejsc pracy, które mogą zostać utworzone dzięki technologii 5G[[13]](#footnote-14). | **Uwaga niezuwględniona**  Dalej patrz stanowisko do uwagi 53. |
|  | Huawei Polska | Uwaga ogólna | Wyłączenie producenta, zwłaszcza wiodącego w branży ICT, spowoduje opóźnienie postępu w całym ekosystemie (patrz pkt III.2.2 powyżej).  Projekt ustawy będzie miał negatywny wpływ na realizację agendy Przemysł 4.0. | **Uwaga nieuwzględniona,** patrz stanowisko do uwagi 55. |
|  | Huawei Polska | Uwaga ogólna | Normy techniczne i schematy certyfikacji   * + - 1. Projekt ustawy powinien raczej koncentrować się na normach technicznych i normach certyfikacji, które powinny zostać wprowadzone, takich jak Network Equipment Security Assurance Scheme (NESAS)[[14]](#footnote-15) czy system certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych przewidziany w Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r..       2. Proces analizy ryzyka powinien być zgodny z uznanymi międzynarodowymi standardami, również w zakresie wyboru strategii ograniczenia ryzyka. Zgodnie z najlepszymi praktykami, znajdującymi odzwierciedlenie między innymi w normie ISO 31000, unikanie ryzyka (np. przez eliminację dostawcy sprzętu) jest tylko jedną z siedmiu opcji postępowania z ryzykiem, a wybór adekwatnej opcji powinien być przedmiotem ustaleń pomiędzy podmiotem Krajowego Systemu Cyberbezpieczeństwa, a odpowiednim regulatorem rynku lub ministerstwem. | **Uwaga nieuwzględniona,** Toolbox 5G wymaga także oceny ryzyka pod kątem nietechnicznym. |
|  | Business Centre Club | Uwaga ogólna | **Opinia do projektu ustawy z punktu widzenia branż niereprezentujących bezpośrednio sektora ICT, m.in. farmaceutycznej.**  Przedmiotowy projekt ustawy wprowadza istotne zmiany w trzech strategicznych, z punktu widzenia podmiotu prowadzącego działalność gospodarczą, obszarach:  **1. w zakresie obowiązków operatora usługi kluczowej**  - obecne rozwiązanie opierające się na wewnętrznych lub zewnętrznych Zespołach zmienia się na zespół pełniący funkcję operacyjnego centrum bezpieczeństwa w danym podmiocie (tzw. SOC), nakładając przy tym dodatkowe obowiązki (np. zgłoszeniowe, rejestracyjne w zakresie takiego zespołu);  - nałożenie dodatkowych obowiązków na nowe zespoły np. w zakresie wprowadzania nowych zabezpieczeń, przeprowadzania analiz ryzyka  **2. w zakresie uznawania, iż sprzęt lub oprogramowanie mają wysokie ryzyko dla cyberbezpieczeństwa państwa**  - dotyczy m.in. operatora usługi kluczowej,  - ocena bez wyraźnych kryteriów;  - obowiązek wycofania sprzętu lub oprogramowania w ciągu 5 lat od komunikatu;  - zakaz instalacji nowego sprzętu (zakaz wprowadzania do użycia);  - wysoka kara za niedostosowanie się do oceny;  - brak odpowiedzialności odszkodowawczej Skarbu Państwa;  **3. Ostrzeżenia i polecenia zabezpieczające Pełnomocnika Rządu**  - polecenie zabezpieczające ma formę decyzji administracyjnej o rygorze natychmiastowej wykonalności;  - ostrzeżenia nie mają ustalonej formy;  - nakaz określonego zachowania się, w tym zakaz zaprzestania użytkowania określonego sprzętu lub oprogramowania;  - okres obowiązywania to 2 lata (ostrzeżenie może być jednorazowo przedłużone);  - brak odpowiedzialności odszkodowawczej Skarbu Państwa;  - dotyczy:   * operatora usługi kluczowej również * właścicieli oraz posiadaczy samoistnych i zależnych obiektów, instalacji lub urządzeń infrastruktury krytycznej, wymienionych w wykazie, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym * przedsiębiorców o szczególnym znaczeniu gospodarczo-obronnym, o których mowa w art. 3 ustawy z dnia z dnia 23 sierpnia 2001 r. o organizowaniu zadań na rzecz obronności państwa realizowanych przez przedsiębiorców.   Wprowadzenie powyższych rozwiązań doprowadzi do sytuacji, w której dotychczasowa praktyka dbania o bezpieczeństwo ogólne – Państwa, poprzez opracowanie i wdrożenie rozwiązań gwarantujących bezpieczeństwo na poziomie poszczególnych podmiotów zastąpione zostanie systemem nakazowym, w którym to organy Państwa będą decydowały o tym jak zadbać o bezpieczeństwo poszczególnych podmiotów. Takie podejście do systemu bezpieczeństwa elektronicznego jest daleko nieefektywne z punktu widzenia rachunku ekonomicznego a także zarządzania ryzkiem w przedsiębiorstwach. To podmioty stosujące na co dzień rozwiązania w zakresie bezpieczeństwa, dbając o swoje własne bezpieczeństwo poprzez stosowanie najlepszych praktyk i metodologii dostępnych na rynku, są najlepszym gwarantem tego bezpieczeństwa. Dotychczasowe rozwiązania, wypracowane wraz z rozwojem cyberbezpieczeństwa i funkcjonujące już od dłuższego czasu, sprawdzały się w dotychczasowej praktyce i są stosowane powszechnie na całym świecie.  Ponadto podnieść należy, iż koszty ekonomiczne proponowanego rozwiązania mogą być niezwykle wysokie i mogą prowadzić do bezpośredniego zagrożenia egzystencji wielu podmiotów. Szczególnie rozszerzenie zakresu ustawy na podmioty spoza tych uznanych za operatora usługi kluczowej może przynieść katastrofalne skutki. Samodzielne zarządzanie bezpieczeństwem opierające się na wewnętrznej, odzwierciedlającej własną architekturę, analizie i szacowaniu ryzyka spowodowały, iż podmioty zbudowały złożone i powiązane wzajemnymi zależnościami systemy zabezpieczeń. Zabezpieczeń analizowanych pod kątem swej skuteczności i aktualności w sposób ciągły, co jest krytyczne dla reagowania na często pojawiające się nowe zagrożenia. Systemy te, w zaproponowanym rozwiązaniu zawartym w projekcie ustawy, mogą być narażone na ograniczenie swojej funkcjonalności lub w ogóle na likwidację w oparciu o komunikaty bezpieczeństwa ogłoszone przez odpowiednie organy Państwa. Podkreślić przy tym trzeba, że wszelkie koszty związane z zawieszeniem i wymianą stosowanych rozwiązań zostały przerzucone w całości na podmioty, które już raz poniosły wymierne koszty. W tej sytuacji brak odpowiedzialności odszkodowawczej po stronie Państwa może spowodować, iż podmioty gospodarcze nie będą w stanie udźwignąć nałożonych na nie zobowiązań, nawet w perspektywie 5 letniej, jaka została założona na wymianę sprzętu uznanego za niebezpieczny. Do tego dołożyć należy również astronomiczne kary nałożone na operatorów usługi kluczowej za brak realizacji obowiązków określonych w projektowanej ustawie.  Podkreślić również należy, iż brak jest jednoznacznych kryteriów jakimi mają posługiwać się organy administracji publicznej w ocenie dostawców sprzętu i oprogramowania. Nie zostały ustalone również minima czasowe w jakich mogłyby się odbywać oceny poszczególnych dostawców co niesie za sobą ryzyko dodatkowego zaskakiwania przedsiębiorców i brakiem możliwości faktycznej reakcji w sytuacji gdy budżet na zapewnienie dostępu do określonego sprzętu został wyczerpany, a dany dostawca z dnia na dzień został uznany za niebezpiecznego. Brak jest również odniesienia, w jakich systemach dane rozwiązanie jest niebezpieczne, co powoduje konieczność wymiany całości sprzętu lub oprogramowania bez względu na to czy w danym podmiocie faktycznie mogą one prowadzić do naruszenia zasad bezpieczeństwa. Mając na uwadze przedstawioną argumentację należy stwierdzić, iż obiektywny i oparty o przejrzystą metodologie proces oceny ryzyka cybernetycznego dostępnych technologii lub produktów miałby dużo większą korzystną wartość dla poziomu bezpieczeństwa i kondycji gospodarczej podmiotów niż nakazowo/zakazowy mechanizm dyskwalifikowania określonych producentów.  Kolejnym argumentem przemawiającym za odstąpieniem od proponowanych rozwiązań jest fakt, iż większość producentów sprzętu elektronicznego korzysta z poddostawców usytuowanych w państwach azjatyckich, które z automatu spełniają przynajmniej jedno kryterium uznania ich za niebezpieczne (ochrona danych osobowych, ale również prawa człowieka). W tej sytuacji bardzo groźnym może być sytuacja, w której przy braku możliwości zakupu sprzętu uznawanego za bezpieczny, podmioty gospodarcze nie będą w stanie sprostać wymaganiom stawianym przez Organy administracji publicznej i tym samym mogą stać przed dylematem: kończyć swoją działalność czy ryzykować nałożenie absurdalnie wysokich kar. Projekt ustawy nie odpowiada na pytanie co w takiej sytuacji powinien dany podmiot uczynić.  Przedstawiając powyższe uwagi obawiamy się sytuacji, w której wskazanie któregoś z wiodących producentów urządzeń elektronicznych, sparaliżuje dostęp do produktów tego producenta a też pośrednio do innych bazujących na jego podzespołach. Może mieć to szczególny znaczenie dla przemysłu farmaceutycznego, gdzie wyśrubowane wymagania ze strony poszczególnych organów, w tym w szczególności na etapie wytwarzania leków – przez Głównego Inspektora Farmaceutycznego, dodatkowo zawężają już dość wąską niszę producentów automatyki i elektroniki przemysłowej, których urządzenia i podzespoły mogłyby stanowić bazę np. dla linii produkcyjnych. Finalnie może skończyć się to zablokowaniem możliwości technicznych produkowania leków, zachwiania dostępności do tanich i sprawdzonych leków dostępnych na rynku od lat, a w konsekwencji do paraliżu polityki lekowej państwa i gwałtownym wzroście wydatków płatnika publicznego na droższe leki pochodzące z importu.  Mając na uwadze powyższe okoliczności uzasadnionym wydaje się odstąpienie od dalszego procedowania przedmiotowego projektu ustawy. | **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.  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3.  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 przekazanym 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.  Przepisy art. 67a -67c zostały 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. Zatem także minister właściwy ds. informatyzacji będzie podejmował decyzje o ewentualnych karach także w formie decyzji administracyjnej. Przepis art. 73 został uzupełniony o wysokość kary za nie zastosowanie się do polecenia zabezpieczającego.  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. |
|  | Excogitate | Uwaga ogólna | Ustawa w oczywisty sposób narusza zasady niedyskryminacji i uczciwej konkurencji przedsiębiorstw oraz podważa wielostronne oraz dwustronne umowy handlowe i inwestycyjne podpisane przez Polskę z innymi krajami. Projekt ustawy oznacza, że rynek biznesowy będzie podlegał wpływom politycznym, co nie sprzyja wolnej konkurencji. Będzie to miało istotny negatywny wpływ na otoczenie biznesowe i całą branżę ICT w Polsce.  Przedstawiamy następujące szczegółowe uwagi:   1. **Nadmierna ochrona handlu tworzy bariery handlowe i tarcia.**   Jednostronny protekcjonizm handlowy wpłynie negatywnie na rozwój gospodarczy Polski. WTO stopniowo ustanowiła międzynarodowy porządek, którego rdzeniem jest ONZ, oraz wielostronny system handlowy, którego rdzeniem jest WTO. Naruszenie zasad międzynarodowego systemu handlowego, budowanego przez dziesięciolecia, utrudniłoby utrzymanie ładu handlowego i mogłoby wywołać tarcia handlowe między Polską, a innymi krajami.   1. **KSC może skutkować brakiem uczciwej konkurencji.**   Protekcjonizm zagroziłby konkurencyjności polskiej gospodarki cyfrowej. W perspektywie krótkoterminowej, stosowanie protekcjonizmu w celu ograniczenia sprzedaży produktów z innych krajów wydaje się pomagać niekonkurencyjnym branżom i przedsiębiorstwom. W przypadku polskiej branży ICT pozbawi to branżę ICT i przedsiębiorstwa motywacji do większych inwestycji i ulepszania technologii, prowadząc do spadku konkurencyjności produktów. Z drugiej strony branża i przedsiębiorstwa w innych krajach podejmą więcej kroków w celu poprawy konkurencyjności. W rezultacie międzynarodowa konkurencyjność polskiej branży ICT i przedsiębiorstw będzie ulegać dalszemu osłabieniu.   1. **Wbrew podstawowej zasadzie wolnego handlu w gospodarce rynkowej, protekcjonizm niszczy ekosystem branży i zwiększa koszty dostaw.**   Wolność i wzajemność są podstawą i warunkiem wstępnym handlu międzynarodowego. Poparcie dla wolnego handlu i sprzeciw wobec protekcjonizmu to podstawowe wartości i podstawowe zasady WTO. Żaden kraj nie jest w stanie w pełni posiadać wszystkich zasobów, technologii i zdolności wymaganych do nowej ery globalnej modernizacji technologicznej i przemysłowej. Ochrona handlu może jedynie osłabić globalny system wolnego handlu i utrudnić odbudowę światowej gospodarki w czasie po epidemii.   1. **Potencjalny wpływ na dwustronne oraz wielostronne umowy handlowe i inwestycyjne podpisane przez Polskę z innymi krajami.**   Projekt zmiany ustawy KSC podważy wielostronne umowy handlowe podpisane przez Polskę z innymi krajami, np. Porozumienie WTO/GATT. Projekt zmiany ustawy KSC narusza zasadę równych i wzajemnych korzyści oraz klauzulę największego uprzywilejowania (KNU) w WTO, a także zasadę równej ochrony i traktowania KNU obiecaną w dwustronnych umowach handlowych i inwestycyjnych między Polską, a innymi krajami. | **Uwaga nieuwzględniona**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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).  Porozumienie o Wolnym Handlu GATT w art. XXI pozwala na stosowanie przez strony porozumienia wszelkich działań, jakie uważają one za niezbędne do ochrony swych żywotnych interesów bezpieczeństwa. Projektowane przepisy wpisują się wobec tego w środki opisane w art. XXI GATT. |
|  | Excogitate | Uwaga ogólna | Jako podmiot odpowiedzialności społecznej, mamy za zadanie aktywnie rozpowszechniać racjonalne rozwiązania. Mając na uwadze utrzymanie dobrego kontaktu środowiska biznesowego z rządem wnosimy o rozważenie następujących uwag do projektu zmiany ustawy KSC:   1. Ministerstwo Cyfryzacji powinno zorganizować otwartą debatę i zaprosić odpowiednie ministerstwa, izby gospodarcze, operatorów i inne zainteresowane strony do pochylenia się i pełnego omówienia kwestii poruszonych w projekcie. 2. Rząd powinien w pełni ocenić wpływ projektu, w tym koszty i straty, na konkurencję handlową, legalność, społeczno-gospodarcze i międzynarodowe stosunki handlowe oraz klimat inwestycyjny w Polsce. 3. Zasadniczo, zablokowanie niektórych dostawców nie może rozwiązać problemów związanych z bezpieczeństwem cybernetycznym. Wnosimy o przyjęcie spójnej strategii w ramach UE, w celu zarządzania za pomocą jasnych specyfikacji technicznych i zharmonizowanych norm, zamiast wykluczania dostawców z określonych krajów. Postulujemy odwołanie się do modelu niemieckiego i równe traktowanie wszystkich dostawców, nie tylko z powodów nietechnicznych.   Z punktu widzenia racjonalności ekonomicznej, rząd musi promować dwustronny wolny handel i zmniejszać bariery w swobodnym przepływie towarów i usług. Rząd powinien ogłosić przepisy ustawowe i wykonawcze oraz środki, które sformułował i wdrożył, a także ich zmiany, jak również powinien informować o nich Światową Organizację Handlu. | **Wyjaśnienie**  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 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 prowadzone 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 Cyfryzacji a obecnie KPRM umożliwiło zajęcie stanowiska do projektu ustawy w ramach konsultacji publicznych. |
|  | Excogitate | Uwaga ogólna | Ustanowienie wspólnego unijnego mechanizmu certyfikacji krytycznego sprzętu i oprogramowania. Wymaganie od dostawców oświadczenia o wiarygodności. Ustalenie wymagań technicznych lub organizacyjnych dla dostawców sieci telekomunikacyjnej i systemu teleinformatycznego. Nawiązanie do modelu niemieckiego.  **Uzasadnienie:**  1) Ustalenie obiektywnych i jasnych kryteriów, upewnienie się, że wyniki zastosowanych kryteriów oceny są prawidłowe.  2) Skuteczniejszym będzie zmotywowanie dostawców do samokontroli i złożenia oświadczenia o wiarygodności.  3) Nietechnologiczne kryteria są bardzo często nieokreślone i wykorzystują niejasne pojęcia, które są bardzo trudne do zweryfikowania i oceny. | **Wyjaśnienie**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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. |
|  | Fundacja Bezpieczna Cyberprzestrzeń | Uwaga ogólna | Fundacja Bezpieczna Cyberprzestrzeń od początku przygląda się pracą nad nowelizacją ustawy. Z uwagą analizowaliśmy wszystkie doniesienia na temat możliwych zmian. Jako Fundacja stoimy na stanowisku, że nowelizacja przepisów ustawy jest potrzebna i oczekiwana przez podmioty krajowego systemu cyberbezpieczeństwa. Uważamy jednak, że nie wszystkie proponowane przepisy i rozwiązania zostały należycie ujęte w w/w projekcie, dlatego pozwoliliśmy sobie przedstawić nasze uwagi do zaproponowanego projektu. | **Wyjaśnienie**  Dziękujemy za uwagi. |
|  | Fundacja Bezpieczna Cyberprzestrzeń | Uwaga ogólna | Konieczne jest dodanie vacatio legis dla przepisów art. 14 – co najmniej 6 miesięcy. | **Uwaga nieuwzględniona**  Zmiana przepisu jest podyktowana zmianą podejścia na *risk based approach*. Jest to zmniejszenie obciążeń regulacyjnych w stosunku do aktualnie obowiązującego tekstu ustawy. |
|  | Fundacja Bezpieczna Cyberprzestrzeń | Uwaga ogólna | Ustawa powinna zapewniać środki budżetowe na realizacje proponowanych zmian, a nie tylko możliwość ubiegania się o nie. | **Uwaga nieuwzględniona**  Środki budżetowe zapewnia ustawa budżetowa. |
|  | KIGEIT | Uwaga ogólna | Zgodnie z dyrektywą 2016/1148 (art. 1 ust. 3), wymogi dotyczące bezpieczeństwa i zgłaszania incydentów nie mają zastosowania do przedsiębiorstw telekomunikacyjnych. Podlegają one bowiem 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, ani do dostawców usług zaufania, którzy podlegają wymogom art. 19 rozporządzenia (UE) nr 910/2014. Jednocześnie dyrektywa 2002/21/WE została zastąpiona przez Europejski Kodeks Łączności Elektronicznej („EKŁE”), który zawiera odpowiednie regulacje sektorowe dotyczące integralności i bezpieczeństwa sieci i usług komunikacji elektronicznej (implementowane w projekcie PKE).  W związku z powyższym uważamy, iż możliwe jest przy uwzględnieniu skonsultowanych postanowień PKE oraz przyjętego rozporządzenia z dnia 22 czerwca 2020 r. z art. 175d p.t., zaproponować, aby wraz z wejściem w życie PKE przyjąć rozporządzenie z art. 39 ust. 4 PKE, które modyfikowałoby obecne rozporządzenie z art. 175d p.t. i wprowadzało model ochrony infrastruktury powiązany z nadzorem Prezesa UKE w porozumieniu z CRSIT Telko, a także certyfikacją składników infrastruktury, które uznane zostałyby za krytyczne. | **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. |
|  | KIGEIT | Uwaga ogólna | **Zasada dwuinstancyjności postępowania i prawo do sądu**  Izba jest zaniepokojona przewidzianym w projekcie przyznaniem Pełnomocnikowi oraz Kolegium kompetencji do wydawania rozstrzygnięć w sprawach indywidualnych bez zachowania należytych procedur przewidzianych w prawie administracyjnym oraz z pominięciem podstawowych uprawnień stron oraz gwarancji ochrony ich interesów, na czele z naruszeniem konstytucyjnej zasady dwuinstancyjności postępowania administracyjnego (art. 78 Konstytucji RP) oraz prawa do jawnego rozpatrzenia sprawy przez właściwy, niezależny, bezstronny i niezawisły sąd (art. 45 Konstytucji RP).  Choć w ustawie zostało wprost określone, że Kolegium jest organem jedynie opiniodawczo-doradczym (art. 64 KSC), a Pełnomocnik – podmiotem koordynującym działania i realizującym politykę rządu (art. 60 KSC), jednak w Projekcie przyznane im zostały kompetencje do wydawania decyzji administracyjnych. W przypadku polecenia zabezpieczającego zostało to wyraźnie wskazane (projektowany art. 67c ust. 1), natomiast w przypadku ostrzeżenia i oceny ryzyka wynika z *meritum* projektowanych przepisów. Nie powinno więc ulegać wątpliwości, że wydawanie przez Pełnomocnika i Kolegium decyzji administracyjnych będzie następować w drodze ogólnego postępowania administracyjnego (w trybie przepisów Kodeksu postępowania administracyjnego) oraz że powinny od nich przysługiwać środki odwoławcze – zarówno w ramach kontroli instancyjnej, jak i na drodze sądowej. Uważniej powinny również zostać uregulowane kwestie proceduralne, jeśli wymagają szczególnej regulacji. Nie powinny być wprowadzane mechanizmy, które nie tyle przewidują dopuszczalne zmiany proceduralne wobec regulacji KPA, co pozostają w sprzeczności z przewidzianymi założeniami systemowymi, jak np. zatwierdzanie przez dany organ decyzji wydawanej przez inny podmiot.  Luki i wady procedur przewidzianych w Projekcie są tak znaczące, że w praktyce unicestwiają cele, jakim ma służyć ustawa. Zachowanie projektowanych przepisów w obecnym brzmieniu spowoduje bowiem, że wadliwe decyzje nie będą mogły w państwie prawa stanowić podstawy do nałożenia kar, o których mowa w projektowanych art. 73 ust. 1 pkt 14 i ust. 2, a jedynie do odpowiedzialności Skarbu Państwa za szkodę wyrządzoną ich wydaniem. Trudno w tym przypadku oczekiwać efektywności projektowanych środków. | **Uwaga uwzględniona**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | KIGEIT | Uwaga ogólna | **Naruszenie przepisów WTO**   1. Układ Ogólny w sprawie Taryf Celnych i Handlu (GATT) zawiera klauzulę o najbardziej uprzywilejowanej pozycji. Członek WTO nie może dyskryminować indywidualnych partnerów handlowych, traktując niektóre kraje bardziej przychylnie niż inne. 2. Zasada krajowego traktowania GATT zobowiązuje członków WTO do traktowania "podobnych" produktów zagranicznych i krajowych, usług i usługodawców w równym stopniu. W przypadku stosowania krajowego obowiązku podejścia, produkty zagraniczne, usługi lub zagraniczni usługodawcy nie mogą podlegać mniej korzystnym regulacjom niż „podobny” produkt krajowy, usługodawca lub usługodawca krajowy (art. III GATT). 3. Naszym zdaniem ustawodawca koncentruje się na ocenie cech dotyczących dostawców, a nie na bezpieczeństwie sprzętu czy oprogramowania, jakie zapewnia. Jedną z istotnych cech ocenianych w profilu dostawcy jest kryterium pochodzenia dostawcy z danego kraju. Rodzi to zagrożenie, że Polska naruszy umowy międzynarodowe zakazujące dyskryminacji ze względu na pochodzenie. | **Uwaga nieuwzględniona**  Porozumienie o Wolnym Handlu GATT w art. XXI pozwala na stosowanie przez strony porozumienia wszelkich działań, jakie uważają one za niezbędne do ochrony swych żywotnych interesów bezpieczeństwa. Projektowane przepisy wpisują się wobec tego w środki opisane w art. XXI GATT. |
|  | KIGEIT | Uwaga ogólna | **Zobowiązania dwustronne w ramach umów międzynarodowych**  Przyjęcie prawodawstwa, które pozwoli na wykluczenie z polskiego rynku podmiotów reprezentujących kapitał zagraniczny narusza zobowiązania podmiotów na mocy umów dwustronnych z innymi państwami. Na przykład, jeżeli dostawca z państwa trzeciego będzie wykluczony na podstawie niejasnych kryteriów, to może to zostać uznane za naruszenie przez Polskę obowiązku równego i sprawiedliwego traktowania na terytorium Polski na mocy Traktatu o Dwustronnej Inwestycji. | **Uwaga nieuwzględniona**  Projekt jest zgodny z dwustronnymi umowami międzynarodowymi, w których stroną jest Polska. |
|  | KIGEIT | Uwaga ogólna | **Uwagi techniczne dotyczące ryzyka i rozwiązań bezpieczeństwa**   1. **Kryteria powinny być neutralne technologicznie, a nie uwzględniać względy polityczne:** 2. Przedmiotem oceny ryzyka powinien być sprzęt i oprogramowanie uznane za krytyczne (takie jak sieć bazowa), zaś charakterystyka dostawcy powinna zostać poddana ocenie pod kątem bezpieczeństwa procesu produkcji i zapewnienia dostaw. 3. Kryteria powinny mieć charakter techniczny, być obiektywne, rozsądne i proporcjonalne oraz zawierać odniesienie do oceny ryzyka zawartej w Toolbox 5G i specyfikacjach technicznych. 4. Projekt ustawy musi być zgodny zarówno z wymogami prawnymi dotyczącymi dobrych praktyk legislacyjnych, jak i z obowiązującymi przepisami, takimi jak prawo Unii Europejskiej, międzynarodowe prawo inwestycyjne, prawami człowieka i Konstytucją RP. 5. **Normy techniczne i normy certyfikacji** 6. Projekt ustawy powinien raczej koncentrować się na normach technicznych i normach certyfikacji, które powinny zostać wprowadzone, takich jak NESAS, system certyfikacji ENISA. 7. **NESAS:** Określany wspólnie przez 3GPP i GSMA. Jest to dobrowolny program stosowany przez sektor telefonii komórkowej, zapewniający podstawowy i kompleksowy audyt bezpieczeństwa dowodzi, że sprzęt sieciowy spełnia wymogi bezpieczeństwa, a sprzedawcy sprzętu sieciowego – standardy bezpieczeństwa w procesie rozwoju produktów i cyklu życia. GSMA posiada radę akredytacyjną, która jest odpowiedzialna za monitorowanie i opracowywanie planów oraz udzielanie akredytacji. 8. **ENISA**: Unijne ramy certyfikacji bezpieczeństwa cybernetycznego: wspólne ramy dla obowiązujących w całej UE systemów certyfikatów bezpieczeństwa cybernetycznego. Unijne ramy certyfikacji bezpieczeństwa cybernetycznego mają na celu przyjęcie wspólnego podejścia i ustanowienie europejskich ram certyfikacji bezpieczeństwa cybernetycznego, które określają główne wymogi dla europejskich systemów bezpieczeństwa cybernetycznego i europejskich certyfikatów zgodności produktów ICT, usługi ICT lub procesy ICT, które mają być uznane i stosowane we wszystkich państwach członkowskich. 9. **Stymulacja budowy krajowego potencjału technologicznego w zakresie cyberbezpieczeństwa**   Projektowane zmiany w ustawie kreują ciała decyzyjne i podmioty opiniotwórcze, których obszar kompetencji ogranicza się wyłącznie do incydentów w obszarze programowania i usług. Pominięto potrzebę prawnego usankcjonowania obowiązku prowadzenia działań zmierzających do zabezpieczenia interesu państwa polskiego na poziomie **rozwiązań sprzętowych.** Kwestia zapewnienia bezpieczeństwa sprzętowego od lat jest podnoszona na poziomie zarówno krajowym jak i europejskim. Na poziomie międzynarodowym działają różne organizacje skupione wokół zagadnienia cyberbezpieczeństwa. Na poziomie europejskim jest to m.in. European Union Agency for Cybersecurity (ENISA), której członkiem jest również Polska. Publicznie dostępne informacje dotyczące polskiej strategii cyberbezpieczeństwa obejmują wyłącznie organizacyjne i softwareowo-systemowe aspekty (cyber)bezpieczeństwa, deklaracje powoływania ciał, gremiów i zespołów analizujących incydenty bezpieczeństwa realizowane, zabezpieczane i neutralizowane na poziomie usług, z podziałem na incydenty:   * wpływające na działalność operatorów usług kluczowych (incydenty poważne), * dostawców usług Cyfrowych (incydenty istotne), * incydenty w podmiotach publicznych.   Incydenty te zgodnie z zapisami ustawy są raportowane do jednego z krajowych zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT), zaś zgodnie z zapisami projektu zmian w ustawie przebudowany ma zostać model współpracy w ramach krajowego systemu cyberbezpieczeństwa | **Uwaga częściowo uwzględniona**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | KIGEIT | Uwaga ogólna | **ZASTRZEŻENIA DO USTAWY**   1. Jedyne miejsce, w którym ustawodawca zbliża się do zagadnień **na poziomie sprzętu** związanych z (cyber)bezpieczeństwem urządzeń przewidzianych do użytku jest ograniczone do warunkowej wzmianki (cyt.): „*Dostawcy* ***sprzętu*** *lub oprogramowania będą mogli zostać poddani* ***procedurze sprawdzającej***”.    1. Nie jest w żaden sposób określony merytoryczny zakres wspomnianej wyżej **procedury sprawdzającej**.    2. Z załączonych w projekcie zmian szacunków pracochłonności wynika, że pod uwagę brana jest niezwłoczna akceptacja gotowych rozwiązań przewidzianych do kwalifikacji i dopuszczenia, poprzedzona jedynie pobieżną analizą stanu faktycznego prowadzącą do ewentualnego wykrycia problemów z oprogramowaniem.    3. Dotyczy to również rozwiązań przewidzianych dla infrastruktury krytycznej (brak ustawowego rozróżnienia) dla bezpieczeństwa państwa.   Dla uzmysłowienia poziomu złożoności zagadnienia wystarczy wziąć pod uwagę, że współczesne rozwiązania układowe (sprzętowe zaszyte w układach scalonych) zawierają nierzadko wiele miliardów elementów składowych ukrytych w monolitycznych strukturach krzemowych, których weryfikacja o ile w ogóle technicznie możliwa – wymaga wielomiesięcznej pracy całych zespołów fachowców a także dostępu do technologii i projektów, które w Polsce w chwili obecnej nie występują.  Lektura skojarzonych z ustawą dokumentów jak „Strategia cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022”, a także planowane działania z zakresu cyberbezpieczeństwa w latach 2021-2027 w ramach programu operacyjnego Polska Cyfrowa 2.0, choć adresują wzmiankowaną w nich **potrzebę** **zwiększenia polskiego potencjału R&D w obszarze cyberbezpieczeństwa** towciąż brak jest jakichkolwiek konkretnych zapisów zmierzających do kreowania takowego potencjału w kraju zarówno w obszarze dostępnej w kraju infrastruktury technologicznej jak i sprzętu polskiego pochodzenia. | **Wyjaśnienie**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | KIGEIT | Uwaga ogólna | **SUGESTIE / REKOMENDACJE**   1. Rzeczywisty poziom cyberbezpieczeństwa z **uwzględnieniem sprzętowych** **aspektów cyberbezpieczeństwa** powinien być kluczowym czynnikiem decyzyjnym warunkującym konkretny zakup/inwestycję/prace R&D. 2. Obowiązek oceny poziomu cyberbezpieczeństwa (dalej ***CyberSecEval***) na poziomie sprzętowym **powinien być ustawowo zapisanym elementem decyzyjnym** towarzyszącym działaniom wpływającym na poziom cyberbezpieczeństwa w Polsce. 3. Niezbędne jest ustawowe **określenie grupy urządzeń**, usług, procesów itd. (***Obszar Zastosowania***) poddawanych **CyberSecEval** „obowiązkowo / opcjonalnie / nie poddawanych” badaniu i / lub ocenie, z uwzględnieniem poziomu szczegółowości prowadzonych działań badawczych i / lub ocennych. Należy ustawowo **określić** **warunki definiujące zakres (kwalifikacja poziomu) i sposób przeprowadzenia działań badawczych/ocennych** **CyberSecEval** w odniesieniu do zastosowanych rozwiązań sprzętowych. 4. Obowiązek prowadzenia kompleksowych działań badawczych **CyberSecEval** zakończonych raportem dotyczącym poziomu ryzyka / bezpieczeństwa, powinien być poprzedzony kwalifikacją poziomu analizy, zależną od prawdopodobieństwa wystąpienia w układzie tzw. hardware trojans oraz potencjalnej szkodliwości ich aktywności w danym zastosowaniu układu. Stąd, najbardziej rygorystyczne i szczegółowe analizy powinny dotyczyć zastosowań krytycznych dla bezpieczeństwa państwa urządzeń. W szczególności badaniu / ocenie danego rozwiązania powinny podlegać krytyczne dla bezpieczeństwa rozwiązania komponenty, w szczególności ich struktura i zastosowane rozwiązania. Hardware Trojans - czyli intencjonalne modyfikacje sprzętowe wprowadzane na etapie projektu lub produkcji podzespołów (mikroprocesory, pamięci, elementy wykonawcze) fragmentów, modułów lub całych rozwiązań umożliwiają przejęcie kontroli nad sprzętem i pozostają fizycznie niewykrywalne większości behawioralnych analiz bezpieczeństwa. Umożliwiają kontekstowe otwarcie dostępu do systemu prowadzące do kompromitacji zabezpieczeń lub pozyskania kluczy kryptograficznych przez jednostki do tego nieupoważnione. 5. Krytycznym zagadnieniem prawnym jest **stworzenie wymogu formalnego** wobec podmiotów krajowych stymulującego do wyjścia poza obecnie dominujący (o ile nie jedynie obowiązujący) model businessowy krajowych podmiotów w branży bazujący na zastosowaniu gotowych komponentów nieznanego pochodzenia w tzw. „polskich produktach” – w tym w produktach warunkujących bezpieczeństwo na poziomie jednostki i społeczeństwa. Z nielicznymi wyjątkami, gdy w zaawansowanych technologiach mikroelektronicznych w kraju wytwarzane są pojedyncze komponenty urządzeń (jak np. specjalizowane detektory promieniowania), opracowanie gotowych urządzeń rynkowych zasadza się na imporcie kluczowych, o ile nie wszystkich (poza PCB i obudową) komponentów systemu od producentów europejskich lub z dowolnego miejsca na świecie (dominuje daleki wschód). 6. Definicja „**incydentu**” powinna zostać rozszerzona o **możliwość** wykorzystania gotowych urządzeń lub podzespołów zawierających świadomie wcześniej zaimplementowane, lecz niewykryte luki w zabezpieczeniach lub nigdy nieujawnione funkcjonalności. Sama możliwość zastosowania urządzeń z ukrytą opcją ukrytego podsłuchu, podglądu w krytycznych urzędach lub miejscach, urządzeń z ukrytą funkcją zdalnej dezaktywacji lub uruchomienia dodatkowych funkcjonalności zakłócających działanie innych urządzeń lub maskowanej transmisji kluczy kryptograficznych (i bardzo wiele innych scenariuszy) samo w sobie **stanowi Incydent** (bezpieczeństwa) **obecnie nieuwzględniony** przez Ustawodawcę. 7. Powinien zostać utworzony dodatkowy CSIRT skupiony wokół analiz:  * prawdopodobieństwa wystąpienia intencjonalnych modyfikacji sprzętowych (Hardware Trojans) wprowadzanych do układów i podzespołów na etapie projektu lub ich produkcji, * szkodliwości aktywacji i działania Hardware Trojans zależnie od konkretnych zastosowania konkretnego podzespołu, * poziomu istotności zagrożenia oraz jego kwalifikacji CyberSecEval na poziomie sprzętu - (gadżety / AGD / mobilność / komunikacja / dane / zdrowie / infrastruktura krytyczna / zastosowania militarne.  1. Prawne usankcjonowanie:    1. wymogu pozyskiwania krajowych podzespołów, które w obecnej chwili nie istnieją i nie są produkowane w kraju z uwagi na zniszczenie krajowego przemysłu mikroelektronicznego w okresie transformacji ustrojowej.    2. uruchomienia procesu rewitalizacji krajowego przemysłu mikroelektronicznego zmierzającej do zbudowania w Polsce zaplecza technologicznego posiadającego potencjał produkcyjny krajowych podzespołów mikroelektronicznych (układy scalone), które w obecnej chwili nie istnieją i nie są produkowane w kraju (nieliczne przypadki krajowej myśli technicznej są produkowane na liniach technologicznych poza granicami Polski). | **Wyjaśnienie**  Podmioty krajowego systemu cyberbezpieczeństwa (przede wszystkim operatorzy usług kluczowych) muszą prowadzić systematyczną analizę ryzyka.  Nie można zmienić definicji incydentu, ponieważ wynika ona z Dyrektywy NIS. |
|  | KIGEIT | Uwaga ogólna | **OCZEKIWANE DZIAŁANIA**  Niezależnie od okoliczności, iż czas na odniesienie się do materii projektu mimo wydłużenia go o kolejne 14 dni, jest zbyt krótki i praktycznie uniemożliwia przeprowadzenie analiz potencjalnego wpływu przedmiotowego aktu na funkcjonowanie całej branży elektronicznej, zdecydowaliśmy się przedłożyć powyższe wstępne uwagi oraz propozycje zmian. Jednocześnie zwracamy się z prośbą o przeprowadzenie następujących działań:   1. **POSTULAT ZORGANIZOWANIA KONFERENCJI UZGODNIENIOWEJ ORAZ WCZEŚNIEJSZEGO WYSŁUCHANIA PUBLICZNEGO**   Zgodnie z § 44 Regulamin pracy Rady Ministrów, zwracamy się z uprzejmą prośbą o zorganizowanie przez Ministerstwo konferencji uzgodnieniowej oraz zaproszenie do udziału wszystkich interesariuszy, którzy wnieśli swoje uwagi, gdyż z pewnością przyczyniłaby się ona do właściwego prowadzenia uzgodnień i zaopiniowania projektu ustawy.   1. **POSTULAT RZETELNEJ ANALIZY SKUTKÓW SPOŁECZNYCH, GOSPODARCZYCH I POLITYCZNYCH ORAZ POKAZANIA W OCENIE SKUTKÓW REGULACJI WYNIKAJĄCYCH Z TEGO PEŁNYCH KOSZTÓW REGULACJI**   W zakresie skutków społecznych należy opisać wpływ na likwidację miejsc pracy, obniżenie dostępności nowoczesnych usług, wzrost wykluczenia cyfrowego wynikający z wyższego kosztu usług dla konsumentów i przedsiębiorstw: w szczególności w obszarach pracy zdalnej, zdalnej edukacji, telemedycyny, rozwoju inteligentnych usług samorządowych (smart cities) oraz nowoczesnych rozwiązań w rolnictwie, ochronie środowiska czy energetyce.   1. **PROPONOWANY KIERUNEK ZMIAN**   Rynek usług łączności elektronicznej powinien nadal pozostać kompleksowo regulowany sektorowo, ze względu na jego szczególne cechy. Dlatego uważamy, że docelowym miejscem uregulowania kwestii obowiązków operatorów telekomunikacyjnych w zakresie bezpieczeństwa sieci i usług jest projektowana ustawa Prawo Komunikacji Elektronicznej. Należy więc pozostawić kompetencje Prezesa UKE uregulowane w art. 39-49 projektu PKE. Model przedstawiony w PKE zapewnia bowiem szereg narzędzi pozwalających zapewnić cyberbezpieczeństwo infrastruktury telekomunikacyjnej.  Jednocześnie zgodnie z prośbą otrzymaną w toku konsultacji wewnątrzizbowych, od trzech członków Izby, firmy EXATEL S.A., NASK-PIB, oraz Nokia Solutions and Networks Sp. z o.o., informuję o wyłączeniu poparcia tych firm dla treści powyższego stanowiska | **Wyjaśnienie**  Umożliwiono wypowiedzenie się interesariuszy poprzez konsultacje publiczne.  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. |
|  | Pracodawcy RP | Uwaga ogólna | Opiniowana ustawa procedowana jest równocześnie z projektem ustawy - Prawo komunikacji elektronicznej. Te dwa zasadnicze projekty aktów prawnych stworzą nowe otoczenie prawno-regulacyjne w sektorze telekomunikacyjnym na najbliższe lata. Do obu tych projektów Pracodawcy RP mają zasadnicze uwagi i zastrzeżenia, o czym w przypadku nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa będzie w dalszej części niniejszego stanowiska. Zanim przejdziemy do uwag należy jednak poświęcić miejsce fatalnej sytuacji, jaką jest rekonstrukcja rządu i związana z tym procesem likwidacja Ministerstwa Cyfryzacji - autora i gospodarza zarówno Prawa komunikacji elektronicznej, jak też nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa. W naszej ocenie niedopuszczalne jest, aby podstawy nowego ładu prawnego w kluczowym dla funkcjonowania państwa sektorze, jakim jest telekomunikacja, powstawały w sytuacji, w której odpowiedzialne za to departamenty i urzędnicy mają na głowie zmianę podległości służbowej, być może przeprowadzkę, zmianę szyldu, pieczątek czy stopek w e-mailach.  Przechodząc do oceny projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa, należy stwierdzić, iż wywołuje on liczne i poważne wątpliwości. Począwszy od kwestii zgodności z Konstytucją RP, przez zgodność z prawem międzynarodowym, po zgodność z prawem unijnym. Zarzuty w tych obszarach przedstawiamy poniżej. W dalszej części stanowiska zwracamy też uwagę na zagrożenie dla konkurencji, możliwy wzrost kosztów i pogorszenie jakości świadczonych usług, a także naruszenie zasady zaufania do państwa oraz swobody działalności gospodarczej. Podkreślenia wymaga fakt, iż projektowane przepisy wprowadzają nową procedurę decyzyjną, która w sposób całkowicie uznaniowy - i ostateczny - rozstrzygnie o możliwości korzystania ze sprzętu określonego dostawcy. Procedura ta nie ma nic wspólnego z zasadą demokratycznego państwa prawnego, zasadą transparentności i zaufania państwa do przedsiębiorcy.  Poniżej prezentujemy szczegółowe uwagi oraz propozycje poprawek do opiniowanego projektu ustawy. Liczymy na to, że projektodawca pochyli się nad naszym stanowiskiem. Cyfryzacja pozwoliła nam kontynuować pracę i naukę w okresie pandemii, zapewniła dostęp do ochrony zdrowia, dóbr kultury i rozrywki. Dzięki cyfryzacji urzędy oraz instytucje publiczne mogły funkcjonować, załatwiać sprawy zgłaszane przez obywateli i przedsiębiorców. Cyfryzacja to, w naszej ocenie, jeden z podstawowych priorytetów Rządu RP na najbliższe lata. Aby procesy cyfryzacyjne mogły być kontynuowane, potrzebne są stabilne, przejrzyste i przyjazne dla rozwoju sektora teleinformatycznego przepisy. Jesteśmy gotowi takie przepisy współtworzyć, wspierać decydentów poprzez wskazywanie słabych punktów istniejących oraz projektowanych regulacji, a także wskazywać - w ramach dialogu społecznego - potencjalne najlepsze rozwiązania. Opiniowany projekt jest przykładem regulacji, które tego dialogu bardzo potrzebują. | **Wyjaśnienie**  Przepisy art. 66a-66c zostaly zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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 został 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.  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 przekazanym 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. |
|  | Narodowy Bank Polski | Uwaga ogólna | Na wstępie uprzejmie informujemy, iż co do zasady Narodowy Bank Polski przyjmuje z aprobatą propozycje zmian w projekcie ustawy, w szczególności dotyczące utworzenia podmiotów mających zapewnić dostęp oraz wymianę wiedzy eksperckiej dotyczącej cyberzagrożeń. Niemniej jednak zwracamy uwagę, że w projekcie ustawy pomimo braku bezpośrednich odwołań do Narodowego Banku Polskiego, propozycje niektórych przepisów mogą wydawać się niezgodne z rolą przypisaną NBP  w przepisach Konstytucji RP i ustawy z dnia 29 sierpnia 1997 r. o Narodowym Banku Polskim w zakresie wartości fundamentalnych z punktu widzenia podstaw funkcjonowania banku centralnego w Polsce, w szczególności jego niezależności. Powyższe odnosi się do propozycji przepisów wedle których projektodawca nadał Pełnomocnikowi Rządu ds. Cyberbezpieczeństwa kompetencje do wydawania,  na podstawie projektowanego art. 67a ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, zwanej dalej „ustawą o KSC”, ostrzeżeń i poleceń zabezpieczających w odniesieniu do podmiotów, o których mowa w art. 4 pkt 1–16 ustawy o KSC. Narodowy Bank Polski, jako jeden z podmiotów tworzących krajowy system cyberbezpieczeństwa (vide art. 4 pkt 9 ustawy o KSC) może być zatem adresatem tego rodzaju działań Pełnomocnika. | **Uwaga nieuwzględniona**  Proponowane przepisy nie wpływają na konstytucyjną niezależność Narodowego Banku Polskiego. Nie dotyczą jego zadań konstytucyjnych i ustawowych. |
|  | Narodowy Bank Polski | Uwaga ogólna | Narodowy Bank Polski jest operatorem systemów płatności o kluczowym znaczeniu dla stabilności całego systemu finansowego w Polsce (tj. SORBNET2 i TARGET2-NBP). Potencjalne zakłócenie funkcjonowania tych systemów może nieść za sobą skutki  w postaci zaburzeń transmisji pieniądza w skali całego kraju. Dlatego też, w ocenie NBP, powierzanie Pełnomocnikowi Rządu ds. Cyberbezpieczeństwa kompetencji umożliwiających ingerowanie w systemy IT będące komponentem infrastruktury płatniczej, której operatorem jest bank centralny, nie znajduje uzasadnienia.  Warto w tym miejscu podkreślić, iż w przypadku, w którym projektowane przepisy wykraczają poza wdrożenie właściwej dyrektywy, wymagają zasięgnięcia opinii Europejskiego Banku Centralnego (EBC). W przypadku opiniowanego projektu ustawy, właściwość EBC do wydania opinii wynika z art. 127 ust. 4 oraz art. 282 ust. 5 Traktatu o funkcjonowaniu Unii Europejskiej, jak również z art. 2 ust. 1 tiret trzecie, piąte i szóste decyzji 98/415/WE gdyż projekt ustawy zawiera postanowienia odnoszące się do zadań NBP, tj. banku centralnego współtworzącego Europejski System Banków Centralnych. Zwracamy uwagę, że ewentualne niezastosowanie się polskich władz publicznych do obowiązku zasięgnięcia opinii EBC w trakcie niniejszego procesu legislacyjnego może przyczynić się do stwierdzenia naruszenia przez władze krajowe przepisów wspólnotowych, określających obowiązek konsultacji poszczególnych projektów aktów prawnych z organami wspólnotowymi.  Konkludując powyższe, w związku z koniecznością zagwarantowania niezależności przy realizowaniu przez bank centralny zadań wynikających zarówno  z polskiego porządku prawnego jak i ze zobowiązań międzynarodowych, proponujemy wprowadzenie do opiniowanego projektu ustawy następujących zmian. | **Wyjaśnienie**  Proponowane przepisy nie wpływają na konstytucyjną niezależność Narodowego Banku Polskiego. Nie dotyczą jego zadań konstytucyjnych i ustawowych. |
|  | Naczelna Organizacja Techniczna. Federacja Stowarzyszeń Naukowo-Technicznych | Uwaga ogólna | Należy zwrócić uwagę, że kryteria na podstawie, których przeprowadzana jest ocena ryzyka dostawcy sprzętu lub oprogramowania są nieprecyzyjne – tym samym pozostawiają dużo swobody do oceny Kolegium. W związku z powyższym rekomendowane jest sprecyzowanie kryteriów – opracowanie skali, na podstawie, której jest przeprowadzana analiza ryzyka dostawcy sprzętu lub oprogramowania.  Wskazać należy, że w przypadku określenia ryzyka, jako umiarkowane lub niskie od dokonanej oceny, nie przysługują dostawcy sprzętu lub oprogramowania żadne środki odwoławcze.  Biorąc pod uwagę skutki gospodarcze, ekonomiczne, które poniesienie dostawca sprzętu  lub oprogramowania zasadne jest, aby w ustawie wprowadzić zapis przyznający prawo dostawcy do wniesienia odwołania również w przypadku, gdy Kolegium oceni ryzyko jako umiarkowane lub niskie. Zaznaczyć należy, że w przypadku określenia ryzyka jako umiarkowanego, to podmioty krajowego systemu cyberbezpieczeństwa nie mogą wprowadzić do użytkowania sprzętu, oprogramowania i usług określonych w ocenie danego dostawcy sprzętu lub oprogramowania oraz mogą jedynie kontynuować używanie dotychczas posiadanego sprzętu, usług lub oprogramowania, wykorzystywanych przed opublikowaniem komunikatu o ocenie danego dostawcy sprzętu lub oprogramowania.  W odniesieniu do dostawcy sprzętu lub oprogramowania w stosunku do którego określono ryzyko jako wysokie, rekomendowane jest, aby termin na wniesienie odwołania wydłużyć  do co najmniej 3 miesięcy, 14 -dniowy termin na wniesienie odwołania jest zbyt krótki, biorąc pod uwagę, że wniesienie odwołania oraz jego pełne uzasadnienie może wymagać sporządzenia specjalistycznych opinii, ekspertyz. Podkreślenia wymaga, że Kolegium ma 2 miesiące od otrzymania odwołania na jego rozpatrzenie.  W związku z powyższym wskazane jest aby sporządzona przez Kolegium ocena ryzyka dostawcy sprzętu lub oprogramowania była ogłaszana przez Pełnomocnika w postaci komunikatu w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski” dopiero  po rozpatrzeniu odwołania, jak również by dopiero po rozpatrzeniu odwołania stosowane były środki wskazane w art. 66b i art. 66c. Ponadto, rekomendowane jest również przyznanie dostawcom sprzętu i oprogramowania prawa do złożenia wniosku o zmianę oceny dokonanej przez Kolegium w przypadku wystąpienia nowych okoliczności – w projektowanym przepisie prawo to zostało przyznane wyłącznie członkowi Kolegium.  Wskazać również należy, że skutki publikacji komunikatu przez Pełnomocnika z perspektywy dostawcy oprogramowania lub sprzętu sprowadzają się do zakazu prowadzenia działalności gospodarczej, jak również zawieszenia planowanych projektów, wycofania poczynionych przez dostawcę inwestycji. Z perspektywy podmiotów krajowego systemu cyberbezpieczeństwa, w operatorów usług kluczowych np. Szpitali wycofywanie sprzętu, oprogramowania i usług oraz brak możliwości zakupu sprzętu, oprogramowania i usług danego dostawcy powodować może ogromnie koszty, ponadto może to również naruszać zasady konkurencji. | **Wyjaśnienie**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3.  Zrezygnowano z planów wycofania sprzętu lub oprogramowania. |
|  | Fundacja Bezpieczna Cyberprzestrzeń | Uwaga ogólna do Rozdziału 4 | Zakres proponowanego rozdziału 4a w znacznej mierze pokrywa się z treścią, która występuje w rozdziale 5 nowego Prawa Komunikacji Elektronicznej. Nie jest to zgodne z zasadami techniki prawodawczej (rozporządzenie Prezesa Rady Ministrów w sprawie „Zasad techniki prawodawczej” §4 ust. 1 - Ustawa nie może powtarzać przepisów zamieszczonych w innych ustawach.). | **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. |
|  | Polski Związek Pracodawców Przemysłu Farmaceutycznego | Uwaga ogólna | Przedmiotowy projekt ustawy wprowadza istotne zmiany w trzech strategicznych, z punktu widzenia podmiotu prowadzącego działalność gospodarczą, obszarach:  **1. w zakresie obowiązków operatora usługi kluczowej**  - obecne rozwiązanie opierające się na wewnętrznych lub zewnętrznych Zespołach zmienia się na zespół pełniący funkcję operacyjnego centrum bezpieczeństwa w danym podmiocie (tzw. SOC), nakładając przy tym dodatkowe obowiązki (np. zgłoszeniowe, rejestracyjne w zakresie takiego zespołu);  - nałożenie dodatkowych obowiązków na nowe zespoły np. w zakresie wprowadzania nowych zabezpieczeń, przeprowadzania analiz ryzyka  **2. w zakresie uznawania, iż sprzęt lub oprogramowanie mają wysokie ryzyko dla cyberbezpieczeństwa państwa**  - dotyczy m.in. operatora usługi kluczowej,  - ocena bez wyraźnych kryteriów;  - obowiązek wycofania sprzętu lub oprogramowania w ciągu 5 lat od komunikatu;  - zakaz instalacji nowego sprzętu (zakaz wprowadzania do użycia);  - wysoka kara za niedostosowanie się do oceny;  - brak odpowiedzialności odszkodowawczej Skarbu Państwa;  **3. Ostrzeżenia i polecenia zabezpieczające Pełnomocnika Rządu**  - polecenie zabezpieczające ma formę decyzji administracyjnej o rygorze natychmiastowej wykonalności;  - ostrzeżenia nie mają ustalonej formy;  - nakaz określonego zachowania się, w tym zakaz zaprzestania użytkowania określonego sprzętu lub oprogramowania;  - okres obowiązywania to 2 lata (ostrzeżenie może być jednorazowo przedłużone);  - brak odpowiedzialności odszkodowawczej Skarbu Państwa;  - dotyczy:   * operatora usługi kluczowej również * właścicieli oraz posiadaczy samoistnych i zależnych obiektów, instalacji lub urządzeń infrastruktury krytycznej, wymienionych w wykazie, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym   przedsiębiorców o szczególnym znaczeniu gospodarczo-obronnym, o których mowa w art. 3 ustawy z dnia z dnia 23 sierpnia 2001 r. o organizowaniu zadań na rzecz obronności państwa realizowanych przez przedsiębiorców. | **Wyjaśnienie**  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.  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.  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3.  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. Zatem także minister właściwy ds. informatyzacji będzie podejmował decyzje o ewentualnych karach także w formie decyzji administracyjnej. Przepis art. 73 został uzupełniony o wysokość kary za nie zastosowanie się do polecenia zabezpieczającego.  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 wskazany 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. zespołu CSIRT poziomu krajowego oraz ustalenia podjęte na Zepole 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. |
|  | Polski Związek Pracodawców Przemysłu Farmaceutycznego | Uwaga ogólna | Wprowadzenie powyższych rozwiązań doprowadzi do sytuacji, w której dotychczasowa praktyka dbania o bezpieczeństwo ogólne – Państwa, poprzez opracowanie i wdrożenie rozwiązań gwarantujących bezpieczeństwo na poziomie poszczególnych podmiotów zastąpione zostanie systemem nakazowym, w którym to organy Państwa będą decydowały o tym jak zadbać o bezpieczeństwo poszczególnych podmiotów. Takie podejście do systemu bezpieczeństwa elektronicznego jest daleko nieefektywne z punktu widzenia rachunku ekonomicznego, a także zarządzania ryzkiem w przedsiębiorstwach. To podmioty stosujące na co dzień rozwiązania w zakresie bezpieczeństwa, dbając o swoje własne bezpieczeństwo poprzez stosowanie najlepszych praktyk i metodologii dostępnych na rynku, są najlepszym gwarantem tego bezpieczeństwa. Dotychczasowe rozwiązania, wypracowane wraz z rozwojem cyberbezpieczeństwa i funkcjonujące już od dłuższego czasu, sprawdzały się w dotychczasowej praktyce i są stosowane powszechnie na całym świecie.  Ponadto podnieść należy, iż koszty ekonomiczne proponowanego rozwiązania mogą być niezwykle wysokie i mogą prowadzić do bezpośredniego zagrożenia egzystencji wielu podmiotów. **Szczególnie rozszerzenie zakresu ustawy na podmioty spoza tych uznanych za operatora usługi kluczowej może przynieść katastrofalne skutki.** Samodzielne zarządzanie bezpieczeństwem opierające się na wewnętrznej, odzwierciedlającej własną architekturę, analizie i szacowaniu ryzyka spowodowały, iż podmioty zbudowały złożone i powiązane wzajemnymi zależnościami systemy zabezpieczeń. Zabezpieczeń analizowanych pod kątem swej skuteczności i aktualności w sposób ciągły, co jest krytyczne dla reagowania na często pojawiające się nowe zagrożenia. Systemy te, w zaproponowanym rozwiązaniu zawartym w projekcie ustawy, mogą być narażone na ograniczenie swojej funkcjonalności lub w ogóle na likwidację w oparciu o komunikaty bezpieczeństwa ogłoszone przez odpowiednie organy Państwa. Podkreślić przy tym trzeba, że wszelkie koszty związane z zawieszeniem i wymianą stosowanych rozwiązań zostały przerzucone w całości na podmioty, które już raz poniosły wymierne koszty. W tej sytuacji brak odpowiedzialności odszkodowawczej po stronie Państwa może spowodować, iż podmioty gospodarcze nie będą w stanie udźwignąć nałożonych na nie zobowiązań, nawet w perspektywie 5 letniej, jaka została założona na wymianę sprzętu uznanego za niebezpieczny. Do tego dołożyć należy również astronomiczne kary nałożone na operatorów usługi kluczowej za brak realizacji obowiązków określonych w projektowanej ustawie.  Podkreślić również należy, iż brak jest jednoznacznych kryteriów jakimi mają posługiwać się organy administracji publicznej w ocenie dostawców sprzętu i oprogramowania. Nie zostały ustalone również minima czasowe w jakich mogłyby się odbywać oceny poszczególnych dostawców co niesie za sobą ryzyko dodatkowego zaskakiwania przedsiębiorców i brakiem możliwości faktycznej reakcji w sytuacji gdy budżet na zapewnienie dostępu do określonego sprzętu został wyczerpany, a dany dostawca z dnia na dzień został uznany za niebezpiecznego. Brak jest również odniesienia, w jakich systemach dane rozwiązanie jest niebezpieczne, co powoduje konieczność wymiany całości sprzętu lub oprogramowania bez względu na to czy w danym podmiocie faktycznie mogą one prowadzić do naruszenia zasad bezpieczeństwa. Mając na uwadze przedstawioną argumentację należy stwierdzić, iż obiektywny i oparty o przejrzystą metodologie proces oceny ryzyka cybernetycznego dostępnych technologii lub produktów miałby dużo większą korzystną wartość dla poziomu bezpieczeństwa i kondycji gospodarczej podmiotów niż nakazowo/zakazowy mechanizm dyskwalifikowania określonych producentów.  Kolejnym argumentem przemawiającym za odstąpieniem od proponowanych rozwiązań jest fakt, iż większość producentów sprzętu elektronicznego korzysta z poddostawców usytuowanych w państwach azjatyckich, które z automatu spełniają przynajmniej jedno kryterium uznania ich za niebezpieczne (ochrona danych osobowych, ale również prawa człowieka). W tej sytuacji bardzo groźnym może być sytuacja, w której przy braku możliwości zakupu sprzętu uznawanego za bezpieczny, podmioty gospodarcze nie będą w stanie sprostać wymaganiom stawianym przez Organy administracji publicznej i tym samym mogą stać przed dylematem: kończyć swoją działalność czy ryzykować nałożenie absurdalnie wysokich kar. Projekt ustawy nie odpowiada na pytanie co w takiej sytuacji powinien dany podmiot uczynić.  Przedstawiając powyższe uwagi obawiamy się sytuacji, w której wskazanie któregoś z wiodących producentów urządzeń elektronicznych, sparaliżuje dostęp do produktów tego producenta, a też pośrednio do innych bazujących na jego podzespołach. Może mieć to szczególny znaczenie dla przemysłu farmaceutycznego, gdzie wyśrubowane wymagania ze strony poszczególnych organów, w tym w szczególności na etapie wytwarzania leków – przez Głównego Inspektora Farmaceutycznego, dodatkowo zawężają już dość wąską niszę producentów automatyki i elektroniki przemysłowej, których urządzenia i podzespoły mogłyby stanowić bazę np. dla linii produkcyjnych. Finalnie może skończyć się to zablokowaniem możliwości technicznych produkowania leków, zachwiania dostępności do tanich i sprawdzonych leków dostępnych na rynku od lat, a w konsekwencji do paraliżu polityki lekowej państwa i gwałtownym wzroście wydatków płatnika publicznego na droższe leki pochodzące z importu.  **Mając na uwadze powyższe okoliczności uzasadnionym wydaje się odstąpienie od dalszego procedowania przedmiotowego projektu ustawy.** | **Uwaga nieuwzględniona**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | T-Mobile Polska | Uwaga ogólna | Projekt ustawy proponuje uwzględnić w krajowym systemie cyberbezpieczeństwa podmioty działające na rynku telekomunikacyjnym. Warto wskazać, iż rynek telekomunikacyjny obecnie określany jest jako rynek komunikacji elektronicznej, na którym sieci oraz usługi dostarczają nie tylko tradycyjnie postrzegani przedsiębiorcy telekomunikacyjni ale również inne podmioty funkcjonujące dzisiaj poza rynkiem telekomunikacyjnym. | **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 przez 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. |
|  | T-Mobile Polska | Uwaga Ogólna | Punktem wyjścia jest przyjęcie założenia, iż przyszłe usługi łączności elektronicznej są (lub będą) świadczone w układzie trójkąta charakterystycznego dla modelu funkcjonowania sieci 5G:  cid:image002.png@01D617EA.6916DB20  Dla tak sformułowanego modelu, trójkąta usług łączności elektronicznej, rozszerza się liczba podmiotów/funkcji realizowanych w ramach komunikacji. Usługi łączności elektronicznej to nie tylko połączenie głosowe, szybki dostęp do sieci Internet (Enhanced Mobile Broadband) ale również:   * sieci dedykowane dla komunikacji masowej IoT np. LTE-M, NB-IoT (Massive machine type communications), * sieci o wysokich parametrach jakościowych np. campus network’s (Ultra-reliable and low latency communications).   Dodatkowo, sieci te będą świadczyć usługi w ramach odpowiednich, wydzielonych warstw - tzw. ‘network slicing’, dedykując odpowiednie parametry jakościowe dla określonych rodzajów/grup usług np. usługi bankowe mogą wymagać wydzielonego zasobu sieciowego o określonych parametrach bezpieczeństwa, tworząc rozwiązanie E2E w ramach network slicing.  Każdy podmiot, który bierze udział w realizacji komunikacji/przesyłaniu sygnałów jest podmiotem, który świadczy usługi łączności elektronicznej, czyli:   * „*tradycyjni*” przedsiębiorcy telekomunikacyjni- operatorzy; * dostawcy urządzeń końcowych oraz systemów operacyjnych np. Samsung, IOS biorący udział w transmisji; * dostawcy rozwiązań chmurowych (np. Paas, Iaas); * dostawcy sieci dla sieci prywatnych (niepublicznych) dla klientów B2B w ramach Przemysłu 4.0. (np. sieci campus network).   Wszystkie te podmioty (nie tylko tradycyjnie postrzegani przedsiębiorcy telekomunikacyjni) powinny realizować działania w zakresie cyberbezpieczeństwa, w zależności od zakresu świadczonych usług oraz posiadanych możliwości technicznych, operacyjnych. Pominięcie, któregoś z tych podmiotów będzie oznaczało, iż albo część usług komunikacji elektronicznej nie będzie spełniać wymagań w zakresie cyberbezpieczeństwa.  W tym zakresie niezbędne jest zweryfikowanie pojęć stosowanych w projekcie prawa komunikacji elektronicznej dotyczących przedsiębiorców świadczących usługi komunikacji elektronicznej oraz dostarczających sieci komunikacji elektronicznej.  Przykładowo proponowane przepisy projektu ustawy najprawdopodobniej nie będą dotyczyć:   * dostawców urządzeń końcowych oraz oprogramowania, biorących udział w transmisji i świadczeniu usług (np. masowa usługa RCS Google Message). Wynika to z przyjętej definicji sieci telekomunikacyjnej (w projekcie PKE), który wyłącza urządzenia końcowe (w domyśle wraz z oprogramowaniem) z pojęcia sieci telekomunikacyjnej. Jest to odmienne podejście od zastosowane EKŁE, gdzie pojęcie sieci łączności elektronicznej[[15]](#footnote-16) nie wyłącza urządzeń końcowych. * dostawców rozwiązań chmurowych (np. usługi Paas, Iaas), pomimo tego, iż biorą udział w transmisji sygnałów. Wynika to z przyjętej definicji usługi komunikacji elektronicznej (w projekcie PKE), która wyłącza usługi, które głównie nie zajmują się transmisji sygnałów. Jest to odmienne podejście od zastosowane w EKŁE, gdzie pojęcie usług łączności elektronicznej obejmuje usługi, które częściowo (nie głównie, jak to jest w PKE), zajmują się transmisją sygnałów. * dostawcy sieci dla sieci prywatnych (niepublicznych) dla klientów B2B w ramach Przemysłu 4.0., pomimo tego, iż realizują sieci oraz usługi, które mają bardzo często charakter kluczowy dla bezpieczeństwa określonych branż. Wydaje się, że wynika to z przyjętej definicji przedsiębiorcy komunikacji elektronicznej (w projekcie PKE), która koncentruje się na dostarczaniu publicznych sieci telekomunikacyjnych. Jest to odmienne podejście od zastosowane w EKŁE, gdzie pojęcie dostarczanie sieci łączności elektronicznejabstrahuje od charakteru sieci, czy ma ona charakter publiczny, bądź niepubliczny oraz obejmuje urządzenia końcowe, które są zainstalowane w maszynach.   Prawidłowo skonstruowane obowiązki w zakresie bezpieczeństwa powinny obejmować wszystkie podmioty działające na rynku komunikacji elektronicznej. W przeciwnym wypadku, może okazać się, iż niektóre podmioty będą miały większą swobodę działania w określonych segmentach rynku np. w budowaniu sieci niepublicznych pod rozwiązania IoT np. rozwiązania smart city, czy też sieci campusowych. W ten sposób może powstać pewna nierównowaga konkurencyjności między podmiotami. | **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 przez ustawę wprowadzającą PKE.  Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowym.  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. |
|  | T-Mobile Polska | Uwaga ogólna | Projekt ustawy proponuje wprowadzenie mechanizmu oceny ryzyka dostawcy sprzętu lub oprogramowania, który będzie mógł istotnie ograniczać działalność dostawcy sprzętu i oprogramowania. Jednakże istotne konsekwencje decyzji podjętej przez Kolegium, poza dostawcą, ponosić będą przede wszystkim operatorzy telekomunikacyjni, dostawcy usług, a nawet użytkownicy końcowi, którzy wykorzystują sprzęt lub oprogramowanie dostawcy będącego przedmiotem decyzji. W szczególności należy mieć na uwadze, iż rynek telekomunikacyjny charakteryzuje się bardzo dużym stopniem złożoności i zróżnicowaniem, które wychodzi poza działalność pojedynczych operatorów. Z tego względu decyzje Kolegium muszą mieć charakter bardzo wyjątkowy (incydentalny) i powinny zostać poprzedzone szeroką i wnikliwą analizą skutków regulacji.  Z uwagi na wysoką rangę polityczną Kolegium, wszelkie analizy skutków regulacji, scenariuszy rozwiązań alternatywnych, źródeł finansowania kosztów oraz ewentualne rekomendacje dla Kolegium powinny każdorazowo być integralnym i niezbędnym elementem wniosku do Kolegium, aby następnie uzyskać wysoki poziom jakościowy ostatecznej decyzji Kolegium. Oznacza to, iż zdecydowany wysiłek merytoryczny powinien zostać położony na etap przygotowania wniosku o przeprowadzenie ostatecznej oceny przez Kolegium. Z kolei pod decyzję Kolegium powinien zostać poddany w pełni przygotowany wniosek, zawierający pełną informację, która umożliwi Kolegium podjęcie odpowiedzialnej decyzji, niosącej ze sobą wielorakie i długofalowe skutki dla rynku i użytkowników końcowych  Z pewnością opinia Kolegium wpływa bezpośrednio na rachunek kosztów po stronie innych podmiotów. Z tego względu regulacja powinna dopuszczać mechanizm rekompensaty finansowej, który będzie mógł być zastosowany w uzasadnionych przypadkach, jak również mechanizm przesunięcia w czasie wdrażania opinii, w celu minimalizacji obciążeń danego sektora.  W celu zwiększenia pewności prawnej, projekt opinii Kolegium powinien zostać poddany konsultacji z zainteresowanymi podmiotami (w trybie właściwym, uznanym przez Kolegium). | **Uwaga nieuzwględniona**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | Polska Izba Komunikacji Elektronicznej | Uwaga ogolna | PIKE stanowczo sprzeciwia się rozszerzeniu zakresu przedmiotowego ustawy o KSC na przedsiębiorców z sektora telekomunikacyjnego. Art. 1 ust. 3 dyrektywy z 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 (dalej: dyrektywa NIS) wprost wyłącza stosowanie ogólnych regulacji dot. cyberbezpieczeństwa wobec przedsiębiorców telekomunikacyjnych w zakresie ich sieci i usług łączności elektronicznej. Pomimo że art. 3 dyrektywy NIS wskazuje poziom harmonizacji minimalnej, czyli umożliwia państwom członkowskim minimalne standardy regulacyjne, to jednak rozszerzenie jakiegokolwiek zakresu stosowania przepisów dyrektywy NIS nie może się odbywać wbrew jej innym bezwzględnie obowiązującym przepisom. Takim przepisem w istocie jest wspomniany art. 1 ust. 3 dyrektywy NIS. Ustawodawca europejski bowiem świadomie rozdzielił kwestie zachowania bezpieczeństwa sieci i usług telekomunikacyjnych od szeroko pojętego cyberbezpieczeństwa i w aktualnym stanie prawnym kompleksowo uregulował je w art. 40 i 41 dyrektywy 2018/1972 ustanawiającej Europejski Kodeks Łączności Elektronicznej (dalej: EKŁE). Ich wdrożenie do prawa polskiego nastąpi pod koniec roku przepisami projektowanej ustawy Prawo komunikacji elektronicznej (dalej: PKE). Tym samym, konsultowana nowelizacja ustawy o KSC niesłusznie oraz niezgodnie z przepisami dyrektywy NIS dubluje regulacje z rozdziału 5 PKE „Bezpieczeństwo sieci i usług oraz zadania i obowiązki na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego” oddział 1 „Bezpieczeństwo sieci i usług”. Odrębność tej regulacji uwarunkowana jest potrzebą zapewnienia bezpieczeństwa w sieciach telekomunikacyjnych w oparciu o współpracę z wyspecjalizowanymi organami telekomunikacyjnymi takimi jak Prezes Urzędu Komunikacji Elektronicznej czy CSIRT TELCO.  Wobec powyższego, **PIKE postuluje o zachowanie odrębności regulacyjnej sektora telekomunikacyjnego w zakresie cyberbezpieczeństwa, a tym samym zrezygnowanie z rozszerzenia zakresu przedmiotowego ustawy o KSC na przedsiębiorców telekomunikacyjnych z uwagi na specyfikę prowadzonej przez nich działalności oraz niezgodność takiej regulacji z przepisami unijnymi**. | **Uwaga nieuwzględniona**  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 przez ustawę wprowadzającą PKE.  Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowym.  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. |
|  | Polska Izba Komunikacji Elektronicznej | Uwaga ogólna | **Niezgodność przepisów ustawy o KSC z projektowanymi przepisami PKE oraz EKŁE – uwagi szczegółowe**  Jak zostało wskazane powyżej, nie dość, że nowelizacja ustawy o KSC niepotrzebnie powiela regulacje projektowane w PKE, to robi to dodatkowo w sposób niezgodny z unijnymi przepisami EKŁE. Sprzeczności te są uwidocznione już w samych definicjach. W PKE (podobnie jak i w EKŁE) *incydent bezpieczeństwa* zdefiniowano jako „*każde zdarzenie, które ma rzeczywisty, niekorzystny skutek dla bezpieczeństwa sieci i usług”.* Tymczasem ustawa o KSC określa *incydent telekomunikacyjny* jako „*incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi komunikacji elektronicznej*”. Łatwo dostrzec, że zakresy obu tych definicji są wyraźnie różne – w PKE mowa o rzeczywistym skutku dotyczącym bezpieczeństwa sieci i usług, podczas gdy ustawa o KSC wskazuje na rzeczywisty lub potencjalny skutek w dodatku tylko dla świadczenia usług. Dodatkowo definicja z ustawy o KSC błędnie obejmuje każdą przerwę ciągłości świadczenia usług bez względu na jej ważność, czas trwania czy jej przyczynę. Tym samym, **definicje te powinny zostać uzgodnione w kierunku zmiany definicji *incydentu telekomunikacyjnego* w ustawie o KSC w zgodzie z art. 2 pkt 42 EKŁE i art. 2 pkt 12 PKE.**  W kontekście precyzyjnego zdefiniowania *incydentu telekomunikacyjnego* na gruncie EKŁE i PKE, tym bardziej **nieuzasadniona jest regulacja art. 20a ust. 4 oraz art. 20b ust. 4 ustawy o KSC, które upoważniają właściwego ministra do dookreślenia w formie aktu wykonawczego – rozporządzenia**, jakie środki będą musieli przedsięwziąć przedsiębiorcy telekomunikacyjni aby takim incydentom zapobiegać, a także progów incydentu telekomunikacyjnego, których przekroczenie spowoduje powstanie obowiązku zgłoszenia incydentu. **W opinii PIKE są to kwestie zasadnicze dla przedmiotu tej ustawy – stanowią element definiujący zakres przedmiotowy regulacji i dlatego powinny być określone w ustawie, a nie w rozporządzeniach**. Forma rozporządzenia pozostawia zbyt duży zakres regulacji w gestii władzy wykonawczej, co może spowodować w skrajnych sytuacjach (w przypadku narzucenia obowiązku wymagającego dużych nakładów finansowych oraz zakresu pracy) koniczność modyfikacji długofalowych strategii konkretnej spółki, zarówno w przypadku określonych zadań kluczowych (poprzez przeniesienie środków), jak i strategii cyberbezpieczeństwa danego operatora telekomunikacyjnego.  **Kolejnym przykładem nieuzasadnionego rozszerzenia zakresu regulacji ustawy o KSC** w porównaniu do przepisów PKE i EKŁE, **jest** **propozycja szczegółowego wyliczenia elementów zgłoszenia incydentu telekomunikacyjnego w art. 20d. Izba ocenia tę regulację jako zbyt szczegółową a także nadmiarową.** Katalog ten zawiera bowiem szereg elementów, których wskazanie w zgłoszeniu incydentu może okazać się niemożliwe, ponieważ przedsiębiorca telekomunikacyjny może nie posiadać na ich temat wiedzy, a co w konsekwencji znacząco utrudni, a czasami nawet uniemożliwi dokonywanie przez przedsiębiorców zgłoszeń.  Dodatkowo, Izba wskazuje na szereg szkodliwych regulacji dotyczących współpracy przedsiębiorców telekomunikacyjnych z różnymi podmiotami i organami w zakresie cyberbezpieczeństwa.  W pierwszej kolejności niepokoją nowe prawa CSIRT MON, CSIRT NASK i CSIRT GOV względem sektora telekomunikacyjnego, ponieważ ich przyznanie następuje kosztem uprawnień Prezesa UKE oraz CSIRT TELCO. Taka regulacja jest wadliwa, ponieważ rozdrabnia ona prace nad zapewnieniem bezpieczeństwa sieci i usług telekomunikacyjnych pomiędzy wiele organów niewyspecjalizowanych w kwestiach telekomunikacyjnych. Przykładowo, **art. 26 ustawy o KSC wyraźnie wskazuje na uprawnienia CSIRT MON, CSIRT NASK i CSIRT GOV przy badaniu wszelkiej podatności i incydentów telekomunikacyjnych, pomijając całkowicie przy tej regulacji Prezesa UKE i CSIRT TELCO. Oznaczać to będzie, że przedsiębiorcy telekomunikacyjni przy zwalczaniu incydentów telekomunikacyjnych nie będą wiedzieć z którym CSIRT w danym momencie współpracować, a ponadto część z tych CSIRT przy swoich działaniach będą kierowały się własnymi priorytetami niezwiązanymi z rynkiem telekomunikacyjnym. Dodatkowo taka treść regulacji jest sprzeczna z przepisami PKE i EKŁE.**  Następny problem to rozszerzenie katalogu podmiotów współpracujących w zakresie cyberbezpieczeństwa z SOC operatorów usług kluczowych (wśród których są też niektórzy przedsiębiorcy telekomunikacyjni). Powoduje to w szczególności pojawienie się nowego **obowiązku współpracy tych SOC z organami wymiaru sprawiedliwości, co PIKE ocenia jako nieproporcjonalne i nadmiarowe.** Przedsiębiorcy telekomunikacyjni mają już własne procedury współpracy z organami wymiaru sprawiedliwości, uwzgledniające kwestie ochrony tajemnicy telekomunikacyjnej. Zachodzi obawa, ze odrębnie uregulowany w ustawie o KSC obowiązek współpracy z organami wymiaru sprawiedliwości w oderwaniu od regulacji telekomunikacyjnych może grozić naruszeniami przepisów o ochronie tajemnicy telekomunikacyjnej.  Jako zbędną należy również ocenić konieczność współpracy przedsiębiorców telekomunikacyjnych z ISAC. Izba wskazuje, że **rola tej instytucji nie dotyczy zwalczania incydentów telekomunikacyjnych, a jedynie dokonywania analizy i wymiany informacji na temat potencjalności zagrożenia incydentami. Tymczasem informacje o incydentach telekomunikacyjnych powinny być gromadzone wyłącznie przez CSRIT TELCO co pozwolili na skoncentrowane działania rządowe do zwalczania tych incydentów we współpracy z rynkiem. Ponadto przepisy PKE ani EKŁE nie przewidują utworzenia takiej instytucji.** | **Uwaga nieuwzględniona**  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 przez ustawę wprowadzającą PKE.  Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowym.  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. |
|  | Polska Izba Komunikacji Elektronicznej | Uwaga ogólna | **Rozszerzenie uprawnień Kolegium oraz Pełnomocnika Rządu ds. Cyberbezpieczeństwa**  PIKE wskazuje, że projektowana ustawa o KSC istotnie rozszerza kompetencje Kolegium ds. Cyberbezpieczeństwa oraz Pełnomocnika Rządu ds. Cyberbezpieczeństwa, **przekształcając je z organów pierwotnie doradczo-opiniujących w organy o uprawnieniach mających fundamentalny wpływ na prowadzoną przez przedsiębiorców działalność gospodarczą**. Chodzi tutaj w szczególności o umożliwienie dokonywania oceny ryzyka dostawcy sprzętu lub oprogramowania istotnego dla cyberbezpieczeństwa oraz wydawanie ostrzeżenia lub polecenia zabezpieczającego w przypadku możliwości wystąpienia lub realnego wystąpienia incydentu telekomunikacyjnego. Szczegółowa analiza powyższych kompetencji prowadzi do wniosku, że **regulacje te naruszają zasadnicze zasady prawa administracyjnego**. Mianowicie, brakuje informacji o charakterze prawnym ostrzeżenia, o konsekwencjach wydanego ostrzeżenia, brakuje określenia obowiązku przeprowadzenia konsultacji z zainteresowanymi podmiotami, określenia mechanizmu odwoławczego od ostrzeżenia i polecenia zabezpieczającego, w sytuacji, w której niezastosowanie się do ich treści zagrożone jest wysokimi karami pieniężnymi. Tym samym, **całość projektowanych regulacji art. 66a-66c oraz 67a-67c ustawy o KSC jest wyjątkowo szkodliwa i naruszające podstawowe zasady prowadzenia działalności gospodarczej przez przedsiębiorców telekomunikacyjnych, pozbawiając ich faktycznego udziału w procesie decyzyjnym, a także realnej kontroli sądowej i administracyjnej wydanych decyzji**.  Co się tyczy uwag szczegółowych dotyczących nowych kompetencji organów, PIKE chciałoby się pochylić przede wszystkim nad przepisami dot. wycofania sprzętu z użytku (czyli również sprzętu telekomunikacyjnego) ze względu na aspekty cyberbezpieczeństwa. W konsekwencji, regulacja ta umożliwia narzucenie zakupu czy wdrożenia konkretnego rozwiązania technicznego, określonego producenta, co w swoich skutkach może spowodować ograniczenie konkurencji, wzrost kosztu budowy sieci telekomunikacyjnych oraz wprowadza możliwość prowadzenia lobbingu przez producentów. Racjonalizacja tej regulacji powinna polegać przede wszystkim na jasnym określeniu norm i standardów dla sprzętu, a następnie na stopniowym wygaszeniu produkcji sprzętu niespełniającego wymogów, nie zaś na zakazywaniu używania sprzętu, który został legalnie wyprodukowany i wprowadzony do obrotu zgodnie z przepisami prawa i normami obowiązującymi w chwili produkcji i wprowadzenia do obrotu.  Skutki ekonomiczne wycofania urządzeń i oprogramowania są wymierzone w przedsiębiorców telekomunikacyjnych, które nie powinny ponosić odpowiedzialności za zgodność tych urządzeń i oprogramowania z nowymi wymogami bezpieczeństwa ustalone przez organy nie związane nawet z rynkiem telekomunikacyjnym. W efekcie proponowanych regulacji ustawy o KSC przedsiębiorcy telekomunikacyjni poniosą ogromne straty finansowe z przyczyn, za które nie ponoszą odpowiedzialności, oraz których nie mogli nawet przewidzieć ani im zapobiec przy zachowaniu najwyższej staranności. Na uwagę zwraca bowiem fakt, ze kontroli przez Kolegium i Pełnomocnika nie podlegają same urządzenia czy oprogramowanie, ale ich producent. W tym zakresie konieczne byłoby zastosowanie mechanizmu pokrycia strat bądź przyznawania rekompensat dla przedsiębiorców telekomunikacyjnych. Co więcej, regulacja ta uderzy jednakowo w małych jak i dużych przedsiębiorców telekomunikacyjnych używających sprzętu, który może zostać uznany za zakazany.  Izba pragnie zwrócić również uwagę na inne aspekty nowego uprawnienia w zakresie nakazania usunięcia urządzeń i oprogramowania z sieci telekomunikacyjnej w ciągu 5 lat. Po pierwsze, termin ten będzie realnie krótszy, dlatego, że przedsiębiorcy telekomunikacyjni będą mieli problemy z serwisowaniem takich urządzeń i oprogramowania. Producent bowiem będzie wycofywał się z polskiego rynku, a ich ilość na rynku będzie się stale zmniejszała co podniesie cenę serwisu. W przypadku uszkodzenia takich urządzeń nie będzie nawet opłacalne ich naprawianie z uwagi na wcześniejszą konieczność ich usunięcia niż wynikałoby to z usługi serwisowej czy gwarancji producenta. Po drugie, nakaz usuwania urządzeń i oprogramowania uderzy w inwestycje telekomunikacyjne realizowane w ramach POPC a także w Ogólnopolską Sieć Edukacyjną. Konieczne będzie modyfikowanie tych sieci jeszcze w okresie ich trwałości, a więc niezgodnie z umowami publiczno-prywatnymi na te inwestycje.  Najważniejszy zarzut Izby związany jest z faktem, że **zaprojektowana w swoim aktualnym brzmieniu regulacja narusza fundamentalne zasady prawa zagwarantowane Konstytucją RP**:   1. w zakresie **zasady praworządności** – nie określa jasnych i konkretnych norm i standardów jakie musi spełniać sprzęt czy też kryteriów, według których sprzęt jest uznawany za zgodny lub niezgodny z wymogami. Nie wskazuje także precyzyjnych procedur postępowania, formy podejmowania rozstrzygnięć itp., 2. w zakresie **zasady *lex retro non agit*** – ustanawia wymagania i reguły postępowania w stosunku do produktów wprowadzonych do obrotu w przeszłości, 3. w zakresie **zasady ochrony praw nabytych** – pozbawia przedsiębiorców prawa do korzystania ze sprzętu i wyposażenia nabytych przed wejściem w życie projektowanych przepisów, 4. w zakresie **zasady dwuinstancyjności postępowania** – projektowane przepisy nie określają niezależnej, obiektywnej, a także znanej przepisom kodeksu postępowania administracyjnego procedury odwoławczej. | **Wyjaśnienie**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano 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 został dołączony do ustawy jako załącznik nr 3.  Zrezygnowano z planów wycofania sprzętu lub oprogramowania.  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. Zatem także minister właściwy ds. informatyzacji będzie podejmował decyzje o ewentualnych karach także w formie decyzji administracyjnej. Przepis art. 73 został uzupełniony o wysokość kary za nie zastosowanie się do polecenia zabezpieczającego.  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 wskazany 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 Zepole 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. |
|  | Polska Izba Komunikacji Elektronicznej | Uwaga ogólna | **Wpływ regulacji na sektor MŚP**  Biorąc pod uwagę znaczące zmiany w zakresie cyberbezpieczeństwa dla przedsiębiorców telekomunikacyjnych, nie można zgodzić się z oceną skutków regulacji ustawy o KSC, która stwierdza brak jej wpływu na małe i średnie przedsiębiorstwa. Znaczną część rynku telekomunikacyjnego objętą tą regulacją stanowią bowiem przedsiębiorcy MŚP, a zatem wpływ tej ustawy, wbrew dokonywanym ocenom, na ich działalność gospodarczą będzie znaczący. | **Uwaga nieuwzględniona**  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 (co jest w ich dobrym interesie) a zgłaszać do CSIRT Telco i CSIRT poziomu krajowego te incydenty telekomunikacyjne, które będą spełniać progi incydentu. |
|  | Polska Izba Komunikacji Elektronicznej | Uwaga ogólna | PIKE wyraża poważne wątpliwości co do zasadności projektowanej nowelizacji ustawy o KSC w kontekście jej rozszerzenia na usługi i sieci telekomunikacyjne. Prezentowana regulacja wykazuje szereg niezgodności z przepisami bezwzględnie obowiązującymi prawa UE (dyrektywą NIS oraz dyrektywą EKŁE implementowaną do polskiego prawa projektem PKE). Ponadto, projektowane przepisy w szczegółach naruszają podstawowe zasady prawa administracyjnego oraz zasady prawa zagwarantowane Konstytucją RP. Tym samym całość projektowanej ustawy PIKE ocenia zdecydowanie negatywnie i postuluje o usunięcie regulacji związanych z rynkiem telekomunikacyjnym, w szczególności usunięcie uprawnień Kolegium oraz Pełnomocnika Rządu ds. Cyberbezpieczeństwa. Jednocześnie PIKE wnosi o pozostawienie wszystkich regulacji dotyczących sektora telekomunikacyjnego do wyłącznej regulacji aktualnie konsultowanego projektu PKE. Kwestie dotyczące bezpieczeństwa usług i sieci telekomunikacyjnych, ze względu na swoją specyfikę powinny być objęte jednym, kompleksowym aktem prawnym.  Biorąc pod uwagę istotność przedmiotowego zagadnienia i jego wpływ na rynek telekomunikacyjny, PIKE wskazuje, że pozostaje do dyspozycji Ministra Cyfryzacji w przypadku potrzeby jakichkolwiek dalszych wyjaśnień i uzupełnień niniejszego stanowiska. | **Uwaga nieuwzględniona**  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 przez ustawę wprowadzającą PKE.  Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowym.  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. |
|  | Fabryka E-Biznesu | Uwaga ogólna | Ustawa w proponowanym brzmieniu prowadzi do dyskryminacji niektórych z operatorów telefonii komórkowej, co w efekcie może doprowadzić do braku konkurencji na rynku telekomunikacyjnym,  wzrostu cen, co bez wątpienia odbije się na konsumentach. Ponadto wejście w życie ustawy w obecnym brzmieniu spowoduje mniej korzystne warunki dla rozwoju sieci 5G w Polsce, czego efektem będzie opóźnienie wprowadzenia 5G w naszym kraju o kilka lat, na czym stracą polskie przedsiębiorstwa.  Ponadto warto zaznaczyć, że krajowy system cyberbezpieczeństwa jest transpozycją dyrektywy NIS (Dyrektywa Parlamentu Europejskiego i Rady (UE) w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii), a dyrektywa NIS nie  ma zastosowania do operatora telekomunikacyjnego, ponieważ prawa i obowiązki operatora telekomunikacyjnego zostały szczegółowo określone w Prawie Komunikacji Elektronicznej (nowe  prawo telekomunikacyjne) poprzez przyjęcie kodeksu komunikacji elektronicznej. Przyczyną takiego rozwiązania jest fakt, że dodanie przedsiębiorstwa komunikacji elektronicznej jako podmiotu, do  którego stosuje się przepisy ustawy o krajowym systemie cyberbezpieczeństwa, spowoduje nakładanie się przepisów i potencjalny konflikt. Zazwyczaj kluczowym dostawcą operatora infrastruktury krytycznej jest operator telekomunikacyjny i ma to ogromne znaczenie. Dlatego PKE ma kompleksowe i  szczególne wymagania wobec operatorów telekomunikacyjnych. Nakładanie się na siebie KSC i PKE powoduje konstruktywne i interpretacyjne wątpliwości i zamieszanie.  Co za tym idzie pozwolę sobie zasugerować postępowanie zgodnie z logiką prawną dyrektywy NIS i EECC oraz przyjęcie, że KSC nie ma zastosowania do przedsiębiorstw komunikacji elektronicznej.  Żywię ogromną nadzieję, że Ministerstwo Cyfryzacji zapozna się z głosem społeczeństwa i wprowadzi niezbędne zmiany w przepisach omawianego projektu ustawy. | **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 przez ustawę wprowadzającą PKE.  Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowym.  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. |
|  | Krajowa Izba Gospodarki Cyfrowej DigiCom  Krajowa Izba Gospodarki Cyfrowej DigiCom | Uwaga ogólna  Uwaga ogólna | Na wstępie trzeba podkreślić, iż zapewnienie bezpieczeństwa sieci i systemów informatycznych jest dziś priorytetowym wyzwaniem, z którym mierzyć się muszą rządy wszystkich rozwiniętych państw, w tym państw członkowskich UE.  Nie ulega wątpliwości, że niezbędna jest regulacja tego obszaru, tak aby, w zgodzie z zasadami konkurencji, z jednej strony stworzyć warunki przyjazne do rozwoju tego sektora gospodarki, z drugiej zaś strony zabezpieczyć interesy podmiotów o słabszej pozycji rynkowej, tj. konsumentów. Projektowana ustawa ma niebagatelne znaczenie dla tempa wdrażania sieci 5G i co się  z tym wiąże, rozwoju gospodarczego państwa. Stąd też procedowanie przedmiotowego projektu ustawy powinno być oparte o dogłębną analizę sytuacji rynkowej podmiotów na nim funkcjonujących, z uwzględnieniem specyfiki tego rynku.  Należy zwrócić uwagę na rozwiązania niejasne i nieprecyzyjne. Regulacja dotyczy sektora zaawansowanego technicznie i technologicznie.  Stąd też konieczne jest takie konstruowanie przepisów, by przesłanki, na podstawie których przyznawane są uprawnienia lub nakładane są obowiązki, były obiektywne i jasne,  a wydawane w oparciu o nie rozstrzygnięcia poprawne i weryfikowalne. Kryteria nietechnologiczne są bardzo często nieokreślone i wykorzystują niejasne pojęcia, które są bardzo trudne do zweryfikowania i oceny. Projektowane rozwiązanie w postaci sporządzania przez Kolegium ds. Cyberbezpieczeństwa oceny ryzyka dostawcy sprzętu lub oprogramowania istotnego dla cyberbezpieczeństwa podmiotów krajowego systemu cyberbezpieczeństwa oparte jest o niejasne kryteria. Jako, że nie są to przesłanki technologiczne, trudno je obiektywnie zweryfikować. Rozwiązanie to powinno raczej zmierzać w kierunku stworzenia mechanizmu certyfikacji dla krytycznego sprzętu  i oprogramowania. Ocena powinna być dokonywana nie tyle w odniesieniu do podmiotu,  tj. dostawcy sprzętu, oprogramowania lub usług, co samego sprzętu czy oprogramowania.       W przypadku sporządzenia oceny ryzyka określającej ryzyko jako wysokie podmioty krajowego systemu cyberbezpieczeństwa nie mogą wprowadzać do użytkowania sprzętu, oprogramowania i usług określonych w ocenie danego dostawcy sprzętu  lub oprogramowania oraz muszą wycofać 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. Taka regulacja, z pewnością, spowoduje ogromne koszty w długiej perspektywie, ponieważ mniejsza liczba dostawców oznacza mniejszą konkurencję na rynku. To z kolei może doprowadzić do opóźnień we wdrożeniu technologii 5G a tym samym spowolnienia gospodarki. By zmniejszyć skutki takiego rozwiązania, okres na wycofanie sprzętu winien ulec wydłużeniu.              Ponadto, warto poddać analizie procedurę odwoławczą od oceny ryzyka sporządzonej przez Kolegium ds. Cyberbezpieczeństwa. Możliwość odwołania istnieje wyłącznie w przypadku oceny określającej ryzyko jako wysokie. Odwołanie rozpatrywane jest przez ten sam organ, który wydał decyzję w przedmiocie oceny ryzyka. Uwzględniając niejasne kryteria dokonywania oceny, mechanizm ten nie zabezpiecza interesów strony  i pozbawia możliwości czynnego udziału w postępowaniu. Na gruncie tej procedury nie są więc respektowane podstawowe zasady postępowania administracyjnego. Regulacja zatem powinna zmierzać w kierunku zabezpieczenia praw strony.  Wątpliwości budzą też rozwiązania dotyczące ostrzeżeń i poleceń zabezpieczających wydawanych przez Pełnomocnika. Wydaje się, że powinny mieć formę decyzji administracyjnej, a polecenia nie powinny być wydawane z rygorem natychmiastowej wykonalności.  Ostrzeżenia mogą zabezpieczać interesy konsumentów, zwiększając ich świadomość rynkową. Natomiast w drodze poleceń mogą być nakładane dość restrykcyjne obowiązki, stąd też fakt, iż wydawane są w oparciu o nieokreślone i niejasne przesłanki budzi niepokój. Tytułem przykładu zakaz połączeń z określonymi adresami IP lub nazwami URL nałożony  w ramach polecenia zabezpieczającego w połączeniu z rygorem natychmiastowej wykonalności jest dość dotkliwą restrykcją.  Jak wskazano powyżej, konieczne jest precyzyjne uregulowanie przedmiotowej materii. Należy podkreślić rolę projektowanej ustawy dla rozwoju sieci 5G i rozwoju gospodarczego w ogólności, którego motorem będzie wdrożenie technologii 5G. Wiele zaproponowanych rozwiązań należy poddać krytycznej analizie i doprecyzować, mając  na względzie specyfikę rynku i wyzwań przed nim stojących. Bez wątpienia istnieje potrzeba funkcjonowania na rynku jak najliczniejszej grupy podmiotów, tak by wdrożenie sieci 5G nie doznało opóźnień i nie spowodowało kosztów, które odczuć by mogli w szczególności konsumenci. | **Uwagi częściowo uwzględnione**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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.  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. Zatem także 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.  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 Zepole 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. |
|  | Install Tech | Uwaga ogólna | Jako firma będąca w pełni zaangażowana w rozwój branży ICT oraz mająca swój wkład w rozwój technologiczny Polski, czujemy się się zaniepokojeni Projektem Ustawy, który może mieć negatywny  wpływ zarówno na naszą firmę, jak i pokrewne branże związane z rynkiem ICT.  Zdajemy sobie sprawę, że Rząd dokłada wszelkich starań, aby poprawić cyberbezpieczeństwo kraju, jednak Projekt Ustawy zawiera kryteria, które z pewnością nie będą sprzyjały konkurencyjności na  rynku, ze względu na możliwość wpływu na przedsiębiorców poprzez ograniczanie zakresu prowadzenia ich działalności. Zapisy proponowane w Projekcie wpłyną zatem negatywnie na  zatrudnienie i rozwój branży telekomunikacyjnej, co w konsekwencji może opóźnić proces cyfryzacji w Polsce. Naszym zdaniem, aby poprawić cyberbezpieczeństwo polskich sieci, warto wziąć pod uwagę  ustalenie obiektywnych i jasnych kryteriów oceny ryzyka, opierając się na zasadzie transparentności oraz upewnienie się, że wyniki zastosowanych kryteriów oceny są prawidłowe. Warto rozważyć  ustanowienie wspólnego unijnego mechanizmu certyfikacji dla krytycznego sprzętu i oprogramowania, który obowiązywałby dla wszystkich, niezależnie od kraju pochodzenia. Wierzymy, że takie podejście wpłynęłoby na zwiększenie poziomu cyberbezpieczeństwa w Polsce. Proponujemy, aby Ministerstwo Cyfryzacji zorganizowało otwartą debatę i zaprosiło zainteresowane strony do pochylenia się i pełnego omówienia kwestii poruszonych w Projekcie. Rząd powinien w pełni ocenić wpływ Projektu, w tym koszty i straty, konkurencję handlową, legalność, społeczno-gospodarcze i międzynarodowe stosunki handlowe oraz klimat inwestycyjny w Polsce. Wyrażamy nadzieję, że nasza opinia zostanie wzięta pod uwagę. | **Uwaga nieuwzględniona**  Przepisy art. 66a-66c zostaly zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | Polska Izba Handlu | Uwaga ogólna | **Potencjalne naruszenia prawa**   1. **Naruszenie polskich przepisów** 2. Naruszenie prawa konstytucyjnego 3. **Zasada proporcjonalności**   Proponowane kryteria procedury ocennej, której efektem może być zakaz prowadzenia działalności gospodarczej w Polsce zostały określone w sposób **nieprecyzyjny**. Przepisy Projektu przyznają Kolegium, które nie jest kompetencyjnie i ustrojowo umocowane, bardzo duże uprawnienia i kompetencję do prowadzenia jednostronnego postępowania ocennego. Konsekwencje tego postępowania mogą wywrzeć olbrzymi wpływ na sytuację ekonomiczną danego dostawcy, ale również operatorów telekomunikacyjnych oraz konsumentów. Postępowanie przed Kolegium do spraw cyberbezpieczeństwa ma się w całości odbywać bez udziału ocenianego dostawcy, który dopiero z komunikatu w Monitorze Polskim dowie się, o przeprowadzonej ocenie. Dlatego też przyjęte rozwiązania legislacyjne są **sprzeczne z zasadą proporcjonalności wyprowadzoną z zasady demokratycznego państwa prawnego** (Art. 2 Konstytucji).   1. **Niedziałanie prawa wstecz i pewność prawa**   Projektowane przepisy w znaczący sposób podważają zaufanie obywateli do Państwa. Projekt zakłada niekonstytucyjny obowiązek usunięcia z rynku przejawów dotychczasowej działalności dostawcy (w tym infrastruktury). W związku z powyższym analizowany zakaz należy poddać kontroli w zakresie zgodności z zasadą *lex retro non agit* (niedziałania prawa wstecz)*.* W związku z tym, że demokratyczne państwo prawne oznacza państwo w którym chroni się zaufanie obywatela do państwa i stanowionego przez nie prawa, ustawodawca dokonując kolejnych zmian stanu prawnego **nie może stracić z pola widzenia interesów podmiotów, jakie ukształtowały się przed dokonaniem zmiany stanu prawnego[[16]](#footnote-17).**   1. **Naruszenie zasady równości wobec prawa**   Projektowane rozwiązania w zakresie wyboru dostawcy sprzętu i oprogramowania sieci 5G pozwalają na arbitralne wykluczenie dostawców z udziału we wdrożeniu sieci 5G w oparciu o dowolne, nieokreślone kryteria. Nie przyznają przy tym dostawcom środków prawnych pozwalających na wniesienie odwołania od decyzji wykluczających. Wobec tego uznać je należy za sprzeczne z konstytucyjnymi zasadami równości wobec prawa (art. 32 Konstytucji).   1. **Brak przeprowadzenia oceny skutków regulacji**   Zmiany zawarte w projekcie nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa mogą wiązać się z daleko idącymi negatywnymi skutkami społecznymi (likwidacja miejsc pracy, obniżenie dostępności nowoczesnych usług, wzrost wykluczenia cyfrowego), gospodarczymi (obniżenie konkurencyjności polskiej gospodarki, spadek zaufania inwestorów oraz wzmocnienie oligopoli) i politycznymi (uderza w harmonizację europejską). Wynika to z konieczności wymiany sprzętu oraz aplikacji, które są obecnie w użyciu, na alternatywne, pochodzące od innych dostawców. Tymczasem w uzasadnieniu Projektu na s. 33 poświęconym skutkom gospodarczym i finansowym w ogóle nie ma o tym mowy. Wspomina się tylko o kosztach związanych z powoływaniem nowych struktur administracyjnych z zakresu cyberbezpieczeństwa (s. 49-52 uzasadnienia Projektu). Jest to istotne naruszenie procesu legislacyjnego (§ 28 Regulamin Pracy Rady Ministrów,t.j. M.P. z 2016 r. poz. 1006) świadczące o niekonstytucyjnym charakterze Projektu.   1. **Naruszenie pozostałych przepisów polskiego prawa** 2. **Naruszenie przepisów procedury administracyjnej**   W projektowanych przepisach nie przewidziano prawa strony do udziału w postępowaniu ocennym, prowadzonym przez Kolegium. Proponowane rozwiązania naruszają więc podstawowe zasady postępowania administracyjnego wyrażone w ogólnych przepisach Kodeksu postępowania administracyjnego., m.in. zasadę pogłębiania zaufania obywateli do władzy publicznej (art. 8 kpa), zasadę udzielenia informacji przez organ (art. 9), zasadę wysłuchania stron (art. 10). Wprowadzone przepisy naruszają więc podstawowe prawo jednostki do czynnego udziału w postępowaniu.   1. **Naruszenie prawa konkurencji w Polsce**   Uregulowanie kwestii wykluczenia dostawców w ustawie KSC narusza również podstawowe zasady prawa konkurencji. Zasady i tryb postępowania w stosunku do pomiotów działających na konkurencyjnym rynku, jeżeli podmioty te naruszają przepisy reguluje inna ustawa tj. ustawa z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów, Dz. U. nr 50, poz. 331 ze zm. Zgodnie z art. 1 ust. 2 tej ustawy, reguluje ona w szczególności zasady i tryb postępowania w stosunku do pomiotów działających na konkurencyjnym rynku, jeżeli podmioty te naruszają przepisy tej ustawy. Oznacza to faktyczne naruszenie przez Kolegium kompetencji właściwego organu administracyjnego, jakim jest Prezes Urzędu Ochrony Konkurencji i Konsumentów. | **Uwagi częściowo uwzględnione**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | Polska Izba Handlu | Uwaga ogólna | 1. **Niezgodność z prawem europejskim** 2. **Brak notyfikacji przepisów Komisji Europejskiej**   Istotnym argumentem, który należy podnieść jest kwestia obowiązku notyfikacji uregulowanego na poziomie prawa krajowego w Rozporządzeniu Rady Ministrów z dnia 23 grudnia 2002 r. (w szczególności w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych). Przedmiotowy obowiązek jest także uregulowany w Dyrektywie 2015/1535 Parlamentu Europejskiego i Rady z dnia 9 września 2015 r. ustanawiającej procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego.   1. **Naruszenie zasad TFUE**   Każda ocena ryzyka lub decyzja o wprowadzeniu ograniczeń rynkowych i pozataryfowych barier w handlu na podstawie niejednoznacznych kryteriów (np. kraj pochodzenia dostawców zawarty w projekcie) i nietransparentne procedury administracyjne, naszym zdaniem, są sprzeczne z podstawowymi zasadami równego traktowania/niedyskryminacji, które znajdują odzwierciedlenie w art. 18 (zakaz dyskryminacji ze względu na narodowość), Art. 34 (zakaz ograniczeń ilościowych w przywozie oraz wszystkich środków o skutku równoważnym), Art. 49 (zakaz ograniczeń swobody przedsiębiorczości) TFUE.   1. **Naruszenie zasady niedyskryminacji w prawie UE**   Kluczową zasadą praworządności jest to, że prawo musi mieć zastosowanie do wszystkich i być stosowane jednakowo i w sposób konsekwentny. Jest to powtórzone w Karcie Praw Podstawowych Unii Europejskiej (art. 20), w której "każdy jest równy wobec prawa”. Karta (art. 21 ust. 2) zabrania „wszelkiej dyskryminacji ze względu na narodowość”. Europejski Trybunał Sprawiedliwości zauważył, że „zakaz dyskryminacji ustanowiony w prawie UE jest szczególnym wyrazem ogólnej zasady równości, która jest jedną z podstawowych zasad prawa wspólnotowego”. Jest zatem zgodne z zasadą praworządności, że wymogi bezpieczeństwa powinny być powszechnie stosowane do wszystkich dostawców, a nie dotyczyć wybranych dostawców lub dostawców z określonych krajów.   1. **Naruszenie zasady proporcjonalności określonej przez ETS**   Pkt 13 w sprawie C-331/88 Fedesa odnosi się do zasady proporcjonalności: Po wprowadzeniu środka dyskryminującego Trybunał przyjrzy się proporcjonalności środka w odniesieniu do jego celu. Innymi słowy, środek taki musi być (1) konieczny do osiągnięcia celu i nie może wykraczać poza to, co jest konieczne do osiągnięcia celu, (2) najmniej restrykcyjny środek do osiągnięcia tego celu, oraz (3) spowodowane niedogodności nie mogą być nieproporcjonalne do zamierzonych celów.   1. **Naruszenie zasady swobodnego przepływu towarów**   Zasada ta może być nadal naruszona, nawet jeśli państwo członkowskie nie ustanawia wyraźnego przepisu zakazującego przywozu produktów od niektórych dostawców. Jak wyjaśnił Europejski Trybunał Sprawiedliwości, każdy zakaz używania produktu na terytorium państwa członkowskiego UE wpłynie na zachowanie nabywców i wpłynie na dostęp tego produktu na rynku tego państwa członkowskiego. Przepisy mające na celu odsunięcie określonego dostawcy od łańcucha dostaw w niektórych państwach członkowskich UE powstrzymają potencjalnych klientów przed kupowaniem produktów/technologii danego dostawcy.   1. **Naruszenie dyrektywy o konkurencji**   Dyrektywa 2002/77/WE w sprawie konkurencji zakazuje przyznawania wszelkich specjalnych praw w sektorze łączności elektronicznej. Projekt przyznaje jednak unijnym przedsiębiorstwom bezsporne przywileje skutecznego eliminowania konkurencji ze strony dostawców spoza UE, dyskryminując tym samym dostawców spoza UE (nawet tych najbardziej zaawansowanych technologicznie). | **Uwaga nieuwzględniona**  Projekt jest zgodny z Traktatami unijnymi, w szczególności są to rozwiązania proporcjonalne i adekwatne do rozwiązywanego problemu. |
|  | Polska Izba Handlu | Uwaga ogólna | 1. **Naruszenie przepisów WTO** 2. Układ Ogólny w sprawie Taryf Celnych i Handlu (GATT) zawiera klauzulę o najbardziej uprzywilejowanej pozycji. Członek WTO nie może dyskryminować indywidualnych partnerów handlowych, traktując niektóre kraje bardziej przychylnie niż inne 3. Zasada krajowego traktowania GATT zobowiązuje członków WTO do traktowania "podobnych" produktów zagranicznych i krajowych, usług i usługodawców w równym stopniu. W przypadku stosowania krajowego obowiązku podejścia, produkty zagraniczne, usługi lub zagraniczni usługodawcy nie mogą podlegać mniej korzystnym regulacjom niż „podobny” produkt krajowy, usługodawca lub usługodawca krajowy (art. III GATT). 4. Naszym zdaniem ustawodawca koncentruje się na ocenie cech dotyczących dostawców, a nie na bezpieczeństwie sprzętu czy oprogramowania, jakie zapewnia. Jedną z istotnych cech ocenianych w profilu dostawcy jest kryterium pochodzenia dostawcy z danego kraju. Rodzi to zagrożenie, że Polska naruszy umowy międzynarodowe zakazujące dyskryminacji ze względu na pochodzenie. 5. **Zobowiązania dwustronne w ramach umów międzynarodowych**   Przyjęcie prawodawstwa, które pozwoli na wykluczenie z polskiego rynku z podmiotów reprezentujących kapitał zagraniczny narusza zobowiązania podmiotów na mocy umów dwustronnych z innymi państwami. Na przykład, jeżeli dostawca z państwa trzeciego będzie wykluczony na podstawie niejasnych kryteriów, to może to zostać uznane za naruszenie przez Polskę obowiązku równego i sprawiedliwego traktowania na terytorium Polski na mocy Traktatu o Dwustronnej Inwestycji. | **Uwaga nieuwzględniona**  Porozumienie o Wolnym Handlu GATT w art. XXI pozwala na stosowanie przez strony porozumienia wszelkich działań, jakie uważają one za niezbędne do ochrony swych żywotnych interesów bezpieczeństwa. Projektowane przepisy wpisują się wobec tego w środki opisane w art. XXI GATT. |
|  | Polska Izba Handlu | Uwaga ogólna | **Uwagi techniczne dotyczące ryzyka i rozwiązań bezpieczeństwa**   1. **Kryteria powinny być neutralne technologicznie, a nie uwzględniać względy polityczne:** 2. Przedmiotem oceny ryzyka powinien być sprzęt i oprogramowanie uznane za krytyczne a nie charakterystyka dostawcy; 3. Kryteria powinny mieć charakter techniczny, obiektywne, rozsądne i proporcjonalne, oraz zawierać odniesienie do oceny ryzyka zawartej w specyfikacjach technicznych 4. Projekt ustawy musi być zgodny zarówno z wymogami prawnymi dotyczącymi dobrych praktyk legislacyjnych, jak i z obowiązującymi przepisami, takimi jak prawo Unii Europejskiej, międzynarodowe prawo inwestycyjne, prawami człowieka i Konstytucją RP;   **OCZEKIWANE DZIAŁANIA**  Niezależnie od okoliczności, iż czas na odniesienie się do materii projektu jest niezwykle krótki i zostaliśmy praktycznie pozbawieni prawa przeprowadzenia pogłębionych analiz potencjalnego wpływu przedmiotowego aktu na funkcjonowanie gospodarki, zdecydowaliśmy się przedłożyć powyższe wstępne uwagi oraz propozycje zmian. Jednocześnie zwracamy się z prośbą o przeprowadzenie następujących działań:  **POSTULAT RZETELNEJ ANALIZY SKUTKÓW SPOŁECZNYCH, GOSPODARCZYCH I POLITYCZNYCH ORAZ POKAZANIA W OCENIE SKUTKÓW REGULACJI WYNIKAJĄCYCH Z TEGO PEŁNYCH KOSZTÓW REGULACJI**  W zakresie skutków społecznych należy opisać wpływ na likwidację miejsc pracy, obniżenie dostępności nowoczesnych usług, wzrost wykluczenia cyfrowego wynikający z wyższego kosztu usług dla konsumentów i przedsiębiorstw: w szczególności w obszarach pracy zdalnej, zdalnej edukacji, telemedycyny, rozwoju inteligentnych usług samorządowych (smart cities) oraz nowoczesnych rozwiązań w rolnictwie, ochronie środowiska czy energetyce. | **Wyjaśnienie**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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 został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | Krajowy Sekretariat Łączności NSZZ Solidarność | Uwaga ogólna | Po analizie przedstawionego do konsultacji projektu ustawy uważamy, że wymaga on istotnych zmian, a przede wszystkim znacznego ograniczenia swojego zakresu. W swoim aktualnym kształcie zakłada on bardzo daleko idące zmiany dotykające przedsiębiorstw telekomunikacyjnych oraz prowadzonej przez nich działalności gospodarczej. Nie mamy żadnych wątpliwości, że jego ewentualne przyjęcie w obecnym kształcie będzie miało negatywny wpływ na kondycję tego sektora gospodarki, a więc i zatrudnianych w nim pracowników.  Projekt nie przewiduje żadnych uproszczeń w zakresie działalności telekomunikacyjnej, o które wielokrotnie wnioskowaliśmy, a wręcz przeciwnie skupia się na nakładaniu nowych obowiązków i ograniczeń, a także bardzo poważnym wzmocnieniu możliwości wpływu instytucji państwowych na nasze bieżące funkcjonowanie.  Przedstawiona propozycja zmian prawnych pojawiła się w okresie, w którym potencjał przedsiębiorców telekomunikacyjnych skupiony jest na realizacji inwestycji w nowoczesne sieci, utrzymanie ciągłości działania usług oraz przygotowanie do wdrożenia Prawa komunikacji elektronicznej. Co więcej, w samym obszarze bezpieczeństwa jesteśmy zaangażowani we wdrożenie do 30 grudnia br. postanowień rozporządzenia w sprawie warunków technicznych i organizacyjnych wydanego do art. 175d PT, nad którym prace trwały ponad pół roku, i które wydawało się, że adresuje już kwestie bezpieczeństwa w zakresie sieci 5G. Niestety, ale wraz z kolejnymi propozycjami zmian prawnych, jesteśmy w sytuacji, w której wciąż trwa dyskusja o rozwiązaniu kluczowych problemów zidentyfikowanych przez administrację, ale wciąż jest brak jest samych rozwiązań. Jakkolwiek jesteśmy przeciwnikami zbytniego pośpiechu we wprowadzaniu istotnych dla sektora regulacji, tak musimy skonstatować, że przedłużająca się faza niepewności nie ułatwia prowadzenia działalności gospodarczej. Szczególnie, że trudno nie zauważyć, że rozwiązania już wprowadzone i planowane powodują istotny chaos. Obecnie trudno już nadać właściwe znaczenie wprowadzonym już: (1) zmianom w rozporządzeniu do art. 175d PT (które mimo że musi być wdrażane nie jest utrzymywane w projekcie nowelizacji PKE i jego los jest faktycznie nieznany), (2) możliwym do wydania rekomendacjom Pełnomocnika Rządu ds. Cyberbezpieczeństwa, (3) opracowywanym wymaganiom dla aukcji częstotliwości określanych przez UKE i opiniowanych przez Kolegium, w kontekście planowanych kolejnych potężnych kompetencji organów administracji, tj.: (1) ocen dokonywanych przez Kolegium, (2) ostrzeżeń Pełnomocnika, (3) poleceń zabezpieczających Pełnomocnika.  Tymczasem projekt nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa zakłada włączenie naszego sektora, już od 21 grudnia br. do zupełnie nowego reżimu prawnego. Niezależnie od oceny takiego działania jako nieuzasadnionego, uważamy, że takie strukturalne zmiany wymagają odpowiedniego przygotowania i czasu na wdrożenie.  Tym samym proponowana ustawa stanowi kolejne obciążenie naszego sektora, które jednocześnie jest przedstawione bez wcześniejszej dyskusji i szerszego uzasadnienia. Obciążenie, które będzie wiązało się z dodatkowymi kosztami i wysiłkiem organizacyjnym. Trudno nam zaakceptować taki sposób procedowania szczególnie, że bardzo skromny zakres przedstawionych w uzasadnieniu i OSR informacji skłania nas do konkluzji, że sam projekt ustawy powstawał w pośpiechu i niekoniecznie był przedmiotem wystarczającej refleksji odnośnie swoich skutków. Tym bardziej, że w naszej ocenie wysiłek ten będzie zupełnie nieproporcjonalny wobec potencjalnych pozytywnych skutków. Wręcz przeciwnie, uważamy, że nagłe wprowadzenie omawianej ustawy w znaczącym stopniu utrudni realizację zadań w zakresie bezpieczeństwa i integralności.  **Włączenie przedsiębiorców komunikacji elektronicznej do krajowego systemu cyberbezpieczeństwa – koncepcja z której należy zrezygnować.**  Za zupełnie niezrozumiałą, szczególnie w kontekście braku przedstawienia uzasadnienia, uważamy koncepcję przeniesienia lub powtórzenia przepisów dot. obowiązków przedsiębiorców telekomunikacyjnych, w tym zakresie zgłaszania naruszeń/incydentów do ustawy o krajowym systemie cyberbezpieczeństwa.  Wszystkie wymagania w tym zakresie są już regulowane ustawą – Prawo telekomunikacyjne oraz w sposób zgodny z EKŁE proponowane w projekcie prawa komunikacji elektronicznej. Przedsiębiorcy są obowiązani do zgłaszania wszystkich naruszeń/incydentów według ustalonych w rozporządzeniu progów oraz formularza. Informacje te Prezes UKE może przekazywać do właściwych CSIRT. CSIRT mogą współpracować z innymi podmiotami krajowego systemu cyberbezpieczeństwa. Regulacja ta jest kompletna i daje podmiotom dla których te informacje mogą być istotne możliwość dostępu do nich.  Jeśli istnieją w tym zakresie jakiekolwiek deficyty proponujemy, aby zostały one w pierwszej kolejności wyartykułowane, a następnie przedyskutowane. Jesteśmy bowiem przekonani, że zwiększenie wiedzy CSIRT o incydentach w obszarze telekomunikacji nie wymaga włączania tego sektora do krajowego systemu cyberbezpieczeństwa. A szczególnie w tak krótkich jak przewidziane terminach i niejasny także z legislacyjnego punktu widzenia sposób.  Na tym etapie uważamy za niezbędne usunięcie z projektu przepisów zakładających włączenie sektora telekomunikacyjnego do krajowego systemu cyberbezpieczeństwa. | **Uwaga nieuwzględniona**  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 przez ustawę wprowadzającą PKE.  Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowym.  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. |
|  | Krajowy Sekretariat Łączności NSZZ Solidarność | Uwaga ogólna | **Ocena bezpieczeństwa dostawców – postulujemy uwzględnienie potencjału narzędzi certyfikacyjnych.**  Dyskusja nt. oceny bezpieczeństwa dostawców ma charakter globalny, a w UE i poszczególnych krajach trwają prace nad regulacjami mającymi tę kwestię właściwie zaadresować. Nie jest przedmiotem niniejszego stanowiska ocena zasadności tych działań, gdyż mają one w dużej mierze charakter polityczny, ekonomiczny, a potencjalnie także wywiadowczy.  Z perspektywy przedsiębiorców telekomunikacyjnych zaznaczamy jednak, że jakiekolwiek decyzje w tym obszarze muszą uwzględniać ich potencjalny wpływ na koszty, dostępność i jakość usług telekomunikacyjnych w Polsce. W praktyce oznacza to, że należało będzie każdorazowo precyzyjnie określać koszty danego rozwiązania, w tym wskazywać czy dane rozwiązanie faktycznie podniesie poziom bezpieczeństwa narodowego w cyberprzestrzeni i czy koszt jego wprowadzenia jest proporcjonalny wobec tego efektu. Nie można bowiem pominąć faktu, że skutki ewentualnych wykluczeń będą miały swój wpływ finansowy oraz konkurencję zarówno na rynku dostawców, jak i wobec użytkowników ich urządzeń, w tym z sektora telekomunikacyjnego. Finalne obciążenia w tym zakresie mogą więc dotykać przede wszystkim konsumentów usług, co zresztą potwierdzono w samym OSR projektu.  Odnosząc się bezpośrednio do zaprezentowanego modelu oceny, w naszej ocenie:   * należy uzupełnić go o element technicznej, w tym opartej na certyfikacji. Ponadto jego zakres jest zbyt szeroki i nie odnosi się do z góry ustalonego zakresu kluczowych zasobów, pod kątem których miałaby być dokonywana ocena danego dostawcy; * skutki ewentualnych wykluczeń muszą odnosić się do z góry określonej kategorii zasobów oraz zastosowań o charakterze kluczowym dla bezpieczeństwa, co ogromnie poprawiłoby przejrzystość tej regulacji oraz pozwalało na dostosowanie strategii działania, w tym obszarze; * procedura oceny oraz jej publikacji muszą być precyzyjnie określone i umożliwiać zainteresowanym stronom przynajmniej przedstawienie stanowiska w toku oceny oraz złożenie odwołania do decyzji finalnej; | **Uwaga częścowo uwzględniona**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | Krajowy Sekretariat Łączności NSZZ Solidarność | Uwaga ogólna | **Kary – zbyt wysoki poziom kar pieniężnych**  W naszej ocenie potencjalne kary pieniężne w wys. 3 lub 1% światowego obrotu karanego podmiotu są zdecydowanie zbyt wysokie, szczególnie, że dla podmiotów publicznych mogą wynosić nie więcej niż 100 tys. zł. Stanowi to w naszej ocenie niczym nie uzasadnioną dysproporcję, szczególnie, że w obszarze bezpieczeństwa publicznego to właśnie organy i jednostki państwa mają do realizacji kluczową rolę. Postulujemy redukcję maksymalnego poziomu kar co najmniej 10-krotnie oraz wykreślenie odwołania do obrotu „światowego”. | **Uwaga nieuwzględniona**  Kary są niezbędne w celu zapewnienia skuteczności przepisów, które mają na celu ochronę bezpieczeństwa narodowego. |
|  | MJC | Uwaga ogólna | W związku z zaproszeniem społeczeństwa, przez Ministerstwo Cyfryzacji, do udziału w konsultacjach dotyczących projektu ustawy o cyberbezpieczeństwie, niniejszym wyrażam swoją dezaprobatę w stosunku do proponowanej regulacji. Projekt ustawy w obecnym brzmieniu, w mojej ocenie narusza podstawowe przepisy prawa polskiego. Koliduje z kluczowymi, konstytucyjnymi zasadami prawa. Wejście w życie tegoż projektu ustawy wywoła ryzyko naruszenia polskich przepisów.  Poniżej pozwoliłem sobie wymienić największe z moich obaw, czyli naruszenie przepisów konstytucyjnych:  1. **Zasada proporcjonalności** - Przepisy Projektu w art. 66a przyznają Kolegium, które nie jest kompetencyjnie i ustrojowo umocowane, nieograniczoną i pozbawioną kontroli sądowej kompetencję do prowadzenia jednostronnego postępowania ocennego, bez udziału ocenianego dostawcy, który o przeprowadzonej ocenie ma dowiedzieć się dopiero z komunikatu w Monitorze Polskim. Konsekwencje takiego postępowania mogą wywrzeć olbrzymi wpływ na sytuację ekonomiczną danego dostawcy, operatorów telekomunikacyjnych oraz konsumentów. Prawo odwołania od decyzji kolegium dotyczy tylko oceny określającej wysokie ryzyko, ocena określająca średnie i niskie ryzyko nie zapewnia prawa do odwołania, a ponadto odwołanie nie zawiesza wykonalności decyzji. Obecne postanowienie upoważnia Kolegium do działania we własnej sprawie, tym samym pozbawia strony zainteresowanej obiektywnej i niezależnej ochrony podstawowych praw stron w postępowaniu.  2. **Pewność prawa** - Projekt, w art. 66b zakłada rażąco niekonstytucyjny obowiązek usunięcia z rynku przejawów dotychczasowej działalności dostawcy. W związku z powyższym analizowany zakaz należy poddać kontroli w zakresie zgodności z zasadą lex retro non agit. Ustawodawca dokonując kolejnych zmian stanu prawnego musi mieć na względzie interesy podmiotów, które ukształtowały się przed dokonaniem zmiany stanu prawnego.  3. **Równość wobec prawa -** Projektowane rozwiązania w zakresie wyboru dostawcy sprzętu i oprogramowania sieci 5G pozwalają na arbitralne wykluczenie dostawców z udziału we wdrożeniu sieci 5G w oparciu o dowolne, nieokreślone kryteria. Nie przyznają przy tym dostawcom środków prawnych pozwalających na wniesienie odwołania od decyzji wykluczających. Wobec tego uznać je należy za sprzeczne z konstytucyjnymi zasadami równości wobec prawa.  **Brak przeprowadzenia analizy skutków jakie wywoła wprowadzenie regulacji -** Zmiany zawarte w projekcie nowelizacji ustawy mogą wiązać się z negatywnymi skutkami wśród społeczeństwa tj. likwidacja miejsc pracy, obniżenie dostępności nowoczesnych usług, wzrost wykluczenia cyfrowego, gospodarczymi - obniżenie konkurencyjności polskiej gospodarki, spadek zaufania inwestorów oraz wzmocnienie oligopoli i politycznymi. Wynika to z konieczności wymiany sprzętu oraz aplikacji, które są obecnie w użyciu, na alternatywne, pochodzące od innych dostawców.  Przepisów prawa konkurencji:  1. Uregulowanie kwestii wykluczenia dostawców w ustawie narusza również podstawowe zasady prawa konkurencji. Zasady i tryb postępowania w stosunku do podmiotów działających na konkurencyjnym rynku, jeżeli podmioty te naruszają przepisy reguluje inna ustawa tj. ustawa z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów, Reguluje ona w szczególności zasady i tryb postępowania w stosunku do podmiotów działających na konkurencyjnym rynku, jeżeli podmioty te naruszają przepisy tej ustawy. Oznacza to faktyczne naruszenie przez Kolegium kompetencji właściwego organu administracyjnego, jakim jest Prezes Urzędu Ochrony Konkurencji i Konsumentów.  Bez wątpienia niniejszy projekt wzbudza więcej kontrowersji i konieczna jest jego dodatkowa analiza oraz naniesienie zmian, tak aby nie wywoływał on negatywnych skutków wśród polskich obywateli. | **Uwaga częściowo uwzględniona**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | IAB Polska | Uwaga ogólna | Ustawa o Krajowym Systemie Cyberbezpieczeństwa, implementująca do polskiego porządku prawnego Dyrektywę 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, została uchwalona dwa lata temu. Okres jaki minął od implementacji skutecznie udowodnił, co jest piętą achillesową polskiego systemu cyberbezpieczeństwa tj. brak przewidzianych adekwatnych środków pieniężnych oraz problem z dostępem odpowiednio wykwalifikowanych specjalistów. Do tej pory nie udało się zakończyć procesu wyznaczania operatorów usług kluczowych oraz powołano tylko jeden zespół odpowiadający za obsługę lub wsparcie obsługi incydentów w konkretnym sektorze tj. CSIRT KNF dla sektora finansowego przy Komisji Nadzoru Finansowego.  W tych okolicznościach polski rząd planuje powołać dalsze CSIRT-y i SOC-i oraz uzupełnić krajowy system cyberbezpieczeństwa o nową grupę podmiotów, która na gruncie dotychczasowej ustawy o KSC była co do zasady sektorowo wyłączona tj. przedsiębiorców komunikacji elektronicznej. | **Wyjaśnienie**  Projekt ma celu zwiększenie cyberbezpieczeństwa na poziomie krajowym, stąd też przewiduje się powołanie CSIRT sektorowych. |
|  | IAB Polska | Uwaga ogólna | 1. **Zmiany dotyczące przedsiębiorców komunikacji elektronicznej**   Jak zostało wskazane w uzasadnieniu Projektu, coraz większe znaczenia dla bezpieczeństwa usług kluczowych ma niezawodność usług telekomunikacyjnych. W *5G Toolbox*, Państwa członkowskie zobowiązały się m.in. do zaostrzenia wymagań w zakresie bezpieczeństwa infrastruktury i usług telekomunikacyjnych. Zgodnie z uzasadnieniem Projektu, analizowane zmiany do ustawy o KSC są elementem działań na rzecz wdrożenia postanowień tego dokumentu. Projekt wdraża również postanowienia Europejskiego Kodeksu Łączności Elektronicznej.  Zgodnie z treścią Projektu, przedsiębiorcy komunikacji elektronicznej staną się częścią krajowego systemu cyberbezpieczeństwa poprzez dodanie w zakresie ustawy o KSC Rozdziału 4a „Obowiązki przedsiębiorców komunikacji elektronicznej”, w którym będą uregulowane kwestie dotyczące obowiązku stosowania przez przedsiębiorców komunikacji elektronicznej środków zapewniających bezpieczeństwo sieci i usług. IAB Polska pragnie zwrócić uwagę, że miejscem przedmiotowych regulacji dotyczących sektora telekomunikacyjnego nie powinna być ustawa o KSC, która do tej pory zawierała wyłączenie sektorowe w zakresie usług telekomunikacyjnych, ale projekt PKE.  Analizowane przepisy posługują się pojęciem przedsiębiorcy komunikacji elektronicznej dla określenia obowiązków tam zawartych. Projektowane brzmienie ustawy o KSC odwołuje się w zakresie definicji pojęcia przedsiębiorcy telekomunikacyjnego do projektu ustawy o PKE.  Zgodnie z obecnym brzmieniem art. 2 pkt 41 projektu PKE **przedsiębiorca komunikacji elektronicznej** to przedsiębiorca telekomunikacyjny lub podmiot świadczący usługę komunikacji interpersonalnej niewykorzystującej numerów. Z kolej **usługa komunikacji interpersonalnej niewykorzystująca numerów** oznacza usługę umożliwiającą bezpośrednią interpersonalną i interaktywną wymianę informacji za pośrednictwem sieci telekomunikacyjnej między skończoną liczbą osób, gdzie osoby inicjujące połączenie lub uczestniczące w nim decydują o jego odbiorcy lub odbiorcach, z wyłączeniem usług, w których interpersonalna i interaktywna komunikacja stanowi wyłącznie funkcję podrzędną względem innej usługi podstawowej, w tym usługę, która nie umożliwia realizacji połączeń z numerami z planu numeracji krajowej lub międzynarodowych planów numeracji (art. 2 pkt 77 projektu PKE).  Należy zauważyć, że pojęciu „usługi komunikacji interpersonalnej” (art. 2 pkt 77 projektu PKE) odpowiada zawarta w EKŁE definicja „usługi łączności interpersonalnej” (art. 2 pkt 5 EKŁE). Nie ulega wątpliwości, że przepisy krajowe stanowiące implementację konkretnej dyrektywy powinny być interpretowane w zgodzie z jej brzmieniem. W związku z powyższym przy interpretacji projektu PKE warto odwołać się do treści EKŁE. Motyw 17 zd. 1 EKŁE wprost wskazuje, że usługi łączności interpersonalnej obejmują wszystkie rodzaje poczty elektronicznej: „*Usługi łączności interpersonalnej są to usługi, które umożliwiają interpersonalną i interaktywną wymianę informacji, obejmujące takie usługi, jak tradycyjne połączenia głosowe między dwiema osobami, lecz również wszystkie rodzaje poczty elektronicznej, usług przekazywania wiadomości lub czatów grupowych*”.  Dodatkowo, poczta elektroniczna spełnia wszystkie przesłanki powyższych analogicznych definicji. W tym zakresie pewną trudność interpretacyjną może sprawiać jedynie przesłanka interaktywności, która jednak została wyjaśniona w przytoczonym już powyżej motywie 17 zd. 4 i 5 EKŁE – „*Łączność interaktywna oznacza, że usługa umożliwia odbiorcy informacji odpowiedź. Usługi, które nie spełniają tych wymogów, takie jak linearne usługi medialne, wideo na żądanie, strony internetowe, sieci internetowe, serwisy społecznościowe, blogi lub wymiana informacji między urządzeniami, nie powinny być uznawane za usługi łączności interpersonalnej*”. Na marginesie należy zauważyć, że poczta elektroniczna nie może mieścić się również w zakresie wyłączenia zawartego w art. 2 pkt 77 PKE tj. „usług, w których interpersonalna i interaktywna komunikacja stanowi wyłącznie funkcję podrzędną względem innej usługi podstawowej”. Nie ulega bowiem wątpliwości, że w przypadku poczty elektronicznej interaktywna komunikacja stanowi jej istotę.  Z powyższej analizy wynika, że posługiwanie się w propozycji nowelizacji ustawy o KSC pojęciem przedsiębiorcy komunikacji elektronicznej powoduje, że wskazane obowiązki znajdą zastosowanie również do podmiotów takich jak np. dostawcy poczty elektronicznej, co należy uznać za podejście zbyt daleko idące. Projekt nowelizacji ustawy o KSC zakłada nałożenie na podmioty świadczące usługi komunikacji interpersonalnej niewykorzystujące numerów analogicznych obowiązków jak na przedsiębiorców telekomunikacyjnych.  W ocenie IAB zasadne jest w tym miejscu zaprezentować analogiczne stanowisko jak w przypadku projektu PKE. Przepisy ustawy o KSC uwzględniając regulacje zawarte w EKŁE powinny różnicować obowiązki dostawców usług lub sieci telekomunikacyjnych (nakładać dalej idące obowiązki) oraz dostawców usług łączności interpersonalnej niewykorzystującej numerów (nakładać obowiązki o mniejszym zakresie). Potwierdza to motyw 95 EKŁE, zgodnie z którym:  *„Z uwagi na rosnące znaczenie usług łączności interpersonalnej niewykorzystujących numerów należy zapewnić aby podlegały one również odpowiednim wymogom bezpieczeństwa zgodnie z ich specyficznym charakterem i istotną rolą w gospodarce. Dostawcy usług powinni również zapewnić poziom bezpieczeństwa proporcjonalny do istniejącego ryzyka. Ze względu na to, że dostawcy usługi interpersonalnej łączności niewykorzystujące numerów zazwyczaj nie sprawują rzeczywistej kontroli nad transmisją sygnałów w sieciach, stopień ryzyka w przypadku takich usług można uznać za niższy pod pewnymi względami niż w przypadku tradycyjnych usług łączności elektronicznej. Dlatego też, jeżeli tylko jest to uzasadnione aktualną oceną ryzyka dla bezpieczeństwa, środki podejmowane przez dostawców usługi interpersonalnej łączności niewykorzystujące numerów powinny być łagodniejsze. Takie samo podejście powinno być stosowane odpowiednio do usług łączności interpersonalnej wykorzystującej numery, jeżeli dostawca nie sprawuje rzeczywistej kontroli nad transmisją sygnału”.*  W związku z powyższym IAB Polska postuluje, aby regulacje wdrażane do ustawy o KSC nie wychodziły poza ramy regulacyjne wynikające z dyrektywy EKŁE, gdyż **zrównywanie obowiązków w zakresie bezpieczeństwa sieci i usług dla wszystkich przedsiębiorców komunikacji elektronicznej nie znajduje uzasadnienia,** natomiast może prowadzić do zaburzenia zasad konkurencyjności poprzez niepotrzebne obciążanie dodatkowymi obowiązkami przedsiębiorców nie sprawujących rzeczywistej kontroli nad transmisją danych. Należy tutaj zauważyć, że w sposób oczywisty realizacja nowych obowiązków pociąga za sobą konieczność poniesienia dodatkowych i wysokich kosztów w zakresie wdrożenia odpowiednich rozwiązań. Postulujemy zatem, aby dostawcy usług komunikacji elektronicznej, którzy nie sprawują rzeczywistej kontroli nad transmisją sygnału, w tym w szczególności dostawcy usług komunikacji interpersonalnej niewykorzystującej numerów byli zwolnieni z obowiązków w zakresie bezpieczeństwa sieci i usług przewidzianych w projektowanym rozdziale 4a nowelizacji KSC. Obowiązki te są właściwe jedynie dla przedsiębiorców telekomunikacyjnych sprawujących kontrolę nad sygnałem i posiadających właściwe ku takiej kontroli środki lub których podjęcie uzasadnia charakter dostarczanych przez nich usług i znajduje oparcie w EKŁE. Warto zauważyć, że zachowanie ciągłości dostarczania sieci telekomunikacyjnej powinno spoczywać na dostawcy usług telekomunikacyjnych a nie bezpośrednio oddziaływać również na korzystających z takiej sieci dostawców usług OTT. Należy zwrócić uwagę, że o ile operatorzy telekomunikacyjni dysponują całością infrastruktury technicznej, to już np.: operatorzy poczty elektronicznej nie mają na nią wpływu i funkcjonują na „cudzym” sprzęcie lub dostępie.  Objęcie tymi samymi obowiązkami co dostawca telekomunikacyjny dostawcy poczty elektronicznej czy czatu wydaje się nie tyle nieuzasadnione co wręcz szkodliwe i niebezpieczne dla zasad prawa konkurencji oraz wolności gospodarczej na rynku usług komunikacji elektronicznej a przede wszystkim nie spełnia intencji stojącej za regulacjami wynikającymi z EKŁE. Dolegliwości finansowe wynikające z konieczności spełnienia nowych obowiązków przez dostawców usług komunikacji interpersonalnej niewykorzystującej numerów mogą prowadzić do tego, że rachunek ekonomiczny dalszego prowadzenia takiej usługi będzie nieopłacalny. Zimniejszy się tym samym katalog oferowanych usług, ich różnorodność oraz próg dostępu dla użytkowników końcowych, co wiąże się nie tylko ze stratą dla nich ale i dla krajowej przedsiębiorczości i konkurencyjności na rynku europejskim.  Dodatkowo, Projekt wydaje się być niekompatybilny z przepisami projektu PKE. Przykładowo, projektowany artykuł 20c ustawy o KSC odwołuje się do przedsiębiorcy komunikacji elektronicznej, o którym mowa w art. 47 ust. 1 projektu PKE. Tymczasem wskazany przepis PKE dotyczy wyłącznie przedsiębiorcy telekomunikacyjnego, czyli nie całej kategorii przedsiębiorców komunikacji elektronicznej.  Mając na uwadze powyższe należy skonstatować, że przedstawiony do konsultacji projekt zmiany ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy – Prawo zamówień publicznych z dn. 7 września 2020 r. jest pełen terminologicznych niejasności i nieprzystających do praktyki rynkowej rozwiązań i obowiązków, co pozwala sądzić, że ujęcie w rozdziale 4a usług komunikacji interpersonalnej, w tym poczty elektronicznej czy innych usług OTT, jest oczywistym przeoczeniem | **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 przez ustawę wprowadzającą PKE.  Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowym.  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.  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 (co jest w ich dobrym interesie) a zgłaszać do CSIRT Telco i CSIRT poziomu krajowego te incydenty telekomunikacyjne, które będą spełniać progi incydentu. |
|  | Federacja Konsumentów | Uwaga ogólna | Z zadowoleniem dostrzegamy inicjatywę zapewnienia bezpieczeństwa świadczonych usług elektronicznych, w tym telekomunikacyjnych, oraz świadomego i odpowiedzialnego korzystania z nowoczesnych technologii. Bezpieczeństwo 5G jest dziś szczególnie ważne, zwłaszcza w kontekście wszechobecnych *fake newsów* dotyczących wpływu 5G na zdrowie i prywatność konsumentów.  Jednocześnie apelujemy do Resortu o to, aby skutki wprowadzanych w tym zakresie rozwiązań nie oddziaływały negatywnie na konsumentów. Wiemy z doświadczenia, że za każdy, nawet najbardziej zasadny, obowiązek nałożony na przedsiębiorców, skutkujący koniecznością rozbudowania struktur czy wdrożenia dodatkowych rozwiązań, zawsze finalnie płaci klient w opłacie za otrzymaną usługę. Analiza konsultowanego Projektu, prowadzi do wniosku, że Krajowy System Cyberbezpieczeństwa po noweli będzie przedsięwzięciem kosztownym, którego skutki są trudne do przewidzenia. Równocześnie dostrzegamy, że przedstawiona wraz z Projektem Ocena Skutków Regulacji nie uwzględnia analizy wpływu projektowanych przepisów na dostępność i zwłaszcza koszty usług dla konsumentów w wyniku wprowadzenia przedmiotowych przepisów. | **Wyjaśnienie**  OSR został uzupełniony o analizę wpływu projektowanych przepisów na konsumentów.  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 przekazanym 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.  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. |
|  | Federacja Konsumentów | Uwaga ogólna | Federacja Konsumentów popiera objęcie Krajowym System Cyberbezpieczeństwa podmiotów działających na rynku telekomunikacyjnym z uwagi na przedmiot ich działalności i zakres świadczonych usług, ale jednocześnie dostrzega, że inwestycje związane z realizacją takiej sieci, w tym jej modernizacją i remontem, są kosztowne i długotrwałe. Należy więc mieć na uwadze, że obowiązek zaprzestania w terminie 5 lat od oceny ryzyka korzystania ze sprzętu lub oprogramowania określonego dostawcy będzie skutkował w praktyce wymianą znacznej części funkcjonującej w Polsce infrastruktury, co zapewne w naturalny sposób przełoży się na koszty świadczenia usług dla odbiorcy końcowego. Skutki tego typu rozwiązań mogą być podwójnie dotkliwe dla konsumenta, gdyż z jednej strony prawdopodobnie nastąpi wzrost cen usług, a z drugiej może dojść do pogorszenia ich jakości w okresie reorganizacji sieci i opóźnienia we wdrożeniu 5G z powodu konieczności przebudowy sieci LTE.  W związku z przedstawionymi powyżej wątpliwościami Federacja Konsumentów stoi na stanowisku, że nowelizacja ustawy nie powinna powodować pogorszenie jakości i wzrost kosztów usług dla konsumentów. Z braku możliwości szczegółowej analizy Projektu ze względu na krótki czas trwania konsultacji, jednocześnie chcąc uniknąć wymienionych powyżej negatywnych konsekwencji, jako minimum wnosimy o rozważenie możliwości wydłużenia terminu na ewentualne wycofanie sprzętu albo oprogramowania dostawców objętych oceną wysokiego ryzyka o 5 lat, czyli łącznie do lat 10, co pozwoli na rozłożenie negatywnych skutków w czasie i mitygację wyżej wspomnianych ryzyk. Akceptowalne ceny usług świadczonych w oparciu o 5G są bowiem warunkiem koniecznym, aby korzyści z wdrożenia były wiodącym przekazem, w miejsce tego, o czym słyszymy i czytamy dzisiaj, a więc wspomnianej wyżej fali niepopartych żadnymi dowodami spekulacji o zagrożeniach.  Jednocześnie, zwracamy uwagę, że globalny rynek technologii, opartej o dostawy sprzętu i oprogramowania przez międzynarodowe korporacje, może być trudny do przewidzenia w dłuższym horyzoncie czasowym. Nie można wykluczyć sytuacji, w której dostawca mający obecnie siedzibę na terenie państwa członkowskiego UE lub NATO przejdzie w wyniku zmian właścicielskich w ręce nowych właścicieli spoza tego obszaru, co mogłoby spowodować potrzebę kolejnej rewolucji w już zainstalowanym sprzęcie i oprogramowaniu. Stąd, oprócz kryteriów geograficznych lub geopolitycznych zasadnym wydaje się uwzględnienie w projekcie ustawy również innych kryteriów, takich jak certyfikacja bezpieczeństwa oparta o międzynarodowe standardy, promowanie otwartych interfejsów przy budowaniu sieci 5G oraz dywersyfikacja dostawców na poziomie sieci krajowej i poszczególnych sieci operatorskich na etapie budowy sieci.  Deklarujemy wsparcie i dalszą współpracę w analizie i tworzeniu rozwiązań pro-konsumenckich. | **Uwaga częściowo uwzględniona**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | Stowarzyszenie „Miasta w Internecie” | Uwaga ogólna | W naszej opinii dynamicznie rozwijające się sektory gospodarki, w tym sektor IT wymagają stałej modernizacji ram instytucjonalno-prawnych, z czego wynika konieczność prowadzenia dyskusji nad kierunkami regulacji obejmującej możliwie szeroką grupę podmiotów. Cyberbezpieczeństwo bowiem dotyczy zarówno wielkich podmiotów takich jak dostawców sprzętu czy operatów, ale także konsumentów, takich m.in. jak samorządy lokalne. Regulacje powinny być wyważone, precyzyjne i niedyskryminujące, tak aby zapewnić ochronę interesów podmiotów o słabszej pozycji rynkowej.  W tym kontekście na szczególną uwagę i analizę zasługuje projektowane rozwiązanie, w myśl którego szerokie kompetencje zyskuje Kolegium ds. Cyberbezpieczeństwa, będące – w świetle zapisów projektu ustawy - ciałem politycznym, nie zaś eksperckim. Kolegium zyskuje narzędzie do eliminowania z rynku podmiotów w oparciu o niesprecyzowane kryteria. Zakłada np. sporządzenie, na wniosek członka Kolegium, ocenę ryzyka dostawcy sprzętu lub oprogramowania istotnego dla cyberbezpieczeństwa podmiotów krajowego systemu cyberbezpieczeństwa.  Ocena taka uwzględnić ma m.in. prawdopodobieństwo pozostawania przez dostawcę sprzętu lub oprogramowania pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, a ponadto uwzględnia:   * • stopień i rodzaj powiązań pomiędzy dostawcą sprzętu lub oprogramowania i tym państwem, * • prawodawstwo tego państwa w zakresie ochrony praw obywatelskich i praw człowieka.   Nie są to kryteria o charakterze technicznym, ale raczej natury uznaniowej, politycznej. W naszym przekonaniu regulacja winna zawierać kryteria odnoszące się do specyfikacji technicznej weryfikowalne merytorycznie. Dlatego też ocena powinna obejmować normy techniczne oraz właściwe certyfikacje.  Sporządzona przez Kolegium ocena ryzyka dostawcy sprzętu lub oprogramowania może określić ryzyko: na niezidentyfikowanym poziomie, niskie, umiarkowane lub wysokie.  W tym ostatnim wypadku podmioty krajowego systemu cyberbezpieczeństwa nie mogą wprowadzać do użytkowania sprzętu, oprogramowania i usług określonych w ocenie danego dostawcy sprzętu lub oprogramowania oraz zobowiązane są wycofać 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.  Rozwiązanie to może pociągać za sobą – jak deklarują operatorzy i eksperci rynku telekomunikacyjnego – nieporównywalnie wysokie koszty dla rynku. Koszt zastąpienia urządzeń dominującego producenta nowymi oznaczać może nawet podwojenie pierwotnych kosztów wdrożenia. A zakaz wprowadzania sprzętu, oprogramowania lub usług, oraz obowiązek ich wycofania, de facto zmniejszy liczbę dostawców, a więc konkurencję na rynku. To z kolei może doprowadzić do obciążenia konsumentów, co nie pozostanie bez negatywnego wpływu na rozwój gospodarki w tym sektorze. Opóźnienia we wdrożeniu infrastruktury 5G mogą natomiast zagrozić zachowaniu ciągłości usług wobec wyczerpywania się zdolności rozwiązań 4G do zaspakajania rosnącego popytu.  Warto również zwrócić uwagę na tryb i procedura postępowania odwoławczego od sporządzonej przez Kolegium oceny ryzyka. Wątpliwości budzi przede wszystkim rozwiązanie przewidujące, iż odwołanie wnosi się do Kolegium, zatem ten sam organ, który sporządzał ocenę ryzyka będzie orzekał o słuszności wydanego przez siebie rozstrzygnięcia.  Dostawca sprzętu lub oprogramowania będzie mógł odwołać się w ciągu zaledwie 14 dni od publikacji komunikatu o sporządzonej ocenie do Kolegium. Kolegium będzie miało natomiast aż 2 miesiące od otrzymania odwołania na jego rozpatrzenie.  Jest to okres relatywnie długi, jednak uwzględniający specyfikę tego sektora gospodarki. Natomiast przy obecnych zapisach projektu ustawy pozycja dostawcy w tym postępowaniu jest słaba. Zgodnie zaś z elementarnymi zasadami postępowania administracyjnego, stronie winno się zagwarantować możliwość czynnego udziału w postępowaniu. Ponadto czas rozpatrywania odwołania może negatywnie oddziaływać na kondycję dostawcy.  Funkcjonowanie na rynku jak największej liczby dostawców sprzętu, oprogramowania i usług ma wielkie znaczenie dla tempa wdrażania w Polsce sieci 5G. Dlatego też zmiany powinny być ukierunkowane na stworzenia takich warunków, które zachęcałyby do wejścia na rynek także nowe podmioty, a klimat panujący na rynku pobudzał rozwój sektora.  Bez wątpienia analizie należy także poddać kompetencje Pełnomocnika do wydawania ostrzeżeń i poleceń zabezpieczających. Ostrzeżenia wydają się być pozytywnym rozwiązaniem, w ramach którego zabezpieczane są interesy konsumentów. Dają bowiem słabszym rynkowo podmiotom wiedzę o ryzyku wiążącym się z pewnymi podmiotami. Natomiast rozwiązanie w postaci poleceń zabezpieczających wydawanych w oparciu o niejasne kryteria mogą doprowadzić do arbitralnego nakazywania przez Pełnomocnika zachowań takich jak np. zakaz połączeń z określonymi adresami IP lub nazwami URL.  Ograniczenie liczby dostawców technologii 5G w połączeniu ze zmianami na rynku telekomunikacyjnym może doprowadzić do opóźnień we wdrożeniu sieci 5G w Polsce, a tym samym do zmniejszenia się konkurencyjności polskiej gospodarki oraz obniżenia jakości życia mieszkańców. Rozwój technologii 5G stymulować będzie z pewnością tworzenie nowych miejsc pracy oraz rozwój innych dziedzin cyfrowych powiązanych z korzystaniem z 5G.  Warto również rozważyć kwestię regulacji obowiązków przedsiębiorców komunikacji elektronicznej wyłącznie na gruncie projektowanej ustawy – Prawo Komunikacji Elektronicznej. Projektowana ustawa ma kompleksowy charakter a przewidziane na jej gruncie kompetencje regulatora, jakim jest Prezes Urzędu Komunikacji Elektronicznej, wydają się w sposób efektywny zapewniać bezpieczeństwo infrastruktury telekomunikacyjnej. | **Uwaga częściowo uwzględniona**  Przepisy art. 66a-66c zostały 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 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3.  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. Zatem także minister właściwy ds. informatyzacji będzie podejmował decyzje o ewentualnych karach także w formie decyzji administracyjnej. Przepis art. 73 został uzupełniony o wysokość kary za nie zastosowanie się do polecenia zabezpieczającego.  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 Zepole 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. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Stowarzyszenie Inżynierów Telekomunikacji | Uwaga ogólna | Z przedstawionego projektu ustawy i zaproponowanych rozwiązań wynika, że zostały one przygotowane z pominięciem niektórych ważnych aspektów dotyczących budowy i funkcjonowania sieci telekomunikacyjnej, wykorzystywanej do świadczenia usług mobilnych. Wprowadzanie nowych regulacji, które będą rzutować na strukturę sieci i które będą determinować wybór producentów dostarczających poszczególne elementy tej sieci, musi  uwzględniać ryzyko jakie niesie ze sobą tego typu regulacja – nie chodzi tu wyłącznie o ryzyko biznesowe właścicieli infrastruktury, ale przede wszystkim o ryzyko dotyczące zapewnienia  stałej, jakościowo najlepszej pracy tych sieci i obsługi użytkowników końcowych. Zwracamy uwagę na fakt, że proponowany, nowy art. 66b w ustawie o cyberbezpieczeństwie, może mieć  dalekosiężne skutki dla pracy całej sieci przedsiębiorcy telekomunikacyjnego, których w całości z góry nie można przewidzieć. Konstrukcja i architektura sieci telekomunikacyjnych to  skomplikowany organizm, w którym nie można dowolnie i bezkonsekwencji wymieniać jednych elementów bez uwzględnienia ich wpływu na inne elementy.  Poniżej przedstawiamy zatem podstawowe wyjaśnienia w tej kwestii:  Każda sieć komórkowa (w uproszczeniu odpowiednim do jasności wyjaśnienia problemu) może być podzielona na trzy warstwy – szkieletową, transmisyjną i dostępową. Każda z nich  jest równie ważna i każda odpowiada za inne działania.  **1. Warstwa szkieletowa** – jest „trzonem” sieci komórkowej. To ona determinuje zasady cyberbezpieczeństwa dla wszystkich pozostałych warstw sieci, odpowiada za prawidłowe i poprawne działanie tych warstw. Na warstwę szkieletową składają się centra danych umieszczone w kilku lokalizacjach w Polsce.  W warstwie szkieletowej znajdują się informacje i zasady umożliwiające prawidłowe kierowanie ruchu telekomunikacyjnego do i od użytkowników. Warstwa szkieletowa stanowi również *jedyny punkt styku ze światem zewnętrznym tj. sieciami innych*  *operatorów telekomunikacyjnych, zagranicznych i krajowych oraz z Internetem.* Dlatego też to właśnie w warstwie szkieletowej znajdują się elementy dedykowane dokontroli cyberbezpieczeństwa – tzw. firewalls.  **2. Warstwa transmisyjna** – odpowiada za transport sygnałów telekomunikacyjnych pomiędzy scentralizowaną warstwą szkieletową oraz rozproszoną warstwą dostępową. Warstwa ta jest zbudowana z łączy światłowodowych lub łączy radiowych o różnych  klasach przepustowości oraz elementów przełączających (*switch)* odpowiadających za kierowanie sygnału transmisyjnego odpowiednią drogą. Łącza transmisyjne oraz elementy *switch* są budowane w oparciu o sprzęt wielu dostawców, ponieważ sposób transmisji sygnału jest wysoce ustandaryzowany i nie powoduje problemów  integracyjnych z pozostałymi elementami sieci.  **3. Warstwa dostępowa** – jest odpowiedzialna za działanie łącza radiowego pomiędzy terminalem użytkownika a siecią komórkową. Na warstwę tą składają się stacje bazowe znajdujące się na terenie całego kraju. Każda stacja bazowa składa się z:  elementów pasywnych – stanowiących konstrukcję nośną dla urządzeń  telekomunikacyjnych (np. maszt, wspornik itp.);  anten nadawczo-odbiorczych wraz z przetwornikami radiowymi RRU (RRUremote  radio unit) – instalowanych osobno dla każdego pasma częstotliwości (np.  900 MHz, 1800 MHz, 2600 MHz) odpowiedzialnych za prawidłową transmisję  sygnału;  modułu przetwarzania sygnału BBU (BBU – baseband unit) – odpowiedzialnego za kontrolę wszystkich systemów znajdujących się na danej stacji bazowej (2G/3G/4G) oraz przetwarzanie sygnału w taki sposób, aby mógł być odczytany wwarstwie szkieletowej.  Z uwagi na konstrukcję stacji bazowej i wymienione powyżej elementy, bez których nie  może ona działać, w praktyce konieczne jest, aby całość systemów anten i przetworników, jak również moduł przetwarzania sygnału BBU były zapewnione przez jednego dostawcę sprzętu. Pozwala to na obsługę wszystkich systemów przez jeden moduł przetwarzania sygnału BBU oraz aktywne współdziałanie poszczególnych  systemów (np. w przypadku, gdy jeden jest przeciążony). Realizacja jednej stacji bazowej przy użyciu poszczególnych jej elementów pochodzących od różnych dostawców jest z punktu widzenia planowania takich inwestycji ryzykowna, nieekonomiczna i niegwarantująca prawidłowej i efektywnej jakościowo pracy stacji  bazowej. Z tego względu w praktyce, nie stosuje się takich rozwiązań.  Przed operatorami telekomunikacyjnymi, właścicielami sieci, stoi w najbliższym czasie ogromne wyzwanie, jakim będzie wprowadzenie standardu 5G. Technologia ta będzie wymagać kolejnych ogromnych nakładów inwestycyjnych na sieci telekomunikacyjne.  Immanentną cechą systemów mobilnych jest istnienie dużej liczby stacji bazowych, które pozwalają zapewnić pokrycie sygnałem radiowym (tzw. zasięgiem sieci komórkowej) na terenie całego kraju, co oznacza, że inwestycje w standard 5G będą największe w warstwie  dostępowej. We wszystkich istniejących lokalizacjach konieczne będzie zainstalowanie nowych anten nadawczo-odbiorczych oraz przetworników radiowych RRU dla częstotliwości dedykowanych standardowi 5G (tj. 700 MHz, 3.4-3.8 GHz, 26 GHz). Jednocześnie będzie musiało dojść do rozbudowy modułów przetwarzania sygnału BBU o dodatkowe moce obliczeniowe oraz funkcjonalności wprowadzane przez standard 5G. Dodatkowo, z uwagi na  dużo krótsze zasięgi częstotliwości (w szczególności w pamie 26 GHz) niż ma to miejsce w przypadku obecnie wykorzystywanych pasm (tj. od 800 MHz do 2.6 GHz) – poza zmianami na istniejących obiektach – niezbędne będzie wybudowanie wielu nowych stacji bazowych.  Kluczowe w tym aspekcie jest uświadomienie sobie, że standard 5G przewiduje ścisłą korelację z istniejącą technologią 4G. Współpraca tych standardów zależy od współistnienia we wspólnym module przetwarzania sygnału BBU, a ten moduł pochodzi od danego dostawcy (tak jak to wyjaśniono powyżej). To oznacza, że wszystkie elementy telekomunikacyjne (tj. 2G/3G/4G oraz 5G) danej stacji bazowej powinny być dostarczone przez jednego dostawcę  (producenta), co pozwoli stacji w pełni korzystać ze wszystkich funkcjonalności standardu 5G o najwyższych parametrach. Brak takiego podejścia odbije się negatywnie na jakości usług  świadczonych przez operatora, co jest sprzeczne samo w sobie z inwestowaniem i wprowadzaniem nowej, lepszej technologii.  Sytuacja, w której nowy sprzęt niezbędny do funkcjonowania standardu 5G w sieci operatora pochodzić będzie musiał od innego dostawcy niż sprzęt obecnie przez niego używany, wymusi na nim konieczność utrzymywania oddzielnych sieci telekomunikacyjnych. Jedna sieć będzie zgodna ze zintegrowanymi standardami 2G/3G/4G, a druga ze standardem 5G. Z technicznego punktu widzenia powodzenie uruchomienia technologii 5G zależy od jej bezbłędnej współpracy z technologią 4G, co możliwe jest jedynie w przypadku, gdy obie technologie będą pochodziły od tego samego producenta.  Podkreślamy, że ***o poziomie cyberbezpieczeństwa standardu 5G (jak również w przypadku pozostałych technologii) będą decydowały rozwiązania wybrane do rozbudowy warstwy szkieletowej, a nie dostępowej****.* Jak już powyżej wskazano to warstwa szkieletowa  pełni nadrzędna rolę w architekturze sieci i to ona komunikuje się z innymi sieciami i otoczeniem zewnętrznym. Nowoczesne sieci telekomunikacyjne są zaprojektowane i zbudowane tak, aby w maksymalnym stopniu zapewnić bezpieczeństwo i prywatność danych  użytkowników oraz integralność transmisji. W tym celu standardy sieci telekomunikacyjnych, w szczególności sieci komórkowych, przewidują wykorzystanie zaawansowanych algorytmów  szyfrowania kanału transmisyjnego – bardzo często opartych o 128- lub 256-bitowe klucze szyfrujące – podczas aktywności użytkowania (rozmowy, korzystania z Internetu, wysyłania wiadomości, itp.) na całym odcinku od urządzenia klienta wyposażonego w kartę SIM, na  którym są zapisane właściwe tylko dla tego użytkownika specjalne klucze szyfrujące, aż do odpowiednich urządzeń w sieci szkieletowej. W związku z tym, naruszenie integralności transmisji danych polegające np. na podsłuchaniu rozmowy lub nieautoryzowanym przejęciu danych podczas transmisji radiowej jest w praktyce mało prawdopodobne.  Powyżej przedstawiono uzasadnienie, z którego wynika, że kwestia doboru dostawców sprzętu w warstwie dostępowej nie ma istotnego znaczenia dla poziomu cyberbezpieczeństwa sieci  komórkowej. Za cyberbezpieczeństwo sieci odpowiadają głównie elementy sieci szkieletowej oraz algorytmy zaimplementowane w urządzeniach końcowych. Odnosząc powyższe do  powołanego na wstępie planowanego do wdrożenia art. 66b ustawy o cyberbezpieczeństwie, uważamy, że w praktyce zakaz wprowadzania części zamiennych sprzętu lub oprogramowania  wskazanych w ocenie wysokiego ryzyka, jak również wycofanie z użytkowania takiego sprzętu lub oprogramowania, nie później niż 5 lat od ogłoszenia komunikatu o ocenie, będzie  skutkować wyłączeniem części lub nawet całości sieci ze świadczenia usług. Ponadto całkowite wyłączenie określonego sprzętu lub oprogramowania w okresie 5 lat wymagać będzie  reorganizacji sieci, z uwagi na konieczność wymiany sprzętu na nowy, także wówczas, gdy przed upływem tych 5 lat jedynie poszczególne elementy sieci będą wymagały wymiany na nowe w całości lub w części. Należy również zwrócić uwagę na sytuację, w której  wprowadzenie do użytkowania nowego sprzętu lub oprogramowania związane jest z usunięciem awarii sieci lub naprawy gwarancyjnej danego elementu sieci. W takiej sytuacji przepis nie pozwoli na naprawę, nakazuje wymianę elementu sieci na nowy (od innego  dostawcy), bez jakiejkolwiek dopuszczalności odstępstw w przypadku, gdyby taka wymiana była z punktu widzenia działania sieci, technicznie lub technologicznie niemożliwa. Zwracamy  uwagę, że zmiana dostawcy w warstwie dostępowej dla sprzętu 5G wymagałaby wymiany wszystkich pozostałych systemów (2G/3G/4G) dla uzyskania optymalnego efektu – czyli *de* *facto* wymianę całej sieci dostępowej, co dla operatorów jest przedsięwzięciem niewykonalnym bez znacznego spadku jakości usług oferowanych klientom. | **Uwaga częściowo uwzględniona**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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 nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. |
|  | Uniwersytet Jagielloński Collegium Medicum | Uwaga ogólna | Chcieliśmy wyrazić swoje obawy w kilku kwestiach, takich jak choćby:  a) naruszanie przez projekt zasad uczciwej konkurencji i równego traktowania podmiotów;  b) wpływanie przez Kolegium w sposób niejasny i bez szczegółowych wytycznych (technicznych) na podmioty w branży;  c) pozbawienie prawa do odwołania od decyzji Kolegium w przypadku ocen określających średnie i niskie ryzyko;  d) Relatywnie krótki termin wycofania z rynku sprzętu, oprogramowania i usług w przypadku wydania niekorzystnej oceny przez Kolegium oraz wysokie koszty wycofywania z rynku sprzętu i oprogramowania  **a) Naruszanie przez projekt zasad uczciwej konkurencji i równego traktowania podmiotów.** Polski rynek jest obecnie jednym z najbardziej atrakcyjnych przestrzeni inwestycyjnych dla branży. Dzisiaj jesteśmy państwem, z którym handluje się w sposób wolny i przejrzysty, mamy przepisy gwarantujące inwestorom uczciwą konkurencję, wolny rynek i sprawiedliwe traktowanie. Proponowany kształt nowych przepisów znacząco wpływa na te atuty, które  stanowią podstawowe przymioty w każdym demokratycznym państwie. Zagraniczny kapitał jest bardzo wrażliwy na tego rodzaju regulacje. Jesteśmy pewni, że w przypadku wprowadzenia przepisów w proponowanym kształcie przełożą się one na rozwój zarówno polskiego przemysłu, sektora usług ale także na życie polskich obywateli.  **b) Wpływanie przez Kolegium w sposób niejasny oraz bez szczegółowych wytycznych (technicznych) na podmioty w branży.** W myśl projektu Kolegium dostałoby bardzo szerokie, niejasne, niekontrolowane przez żaden zewnętrzny podmiot uprawnienia do wpływania na konkretnego dostawcę. To z kolei w dalszej kolejności przekłada się na inne podmioty gospodarcze, a na samym końcu na konsumenta. Postępowanie które pozbawia prawa do możliwości składania wyjaśnień wydaje się wysoce niesprawiedliwe. Natomiast pozbawienie możliwości odwołania (w niektórych przypadkach) zgodnie z przepisami KPA wyraźnie narusza porządek prawny oraz zasady równego traktowania zagwarantowane w Konstytucji. Proponowane przepisy stworzą potencjalne ryzyko wpływania w sposób nieuczciwy i niezgodny z prawem na podejmujących decyzję w sprawie oceny. Powstanie szczegółowych wytycznych – jasnych, obiektywnych kryteriów oceny powinno zminimalizować to ryzyko.  **c)pozbawienie prawa do odwołania od decyzji Kolegium w przypadku ocen określających średnie i niskie ryzyko.** Każdy podmiot – zarówno w przypadku oceny określającej wysokie ryzyko, jak i ocen określających średnie i niskie ryzyko - powinien mieć takie same możliwości odwoławcze od oceny. Blokowanie możliwości odwoławczych niektórych z nich wpływa przede wszystkim na równość podmiotów względem innych. Każdy zasługuje na możliwość odwołania od oceny, która w założeniu nowych przepisów ma się odbywać bez udziału zainteresowanego podmiotu. Odwołanie powinno zawieszać postępowanie do czasu wydania prawomocnego wyroku w sprawie przez sąd powszechny w myśl przepisów KPA. Taki stan rzeczy byłby w sposób oczywisty najbardziej sprawiedliwy.  **d)Relatywnie krótki termin wycofania z rynku sprzętu, oprogramowania i usług w przypadku wydania niekorzystnej oceny przez Kolegium oraz wysokie koszty wycofywania z rynku sprzętu i oprogramowania.** Pięcioletni termin wycofania z rynku jest bardzo krótkim terminem na wycofanie z rynku całego sprzętu, oprogramowania i usługi z rynku. Proponujemy termin 10–cio letni, który jest dużo bardziej adekwatny do sytuacji. Należy pamiętać o tym, że operatorzy poniosą również gigantyczne koszty związane wprost z nowymi przepisami i w żaden sposób przez siebie nie zawinione. Dlatego też rząd powinien  wprowadzić rekompensaty dla tych podmiotów, które takie koszty będą musiały ponieść. Oczywistym jest, że każdy podmiot który poniesie takie straty będzie szukał możliwości ich odrobienia. To z kolei wprost przełoży się na ceny usług dla końcowego odbiorcy, czyli obywatela. Sam termin 5–cio letni jest tak krótki, że może również wpłynąć na stabilność sieci, która będzie miała również szeroko idące konsekwencje.  W związku ze wszystkimi powyżej przytoczonymi argumentami, będziemy ogromnie wdzięczni za uwzględnienie przedstawionych propozycji zmian w treści projektowanych przepisów. Jedynie sprawiedliwe, przejrzyste i obiektywne mechanizmy ustawowe dadzą pozytywny skutek zarówno dla przedsiębiorców, jak i dla obywateli. Wierzymy, że zagadnienia na które zwracamy uwagę będą przyczyną do poddania ponownej analizie oraz weryfikacji tych projektowanych przepisów, które naszym zdaniem mogą wpływać negatywnie na sposób funkcjonowania ustawy w praktyce. | **Uwaga częściowo uwzględniona**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | Sektorowa Rada ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo  Sektorowa Rada ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo | Uwaga ogólna | Rolą Sektorowej Rady ds. kompetencji Telekomunikacja i Cyberbezpieczeństwo jest przede wszystkim działanie na styku edukacji i praktyki w obu wskazanych dziedzinach. Obejmuje to m. in. rekomendowanie rozwiązań legislacyjnych w obszarze edukacji i dostosowanie do potrzeb rynku pracy oraz formułowanie rekomendacji dotyczących zapotrzebowania na kompetencje w danym sektorze. Z powyższych względów, w kręgu zainteresowania Rady są wszelkie rozwiązania legislacyjne, które mają wpływ na kształt rynku pracy oraz potrzeby edukacyjne w dziedzinie telekomunikacji i cyberbezpieczeństwa.  Sektorowa Rada do spraw Kompetencji Telekomunikacja i Cyberbezpieczeństwo uczestniczy w konsultacjach i wypracowuje rekomendacje zmian regulacji m.in. organizując konferencje naukowe ekspertów z administracji, biznesu i edukacji.  Debaty skupiają się na problemach kompetencji w ich podwójnym znaczeniu: „wiedzy i umiejętności” oraz „uprawnień i obowiązków” a także na elementach „siatki pojęciowej” w regulacjach, które dotyczą obu dziedzin.  Rada była głównym organizatorem konferencji „Leksykon cyberbezpieczeństwa” (31.07.2020), „Działalność w zakresie cyberbezpieczeństwa. Aspekty prawne, organizacyjne i techniczne”, 7.08.2020 oraz „Potrzeby kompetencyjne w zakresie cyberbezpieczeństwa i łączności elektronicznej w świetle planowanych zmian w przepisach” (2.10.2020), podczas których omawiano m. in. kwestie związane z kwalifikacjami i kompetencjami w związku z projektem nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa. Rezultatem konferencji są poniższe uwagi i propozycje do ww. projektu.  Problemy definicyjne  W pierwszej kolejności, Rada pragnie zwrócić uwagę na problemy związane z definiowaniem cyberbezpieczeństwa w różnych aktach prawnych. 2  W ustawie o krajowym systemie cyberbezpieczeństwa (UKSC) cyberbezpieczeństwo jest definiowane jako odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy (art. 2 pkt 4). Definicja ta jest zbliżona do definicji „bezpieczeństwa sieci i systemów informatycznych” zawartej w art. 4 ust. 2 Dyrektywy NIS, które „oznacza odporność sieci i systemów informatycznych, przy danym poziomie zaufania, na wszelkie działania naruszające dostępność, autentyczność, integralność lub poufność przechowywanych lub przekazywanych, lub przetwarzanych danych lub związanych z nimi usług oferowanych lub dostępnych poprzez te sieci i systemy informatyczne”. Pomimo, że UKSC to implementacja Dyrektywy NIS to jednak powyższe, zasadnicze pojęcia są określane i definiowane w różny sposób.  W akcie o cyberbezpieczeństwie (Rozporządzenie 2019/881), „cyberbezpieczeństwo” oznacza działania niezbędne do ochrony sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób przed cyberzagrożeniami (art. 2 ust. 1). „Cyberzagrożenie” oznacza wszelkie potencjalne okoliczności, zdarzenie lub działanie, które mogą wyrządzić szkodę, spowodować zakłócenia lub w inny sposób niekorzystnie wpłynąć w przypadku sieci i systemów informatycznych [information system], użytkowników takich systemów oraz innych osób.  Z kolei projekcie nowelizacji UKSC z 7.09.2020 r. proponuje się nowy termin – „bezpieczeństwo sieci i usług” i definiuje się go jako zdolność sieci telekomunikacyjnych lub usług komunikacji elektronicznej do odpierania wszelkich działań naruszających dostępność, autentyczność, integralność lub poufność: a) tych sieci lub usług, b) przetwarzanych danych i treści objętych tajemnicą komunikacji elektronicznej, c) innych świadczonych przez przedsiębiorcę komunikacji elektronicznej usług związanych z usługami komunikacji elektronicznej lub sieciami telekomunikacyjnymi tego przedsiębiorcy [art. 2 pkt 8f projektu]. Jednocześnie, pozostawia się dotychczasową definicję cyberbezpieczeństwa.  Rada zwraca uwagę na niejednoznaczność terminu „cyberbezpieczeństwo”. Termin ten jest również wadliwie tłumaczony z języka angielskiego, często jako „bezpieczeństwo cybernetyczne”, i „bezpieczeństwo systemów informatycznych” – co, zdaniem Rady wymaga korekty.  Wymagałoby pogłębionej analizy ustalenie czy i w jaki sposób do różnic pomiędzy polską ustawą a unijnym rozporządzeniem odnoszą się reguły kolizyjne, ponieważ przyjęcie poglądu o krzyżowaniu się zakresów ustawy o ksc i rozporządzenia UE 2019/881 pociągałoby za sobą konieczność uchylenia dotychczasowej definicji cyberbezpieczeństwa. Niewątpliwie potrzebne jest wdrożenie procedury corrigendum nieodpowiednich spolszczeń w Dz. Urz. UE Pl. [m.in. cybersecurity jako „bezpieczeństwa cybernetycznego” zamiast cyberbezpieczeństwa, a information systems jako systemów informatycznych zamiast systemów informacyjnych] a także zestawienie i adekwatnie objaśnienie innych elementów leksykonu cyberbezpieczeństwa.  Rada rekomenduje uzgodnienie znaczenia terminu cyberbezpieczeństwo jako zbiorczego określenia o rosnącej wadze w różnych kontekstach, dla uzyskania spójności wielopoziomowej regulacji oraz zestawienie i adekwatne objaśnienie innych elementów siatki pojęciowej. Ułatwi to jasne określenie uprawnień i obowiązków podmiotów krajowego systemu cyberbezpieczeństwa.  Jednocześnie Rada zwraca uwagę na brak cyberbezpieczeństwa w klasyfikacjach rodzajów działalności. Dotyczy to zarówno Międzynarodowej Standardowej Klasyfikacji Rodzajów Działalności (ISIC), Statystycznej Klasyfikacji Rodzajów Działalności Gospodarczej w Unii Europejskiej (NACE), jak i Polskiej Klasyfikacji Działalności (PKD). Działalność ma miejsce wówczas, gdy czynniki takie jak: wyposażenie, siła robocza, technologia produkcji, sieci informacyjne lub produkty są powiązane w celu wytworzenia określonego wyrobu lub wykonania usługi. Działalność charakteryzowana jest przez produkty wejściowe (wyroby lub usługi), proces technologiczny oraz przez produkty wyjściowe. Wyróżnia się działalność: przeważającą, drugorzędną i pomocniczą. Cyberbezpieczeństwo nie jest wyodrębniane jako rodzaj działalności.  Klasyfikacja PKD 2007 stosowana jest do podmiotów gospodarczych dla potrzeb: Centralnej Ewidencji i Informacji o Działalności Gospodarczej (CEIDG), Krajowego Rejestru Sądowego (KRS), Krajowego Urzędowego Rejestru Podmiotów Gospodarki Narodowej (REGON), Krajowej Ewidencji Podatników (KEP).  Niewyodrębnienie w PKD cyberbezpieczeństwa utrudnia realizację zadań publicznych wyznaczonych podmiotom krajowego systemu cyberbezpieczeństwa i rozwój działalności gospodarczej. Uwaga powyższa dotyczy wprawdzie tylko pośrednio projektu nowelizacji UKSC, ale Rada stoi na stanowisku, że minister właściwy do spraw informatyzacji powinien zainicjować kompleksowe uporządkowanie kwestii związanych z terminologią oraz klasyfikacją działalności związaną z tematyką cyberbezpieczeństwa. | **Uwaga częściowo uwzględniona**  Definicje cyberbezpieczeństwa i bezpieczeństwa sieci i systemów informatycznych został zmienione. |
|  | Sektorowa Rada ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo | Uwaga ogólna | *Kwalifikacje i umiejętności związane z cyberbezpieczeństwem*  Rada zwraca uwagę, że w UKSC brak wyraźnych wymogów w zakresie kwalifikacji, wiedzy i umiejętności.  Art. 14 stanowi, że operator usługi kluczowej w celu realizacji niektórych zadań powołuje wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo lub zawiera umowę z podmiotem świadczącym usługi z zakresu cyberbezpieczeństwa (po nowelizacji ma to być SOC)  Według § 1 ust. 1 pkt 4 rozporządzenia Ministra Cyfryzacji z 4.12.2019. podmiot świadczący usługi z zakresu cyberbezpieczeństwa jest obowiązany w zakresie realizowanych obowiązków, o których mowa w art. 8 pkt 4 i 6, art. 11 ust. 1 pkt 1–5, art. 12 i art. 13 UKSC, dysponować personelem posiadającym umiejętności szczegółowo określone w punktach a-d.  Pojawiają się wątpliwości dotyczące dokumentowania faktu dysponowania odpowiednim personelem [czy ma on posiadać stosowne certyfikaty, szkolenia, itp.] oraz braku wymogów w odniesieniu do personelu wewnętrznych struktur. 4  Rada zdaje sobie sprawę z różnicy w podejściu do wymogów kwalifikacyjnych w sferze prywatnej i publicznej. Sfera prywatna jest z jednej strony często lepiej motywowana do podnoszenia kwalifikacji, z drugiej – wszelkie ustawowe wymogi tego typu traktuje jako dodatkowe, kosztowne obowiązki nakładane na sektor gospodarczy. W sferze publicznej z kolei, brak ustawowych wymogów co do posiadania określonych kwalifikacji powoduje niechęć do wydawania publicznych pieniędzy na te cele, a tym samym brak motywacji do podnoszenia poziomu umiejętności. W raporcie NIK z 2019 r. dotyczącym zapewniania bezpieczeństwa e-usług oceniono krytycznie 70% badanych podmiotów publicznych.  Pewnym wzorem mogą być przepisy dotyczące ochrony danych osobowych dotyczące inspektorów ochrony danych. W art. 37 ust. 5 RODO stanowi, że Inspektor ochrony danych wyznaczany jest na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk ochrony danych oraz umiejętności wypełniania swoich zadań. Do szkolenia innych osób upoważnianych do przetwarzania, mobilizują administratorów zasada rozliczalności i dolegliwe sankcje.  Rada stoi na stanowisku, że efektywność nowych regulacji cyberbezpieczeństwa może być ograniczona ze względu na niewystarczający potencjał kadrowy, zwłaszcza SOC i CSIRT sektorowych. W związku z tym Rada rekomenduje, aby w UKSC umieścić przepisy skłaniające do podnoszenia kwalifikacji. | **Uwaga nieuwzględniona**  Kwestie związane z zobowiązaniem podmiotów krajowego systemu cyberbezpieczeństwa do podnoszenia kwalifikacji kadr wykracza poza zakres przedmiotowy nowelizacji. Operatorzy usług kluczowych, jak słusznie zauważył autor opinii mają obowiązek zapewnić dysponowanie odpowiednio wykwalifikowanym personelem. |
|  | Polskie Towarzystwo Informatyczne | Uwaga ogólna | Z zadowoleniem witamy projekt ustawy o zmianie ustawy o Krajowym Systemie Cyberbezpieczeństwa, który zgodnie z uzasadnieniem, ma zrealizować to co już wielokrotnie nasza organizacja podnosiła w toku prac nad innymi projektami aktów prawnych  tj. konieczność dostosowywania RP do zestawu narzędzi na potrzeby cyberbezpieczeństwa sieci 5G UE (zwanego dalej “5G Toolbox”) w opracowaniu którego Polska brała udział, i w którym zawarto środki na poziomie strategicznym i technicznym oraz wskazano działania wspierające stosowanie tych środków dla ograniczenia ryzyk cyberbezpieczeństwa europejskich sieci 5G.  Nie jest prawdziwa teza że ustawa ta jest wymierzona przeciwko jakiejkolwiek firmie na świecie, co sugeruje prasa choć nie oznacza to wcale ze nie może być użyta przeciwko jakiejkolwiek firmie rodem z Chin czy Rosji lub Korei Północnej, z której pochodzą pierwsze podmioty objęte sankcjami UE za cyberataki, choć jak słusznie zauważa p. Izabela Albrycht  w <https://ik.org.pl/publikacje/5g-made-by-america/>:  „Całkowicie swoje sieci telekomunikacyjne na komponenty z ChRL zamknęły Australia, Nowa Zelandia i Japonia, a zapowiedziała – Wielka Brytania. Wiele krajów podpisało natomiast z USA deklaracje polityczne wyrażające wolę współpracy w zakresie zapewnienia bezpieczeństwa sieci 5G w tym Polska, Łotwa, Rumunia, Polska, Czechy, Estonia, Słowenia”.  W tej ogólnoświatowej debacie na pewno firmie Huawei nie służy postawa macierzystego państwa, oskarżanego o cyberataki na szpitale w Unii Europejskiej w okresie pandemii COVID 19, co spotkało się ze zdecydowanym sprzeciwem Komisji Europejskiej:  <https://www.cyberdefence24.pl/szefowa-ke-oskarza-chiny-o-ataki-na-szpitale>  Projektowana nowelizacja wprowadza kolejne zmiany systemowe, które pozwolą zwiększyć poziom bezpieczeństwa w sektorze komunikacji elektronicznej i telekomunikacji. Uważamy za słuszny postulat włączenia telekomunikacji do ogólnego systemu prawnego cyberbezpieczeństwa przy ograniczaniu obowiązków informacyjnych, które i tak są liczne na tym bardzo dziś regulowanym rynku. Nie da się jednak współcześnie tworzyć rozwiązań systemowych w skali państw wyłączając z niego telekomunikację.  Opiniowany projekt ustawy projektuje narzędzia do realizacji wyżej wymienionych celów zwłaszcza w nowo tworzonych art. 66 „a”- 67 „c” które przyznają nowe szerokie kompetencje Kolegium ds. Cyberbezpieczeństwa oraz Pełnomocnikowi Rządu ds. Cyberbezpieczeństwa.  Możliwość przeprowadzenia oceny ryzyka przez Kolegium ds. Cyberbezpieczeństwa oraz ostrzeżenia i polecenia wydawane przez Pełnomocnika Rządu ds. Cyberbezpieczeństwa, z wiążącymi skutkami , co proponuje ustawa , to absolutnie krok w dobrym kierunku.  Zwracamy uwagę że ,ryzyka opisane w 5G Toolbox są szersze i bardziej różnorodne np „R4. Dependency on a single supplier”. W Polsce że sprzęt i oprogramowanie od jednego dostawcy stanowią większość całej infrastruktury LTE (4G) i 5G a w przypadku niektórych operatorów jest to ponad 80% ich zasobów . Jest to zjawisko głęboko niepożądane, gdyż problem z jednym tylko dostawcą stawia pod znakiem zapytania cyberbezpieczeństwo całego kraju.  Na przykład w przypadku zakłócenia łańcucha dostaw tak z powodów np. pandemii jak i ew. regionalnych czy światowych. Zgodnie z 5GToolbox środkami zaradczymi (Measures) niwelującymi to ryzyko są:  - Dywersyfikacja dostawców.  - Zrównoważony i zróżnicowany łańcuch dostaw i wartości 5G.  Skuteczność tych środków zaradczych w opracowanym 5GToolbox określono jako „bardzo wysoką” (Very High) i są to jedyne środki zaradcze. Ustawa powinna wprowadzać zarówno środki dywersyfikacji ze względu na kraje pochodzenia jak i kategorie produktów  i wykorzystywać technologie otwarte takie jak np. oparte na OPEN RAN.  Zwracamy uwagę że należy zmienić drobną nieścisłość w obecnie obowiązującej ustawie która nakazuje by Pełnomocnikiem rządu ds. cyberbezpieczeństwa była osoba w randze podsekretarza lub sekretarza stanu (art.61 ust.3 obecnie obowiązującej ustawy). Nie obejmuje to Ministra, a obecnie Pan Minister Marek Zagórski pełni tę ważną rolę. Nie można wykluczyć iż w przyszłości tę funkcję także będzie pełnił Minister. Można naprawić przy okazji nowelizacji tę niezręczność, która może prowadzić jednak do podważania decyzji pełnomocnika.  W ocenie PTI projektowana nowelizacja wprowadza kolejne poziom zmiany systemowe, które pozwolą zwiększyć bezpieczeństwa w sektorze komunikacji elektronicznej  i telekomunikacji a niedoskonałości projektu można usunąć na kolejnych etapach prac legislacyjnych. | **Wyjaśnienie**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | ISSA Polska | Uwaga ogólna | Naszym celem statutowym jest m.in. dostarczanie wiedzy związanej z tematyką szeroko pojętego bezpieczeństwa, jak również edukacja i promowanie standardów oraz opiniowanie wydarzeń i rozwiązań z zakresu cyberbezpieczeństwa uznaliśmy za istotne wskazanie najistotniejszych problemów związanych z projektowanymi rozwiązaniami. Projekt zmian w naszej ocenie jest niezwykle potrzebny, jednakże wprowadza pewne dyskusyjne zagadnienia. Niektóre zawarte w projekcie zapisy (w tym, co najmniej Art. 66 i 66a) w naszej ocenie wykraczają poza merytorykę zagrożeń cyberbezpieczeństwa w perspektywie technicznej i dziedzinowo uznawanej za merytoryczną. | **Wyjaśnienie**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | ISSA Polska | Uwaga ogólna | **Definicje**  Wprowadzając do ustawy o Krajowym Systemie Cyberbezpieczeństwa Art. 8f), projekt wprowadza kolejną definicję z zakresu bezpieczeństwa a mianowicie „bezpieczeństwo sieci i usług”. Uważamy, że nowelizację warto wykorzystać do uporządkowania istniejących definicji dotyczących szeroko pojętego bezpieczeństwa telekomunikacyjnego, a nie wprowadzania kolejnej definicji - szczególnie, że obecna propozycja rodzi pytania czym są te „sieci” oraz „usługi”, których bezpieczeństwo należy zapewnić.  Doprecyzowania wymaga definicja incydentu telekomunikacyjnego w Art. 8b). W większych firmach telekomunikacyjnych każdego dnia rejestrowane są nawet miliony zdarzeń typu  skanowanie portów atak DDOS. Teoretycznie każdy z nich „może” - np. w sposób pośredni doprowadzić do obniżenia jakości usługi komunikacji elektronicznej. W tym momencie brak jest  jakichkolwiek dalszych informacji w tym zakresie. Dodatkowo przekazywanie zgodnie z art 20b pkt 2 (oraz 20c ust 3 pkt 3) informacji o incydentach w takiej ilości powinno być wykonywane  jedynie w sposób automatyczny a systemy ku temu potrzebne powinny być dostarczone przez CSIRTy. | **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 przez ustawę wprowadzającą PKE.  Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowym.  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.  Dlatego potrzebne jest przeniesienie odpowiednich definicji z PKE do ustawy KSC. |
|  | ISSA Polska | Uwaga ogólna | **Zadania SOC**  Zespoły SOC funkcjonują na polskim rynku od ponad 15 lat – działają zatem w dobrze opisanej roli w organizacjach, jak również w konkretnej rzeczywistości rynkowej, zarówno w zakresie usług  zlecanych, jak i dostarczanych klientom. W związku z powyższym proponujemy uwzględnienie dotychczasowych doświadczeń w dotyczących zespołów SOC propozycjach zapisów:   Częstym modelem realizacji SOC jest wariant, w którym jedynie część zadań SOC jest realizowana przez podmiot zewnętrzny – brzmienie proponowanego Art. 14 ust 2) do Ustawy o Krajowym Systemie Cyberbezpieczeństwa powinno zapewniać taką możliwość. | **Wyjaśnienie**  Operator usługi kluczowej może zawrzeć umowę z kilkoma podmiotami realizujących inne zadania o których mowa w art. 14 ust. 1. |
|  | ISSA Polska | Uwaga ogólna | **Postulat rzetelnych konsultacji społecznych**  Ponieważ nowe regulacje, będą oddziaływały na szeroki zakres odbiorców, dlatego też Ministerstwo Cyfryzacji powinno przygotować pełną listę interesariuszy i umożliwić ich rzeczywisty udział w konsultacjach, w szczególności: organizacje samorządów terytorialnych, organizacje przedsiębiorców, organizacje konsumentów, instytucje odpowiedzialne za ochronę  konkurencji i konsumenta, Radę Dialogu Społecznego.  2. Postulat zorganizowania konferencji uzgodnieniowej oraz wcześniejszego wysłuchania publicznego  Zgodnie z § 44 Regulamin pracy Rady Ministrów, zwracamy się z uprzejmą prośbą o zorganizowanie przez Ministerstwo konferencji uzgodnieniowej oraz zaproszenie do udziału wszystkich interesariuszy, którzy wnieśli swoje uwagi, gdyż z pewnością przyczyniłaby się ona do właściwego prowadzenia uzgodnień i zaopiniowania projektu ustawy.  Z uwagi na szeroki wpływ projektowanych zmian na kwestie dotykające wszystkich obywateli,  uznajemy także za celowe przeprowadzenie wysłuchania publicznego, już na etapie prac rządowych.  3. Postulat dokonania notyfikacji projektu  Zwracamy uwagę na równoległe prace Komisji Europejskiej w zakresie rewizji dyrektywy NIS1, która jak dotąd jest głównym źródłem regulacji z zakresu cyberbezpieczeństwa. Tym samym sugerowalibyśmy, aby zmiany naszego prawa krajowego nie wyprzedzały regulacji UE, tym bardziej jeśli kierunek obranych zmian może pójść w przeciwnym kierunku niż regulacje europejskie.  4. Postulowane kluczowe zmiany projektu  Przyjęta w projekcie nowelizacji koncepcja powstania CSIRT Telko i SOC’ów jest godna poparcia w zakresie, w jakim służy zapewnieniu koordynacji działań i wymiany informacji podmiotami  należącymi do KSC a dostawcami sieci i usług komunikacji elektronicznej. Zwracamy przy tym uwagę, że skuteczne wymiana informacji o incydentach wymaga nie tworzenia osobnych  organizacji a zniesienia prawnych ograniczeń dotyczących dzielenia się informacjami, które mogą być klasyfikowane jako tajemnica w firmach telekomunikacyjnych oraz finansach i bankowości.  Proponujemy więc przede wszystkim stworzyć mechanizmy, które pozwolą tym podmiotom dzielić się informacjami o incydentach i oszustwach – również tych jedynie podejrzewanych.  Uważamy również, że implementacja dyrektywy NIS poprzez przyjęcie i uchwalenie ustawy o KSC na terenie RP powinna w sposób bardziej świadomy rzutować na istotność ochrony kluczowych elementów infrastruktury w sieciach industrialnych, przemysłowych – OT. Istotność zagrożeń dla całej infrastruktury krytycznej od strony sieci przemysłowych OT podkreśla fakt złożoności  infrastruktury sieci IT, ICT oraz OT oraz ich wzajemnej korelacji, zależności fizyczno -logicznych od siebie i wymienianych danych. Naszym zdaniem rekomendacje i wymagania w obszarze urządzeń  automatyki przemysłowej oraz urządzeń aktywnych infrastruktury powinny nawiązywać do szeregu dobrych praktyk i uznanych standardów branżowych IEC62443, NIST SP 800-82,  wytycznych Komisji Europejskiej oraz Europejskiej Agencji do spraw Bezpieczeństwa Sieci i Informacji (ENISA) przedstawionych np. w publikacji "Communication network dependencies for ICS-SCADA Systems". | **Wyjaśnienie**  Umożliwiono wypowiedzenie się wszystkim interesariuszom w trakcie konsultacji publicznych. |
|  | ISSA Polska | Uwaga ogólna | Całość zagadnienia powinna zostać opracowana w odrębnej sektorowej i branżowej publikacji zawierającej wymagania i wytyczne wyczerpującą tematykę:   metodyki przeprowadzania audytów systemów ICS, sieci przemysłowych oraz zasobów bezpośrednio sklasyfikowanych jako urządzenia czynne i aktywne pod kątem wytwarzania  dóbr, zarządzania i nadzorowania procesem produkcyjnym,   szacowania ryzyka w oparciu przeprowadzony audyt z opracowaniem metod zmniejszenia ryzyka utraty ciągłości produkcyjnej, podania rekomendacji związanych z zarządzaniem  ryzykiem,   sposobu określenia istniejących podatności urządzeń sieci produkcyjnej i systemów automatyki przemysłowej ICS/OT, urządzeń sieciowych,   określenia wytycznych służących zwiększeniu niezawodności systemów produkcyjnych zmniejszających potencjalne następstwa w przerwaniu ciągłości świadczonych usług komunikacji tychże urządzeń   określeniu metod prewencji poprzez ciągłe monitorowanie zasobów sieciowych oraz urządzeń automatyki przemysłowej, komunikacji tychże urządzeń z uwzględnieniem specyfiki protokołów przemysłowych   nadaniu wytycznych sektorowych służących zbudowaniu wielowarstwowego systemu ochrony kluczowych zasobów, urządzeń, instalacji i systemów wytwórczych.   wytycznych do projektantów co do projektowania systemów bezpieczeństwa systemów komputerowych dla otoczenia OT/ICS oraz komponentów systemów sterowania, doboru elementów systemu  Jednocześnie jako ISSA Polska pozostajemy do dyspozycji Ministerstwa Cyfryzacji w zakresie wsparcia eksperckiego i wiedzy związanej z tematyką szeroko pojętego bezpieczeństwa  systemów informacyjnych. | **Wyjaśnienie**  Dziękujemy ISSA Polska za przedstawioną propozycję. Mając na uwadze naszą dotychczasową współpracę z ekspertami z ISSA Polska m.in. przy przygotowaniu szablonu sprawozdania z audytu bezpieczeństwa u operatorów usług kluczowych DC KPRM wyraża gotowość do kontynuowania współpracy. |
|  | ISSA Polska | Uwaga ogólna | Proponujemy dodanie proaktywnej funkcji CSIRT sektorowego w zakresie obowiązku wysyłania cotygodniowej uproszczonej informacji o aktualnym stanie dynamicznej analizy ryzyka, skali zarejestrowanych incydentów z ich priorytetami, trendem dla wszystkich zarejestrowanych uczestników systemu cyberbezpieczeństwa. W związku tym proponujemy dodanie ust. 1.c w brzmieniu:  1.c CSIRT sektorowy zapewnia co tygodniowy raport sytuacyjny w zakresie cyberbezpieczeństwa sektora, zawierający co najmniej informacje o:  1) Poziomie stanu dynamicznej analizy ryzyka dla sektora;  2) ilości otrzymanych incydentów od uczestników sektora;  3) Istotnych zidentyfikowanych podatnościach | **Wyjaśnienie**  CSIRT sektorowy zapewnia wymianę informacji o podatnościach i zagrożeniach w sektorze. Jest to wskazane w art. 44 w ust 1 pkt 3 i 4. |
|  | Związek Przedsiębiorców i Pracodawców | Uwaga ogólna | Bez wątpienia istotnym wyzwaniem pozostaje zapewnienie cyberbezpieczeństwa. Wraz ze wzrostem znaczenia sieci telekomunikacyjnych i wykorzystywaniem jej do realizacji coraz szerszego katalogu usług publicznych, niekiedy krytycznych, wprowadzenie regulacji minimalizujących ryzyko występowania incydentów zakłócających świadczenie usług wydaje się być oczywiste.  Przedstawiony projekt nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa rozumiemy jako próbę odpowiedzi na to wyzwanie, sformułowaną po dwuletnim okresie obowiązywania zmienianego aktu. W tym sensie zrozumiałe wydaje się być zaproponowanie przepisów wprowadzających centra wymiany informacji między podmiotami krajowego systemu cyberbezpieczeństwa oraz wprowadzających obowiązek ustanawiania sektorowych CSIRT (zamiast dotychczasowego trybu fakultatywnego).  Niemniej jednak niektóre z przepisów budzą kontrowersje. Dotyczy to przede wszystkim przepisów zaproponowanych w odniesieniu do możliwości weryfikowania dostawców sprzętu lub oprogramowania. Uwzględnione w projekcie regulacje zakładają, że możliwe będzie wyłączenie podmiotów zidentyfikowanych jako źródło zagrożenia z systemu zamówień publicznych w Polsce, czy zobowiązanie podmiotów krajowego systemu cyberbezpieczeństwa do ograniczenia korzystania z produktów, oprogramowania i usług takich dostawców. Tego rodzaju oceny ryzyka może, zgodnie z art. 66a projektu, dokonać Kolegium ds. Cyberbezpieczeństwa.  Jednym z bardziej wrażliwych elementów sporządzania oceny w projekcie ustawy, są kryteria brane pod uwagę w toku procesu. Zgodnie z projektem, przy sporządzaniu oceny przeprowadzać ma się analizy dotyczące w szczególności m.in.:  - zagrożeń bezpieczeństwa narodowego o charakterze ekonomicznym, kontrwywiadowczym i terrorystycznym oraz zagrożeń dla realizacji zobowiązań sojuszniczych i europejskich, jakie stanowi dostawca sprzętu i oprogramowania;  - prawdopodobieństwa, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza UE bądź NATO (analiza ta ma uwzględniać m.in. stopień i rodzaj powiązań między dostawcą a tym państwem, prawodawstwo państwa w zakresie ochrony praw obywatelskich i praw człowieka, czy strukturę własnościową dostawcy).  Przedstawione kryteria mają charakter nieostry i podmiotowy, a nie przedmiotowy, co umożliwia uznanie takiego samego sprzętu lub oprogramowania za stanowiące zagrożenie albo nie, w zależności wyłącznie od jego dostawcy.  Kryteria (*de facto*) doboru dostawców sprzętu i oprogramowania uznajemy zatem za przejaw chęci pozostawienia otwartego pola gry i możliwości podjęcia każdej decyzji, w zależności od rozwoju sytuacji geopolitycznej, jak i dynamiki wydarzeń w innych państwach. W tym sensie – polityki międzynarodowej, a niekoniecznie bezpośredniego interesu gospodarczego – przyjęte przez projektodawcę podejście pozwala na dostosowanie aktywności Polski do uwarunkowań międzynarodowych i podjęcie dowolnej decyzji. Należy jednak pamiętać o konieczności zapewnienia pewnej przewidywalności otoczenia regulacyjnego dla działających w Polsce przedsiębiorców  Zwracamy również uwagę na specyfikę niektórych sektorów – sparaliżowanie dostępu do produktów niektórych producentów urządzeń elektronicznych może spowodować np. istotne trudności w zakresie technicznych możliwości produkowania leków. | **Uwaga częściowo uwzględniona**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | Związek Przedsiębiorców i Pracodawców | Uwaga ogólna | Ponadto, pragniemy poddać pod rozwagę ustawodawcy możliwość zastosowania uzupełniających rozwiązań w zakresie cyberbezpieczeństwa, które zminimalizują negatywne skutki finansowe dla przedsiębiorców telekomunikacyjnych, przy równoczesnym zapewnieniu najwyższych standardów cyberbezpieczeństwa. W szczególności zwracamy uwagę na zbyt krótki przewidziany 5-cio letni okres na eliminację sprzętu dostawcy określonego jako dostawcy wysokiego ryzyka. Użytkownicy tego sprzętu lub oprogramowania nabywali go w dobrej wierze i z założeniem pełnego wykorzystania biznesowego przez okres zdecydowanie dłuższy, niż 5 lat. Realny czas na amortyzację sprzętu wykorzystywanego w sieciach telekomunikacyjnych stanowi minimum 7-8 lat. W tym okresie zasadne byłoby również dopuszczenie dokonywania dalszych niezbędnych zakupów i wdrożeń, w tym np. aktualizacji oprogramowania kluczowego dla bezpieczeństwa. Dodatkowo, zwracamy uwagę na ewentualną możliwość uzależnienia zasad eliminacji sprzętu dostawcy określonego jako dostawcy wysokiego ryzyka od poziomu wrażliwości danego obszaru dla krajowego systemu cyberbezpieczeństwa, na którym sprzęt jest wykorzystywany. Ustawodawca może wskazać regiony, w których należy zastosować najbardziej rygorystyczne podejście ze względu na ich krytyczną i strategiczną rolę w krajowym systemie cyberbezpieczeństwa. | **Wyjaśnienie**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | Związek Przedsiębiorców i Pracodawców | Uwaga ogólna | Istotnym wątkiem jest również kwestia rozszerzenia zakresu ustawy na podmioty spoza tych uznanych za operatora usługi kluczowej. Należy podkreślić, że autonomiczne zarządzanie bezpieczeństwem przez te podmioty doprowadziło do zbudowania złożonych i wzajemnie powiązanych systemów zabezpieczeń, w trybie ciągłym analizowanych pod kątem skuteczności i aktualności. Omawiana regulacja może spowodować, że funkcjonalność tych systemów zostanie ograniczona z uwagi na komunikaty bezpieczeństwa ogłaszane przez organy administracji. Tym samym, podmioty gospodarcze poniosą niejako podwójne koszty. | **Wyjaśnienie**  Katalog podmiotów wchodzących w skład krajowego systemu cyberbezpieczeństwa jest bardzo szeroki i wskazany w art. 4. |
|  | Związek Przedsiębiorców i Pracodawców | Uwaga ogólna | Należy ponadto zwrócić uwagę na regulacje dot. ostrzeżeń oraz poleceń zabezpieczających, wydawanych przez Pełnomocnika ds. Cyberbezpieczeństwa. Zarówno ostrzeżenia jak i polecenia zabezpieczające w swojej treści wskazują określone zachowanie, które należy podjąć i które ma w swoim założeniu zmniejszyć ryzyko incydentu. Jednym ze wskazanych w ustawie zachowań zmniejszających ryzyko incydentu jest nakaz wprowadzenia reguły ruchu sieciowego zakazującego połączeń z określonymi adresami IP lub nazwami URL (art. 67b ust. 3 pkt 7 uksc), czyli działanie polegające na ograniczaniu (blokowaniu) dostępu do niektórych stron lub usług. Zgodnie z regulacją Rozporządzenia EU dot. otwartego internetu, użytkownicy końcowi mają prawo do uzyskania za pomocą internetu dostępu do informacji i treści oraz do ich rozpowszechniania, a także do korzystania z wybranych aplikacji i usług oraz ich udostępniania, jak również do korzystania z wybranych urządzeń końcowych, niezależnie od lokalizacji użytkownika końcowego lub dostawcy usług czy też od lokalizacji, miejsca pochodzenia lub miejsca docelowego informacji, treści lub usługi. Zasada otwartego internetu może podlegać ograniczeniu tylko wyjątkowo i przy zachowaniu proporcjonalnych środków – należałoby zatem uzupełnić projekt ustawy o regulacje gwarantujące wyjątkowość i proporcjonalność radykalnego środka, jakim jest zablokowanie dostępu do niektórych stron lub usług | **Wyjaśnienie**  Projektowane przepisy dot. ostrzeżenia i polecenia zabezpieczającego nie mają na celu ograniczenie wolności słowa i dostępu do internetu.  Ich stosowanie jest ograniczone tylko do niektórych grup podmiotów z  sektorów gospodarki kluczowych dla społeczno-ekonomicznego bezpieczeństwa państwa  m.in. do operatorów usług kluczowych, administracji publicznej, czy przedsiębiorców  telekomunikacyjnych. Co więcej, środki te mogą być aktywowane w sytuacji zagrażającej  wystąpieniu incydentu krytycznego  (ostrzeżenie) lub w trakcie jego trwania, w związku z  potrzebą zapewnienia koordynacji i odpowiednio szybkiej reakcji na zażeganie sytuacji  kryzysowej wywołanej cyberatakiem (polecenie zabezpieczające). |
|  | Związek Przedsiębiorców i Pracodawców | Uwaga ogólna | Niezależnie od potrzeby ujednolicenia i skoordynowania prawodawstwa w zakresie obowiązków ciążących na przedsiębiorcach komunikacji elektronicznej, ważne jest aby na etapie projektowania aktów wykonawczych pamiętać o konieczności zachowania zasady proporcjonalności i nieobciążania przedsiębiorców dodatkowymi obowiązkami w stopniu wyższym, niż jest to konieczne dla zrealizowania celów ustawy.  Jednocześnie, wszelkie mechanizmy ocenne należy umocować w istniejących już przepisach, takich jak te zawarte w ustawie Prawo przedsiębiorców oraz ustawie Kodeks postępowania administracyjnego. Gwarantują one przejrzystość procedur i ich zasad, umożliwiają udział dostawcy w postępowaniu oraz zapewniają niedyskryminującą procedurę odwoławczą.  Mając na uwadze wszelkie powyższe aspekty, postulujemy o dalsze prace nad przedstawionym projektem ustawy i kontynuowanie szerokich konsultacji tego aktu, tak aby każdy zainteresowany podmiot miał możliwość skutecznego przekazania swojej opinii na jego temat. Nie ulega wątpliwości, że projekt będzie miał bezpośredni wpływ na wiele podmiotów obecnych na polskim rynku, dlatego szczególnie istotne jest, by wysłuchać wszystkich racji i rozważyć np. możliwość przeprowadzenia konferencji uzgodnieniowej, zgodnie z bardzo dobrą praktyką obecną w niektórych procesach legislacyjnych. | **Wyjaśnienie**  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. |
|  | EXATEL | Uwaga ogólna | W pierwszej kolejności należy wyrazić uznanie dla większości zmian zaproponowanych w przedmiotowym projekcie, ponieważ bez wątpienia wpłyną one pozytywnie na system cyberbezpieczeństwa w Polsce. Dodanie do krajowego systemu cyberbezpieczeństwa ISAC, utworzenie CSIRT Telco czy też poddanie dostawców sprzętu lub oprogramowania procedurze sprawdzającej pod kątem zagrożeń dla społeczno-ekonomicznego bezpieczeństwa państwa to kroki zwiększające cyberbezpieczeństwo Polski.  Projekt przewiduje również obowiązek powoływania CSIRT sektorowych, które zastąpić mają dotychczasowe sektorowe zespoły do spraw cyberbezpieczeństwa. Do ich 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) współpraca z operatorami usług kluczowych w zakresie wymiany dobrych praktyk oraz informacji  o podatnościach i zagrożeniach, organizację i uczestniczenie w ćwiczeniach oraz wspieranie inicjatyw szkoleniowych;  5) współpraca z CSIRT MON, CSIRT NASK i CSIRT GOV w zakresie wymiany informacji i reagowania na incydenty poważne i krytyczne oraz wymianę informacji o zagrożeniach;  6) zapewnianie dynamicznej analizy ryzyka i incydentów oraz wspomaganie w podnoszeniu świadomości zagrożeń cyberbezpieczeństwa (opcjonalnie);  7) koordynowanie w uzgodnieniu z operatorami usług kluczowych obsługi incydentów, które dotyczą różnych podmiotów w danym sektorze lub podsektorze (opcjonalnie).  Należy zauważyć, że organami właściwymi są: minister właściwy do spraw energii; minister właściwy do spraw transportu; minister właściwy do spraw gospodarki morskiej i minister właściwy do spraw żeglugi śródlądowej; Komisja Nadzoru Finansowego (ma być to zgodnie z projektem Urząd KNF); minister właściwy do spraw zdrowia; Minister Obrony Narodowej; minister właściwy do spraw gospodarki wodnej; minister właściwy do spraw informatyzacji. Co do zasady organ właściwy będzie musiał zbudować strukturę CSIRT w urzędzie go obsługującym lub powierzyć realizację zadań CSIRT sektorowego jednostkom mu podległym lub przez niego nadzorowanym. W przypadku braku możliwości realizacji zadań CSIRT sektorowego w trybie określonym w ust. 1 lub ust. 5, organ właściwy może, po zasięgnięciu opinii Pełnomocnika Rządu do spraw Cyberbezpieczeństwa, 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. Do tych podmiotów z art. 4 ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych (Dz. U. poz. 2019) zaliczamy:  1) jednostki sektora finansów publicznych w rozumieniu przepisów ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2019 r. poz. 869, 1622 i 1649);  2) inne, niż określone w pkt 1, państwowe jednostki organizacyjne nieposiadające osobowości prawnej;  3) inne, niż określone w pkt 1, osoby prawne, utworzone w szczególnym celu zaspokajania potrzeb o charakterze powszechnym, niemających charakteru przemysłowego ani handlowego, jeżeli podmioty, o których mowa w tym przepisie oraz w pkt 1 i 2, pojedynczo lub wspólnie, bezpośrednio lub pośrednio przez inny podmiot:  a) finansują je w ponad 50% lub  b) posiadają ponad połowę udziałów albo akcji, lub  c) sprawują nadzór nad organem zarządzającym, lub  d) mają prawo do powoływania ponad połowy składu organu nadzorczego lub zarządzającego;  4) związki podmiotów, o których mowa w pkt 1 lub 2, lub podmiotów, o których mowa  w pkt 3.  Podsumowując powyższy wyciąg z przepisów trzeba wskazać, że nie ma możliwości zlecenia pełnienia funkcji CSIRT sektorowego „na zewnątrz” – krąg podmiotów mogących pełnić tą funkcję został ściśle ograniczony i w ograniczeniu pominięto również spółki Skarbu Państwa działające na rynku komercyjnym. Tylko nieliczne z organów właściwych mają jednostki podległe lub nadzorowane, które mają zbudowaną podstawową bazę umiejętności w zakresie cyberbezpieczeństwa. Wskazać tutaj można jednostki podległe Ministrowi Obrony Narodowej oraz ministrowi właściwemu do spraw cyfryzacji. W tym miejscu jednak trzeba wskazać, że jednostki te pełnią już rolę CSIRT na poziomie krajowym i nie powinny one dublować swojej funkcji, pełniąc jednocześnie rolę CSIRT na poziomie sektorowym. Efektem przyjętego rozwiązania jest więc konieczność stworzenia przez 8 organów właściwych CSIRT sektorowych od podstaw, na co ustawodawca przewiduje 18 miesięcy od dnia wejścia w życie projektowanej ustawy.  Tymczasem należy wskazać, że budowanie, szkolenie i utrzymanie zespołu do spraw cyberbezpieczeństwa wraz z pozyskaniem lub przygotowaniem odpowiednio skutecznego zestawu wykorzystywanych przez zespół narzędzi jest skomplikowanym i długotrwałym procesem. Jego przeprowadzenie wiąże się często ze sporymi komplikacjami, tymczasem zgodnie z projektem taki proces będzie musiał zostać przeprowadzony w urzędach nie mających doświadczenia w takiej działalności. | **Wyjaśnienie**  CSIRT sektorowy nie może prowadzić działalności komercyjnej, dlatego zastosowano katalog podmiotów z art. 4 PZP. |
|  | EXATEL | Uwaga ogólna | Wskazać można następujące zagrożenia, które w znaczny sposób utrudnią samodzielną budowę CSIRT sektorowych przez organy właściwe:   1. **Deficyt wyspecjalizowanej kadry na rynku niezbędnej do powołania CSIRT**   Nawet pomimo proponowania rynkowych stawek wynagrodzeń (chociaż z wyliczeń zawartych w OSR nie do końca wiadomo, czy przyjęte koszty uwzględniają też koszty zatrudnienia po stronie pracodawcy) nie ma gwarancji, że uda się zrekrutować zespół odpowiednich specjalistów. W szczególności należy wskazać na niedobór specjalistów  z obszaru cyberbezpieczeństwa na rynku, co dotyczy zarówno kadry technicznej mającej doświadczenie w pracy w SOC/CSIRT, jak i kadry posiadającej doświadczenie w budowie  i organizacji pracy zespołów SOC/CSIRT. Ponadto nagłe ogłoszenie naborów do kilku nowych organizacji zajmujących się cyberbezpieczeństwem doprowadzi do powstania na rynku takich specjalistów nadmiernego popytu, co z kolei przełoży się na dodatkową presję płacową i w konsekwencji może zdestabilizować działanie aktualnie funkcjonujących zespołów (w tym np. migrację kadry eksperckiej z CSIRT MON, CSIRT NASK i CSIRT GOV do innych podmiotów).   1. **Dostosowanie kultury organizacyjnej do warunków rynkowych istniejących w sektorze IT** Specjaliści IT zajmujący się cyberbezpieczeństwem preferują elastyczne formy zatrudnienia, które obecnie nie są proponowane ani stosowane w polskiej administracji. Ponadto często interesuje ich praca projektowa. Dodatkowo, rekrutując tego typu specjalistów trzeba często stosować nieszablonowe strategie rekrutacji, nieznane w administracji publicznej. 2. **Konieczność pozyskania doświadczeń organów właściwych co do sposobu utworzenia i funkcjonowania CSIRT**   Samo przygotowanie koncepcji funkcjonowania CSIRT jest procesem długotrwałym i skomplikowanym. W jego trakcie trzeba podejmować szereg kluczowych decyzji dotyczących sposobu działania poszczególnych linii, wyboru platformy sprzętowej na której CSIRT będzie działać, zasad prowadzenia rekrutacji na poszczególne stanowiska. Samo opracowanie takiej rzetelnej koncepcji jest wyceniane na kwoty od kilkuset tysięcy do ponad miliona złotych.   1. **Krótki czas przewidziany na powołanie i osiągnięcie pełnej sprawności operacyjnej CSIRT**   Wskazać należy, że rekrutacje na stanowiska związane z cyberbezpieczeństwem mogą trwać nawet kilka miesięcy, gdzie przy pozyskiwaniu kompetentnych, doświadczonych pracowników standardem jest minimum 6-9 miesięcy od momentu rozpoczęcia rekrutacji, przy założeniu dysponowania odpowiednio wysokiego budżetu na wynagrodzenia. Czas pozyskiwania pracowników może ulec wydłużeniu lub wręcz uniemożliwić realizacje założeń projektu (istnieje wysokie ryzyko braku osiągnięcia zamierzonego celu gotowości operacyjnej). Należy zauważyć, że zrekrutowanie odpowiednich kandydatów jest pierwszym, ale nie jedynym wyzwaniem z perspektywy zasobów ludzkich – najważniejszym jest utrzymanie zrekrutowanej kadry. Ponadto, w przypadku zlecenia przygotowania samej koncepcji budowy CSIRT na zewnątrz w ramach zamówienia publicznego, doliczyć należy czas niezbędny na przeprowadzenie stosownego postepowania i zawarcie umowy, a następnie jej realizację. W końcu, już po pomyślnym zrekrutowaniu wszystkich pracowników i zakupie niezbędnego sprzętu i licencji konieczny będzie okres przygotowawczy pozwalający na budowę i wdrożenie jednolitych procedur i instrukcji pozwalających obsługę klientów CSIRT. W przewidzianym w ustawie okresie 18 miesięcy wykonanie wszystkich wyżej wymienionych zadań wydaje się być bardzo trudne. | **Wyjaśnienie**  Termin 18 miesięcy na powołanie CSIRT sektorowych jest realny. Niezależnie od zmian legislacyjnych KPRM prowadzi działania mające na celu zaadresowanie problemów o których mówi autor uwagi m. in. w obszarze podnoszenia kompetencji i kwalifikacji kadr, pozyskania finansowania ze źródeł europejskich na działania wzmacniający krajowy system cyberbezpieczeństwa. |
|  | S4IT Michał Podgórski | Uwaga ogólna | Uważam, że projekt może w pewnym stopniu zagrozić rzeczywistym interesom naszych obywateli wpływając negatywnie na koszty oraz dostępność do usług telekomunikacyjnych, zatrudnienie i przyszłe możliwości. Zgłaszam niniejszym następujące uwagi do projektu ustawy:   1. Projekt wymaga wycofania całego sprzętu danego dostawcy w ciągu 5 lat, co spowoduje, że rząd/dany sektor będzie potrzebował dużej ilości dodatkowych nakładów finansowych, a tym samym wpłynie negatywnie na proces kształtowania społeczeństwa cyfrowego i może spowodować podwyższenie cen u dostawców, którzy zostali zweryfikowani i zatwierdzeni przez specjalistów. 2. Projekt doprowadzi do wzrostu kosztów po stronie operatorów, co spowoduje konieczność wprowadzenia wyższych taryf telekomunikacyjnych i wpłynie negatywnie na i doprowadzi do podwyższenia abonamentu, co bezpośrednio uderzy w klientów końcowych. 3. Wykluczenie poszczególnych producentów doprowadzi do zmniejszenia konkurencji na rynku, co negatywnie wpłynie na koszty operatorów, a tym samym zaszkodzi interesom konsumentów. 4. Projektowane przepisy faktycznie zmierzają do wykluczenia dostawców przez wzgląd na ich kraj pochodzenia, co doprowadzi do stawiania barier handlowych i wpłynie negatywnie na zaufanie inwestorów zagranicznych oraz na rozwój gospodarczy Polski. 5. Projekt spowolni rozwój cyfrowy oraz wpłynie negatywnie na modernizację przemysłu i tworzenie nowych możliwych miejsc pracy. 6. Brak technicznych kryteriów oceny: Rząd ingeruje w wybór dostawcy zamiast ustanowić jednolite standardy techniczne. Nie określa również sprzętu objętego zakresem nowych obowiązków. Operatorzy są zobowiązani do zaprzestania kupowania sprzętu od dostawców wysokiego/ średniego ryzyka oraz do wymiany całego sprzętu od dostawców wysokiego ryzyka w ciągu pięciu lat. 7. Projekt doprowadzi do opóźnienia rozwoju sieci 5G, co negatywnie wpłynie na wygodę i łatwość obywateli w korzystaniu z zaawansowanej technologii cyfrowej, np. praca zdalna, telemedycyna, zdalna edukacja, inteligentny przemysł oraz inteligentne rolnictwo. | **Uwaga częściowo uwzględniona**  Przepisy art. 67a -67c zostały 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. Zatem także minister właściwy ds. informatyzacji będzie podejmował decyzje o ewentualnych karach także w formie decyzji administracyjnej. Przepis art. 73 został uzupełniony o wysokość kary za nie zastosowanie się do polecenia zabezpieczającego.  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 wskazany 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 Zepole 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. |
|  | S4IT Michał Podgórski | Uwaga ogólna | Z punktu widzenia rzeczywistych interesów polskich obywateli oraz przedsiębiorców, sugerujemy przeprowadzenie szerokich konsultacji społecznych, pełne wysłuchanie opinii publicznej oraz dokonanie wyczerpującej analizy skutków regulacji.   * Przyniesienie realnych korzyści dla konsumentów przez obniżenie kosztów po stronie operatorów utrzymując uczciwość równą konkurencję na rynku telekomunikacyjnym. * Uwzględniając zmniejszenie kosztów po stronie operatorów, sugerujemy przedłużyć termin usunięcia sprzętów wymienionych w art. 66b ust. 1 pkt 2 do 10 lat od daty publikacji oceny w przypadku konieczności zmiany dostawcy. * W celu umocnienia zaufania inwestycyjnego, sugerujemy ustalać jasne, wymierne i wykonalne kryteria w art. 66a ust. 4 pkt 2 i 5 i pozwolić operatorom na wybór dostawców na podstawie przejrzystych kryteriów, np. zgodnie z rozwiązaniem stosowanym w Niemczech. * Przyspieszenie rozwoju sieci 5G, aby zapewnić polskim obywatelom wygodę w korzystaniu z bardziej zaawansowanych technologii cyfrowych oraz utworzyć więcej miejsc pracy. | **Uwaga częściowo uwzględniona**  Przepisy art. 67a -67c zostały 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. Zatem także minister właściwy ds. informatyzacji będzie podejmował decyzje o ewentualnych karach także w formie decyzji administracyjnej. Przepis art. 73 został uzupełniony o wysokość kary za nie zastosowanie się do polecenia zabezpieczającego.  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 wskazany 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 Zepole 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. |
|  | Orange | Uwaga ogólna | P*rojekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy – Prawo zamówień publicznych* (dalej „Projekt”) jest bardzo rozległy, a jego treść trudna w interpretacji, co potęguje skromna treść uzasadnienia, zaskoczenie przedsiębiorców telekomunikacyjnych kształtem planowanych zmian oraz nakładanie się przepisów na projektowane nowe Prawo Komunikacji Elektronicznej, i to na 3 miesiące przed planowanym jego wejściem w życie.  Krajowy system cyberbezpieczeństwa jest w porównaniu do zawartych w Prawie telekomunikacyjnym przepisów dot. bezpieczeństwa sieci i usług telekomunikacyjnych osiągnięciem bardzo młodym, o zaledwie 2 letnim okresie obowiązywania. W okresie tym nie została wydana ani jedna rekomendacja Pełnomocnika Rządu ds. Cyberbezpieczeństwa, a podstawowe struktury tego systemu są wciąż tworzone. Dlatego poważne wątpliwości budzi destabilizacja dotychczasowego porządku regulacji bezpieczeństwa sieci i usług telekomunikacyjnych (realizowanego na gruncie Pt jako przepisów sektorowych), w szczególności przez włączenie go do systemu, który dopiero powstaje (UKSC). W połączeniu z rozszerzeniem liczby podmiotów administracyjnych o niejednoznacznych kompetencjach i odpowiedzialności, z uprawnieniami ingerowania w procesy zachodzące u przedsiębiorców prywatnych, **Projekt może wywołać skutek odwrotny od zamierzonego – zwiększy zagrożenia bezpieczeństwa, zamiast je poprawić**  **Włączenie przedsiębiorców komunikacji elektronicznej do KSC**  **Zmiana prowadzi do poważnego zaburzenia istniejącego obecnie porządku prawnego, wyznaczonego zarówno na poziomie regulacji unijnych jak i polskich**. Dyrektywy NIS, a co za tym idzie również ustawy o krajowym systemie cyberbezpieczeństwa, nie stosuje się do przedsiębiorców telekomunikacyjnych dlatego, że regulacje prawne dotyczące bezpieczeństwa sieci i usług telekomunikacyjnych znajdują się w unijnych dyrektywach telekomunikacyjnych, zastąpionych obecnie przez Europejski Kodeks Łączności Elektronicznej, który ma być przeniesiony do polskiego porządku prawnego przepisami projektowanej ustawy – Prawo komunikacji elektronicznej (PKE, która ma zastąpić obecnie obowiązującą ustawę – Prawo telekomunikacyjne).  **Demontowany jest funkcjonujący obecnie, na poziomie unijnym jak i krajowym, zrozumiały i czytelny podział** na system cyberbezpieczeństwa, który obejmuje operatorów usług kluczowych i dostawców usług cyfrowych (ustawa o krajowym systemie cyberbezpieczeństwa) oraz system bezpieczeństwa sieci i usług telekomunikacyjnych, obejmujący przedsiębiorców telekomunikacyjnych (ustawa – Prawo telekomunikacyjne, którą niebawem zastąpi ustawa – Prawo komunikacji elektronicznej). **Działanie to nie znajduje żadnego uzasadnienia w poziomie incydentów, czy wzroście zagrożeń w obszarze sieci telekomunikacyjnych**. Polscy przedsiębiorcy telekomunikacyjni od co najmniej dwóch dekad **skutecznie dbają o bezpieczeństwo swoich sieci telekomunikacyjnych oraz o bezpieczeństwo świadczonych przez siebie usług telekomunikacyjnych, na gruncie dedykowanych sektorowi telekomunikacyjnego regulacji unijnych i krajowych, z wykorzystaniem ugruntowanych, najlepszych praktyk i gromadzonej latami wiedzy eksperckiej**. Natomiast system opisany ustawą o krajowym systemie cyberbezpieczeństwa tak naprawdę dopiero powstaje. Nie ma zatem żadnego uzasadnienia, ani z perspektywy przedsiębiorców telekomunikacyjnych, ani z perspektywy operatorów usług kluczowych oraz dostawców usług cyfrowych, aby oba systemy zaburzyć, przez próbę ich łączenia na siłę, w sposób chaotyczny i nieuporządkowany, tworząc sprzeczne ze sobą albo powielające lub krzyżujące się regulacje prawne, które są sprzeczne z prawem Unii Europejskiej, na domiar złego zakładając, że polscy przedsiębiorcy będą w stanie dostosować się do nowych albo istotnie zmienionych regulacji prawnych w terminie do dnia 21 grudnia 2020 r., a więc terminie, w którym projektowana ustawa zmieniająca UKSC ma wejść w życie.  Polscy przedsiębiorcy telekomunikacyjni prowadzą zaawansowane prace nad dostosowaniem się do długo opracowywanego i konsultowanego, a niedawno przyjętego, *rozporządzenia Ministra Cyfryzacji z dnia 22 czerwca 2020 r. w sprawie minimalnych środków technicznych i organizacyjnych oraz metod, jakie przedsiębiorcy telekomunikacyjni są obowiązani stosować w celu zapewnienia bezpieczeństwa lub integralności sieci lub usług* (dalej „rozporządzenie”), którego wejście w życie dopiero przed nami, gdyż *vacatio legis* upływa 30 grudnia 2020 r. Procesy w tym zakresie są zaawansowane i poniesiono na ten cel konkretne wydatki. Tym bardziej zaskakująca jest proponowana rewolucja w systemie, skoro istotny dla bezpieczeństwa sieci i usług telekomunikacyjnych akt prawny, czyli wyżej przytoczone rozporządzenie, został dopiero co ogłoszony w Dzienniku Ustaw i oczekuje na wejście w życie, a przedsiębiorcy telekomunikacyjni są w trakcie wdrażania wymogów wynikających z tego rozporządzenia, ponosząc w tym celu wymierne koszty i podejmując istotny wysiłek organizacyjny.  Podsumowując, Projekt oznacza nieuzasadnioną, kosztowną i niemożliwą do przeprowadzenia w założonych terminach rewolucję w obszarze bezpieczeństwa sieci i usług telekomunikacyjnych. Biorąc powyższe pod uwagę, głównym i zasadniczym postulatem jest, aby utrzymać obecny, dychotomiczny model regulacji wymogów w zakresie bezpieczeństwa, tak, aby: **1) zagadnienia dotyczące bezpieczeństwa sieci i usług telekomunikacyjnych były przedmiotem regulacji ustawy – Prawo telekomunikacyjne, a w przyszłości ustawy – Prawo komunikacji elektronicznej i towarzyszących rozporządzeń wykonawczych, natomiast 2) zagadnienia dotyczące cyberbezpieczeństwa powinny pozostać przedmiotem regulacji ustawy o krajowym systemie cyberbezpieczeństwa. Należy natomiast zapewnić koordynację i wymianę informacji między tymi oboma systemami, zachowując jednak na rynku telekomunikacyjnym jednego głównego regulatora.**  Jednocześnie, rozumiejąc potrzebę stałego podnoszenia bezpieczeństwa sieci i usług telekomunikacyjnych oraz potrzebę zbudowania w pełni funkcjonalnego krajowego systemu cyberbezpieczeństwa, należy stosować logikę stopniowych i ewolucyjnych zmian. Zatem dalsze podnoszenie bezpieczeństwa sieci i usług telekomunikacyjnych powinno opierać się na następujących założeniach:   1. **wymagania w zakresie bezpieczeństwa sieci i usług telekomunikacyjnych powinny być przedmiotem regulacji zawartych w projektowanej ustawie – Prawo komunikacji elektroniczne**; już dzisiaj regulacje rynku telekomunikacyjnego dają Państwu Polskiemu, reprezentowanemu przez Ministra Cyfryzacji i Prezesa UKE, szeroki wachlarz narzędzi gwarantujących wysoki poziom bezpieczeństwa sieci i usług telekomunikacyjnych, wliczając w to możliwość określania przez Prezesa UKE, po zasięgnięciu opinii Kolegium do Spraw Cyberbezpieczeństwa, wymagań cyberbezpieczeństwa w ramach aukcji częstotliwości radiowych oraz długo opracowywane i konsultowane, niedawno przyjęte rozporządzenie Ministra Cyfryzacji z dnia 22 czerwca 2020 r. w sprawie minimalnych środków technicznych i organizacyjnych oraz metod, jakie przedsiębiorcy telekomunikacyjni są obowiązani stosować w celu zapewnienia bezpieczeństwa lub integralności sieci lub usług. System ten przewiduje branie pod uwagę zaleceń ENISA i nie ma przeszkód, by dodać do tego katalogu również zalecenia Kolegium przy czym mechanizm musiałby zostać doprecyzowany w taki sposób, aby uwzględnienie ewentualnych rekomendacji Kolegium odbywało się z poszanowaniem naturalnych procesów rozwoju i utrzymania, m.in. w zakresie sieci telekomunikacyjnych, tak, aby ograniczyć potencjalnie istotne skutki dla możliwości zachowania ciągłości i jakości usług dla ich użytkowników; 2. biorąc pod uwagę przepisy i narzędzia przewidziane w projekcie PKE, razem z przeniesionymi z ustawy – Prawo telekomunikacyjne narzędziami w zakresie wymagań dla aukcji częstotliwości oraz wdrażane właśnie rozporządzenie dotyczące bezpieczeństwa sieci i usług, jedynym racjonalnym i uzasadnionym rozwiązaniem jest wstrzymanie się z jakimikolwiek radykalnymi posunięciami do czasu wejście w życie ustawy – Prawo komunikacji elektronicznej oraz wyżej przytoczonego rozporządzenia; dalsze działania powinny być poprzedzone rzetelną oceną skuteczności obowiązujących regulacji, a ewentualne zmiany w prawie powinny być inicjowane tylko wtedy, gdy obowiązujące już i niebawem wchodzące w życie przepisy okażą się niewystarczające; 3. jeśli na podstawie analizy ww. przepisów Państwo Polskie uzna, że istniejące przepisy telekomunikacyjne są niewystarczające, to wszelkie nowe obowiązki i wymagania w tym zakresie powinny być wprowadzane do przepisów sektorowych, właściwych dla rynku telekomunikacyjnego (obecnie ustawa – Prawo telekomunikacyjne, a w przyszłości ustawa – Prawo komunikacji elektronicznej, wraz z aktami wykonawczymi), np. poprzez zmianę albo wydanie nowego rozporządzenia Ministra Cyfryzacji w sprawie minimalnych środków technicznych i organizacyjnych oraz metod, jakie przedsiębiorcy telekomunikacyjni są obowiązani stosować w celu zapewnienia bezpieczeństwa lub integralności sieci lub usług, pamiętając, że prymat należy dawać stosowaniu istniejących już przepisów i narzędzi, w miejsce tendencji do mnożenia regulacji prawnych nawet tam, gdzie nie podjęto próby wykorzystania istniejących już narzędzi – podejście takie pozwoli zachować zgodność z regulacjami unijnymi oraz zapewni jednego regulatora wiodącego, posiadającego wiedzę we wszystkich aspektach działalności przedsiębiorców telekomunikacyjnych.   Celem zachowania zgodności z prawem Unii Europejskiej oraz utrzymania obecnej, ugruntowanej, wynikającej ze specyfiki zagadnienia, jasnej i zrozumiałej formuły nie należy obejmować przedsiębiorców telekomunikacyjnych przepisami ustawy o krajowym systemie cyberbezpieczeństwa, co można osiągnąć utrzymując obecne w tej ustawie wyłączenie (wynikające z dyrektywy NIS), na mocy którego przepisów tej ustawy nie stosuje się do przedsiębiorców telekomunikacyjnych w zakresie wymogów dotyczących bezpieczeństwa i zgłaszania incydentów; jakiekolwiek ewentualne zmiany w zakresie podmiotów objętych ustawą o krajowym systemie cyberbezpieczeństwa powinny być poprzedzone zakończeniem toczącego się obecnie przeglądu dyrektywy NIS, prowadzonego przez Komisję Europejską, | **Uwaga nieuwzględniona**  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. |
|  | Orange | Uwaga ogólna | **Ocena bezpieczeństwa dostawców**  W pierwszej kolejności podkreślamy, że dotychczasowe stosowanie urządzeń różnych dostawców, w tym z krajów spoza UE nie skutkowało w naszej ocenie zwiększeniem poziomu ryzyka w sieciach telekomunikacyjnych, ani istotnymi incydentami w tym zakresie. Jako kluczowe przedsiębiorstwa branży telekomunikacyjnej w sposób stały i dogłębny analizujemy funkcjonowanie naszych sieci pod kątem możliwych naruszeń i incydentów. Nasze stanowisko wynika przede wszystkim z oceny technicznych i organizacyjnych aspektów takiej współpracy z dostawcami. Ryzyka jakie faktycznie miały wpływ na funkcjonowanie naszych sieci dobrze oddaje statystyka zgłaszanych do UKE naruszeń, przywołana również w uzasadnieniu do przyjętego ostatnio rozporządzenia do art. 175d PT gdzie wskazano: *Najczęstszymi przyczynami naruszeń były awarie sprzętu i oprogramowania (168 przypadków). Dewastacja infrastruktury spowodowała 16 naruszeń, przerwa w zasilaniu – 6, a błąd ludzki – 5. Marginalne były przyczyny spowodowane klęską żywiołową i cyberatakiem.* Taki stan rzeczy wynika w dużej mierze również z bardzo wysokiego poziomu zabezpieczenia sieci przed cyberatakami. W tym kontekście uważamy jednocześnie, że bardzo istotny nacisk należy położyć przede wszystkim na bezpieczeństwo aplikacji i urządzeń końcowych, które z naszej perspektywy stanowią kluczowe wektory ataków i zagrożeń.  Podkreślamy również wagę i potrzebę kontynuowania pogłębionej dyskusji nt. bezpieczeństwa sieci i usług telekomunikacyjnych dla procesu dystrybucji częstotliwości z pasma C. W tym kontekście, szczególnej wagi nabiera konieczność określenia zrozumiałych, racjonalnych i akceptowalnych warunków dotyczących bezpieczeństwa sieci i usług telekomunikacyjnych, jakie będą stawiane uczestnikom postępowania w sprawie rezerwacji częstotliwości z pasma C.. Jest to kluczowe dla perspektywy rozwoju sieci 5G w Polsce.  Z perspektywy operatorów telekomunikacyjnych planowany do wprowadzenia mechanizm oceny bezpieczeństwa dostawców stanowi jednocześnie rozwiązanie, które wymaga bardzo dobrego przygotowania, zarówno w warstwie konstrukcji przepisów prawnych, jak i sfery organizacyjnej i merytorycznej do dokonywania takich ocen przez instytucje państwowe. Szczególnie, że jak zauważamy nie dotyczy on wyłączenie sieci 5G, ale co uznajemy za zasadniczo słuszne także wszystkich podmiotów krajowego systemu cyberbezpieczeństwa. Nie widzimy bowiem żadnych powodów, aby sprzęt lub oprogramowanie danego dostawcy nie mogło być stosowane w sieci 5G, ale mogło być stosowane przez operatorów usług kluczowych czy podmioty publiczne, co jak wiadomo nie jest wyłącznie konstrukcją teoretyczną, ale stanem faktycznym.  Zastosowanie mechanizmu oceny będzie miało bardzo poważne konsekwencje w wielu sferach dotyczących użytkowników sprzętu i oprogramowania dostawcy ocenionego jako stwarzającego ryzyko wysokie lub umiarkowane, konkurencji na rynku, użytkowników usług czy wreszcie relacji międzynarodowych. Skala konsekwencji, których w tym stanowisku nie przedstawiamy już szczegółowo, jest tak znacząca, że uzasadnia przynajmniej pogłębioną refleksję nad przedłożoną propozycją.  Stąd uważamy, że w pierwszej kolejności należy rozważyć czy sam mechanizm oceny funkcjonującego już na rynku dostawcy w zaproponowanej formie jest najbardziej efektywny, właściwie rozkłada akcenty i czy przede wszystkim nie przenosi zbyt dużej odpowiedzialności za dokonane oceny na samą administrację publiczną i to w jej najwyższych rangach. Należy bowiem zakładać, że kluczowe decyzje będą przedmiotem wnikliwych analiz i będą mogły być w różnych formach kontestowane. Uwzględniając zaś przedstawione w projekcie ustawy kryteria oceny, wydaje się, że zarzuty mogą okazywać się zasadne narażając na niepotrzebne ryzyko i koszty zarówno podmioty wydające ocenę, jak i podmioty nią objęte.  Zanim przedstawimy nasze kluczowe postulaty odnoszące się do zaprezentowanego w projekcie ustawy modelu oceny, chcielibyśmy poddać pod rozwagę alternatywne i możliwe do równoległego stosowania sposoby działania, których wdrożenie pozwoliłoby osiągnąć podobne efekty, ale z ograniczeniem kluczowych ryzyk:   * Włączenie dostawców sprzętu lub oprogramowania do krajowego systemu cyberbezpieczeństwa i wprowadzenie odpowiednich wymagań dot. bezpieczeństwa oraz wdrożenia środków technicznych i organizacyjnych mających ograniczać poziom ryzyka. * Stworzenie mechanizmu generalnego dopuszczenia dostawców do rynku w określonych z góry sektorach krajowego systemu cyberbezpieczeństwa oraz spoza niego, jak np. w zakresie telekomunikacji, a także obszarów tych sektorów, tj. zdefiniowanie listy kluczowych zasobów/zastosowań, pod których kątem powinna być prowadzona ocena dopuszczająca dostawcę. Rozwiązanie to dawałoby możliwość instytucjom stworzenia warunków dostępu oraz przeniesienie przynajmniej części ciężaru dowodowego na dostawcę. Mechanizm ten, jako powszechny pozwalałby też na ograniczenie zarzutu stronniczości. * Oparcie się na schematach certyfikacji, które istnieją już w poszczególnych sektorach lub które są opracowywane w ramach wdrożenia „Cybersecurity Act”. Uzyskanie takiej certyfikacji powinno zostać wprowadzone jako obowiązkowe dla kluczowych zasobów/zastosowań dostawców. Ten sposób weryfikacji zapewniałby niezależną i trudną do podważenia ocenę czynników technicznych. Uwzględniając jednocześnie zalecenia wskazane w 5G Toolbox mógłby być, szczególnie dla kluczowych ryzyk, uzupełniany przez ocenę kwestii pozostających poza sferą techniki, o ile identyfikowany jest ich istotny wpływ na poziom bezpieczeństwa narodowego. * Opracowanie listy kluczowych zasobów/zastosowań oraz określenie konkretnych wymagań wobec dostawców, które takie zasoby dostarczają dla określonych sektorów. Weryfikacja ich spełnienia byłaby niezbędna dla dopuszczenia nowego sprzętu lub oprogramowania do obrotu. * Niezależnie od powyższych rozwiązań alternatywnych, w każdym przypadku jakiekolwiek decyzje skutkujące wykluczeniem muszą w pełni uwzględniać istniejącą sytuację rynkową, skutki rekomendacji, a przede wszystkim być ograniczone do kluczowych zasobów danego dostawcy oraz zapewniać użytkownikom sprzętu lub oprogramowania odpowiedni czas na dostosowanie. Generalną zasadą powinna być skuteczność oceny jedynie dla przyszłych stanów prawnych i faktycznych, a jedynie w ograniczonych przypadkach skuteczność wobec istniejących już, zakupionych lub użytkowanych urządzeń lub oprogramowania. Z tych względów jakiekolwiek wykluczenia mogące mieć skutki retroaktywne muszą posiadać odpowiednio długie okresy na wycofanie stosowania danych urządzeń lub oprogramowania, określone jako minimum 8-10 lat, co pozwoli na ograniczenie negatywnych skutków finansowych i organizacyjnych procesu wycofania. * Jednocześnie uważamy, że takie rozwiązania powinny być wprowadzane w sposób zharmonizowany na poziomie UE.   Odnosząc się natomiast wprost do zaproponowanego w projekcie mechanizmu oceny dostawców postulujemy przede wszystkim:   * Ocena dostawców nie powinna być oparta tylko o kryteria nietechniczne, które przedstawiono w projekcie ustawy. Każda ocena tego typu musi również uwzględniać kwestie techniczne w odniesieniu do zidentyfikowanych kluczowych zasobów dostarczanych przez danego dostawcę. Brak takiego elementu może skutkować zarzutami dot. zbytniej uznaniowości dokonanej oceny. Najlepszą natomiast metodą oceny kwestii technicznych jest wykorzystanie mechanizmów certyfikacji, które poza efektem w obszarze bezpieczeństwa, mają również potencjał do pobudzenia rynku, w tym budowy narodowych kompetencji w tym zakresie. * Jakiekolwiek restrykcje wprowadzane w wyniku oceny, muszą zgodnie z 5G Toolbox odnosić się wyłącznie do zdefiniowanych uprzednio kluczowych zasobów. Jednocześnie ich skutek w zakresie istniejących już stanów prawnych i faktycznych musi uwzględniać co najmniej 8-10 letni okres na wycofanie danych urządzeń lub oprogramowania, co odpowiada okresom amortyzacji oraz daje szanse na ograniczenie negatywnych skutków finansowych i organizacyjnych. Jednocześnie, niezbędne jest aby w zakresie w jakim dopuszczone jest stosowanie określonego sprzętu lub oprogramowania istniała możliwość dokonywania zakupów i wdrożeń służących zabezpieczeniu jakości i ciągłości świadczenia użytkownikom usług, w tym w przypadku sieci ruchomych w zakresie zapewniania adekwatnej do zapotrzebowania pojemności sieci. * Kryteria oceny nie mogą abstrahować zupełnie od konkretnych zastosowań danego sprzętu lub oprogramowania. Wszak, niektóre zastosowania kluczowych zasobów mogą uzasadniać nałożenie restrykcji, a inne zupełnie nie. W tym sensie inny będzie ciężar stosowania danego sprzętu lub oprogramowania w określonych systemach lub strategicznych lokalizacjach, a inny w usługach masowych. * Wniosek o sporządzenie oceny musi zostać doprecyzowany tak, aby wyraźnie określał przynajmniej kluczowe zasoby danego dostawcy pod kątem, których ma zostać dokonana ocena, identyfikować aktualnych i potencjalnych użytkowników tych zasobów oraz szczegółowo oceniać skutki ewentualnej oceny negatywnej. * Ocena dokonywana przez Kolegium powinna mieć formę decyzji administracyjnej, a ścieżkę odwoławczą należy zapewnić wszystkim zainteresowanym stronom, w tym użytkownikom sprzętu lub oprogramowania niezależnie czy poziom oceny to ryzyko wysokie, umiarkowane czy niskie.   Sposób określenia poziomów ryzyk posługuje się obecnie pojęciami nieprecyzyjnymi, jak poważne, niewielkie, znikome. W naszej ocenie wymaga to istotnego doprecyzowania. | **Uwaga częściowo uwzględniona**  Przepisy art. 67a -67c zostały 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. Zatem także minister właściwy ds. informatyzacji będzie podejmował decyzje o ewentualnych karach także w formie decyzji administracyjnej. Przepis art. 73 został uzupełniony o wysokość kary za nie zastosowanie się do polecenia zabezpieczającego.  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 Zepole 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. |
|  | Orange | Uwaga ogólna | **Ostrzeżenia i polecenia zabezpieczające**  W naszej ocenie proponowane środki są zbyt daleko idące i dają Pełnomocnikowi uprawnienia, które mogą faktycznie wpływać na sposób prowadzenia działalności gospodarczej także przez podmioty prywatne. W szczególności takie obawy budzi instytucja ostrzeżenia, która jedynie w wyniku identyfikacji zagrożenia wystąpieniem jakiegokolwiek incydentu krytycznego może skutkować nałożeniem konkretnych obowiązków, w tym w zakresie wycofania urządzeń lub oprogramowania danych dostawców (co zasadniczo powinno być przedmiotem oceny Kolegium) i to na długi 2-letni okres. Planowane do wprowadzenia rozwiązania stanowią bardzo poważne oręże w rękach Pełnomocnika, którego stosowanie w obecnym kształcie będzie wymagało bardzo wysokiego poziomu wstrzemięźliwości i dopuszczalne jedynie jako rozwiązanie zupełnie ostateczne. W innym przypadku istnieje znaczące ryzyko, że ostrzeżenia i polecenia będą wykorzystywane zbyt często, zapobiegawczo, nieproporcjonalnie i bez uwzględniania skutków finansowych po stronie podmiotów, których będą dotyczyły skutki wydania ostrzeżeń lub poleceń.  W tym obszarze przedstawiamy następujące postulaty kluczowe:   * Instytucja ostrzeżenia powinna zostać zmodyfikowana w sposób odpowiadający jej nazwie. Oznacza to, że należy usunąć odwołania do jej skutków jako poleceń, nakazów lub zakazów. W tym ujęciu ostrzeżenie powinno być wydawane jako sygnalizacja określonego ryzyka wraz ze szczegółowym uzasadnieniem oraz przedstawieniem możliwości przeciwdziałania. * W przypadku utrzymania obecnego kształtu ostrzeżenia powinno ono być wydawane w formie decyzji administracyjnej oraz ograniczone do podmiotów publicznych. * Okres na jaki mają być wydawane ostrzeżenia lub polecenia zabezpieczający musi zostać dostosowany do każdej indywidualnej sytuacji i być liczony w dniach/tygodniach, a nie wynosić, aż 2 lata. Tak długi okres wskazuje, że intencją może być stosowanie tych instrumentów nie jako reakcji na konkretne wydarzenia, ale jako instrument realizacji długoterminowej polityki. * Adresowanie ostrzeżeń lub poleceń zabezpieczających, szczególnie w ich obecnym kształcie, do podmiotów prywatnych powinno wiązać się rekompensatą kosztów i strat. * Przed wydaniem ostrzeżenia lub polecenia niezbędne jest przeprowadzenie konsultacji z podmiotem, który ma zostać nim objęty, w celu ustalenia okoliczności, stanu faktycznego oraz potencjalnych działań alternatywnych.   W ramach wskazywania oczekiwanych działań od podmiotu do którego adresowane jest polecenie lub ostrzeżenie należy każdorazowo dokonać wnikliwej analizy technicznej możliwości wdrożenia danej rekomendacji. | **Uwaga częściowo uwzględniona**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 zostałdołączony do ustawy jako załącznik nr 3. |
|  | Polsko-Chińska Główna Izba Gospodarcza SinoCham | Uwaga ogólna | Ustawa w oczywisty sposób narusza zasady niedyskryminacji i uczciwej konkurencji pomiędzy przedsiębiorcami oraz międzynarodowe umowy handlowe zawarte przez Polskę z innymi państwami. Projekt ustawy może doprowadzić do sytuacji , w której rynek będzie podlegał wpływom politycznym, co nie sprzyja wolnej konkurencji. Będzie to miało istotny negatywny wpływ na otoczenie biznesowe i całą branżę ICT w Polsce.  **Projekt narusza również zasadę niedyskryminacji opracowaną przez UE i zasadę uczciwej konkurencji zgodnie z wytycznymi Światowej Organizacji Handlu (WTO).** Jeśli Projekt zostanie przyjęty, wpłynie to na inwestycje UE w Polsce i rozwój polskiej branży ICT. Co więcej, projekt negatywnie wpłynie na wolny handel z członkami WTO i zaufanie inwestorów zagranicznych do Polski.  **Naruszenie zasad uczciwej konkurencji:** Jeśli nowe przepisy zostaną przyjęte, Kolegium uzyska de facto prawo wyboru dostawców, a rynek komercyjny będzie podlegał politycznej ingerencji, która nie sprzyja konkurencji rynkowej. Obecnie jest tylko trzech głównych dostawców sprzętu 5G. Ograniczenie do tylko jednego z nich spowoduje stłumienie konkurencji na rynku ICT i negatywnie wpłynie na rozwój branży  **Wbrew podstawowej zasadzie wolnego handlu w gospodarce rynkowej, dyskryminacja niszczy ekosystem branży ICT i zwiększa koszty dostaw i obsługi**  sprzedaży produktów z innych krajów wydaje się pomagać niekonkurencyjnym branżom i przedsiębiorstwom. W przypadku polskiej branży ICT pozbawi to branżę ICT i przedsiębiorstwa motywacji do większych inwestycji i ulepszania technologii, prowadząc do spadku konkurencyjności produktów. Z drugiej strony branża i przedsiębiorstwa w innych krajach podejmą więcej kroków w celu poprawy konkurencyjności. W rezultacie międzynarodowa konkurencyjność polskiej branży ICT i przedsiębiorstw będzie ulegać dalszemu osłabieniu. | **Wyjaśnienie**  Projekt nowelizacji jest zgodny z prawem europejskim i międzynarodowym.  Porozumienie o Wolnym Handlu GATT w art. XXI pozwala na stosowanie przez strony porozumienia wszelkich działań, jakie uważają one za niezbędne do ochrony swych żywotnych interesów bezpieczeństwa. Projektowane przepisy wpisują się wobec tego w środki opisane w art. XXI GATT.  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. |
|  | Polsko-Chińska Główna Izba Gospodarcza SinoCham | Uwaga ogólna | Jako podmiot odpowiedzialny społecznie, mamy za zadanie aktywnie rozpowszechniać racjonalne rozwiązania. Mając na uwadze utrzymanie dobrych relacji środowiska biznesowego z Rządem Polski i apelujemy o rozważenie i podjęcie następujących działań   1. Ministerstwo Cyfryzacji powinno zorganizować otwartą debatę i zaprosić odpowiednie ministerstwa, izby gospodarcze, operatorów i inne zainteresowane strony do pochylenia się i pełnego omówienia kwestii poruszonych w projekcie. 2. Rząd powinien w pełni ocenić wpływ projektu, w tym koszty i straty, na konkurencję handlową, legalność, społeczno-gospodarcze i międzynarodowe stosunki handlowe oraz klimat inwestycyjny w Polsce. 3. Zasadniczo, zablokowanie niektórych dostawców nie może rozwiązać problemów związanych z bezpieczeństwem cybernetycznym. Wnosimy o przyjęcie spójnej strategii w ramach UE, w celu zarządzania za pomocą jasnych specyfikacji technicznych i zharmonizowanych norm, zamiast wykluczania dostawców z określonych krajów. Postulujemy odwołanie się do modelu niemieckiego i równe traktowanie wszystkich dostawców, nie tylko z powodów nietechnicznych.   Z punktu widzenia racjonalności ekonomicznej, rząd musi promować dwustronny wolny handel i zmniejszać bariery w swobodnym przepływie towarów i usług. Rząd powinien ogłosić przepisy ustawowe i wykonawcze oraz środki, które sformułował i wdrożył, a także ich zmiany, jak również powinien informować o nich Światową Organizację Handlu | **Wyjaśnienie**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | Polsko-Chińska Główna Izba Gospodarcza SinoCham | Uwaga ogólna | Operatorzy telekomunikacyjni powinni otrzymać rekompensatę za koszty poniesione w związku z wymianą sprzętu lub oprogramowania, a rekompensatę powinno obliczać się na podstawie wydatków poniesionych na zakup infrastruktury lub oprogramowania, z uwzględnieniem amortyzacji i kosztów usunięcia.  **Uzasadnienie:**  Wprowadzenie przepisów art. 66b Projektu spowoduje oczywiste dla operatorów telekomunikacyjnych koszty, niezawinione przez nich, spowodowane nowymi regulacjami, które to koszty powinny być operatorom zrekompensowane przez Skarb Państwa reprezentowany przez Prezesa UKE. | **Uwaga nieuwzględniona**  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 przekazanym 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. |
|  | Polsko-Chińska Główna Izba Gospodarcza SinoCham | Uwaga ogólna | Wprowadzenie wspólnego unijnego mechanizmu certyfikacji krytycznego sprzętu i oprogramowania wykorzystywanego do weryfikacji bezpieczeństwa.  **Uzasadnienie:**  1) Ustalenie obiektywnych i jasnych kryteriów, upewnienie się, że wyniki zastosowanych kryteriów oceny są prawidłowe.  2) Skuteczniejszym będzie zmotywowanie dostawców do samokontroli i złożenia oświadczenia o wiarygodności.  3) Nietechnologiczne kryteria są bardzo często nieokreślone i wykorzystują niejasne pojęcia, które są bardzo trudne do zweryfikowania i oceny. |  |
|  | Aberit | Uwaga ogólna | Działając w imieniu spółki Aberit sp. z o. o. działającej w branży IT, chciałbym wyrazić swoje obawy związane bezpośrednio z planem wprowadzenia projektu cytowanej ustawy. Po zapoznaniu się z przepisami sądzę, że spółka w imieniu, której występuje może zostać dotknięta nowymi regulacjami. Co za tym idzie zwracam się do Państwa z prośbą o zapoznanie się z poniższymi wątpliwościami oraz rozważeniem ich w ramach prowadzonych konsultacji społecznych.  Celem naszego Państwa jest dążenie do ciągłego rozwoju, poprawy infrastruktury, ochrony praw i interesów obywateli. Niemniej jednak proponowany projekt ustawy w moim odczuciu może zaszkodzić rzeczywistym interesom obywateli Polski. Przepisy w proponowanej formie mogą wpłynąć negatywnie na ceny, wygodę i dostępność korzystania z usług komunikacyjnych, a także na zatrudnienie i przyszłe możliwości przedsiębiorców działających w objętej regulacjami branży.  1, Wprowadzenie art, 66b ust. 1 w proponowanej formie doprowadzi do powstania istotnych, wysokich kosztów dla operatorów telekomunikacyjnych, których nie powinni oni ponosić. Koszty spowodowane wprowadzeniem nowych regulacji, powinny zostać pokryte przez Skarb Państwa. Jeżeli Państwo wymaga od operatorów wymiany sprzętu i oprogramowania, narzucając im to poprzez zmiany w ustawie, powinni oni otrzymać odszkodowanie za koszty poniesione w związku z przeprowadzoną wymianą.  W przeciwnym razie wysokie koszty po stronie operatorów doprowadzą do podniesienia cen usług telekomunikacyjnych, co odbije się bezpośrednio na obywatelach korzystających z usług i ich jakości życia.   1. Projekt zakłada także wykluczenie dostawców infrastruktury ze względu na ich kraj   pochodzenia. Wykluczenie części dostawców doprowadzi do braku konkurencyjności na rynku telekomunikacyjnym, co ponownie odbije się na konsumentach i bez wątpienie zaszkodzi ich interesom. Ponadto tego rodzaju ograniczenie wywoła negatywne nastawienie zagranicznych inwestorów, przyczyniając się tym samym do zahamowania rozwoju gospodarczego Polski.  3, Projekt prowadzi także do opóźnienia rozwoju sieci 5G w Polsce. Warto podkreślić, że sieć ta jest już wysoce rozwinięta i sprawnie działa w krajach zachodnich UE. Tego rodzaju zabieg przyczyni się do poszerzenia przepaści pomiędzy Polską, a innymi, rozwiniętymi technologicznie krajami Europy. Opóźnienie rozwoju sieci 5G wpłynie również negatywnie na wygodę i łatwość obywateli w korzystaniu z zaawansowanej technologii cyfrowej, np. praca zdalna, telemedycyna, zdalna edukacja, inteligentny przemysł oraz inteligentne rolnictwo.  Biorąc pod uwagę powyższe argumenty, wyrażam swoje obawy i niezadowolenie względem przepisów ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy - Prawo zamówień publicznych. Mając na względzie dobro obywateli i rozwój gospodarczy naszego kraju żywię nadzieję, że Ministerstwo Cyfryzacjl weźmie pod uwagę opinię publiczną i podda przepisy niniejszej ustawy dodatkowym konsultacjom. | Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | Osoba fizyczna | Uwaga ogólna | Przedmiotem oceny ryzyka zakładanym w projekcie nie powinien być dostawca. Ocena ryzyka powinna dotyczyć sprzętu i oprogramowania. Uważamy, że elementem stosunkowo najmniej istotnym jest podmiot, który sprzedaje oprogramowanie i sprzęt, zaś zdecydowanie najważniejszą rzeczą jest sposób korzystania z nich. Narzędzia Unii Europejskiej - toolbox zabezpieczyły już sposób ograniczenia w odniesieniu do kluczowych aktywów. Nie widzimy potrzeby, aby polskie regulacje wykraczały poza system zabezpieczający UE. Natomiast jeżeli przepisy te wejdą w życie w proponowanym kształcie, to wpłynie w niekorzystny sposób na polskie podmioty utrudniając im poruszanie się po wolnym rynku i sprawiając, że będziemy odstawać od zachodnioeuropejskich podmiotów z branży IT. Jednocześnie poważnie Zachwieje to równowagą rynkową, konkurencyjnością polskich firm, a także atrakcyjnością Polski jako miejsca do inwestycji kapitału. Wprost wynikającym z tego problemem będzie zas wolniejszy rozwój gospodarczy Polski (np. w zakresie rozwoju firm, modernizacji przemysłu, tworzenia nowych miejsc pracy etc.} a także - co oczywiste - spowoduje to podwyższenie cen usług telekomunikacyjnych. | **Wyjaśnienie**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | Osoba fizyczna | Uwaga ogólna | Operatorzy telekomunikacyjni w myśl proponowanych przepisów zostaną obciążeni gigantycznymi kosztami wymiany sprzętu i oprogramowania, co Zachwieje wolnym rynkiem i konkurencyjnością w branży. Uważamy, że podmioty zmuszone do w/w wymian powinny uzyskać rekompensaty od Skarbu Państwa za poniesione straty. Ponieważ koszty, które powstaną wynikają bezpośrednio ze zmiany przepisów wprowadzanych przez Państwo Polskie. Prawie oczywistym wydaje się, że koszty poniesione przez operatorów zostaną przełożone na polskiego obywatela w postaci podniesionych cen abonamentów i usług telekomunikacyjnych, a co za tym idzie odbiją się wprost na polskiej gospodarce. | **Uwaga nieuwzględniona**  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 przekazanym 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. |
|  | Osoba fizyczna | Uwaga ogólna | Projekt zakłada również wyraźną dyskryminację poszczególnych dostawców. Zakładane kryteria oceny ryzyka dostawcy to wyłącznie czynniki nietechniczne np. powiązania dostawcy a polityką rządu kraju macierzystego. Dostawcy nie mają wpływu na politykę swojego kraju a są za to w myśl zaproponowanych przepisów dyskryminowani. Jest to sprzeczne z zasadami wolnego rynku i wolnego handlu. Zakazanie działań dostawców ze względu na w/w kryteria doprowadzi do zlikwidowania lub znacznego ograniczenia konkurencji rynkowej, co nigdy nie przynosi pozytywnych rezultatów. Tylko zdrowa konkurencja może nas uchronić przed ponoszeniem niepotrzebnych kosztów związanych np. z budową i renowacją infrastruktury 1T  Kolejnym szczególnie istotnym problemem, który zauważamy w projekcie jest ocena ryzyka dostawcy sprzętu lub oprogramowania ważnego z punktu państwowego systemu cyberbezpieczeństwa. Rozpoczęcie oceny ryzyka powinno być możliwe jedynie w przypadkach określonych w ustawie, aby skupić analizę ryzyka jedynie na kluczowych aktywach, nie zaś na wszystkich aktywach. Postulujemy zatem, aby kontroli podlegało wyłącznie realnie zidentyfikowane ryzyko, a ocena ryzyka była przeprowadzana w stosunku do sprzętu krytycznego z punktu widzenia bezpieczeństwa lub wówczas, gdy miały miejsce poważne naruszenia bezpieczeństwa lub wysokie podatności, których nie można złagodzić | **Wyjaśnienie**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | Osoba fizyczna | Uwaga ogólna | Dyskryminującym jest również pozbawienie możliwości zmiany wyniku oceny dokonanej przez kolegium. Dostawca powinien mieć prawo do złożenia wniosku o zmianę oceny zarówno w przypadku sprzętu i oprogramowania wysokiego, średniego jak i niskiego ryzyka. Każdy z dostawców powinien mieć takie samo - równe prawo do zaproponowania wprowadzenia planu naprawczego i środków zaradczych. Kolegium powinno posiadać możliwość zaakceptowania programu naprawy podmiotu, a co za tym idzie zmianę oceny. Tylko taka regulacja pozwoli na równe traktowanie wszystkich podmiotów | **Uwaga nieuwzględniona**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | Osoba fizyczna  Pan Filip Walczak  Młodzieżowy Delegat RP do NATO | Uwaga ogólna  Uwaga ogólna | Projekt zmian, jakkolwiek konieczny w zmieniającej się rzeczywistości, budzi pewne konkretne obawy. Wierzę, że społeczny głos w tej sprawie zostanie wzięty pod uwagę i pozwoli uniknąć stworzenia niekorzystnych bądź nieefektywnych przepisów.  Z projektu w obecnym kształcie wynikną niepokojące różnice w traktowaniu poszczególnych dostawców. Proponowane kryteria oceny to wyłącznie kryteria nietechniczne, które w tak specjalistycznej branży powinny mieć możliwie najmniejsze znaczenie. Tylko jasne, szczegółowo sprecyzowane kryteria techniczne są w stanie ocenić ryzyko wiążące się z danym dostawcą i jego sprzętem bądź usługami. Kryterium decydującym nie może być np. polityka rządu kraju pochodzenia dostawcy lub sprzętu. W obecnej globalnej sytuacji rynkowej, w której największe podmioty w branży są w skomplikowany sposób powiązane z całym szeregiem państw, tak szerokie, nietechniczne kryteria oceny mogą prowadzić do paraliżu całej branży. Jest to w sposób oczywisty sprzeczne z zasadami wolnego rynku i wolnego handlu zagwarantowanego w wielu przepisach i umowach międzynarodowych. Jawna dyskryminacja będzie zaś prowadziła do znacznego ograniczenia konkurencji rynkowej, co zawsze okazuje się ostatecznie niekorzystne dla wszystkich, w szczególności zaś dla końcowego odbiorcy usługi.  Pokrewnym elementem, istotnym z gospodarczego punktu widzenia, jest konieczność zmiany przedmiotu oceny ryzyka: zamiast charakterystyki dostawcy, w pierwszej kolejności winien być oceniany sam sprzęt i jego oprogramowanie. W ramach Unii Europejskiej wypracowano już w tym zakresie odpowiednie zabezpieczenia, potocznie określane jako EU Toolbox, i nie ma podstaw, dla których polskie normy powinny być bardziej restrykcyjne niż wspólnotowe. Proponowane przepisy sprawią, że poruszanie się na rynku IT będzie znacznie utrudnione w porównaniu do naszych zachodnioeuropejskich partnerów, i w wyraźny sposób wpłynie na naszą atrakcyjność inwestycyjną. Polska jako miejsce do inwestycji kapitału jest dzisiaj wyjątkowo atrakcyjna, a wprowadzenie niepotrzebnych ograniczeń prawnych może tę atrakcyjność zmniejszyć. Dynamiczny rozwój gospodarczy Polski jest w interesie wszystkich podmiotów, ale przede wszystkim w leży on w interesie nas - obywateli, którzy mogą korzystać z rozwijającej się rzeczywistości gospodarczej i ekonomicznej, w której żyjemy.  Obciążanie operatorów komunikacyjnych znacznymi kosztami wymian sprzętu i oprogramowania, niczym niezawinionych przez podmiot, a wynikających wprost z proponowanych przepisów, jest wysoce niesprawiedliwe. Koszty te powinny być przynajmniej częściowo rekompensowane przez państwo. W przypadku wejścia w życie ustawy w obecnym kształcie, bardzo realnym wydaje się być scenariusz, w którym to operatorzy przeniosą swoje koszty na abonentów, co z kolei wpłynie niekorzystnie na rozwój gospodarczy Polski i na odbiorców końcowych.  Pozbawienie niektórych podmiotów możliwości zmiany oceny dokonanej przez Kolegium prowadzi do nierówności poszczególnych podmiotów z branży wobec prawa. Projekt odmawia prawa do złożenia wniosku o zmianę oceny ryzyka przez podmioty najsurowiej ocenione przez Kolegium. Wydaje się to wysoce niesprawiedliwe, gdyż każdy z dostawców powinien mieć zagwarantowane takie same uprawnienia, niezależnie od przypisywanego mu ryzyka. Kolegium nie może być uznane za organ nieomylny. Każdy z podmiotów powinien mieć również równe prawo do wprowadzenia programu naprawczego i środków zaradczych, a samo Kolegium powinno mieć możliwość zmiany decyzji | Przepisy art. 66a-66c zostały 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 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  |
|  | Pan Filip Walczak  Młodzieżowy Delegat RP do NATO | Uwaga ogólna | Projektowany Art. 67b ust. 3 Ustawy ustanawia zamknięty katalog określonych zachowań, jakie mogą zostać wskazane przez Pełnomocnika w ostrzeżeniu. Dynamiczny rozwój nowych technologii i stale zmieniająca się natura cyberzagrożeń powodują, że katalog ten winien być otwarty poprzez dodanie określenia „w szczególności". Pozwoli on Pełnomocnikowi na bardziej elastyczne i skuteczne reagowanie na potencjalne zagrożenia, bez niepotrzebnego związania wąskimi normami kompetencyjnymi. W tym miejscu należy nadmienią iż *a contrario* Art. 67c ust. 4 słusznie zawiera zamknięty katalog określonych zachowań możliwych do nakazania przez Pełnomocnika. Potrzeba pewności prawa wymaga, aby polecenia podlegające natychmiastowemu wykonaniu były ściśle i jasno umocowane w prawie. Odmienny, mniej rygorystyczny charakter ostrzeżeń, zasługuje na odmienne podejście i przyznanie większej swobody Pełnomocnikowi. | Przepisy art. 67a -67c zostały zmienione. Ostrzeżenia w dalszym ciągu będzie wydawał Pełnomocnik.  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. |
|  | ERSTAR | Uwaga ogólna | Jako firma będąca w pełni zaangażowana w rozwój branży ICT oraz mająca swój wkład w rozwój technologiczny Polski, czujemy się zaniepokojeni Projektem Ustawy, który może mieć negatywny wpływ zarówno na naszą firmę, jak i pokrewne branże związane z rynkiem ICT.  Zdajemy sobie sprawę, że Rząd dokłada wszelkich starań, aby poprawić cyberbezpieczeństwo kraju, jednak Projekt Ustawy zawiera kryteria, które z pewnością nie będą sprzyjały konkurencyjności na rynku, ze względu na możliwość wpływu na przedsiębiorców poprzez ograniczanie zakresu prowadzenia ich działalności. Zapisy proponowane w Projekcie wpłyną zatem negatywnie na zatrudnienie i rozwój branży telekomunikacyjnej, co w konsekwencji może opóźnić proces cyfryzacji w Polsce. Naszym zdaniem, aby poprawić cyberbezpieczeństwo polskich sieci, warto wziąć pod uwagę ustalenie obiektywnych i jasnych kryteriów oceny ryzyka, opierając się na zasadzie transparentności oraz upewnienie się, że wyniki zastosowanych kryteriów oceny są prawidłowe. Warto rozważyć ustanowienie wspólnego unijnego mechanizmu certyfikacji dla krytycznego sprzętu i oprogramowania, który obowiązywałby dla wszystkich, niezależnie od kraju pochodzenia. Wierzymy, że takie podejście wpłynęłoby na zwiększenie poziomu cyberbezpieczeństwa w Polsce. Proponujemy, aby Ministerstwo Cyfryzacji zorganizowało otwartą debatę i zaprosiło zainteresowane strony do pochylenia się i pełnego omówienia kwestii poruszonych w Projekcie. Rząd powinien w pełni ocenić wpływ Projektu, w tym koszty i straty, konkurencję handlową, legalność, społeczno-gospodarcze i międzynarodowe stosunki handlowe oraz klimat inwestycyjny w Polsce. Wyrażamy nadzieję, że nasza opinia zostanie wzięta pod uwagę. | **Wyjaśnienie**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | ETOB-RES | Uwaga ogólna | Łączenie zagrożeń gospodarczych, kontrwywiadowczych i terrorystycznych z dostawcą sprzętu i oprogramowania jest nieracjonalne i nielogiczne. Ważniejszym pytaniem powinno być, jak nie korzystać z tego sprzętu tak, aby stanowił on takie zagrożenie, a nie kto go sprzedaje. Zestaw narzędzi UE (Toolbox) przewiduje możliwość podjęcia środków ograniczających w odniesieniu do kluczowych aktywów. Polskie propozycje w projekcie wykraczają poza wymagania zestawu narzędzi UE.  Zaproponowane w art. 66a ust. 4 kryteria oceny ryzyka nie są jasne. Powinny one zostać ustalone w sposób obiektywny, pozbawiony wątpliwości, co zagwarantowało by, że ich zastosowanie da rzetelne wyniki oceny ryzyka. W chwili obecnej kryteria nietechnologiczne wykorzystują niejasne pojęcia, które są trudne do zweryfikowania i oceny.    Wycofanie i wymiana sprzętu z krytycznym oprogramowaniem będzie wymagała zmiany całego projektu sieci i ogromnej części sieci, zajmie to dużo czasu, w przeciwnym razie wpłynie to na stabilność sieci. Również koszty będą bardzo wysokie. Narzucony okres 5 lat jest zbyt krótki aby przeprowadzić tego typu zmiany. Celowym jest wydłużenie okresu do co najmniej 10 lat. Ponadto okres 3 miesięcy dla przygotowania i przedstawienia planu i harmonogramu dla wycofania z infrastruktury dostawcy usług sprzętu i oprogramowania jest praktycznie niemożliwy do wdrożenia i powinien zostać wydłużony co jednego roku. | **Uwaga częściowo uwzględniona**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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 został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | Fundacja Alatum | Uwaga ogólna | Proponowany termin wycofywania z rynku sprzętu, usług i oprogramowania w przypadku wydania niekorzystnej oceny przez Kolegium jest bardzo niepokojący. W branży IT proponowany 5-cio letni termin jest okresem wyjątkowo krótkim, który niewątpliwie wpłynie na stabilność całej sieci. Oczywistym wydąje się, że stabilność sieci leży w interesie wszystkich - zarówno rządzących, jak i przedsiębiorców. Dlatego też dużo bardziej adekwatnym i mniej niepokojącym byłby termin 10-cio letni. Musimy pamiętać, że wycofanie z rynku sprzętu, usługi i oprogramowania niesie za sobą gigantyczne koszty i jest to bardzo skomplikowany proces. Rozsądnym byłoby również wprowadzenie rekompensat rządowych dla podmiotów zmuszonych nowymi przepisami do poniesienia tych kosztów. Podmiot nie ma wpływu na nowo tworzone przepisy, które mogą w konsekwencji zmuszać go do poniesienia gigantycznych nakładów finansowych. Pamiętajmy również o tym, że podmioty będą starały się zrekompensować sobie takie straty przenosząc ten koszt bezpośrednio na beneficjentów usług czyli przedsiębiorców i obywateli, co będzie skutkowało znaczącym wzrostem cen usług abonamentowych. | **Uwaga częściowo uwzględniona**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | Fundacja Alatum | Uwaga ogólna | Nowe przepisy zakładają możliwość wpływania przez Kolegium w sposób bardzo niejasny na niektóre podmioty. W branży cybernetycznej można stworzyć szczegółowe wytyczne techniczne, które zablokują możliwość niejasnych i niczym niekontrolowanych możliwości oceny przez Kolegium. Takie techniczne przepisy odsuną od nas widma niejasnego, niesprawiedliwego i nierównego traktowania. Ograniczą też potencjalną korupcję i patologiczne możliwości wpływania na werdykt Komisji. Zasadnym wydąje się też włączenie w postępowanie oceniające samego podmiotu ocenianego np. poprzez możliwość złożenia wyjaśnień. Uważamy również, że jedynie możliwość odwołania od decyzji równa dla wszystkich podmiotów oraz zgodna z przepisami KPA będzie gwarantowała równe traktowanie zagwarantowane nam w Konstytucji.  W projekcie zauważamy również niesprawiedliwość społeczną związaną z zakładanymi kryteriami ryzyka. Wszystkie te kryteria to wyłącznie czynniki nietechniczne, które w branży IT powinny mieć drugorzędne znaczenie. Proponowane przepisy zakładają, że dostawcy mają jakikolwiek wpływ na politykę rządu państwa z którego się wywodzą, podczas gdy doskonale wiadomo, że nie odpowiada do rzeczywistości. Wykluczanie w ten sposób podmiotów za nieswojej winy znacząco wpływa natomiast na wolny rynek i ograniczenie konkurencji. Sztuczne zmniejszanie ilości podmiotów na rynku wpłynie zdecydowanie na wzrost kosztów związanych np. z budową i renowacją infrastruktury technicznej.  W naszej ocenie proponowany projekt zmian przyniesie wiele opóźnień we wprowadzaniu najnowszych technologii na polski rynek, a tylko szybka budowa sieci 5G może zmniejszyć przepaść między naszym krajem a zachodnią Europą. Perspektywa nowoczesnej gospodarki jest bliska każdemu z nas i tylko ona zagwarantuje nam konkurencyjność w starciu z bogatszymi i lepiej rozwiniętymi państwami UE. Nowe przepisy powinny wspierać innowację i technologię, która w bezpośredni sposób przekłada się na szybki rozwój polskiej gospodarki.  Ostatnią rzeczą na którą pragniemy zwrócić uwagę jest umieszczanie w ustawie przepisów dotyczących przedsiębiorstw komunikacji elektronicznej. Przedsiębiorstwa te objęte są szczegółowymi przepisami Prawa Komunikacji Elektronicznej, a nakładanie się tych przepisów niewątpliwie wprowadzi chaos interpretacyjny i konflikty prawne. Sytuacja taka - podobnie jak wcześniejsze przez nas wymienione - zdecydowanie nie będzie korzystnie wpływać na szybki rozwój branży IT. Przepisy dotyczą bardzo specyficznej części gospodarki, w której każde opóźnienie znacząco wpływa na rynek, a przepaść która będzie się tworzyć będzie za chwilę niemożliwa do nadrobienia. Polska powinna dbać o zmniejszanie dystansu miedzy naszym krajem a krajami wysokorozwiniętymi, bo jest to w sposób oczywisty korzystne dla każdego polskiego obywatela.  Konsultacje społeczne mają na celu zwrócenie rządzącym uwagi na problemy, których dotykają proponowane zmiany przepisów tak, aby stworzone przepisy dawały zarówno rządowi jak i obywatelowi korzystne, jasne, sprawiedliwe i równe prawo. Wierzymy, że również i te konsultacje doprowadzą do pozytywnych rezultatów dla wszystkich stron. Dziękujemy za możliwość zabrania głosu i za potencjalny wkład w powstanie jak najlepszych regulacji prawnych. | **Uwaga częściowo uwzględniona**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3.  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 krajowym.  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. |
|  | GBX Soft | Uwaga ogólna | Z uwagi na fakt, że Ustawa dotyczy bezpośrednio mojej osoby oraz działalności jaką prowadzę, szczegółowo zapoznałem się z projektem, który wydaje się być w pewnym zakresie niekorzystny. Moją szczególną uwagę przykuły przepisy, dotyczące oceny ryzyka, które pozwoliłem sobie wskazać w dalszej treści pisma. |  |
|  | Instytut Lema | Uwaga ogólna | Na wstępie należy wskazać na potrzebę publicznej dyskusji nad kwestią cyberbezpieczeństwa i jej regulacji. Jest to temat niezwykle aktualny i istotny dla społeczeństwa. Projekt ustawy to regulacja o szerokim zakresie przedmiotowym, mająca duże znaczenie dla rynków regulowanych oraz procesu wdrażania sieci 5G, dostawców infrastruktury i oprogramowania a także użytkowników. Z tych też powodów konieczna jest precyzja i spójność regulacji.  W pierwszej kolejności, należy zwrócić uwagę na zaproponowane w projekcie rozwiązanie, w ramach którego Kolegium ds. Cyberbeczpieczeństwa zyskuje uprawnienie do możliwość oceny ryzyka dostawcy sprzętu lub oprogramowania istotnego dla cyberbezpieczeństwa podmiotów krajowego systemu cyberbezpieczeństwa. Kryteria dokonywania oceny nie zostały w projekcie dostatecznie jasno sprecyzowane i mogą budzić wątpliwości. Jeżeli ocena danego dostawcy sprzętu lub oprogramowania określi ryzyko jako umiarkowane lub niskie, to dostawca może przedstawić środki zaradcze i plan naprawczy. Jeżeli Kolegium zaakceptuje tę propozycję, to ocena ryzyka tego dostawcy może być zmieniona. W przypadku oceny ryzyka określającej wysokie ryzyko, podmioty krajowego systemu cyberbezpieczeństwa nie będą mogły wprowadzać do użytkowania sprzętu, oprogramowania i usług określonych w ocenie danego dostawcy sprzętu lub oprogramowania. Z kolei dotychczas używany sprzęt, oprogramowanie i usługi określone także oddziaływać na rynek pracy, bowiem rozwój sieci 5G, z pewnością wiązać się będzie ze zwiększeniem zatrudnienia w branży. Dlatego też niezbędne jest zaprojektowanie takiej regulacji, która tworzyłaby przyjazne warunki dla podmiotów, m.in. dostawców sprzętu i oprogramowania, które poprzez swoją działalność będą napędzać także rozwój gospodarczy kraju.  Podsumowując, należy wskazać, iż procedowana regulacja wymaga szerszego spojrzenia na kontekst gospodarczy. Projektowane przepisy powinny w sposób maksymalnie precyzyjny i jasny wskazywać kryteria wyboru dostawców sprzętu, oprogramowania oraz usług, oparte o wymogi techniczne i specjalistyczne. Taki kierunek regulacji jest niezbędny dla utrzymania na rynku konkurencyjności, która pozytywnie będzie wpływać na rozwój gospodarczy kraju, nowych technologii a także sieci 5G. Przepisy powinny w najwyższym stopniu zabezpieczać pluralizm podmiotów funkcjonujących na rynku. Takie rozwiązanie daje gwarancje ochrony interesów podmiotów słabszych, a więc konsumentów, z drugiej zaś strony ma przełożenie na konkurencyjność i stan gospodarki.  Niewątpliwie, z uwagi na wagę regulacji, powinno się jak najszerzej rozpatrywać skutki jakie może ona nieść dla rynku. Wybór dostawców oparty o niejasne kryteria, jak wskazano wyżej, może spowodować nie tylko ograniczenie konkurencyjności i co się z tym wiąże opóźnienia we wdrożeniu sieci 5G, ale także, w przypadku wydania wobec dostawcy oceny określającej wysokie ryzyko oraz idący za tym zakaz wprowadzania do użytkowania sprzętu, oprogramowania i usług określonych w ocenie danego dostawcy sprzętu lub oprogramowania przez podmioty krajowego systemu cyberbezpieczeństwa, kosztów związanych z wycofaniem. Dlatego też projektowane przepisy powinny być redagowane w sposób jasny i precyzyjny po dokonaniu wnikliwej i wszechstronnej analizy skutków regulacji.  Liczymy, iż nasze uwagi zostaną wzięte pod rozwagę i będą pomocne dla dalszego procedowania projektu. | **Wyjaśnienie**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | Mobile Logic | Uwaga ogólna | Niestety proponowane przepisy wydają nam się być nie do przyjęcia. Ich wdrożenie wywoła negatywne skutki zarówno dla gospodarki kraju jak i samych obywateli. Spowoduje to zahamowanie rozwoju sieci 5G, która dobrze działa w rozwiniętych technologicznie krajach zachodnich. Polska chcąc być partnerem biznesowym na arenie międzynarodowej powinna nadążać za digitalowym rozwojem Europy i nadążać za wprowadzanymi trendami. Przyjęcie przepisów w aktualnym brzmienie wywoła opóźnienie wprowadzenia i rozwoju sieci 5G o co najmniej kilka lat, co w dobie technologicznego pędu będzie nie do nadrobienia. Ponadto bez wątpienia polska gospodarka straci w oczach zagranicznych inwestorów, którzy zostaną bezpośrednio dotknięci niniejszą regulacją oraz stracą zaufanie, być może poczują się także dyskryminowani, a samo ograniczenie wywoła w Polsce brak konkurencji co może powodować wzrost kosztów dla usług telekomunikacyjnych, co odbije się także na konsumentach. | **Wyjaśnienie**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | Mobile Logic | Uwaga ogólna | Przepisy ustawy nie są jasne, chociażby w zakresie kryteriów oceny ryzyka, co powodować będzie w przyszłości wiele zamieszania, sporów i niedomówień o wysoce kosztownych skutkach  Niezapewnienie stronom zainteresowanym możliwości wniesienia odwołania od oceny ryzyka jest niezgodne z przepisami konstytucji oraz postępowania administracyjnego i wymagają bezwzględnej zmiany.  Terminy jakie projekt ustawy nakłada na przedsiębiorców są przez nich niemożliwe do dochowania. Działania jakich się od nich wymaga są długoterminowe oraz niezwykle kosztowne. Niemożliwym jest całkowite przeorganizowanie sieci w terminie pięciu lat z jednoczesnym zachowaniem jej stabilnego funkcjonowania  Ponadto w ustawie nie ma słowa o tym kto pokryje związane z ww. zmianami koszty. Jeśli zrobić będą to mieli sami operatorzy związane to będzie zapewne z podniesieniem ceny oferowanych przez nich usług. Zapłacą więc konsumenci. Zasadnym jest zatem aby operatorzy dotknięci obowiązkiem wprowadzenia zmian w związku z wejściem w życie nowych przepisów otrzymali odszkodowanie pokryte z budżetu państwa  Projekt ustawy jak mam nadzieję Państwo zauważą spotyka się z wieloma kontrowersjami, a co za tym idzie wymagane jest jego poprawienie i dostosowanie do realiów oraz gospodarki. Na chwilę obecną wywołać on może wiele szkodliwych i trudnych w usunięciu skutków | Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | Mobilne Miasto | Uwaga ogólna | **POSTULAT RZETELNYCH KONSULTACJI SPOŁECZNYCH**  Termin konsultacji społecznych należy zdecydowanie przedłużyć, z uwagi na wskazaną wyżej, a także w naszym piśmie z dnia 15.09.2020 r. wagę dokumentu, do 45 dni. Należałoby przy tym przygotować pełną listę interesariuszy i umożliwić ich rzeczywisty udział w konsultacjach, w szczególności: organizacje samorządów terytorialnych, organizacje przedsiębiorców, organizacje konsumentów, instytucje odpowiedzialne za ochronę konkurencji i konsumenta, Radę Dialogu Społecznego.  **POSTULAT ZORGANIZOWANIA KONFERENCJI UZGODNIENIOWEJ ORAZ WCZEŚNIEJSZEGO WYSŁUCHANIA PUBLICZNEGO**  Zgodnie z § 44 Regulamin pracy Rady Ministrów, zwracamy się z uprzejmą prośbą o zorganizowanie przez Ministerstwo Cyfryzacji konferencji uzgodnieniowej oraz zaproszenie do udziału wszystkich interesariuszy, którzy wnieśli swoje uwagi, gdyż z pewnością przyczyniłaby się ona do właściwego prowadzenia uzgodnień i zaopiniowania projektu ustawy.  **POSTULAT RZETELNEJ ANALIZY SKUTKÓW SPOŁECZNYCH,**  **GOSPODARCZYCH I POLITYCZNYCH ORAZ POKAZANIA W OCENIE SKUTKÓW REGULACJI WYNIKAJĄCYCH Z TEGO PEŁNYCH KOSZTÓW REGULACJI**  W zakresie skutków społecznych należałoby opisać wpływ projektowanych przepisów na likwidację miejsc pracy, obniżenie dostępności nowoczesnych usług (w tym usług mobilności, do których zarejestrowanych jest ok. 4 milionów Polaków), wzrost wykluczenia cyfrowego wynikający z wyższego kosztu usług dla konsumentów i przedsiębiorstw: nie tylko w obszarze, transportu i mobilności, ale także w obszarach pracy zdalnej, zdalnej edukacji, telemedycyny, rozwoju inteligentnych usług samorządowych (smart cities) oraz nowoczesnych rozwiązań w rolnictwie, ochronie środowiska czy energetyce.  **PROPONOWANY KIERUNEK ZMIAN**  Rynek usług łączności elektronicznej powinien wg nas nadal pozostać kompleksowo regulowany sektorowe, ze względu na jego szczególne cechy. Dlatego uważamy, że docelowym miejscem uregulowania kwestii obowiązków operatorów telekomunikacyjnych w zakresie bezpieczeństwa sieci i usług jest projektowana ustawa Prawo Komunikacji Elektronicznej (PKE),. Należałoby więc pozostawić kompetencje Prezesa UKE uregulowane w art. 39-49 projektu PKE. Model przedstawiony w PKE zapewnia bowiem szereg narzędzi pozwalających zapewnić cyberbezpieczeństwo infrastruktury telekomunikacyjnej | **Uwwaga nieuwzględnioana**  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 krajowym.  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. |
|  | Nanocoder | Uwaga ogólna | Niniejszym pismem chciałbym wyrazić swoją opinię względem projektu o krajowym systemie cyberbezpieczeństwa. Nie ukrywam, że proponowany projekt wywołuje we mnie ogromne oburzenie i moim zdaniem jest nie do zaakceptowania w proponowanej formie.  Nie dość, że koliduje on z przepisami prawa polskiego, prawa unijnego to także jest niezwykle niekorzystny dla przedsiębiorców działających na terenie naszego kraju oraz dla pozostałych obywateli, występujących w roli konsumentów.  Przede wszystkim warto zaznaczyć, że KSC jest transpozycją dyrektywy NIS w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, która nie ma zastosowania do operatorów telekomunikacyjnych. Ich prawa i obowiązki zostały szczegółowo określone w prawie telekomunikacyjnym poprzez przyjęcie kodeksu komunikacji elektronicznej. W związku z tym dodanie przedsiębiorstwa komunikacji elektronicznej jako podmiotu, do którego stosuje się KSC, powoduje nakładanie się i potencjalny konflikt w przepisach. Przepisy komunikacji elektronicznej zawierają już kompleksowe wymagania wobec operatorów telekomunikacyjnych.  Przyjęcie przepisów ustawy w takiej formie spotka się bez wątpienia z ogromnym niezadowoleniem społeczeństwa oraz wywrze negatywne skutki w branży telekomunikacyjnej, które odczują także konsumenci.    W związku z powyższym liczę, że Ministerstwo Cyfryzacji  szczegółowo zapozna się z wyrażoną opinią społeczeństwa i zdecyduje o naniesieniu niezbędnych zmian do projektu ustawy. | **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 krajowym.  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. |
|  | NeuroGames Lab | Uwaga ogólna | Odbieram ze znacznym niepokojem planowaną nowelizację przepisów ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy - Prawo zamówień publicznych i w związku z tym chcę skorzystać z możliwości związanych z prowadzonymi konsultacjami społecznymi projektu ustawy. Propozycje umieszczone w projekcie odbieram jako bezpośredni atak na operatorów telekomunikacyjnych w Polsce, który pośrednio odbije się także na sytuacji wszystkich ich abonentów.  Po pierwsze olbrzymie koszty po stronie operatorów telekomunikacyjnych zostaną wygenerowane wprowadzeniem przepisów art. 66b, zakazujących użytkowania sprzętu lub oprogramowania pochodzącego od dostawców obarczonych oceną średniego i wysokiego ryzyka oraz w przypadku wysokiego ryzyka także nakazujących ich wycofanie w ciągu 5 lat od ogłoszenia komunikatu o takiej ocenie. Koszty wymiany sprzętu ostatecznie poniosą oczywiście abonenci. Przyjęcie rozwiązań proponowanych w nowelizacji ustawy przez operatorów spowoduje ich zmuszenie do wymiany posiadanej infrastruktury, pomimo że nie ponoszą przecież żadnej winy za podejmowane na etapie zakupu wynagrodzenia decyzje biznesowe dotyczące wyboru dostawców. Koszty te powinny zostać poniesione przez Skarb Państwa. W innym wypadku mówimy o jawnym pogwałceniu prawa własności i niejako wywłaszczeniu wcześniej zakupionego przez tych operatorów sprzętu. Poniosą oni nie tylko koszty zakupu nowego sprzętu, które nie byłyby konieczne w dotychczasowym stanie prawnym, ale także dodatkowe koszty związane z wycofaniem starego sprzętu. Dlatego konieczne jest wprowadzenie mechanizmu rekompensującego operatorom koszty poniesione w związku z wymianą sprzętu lub oprogramowania obarczonego wysokim ryzykiem. Rekompensata ta powinna być wypłacona w wysokości, która pokryje wydatki poniesione w związku z zakupem odpowiedniego sprzętu lub oprogramowana, koszty amortyzacji i wydatków związanych z wycofaniem z użycia dotychczasowego wyposażenia | **Wyjaśnienie**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3.  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 przekazanym 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. |
|  | NeuroGames Lab | Uwaga ogólna | Po drugie zdecydowanie za krótki jest przewidziany w art. 66b ustawy 5-letni okres na wycofanie z użytkowania sprzętu, oprogramowania i usług świadczonych przez dostawcę, którego ryzyko oceniono jako wysokie. Decyzje o inwestycji w sprzęt i oprogramowanie są podejmowane w wieloletniej perspektywie i aby umożliwić amortyzację poniesionych kosztów. Projektowany obowiązek wycofania sprzętu z użytkowania mniej dotkliwie dotknie operatorów komunikacyjnych, którzy zakupili sprzęt wiele lat wcześniej, niż tych, którzy dokonali inwestycji krótko przed ogłoszeniem komunikatu o wysokim ryzyku danego dostawcy. Te różnice z jednej strony powinny zostać uwzględnione przy udzielaniu rekompensat (których aktualnie projekt ustawy w ogóle nie przewiduje, o czym mowa powyżej), a z drugiej powinny wpłynąć na wydłużenie okresu na wycofanie z użytkowania sprzętu, oprogramowania i usług świadczonych przez dostawcę do lat 10. Z tych samym względów powinien również zostać wydłużony (do 1 roku) jeszcze bardziej nierealistyczny zakładany przez art. 66c ustawy 3-miesięczy termin na sporządzenie i dostarczenie planu i harmonogramu wycofania z użytkowania sprzętu, oprogramowania i usług dostawcy sprzętu lub oprogramowania, którego dotyczy ocena określająca wysokie ryzyko.  Mam nadzieję, że Ministerstwo ponownie rozważy potencjalny wpływ projektowanych rozwiązań na koszty prowadzenia działalności gospodarczej w Polsce oraz dodatkowe koszty, którymi w ich rezultacie zostaną obarczeni abonenci i wypracuje modeł, który nie będzie za sobą niósł tak szkodliwych gospodarczo konsekwencji. | **Uwaga częściowo uwzględniona**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3.  Zrezygnowano z planów wycofania sprzętu lub oprogramowania. |
|  | SmartWeb Media | Uwaga ogólna | Szczególne wątpliwości budzi przedstawiony w Projekcie mechanizm dokonywania oceny ryzyka dostawcy sprzętu lub oprogramowania istotnego dla cyberbezpieczeństwa podmiotów krajowego systemu cyberbezpieczeństwa.  Zgodnie z dodawanym Projektem art. 66a ustawy o krajowym systemie cyberbezpieczeństwa, ocena ta dokonywana jest przez Kolegium w oparciu o otwarty katalog kryteriów przedstawionych w ust. 4 projektowanego art. 66a tejże ustawy. Kryteria te opierają się o kryteria, które można podzielić na:  1) zewnętrzne - tj. analizę zagrożeń bezpieczeństwa narodowego o charakterze ekonomicznym, kontrwywiadowczym i terrorystycznym oraz zagrożeń dla realizacji zobowiązań sojuszniczych i europejskich, jakie stanowi dostawca sprzętu i oprogramowania, jego powiązania z państwami spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, a także zdolność ingerencji w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania oraz ich prawodawstwo tych państw w zakresie ochrony danych osobowych,  2) wewnętrzne - związane ze strukturą własnościową dostawcy sprzętu lub oprogramowania oraz stopniem sprawowanego nadzoru nad procesem wytwarzania i dostarczania sprzętu lub oprogramowania  3)administracyjne — związane z liczbą i rodzajem oraz sposobem i czasem eliminowania wykrytych podatności i incydentów oraz treścią wydanych wcześniej rekomendacji, dotyczących sprzętu lub oprogramowania danego dostawcy.  Analiza przedstawionych kryteriów prowadzi do wniosku, że kryteria te trudno określić jako przejrzyste i wymierne. Opierają się one m.in. o czynniki nietechniczne, zewnętrzne, związane z zależnościami politycznymi między dostawcą a jego krajem pochodzenia oraz otoczeniem regulacyjnym, w którym dany dostawca funkcjonuje, co stanowi jawną dyskryminację dostawców ze względu na pochodzenie. Kryteria te nie przedstawiają jednolitych standardów technicznych, lecz subiektywne przesłanki, które mają decydować o wyborze dostawcy. Rozwiązanie to zdecydowanie odbiega od standardów przyjętych w innych państwach Unii Europejskiej stosujących transparentne i techniczne standardy cyberbezpieczeństwa oraz systemy certyfikacji sprzętu oraz oprogramowania.  W związku z powyższym, sugerujemy zastąpienie projektowanych kryteriów oceny zobiektywizowanymi przesłankami technicznymi, opierającymi się o przestrzeganie międzynarodowych lub uznawanych w UE standardów cyberbezpieczeństwa, np. IS027001, Wspólne Kryteria, Network Equipment Security Scheme, EU Cybersecurity Certification Scheme, certyfikację sprzętu oraz monitoring bezpieczeństwa.  Niezależnie od przedstawionych powyżej wątpliwości związanych z metodologią oceny ryzyka, dostawcy sprzętu lub oprogramowania istotnego dla cyberbezpieczeństwa podmiotów krajowego systemu cyberbezpieczeństwa, niepokój wzbudza już sama procedura administracyjna związana z procesem dokonywania tejże oceny, sprzeczna z fundamentalnymi zasadami postępowania administracyjnego wyrażonymi w ustawie z dnia 14 czerwca 1960 r. - Kodeks postępowania administracyjnego **(„k.p.a.”),** w szczególności z art. 10 k.p.a. wprowadzającym zasadę czynnego udziału strony w postępowaniu. Projektowane regulacje nie przewidują możliwości udziału poddawanego ocenie dostawcy w postępowaniu, który (zgodnie z obecnym brzmieniem projektowanych przepisów) dowiaduje się o sporządzonej przez Kolegium ocenie ryzyka za pośrednictwem ogłoszonego przez Pełnomocnika komunikatu w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski”. Należy zatem zapewnić poddawanemu ocenie dostawcy aktywny udział w postępowaniu ocennym na każdym jego etapie.  Co więcej, zgodnie z art. 15 k.p.a., postępowanie administracyjne jest dwuinstancyjne, chyba że przepis szczególny stanowi inaczej. W tym kontekście uzasadnione wątpliwości budzi projektowany art. 66a ust. 8 zd. pierwsze ustawy o krajowym systemie cyberbezpieczeństwa, który zawęża możliwość odwołania się od oceny sporządzonej przez Kolegium wyłącznie w przypadku uzyskania oceny określającej ryzyko jako wysokie. W świetle konstytucyjnej zasady równości wobec prawa, ocena określająca ryzyko jako średnie i niskie również powinna upoważniać dostawcę do wniesienia odwołania. Przepisy dotyczące wniesienia sprzeciwu do sądu administracyjnego powinny być stosowane odpowiednio. | **Uwaga częściowo uwzględniona**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | TELDATA | Uwaga ogólna | Jako firma będąca w pełni zaangażowana w rozwój branży ICT oraz mająca swój wkład w rozwój technologiczny Polski, czujemy się się zaniepokojeni Projektem Ustawy, który może mieć negatywny wpływ zarówno na naszą firmę, jak i pokrewne branże związane z rynkiem ICT.  Zdajemy sobie sprawę, że Rząd dokłada wszelkich starań, aby poprawić cyberbezpieczeństwo kraju, jednak Projekt Ustawy zawiera kryteria, które z pewnością nie będą sprzyjały konkurencyjności na rynku, ze względu na możliwość wpływu na przedsiębiorców poprzez ograniczanie zakresu prowadzenia ich działalności. Zapisy proponowane w Projekcie wpłyną zatem negatywnie na zatrudnienie i rozwój branży telekomunikacyjnej, co w konsekwencji może opóźnić proces cyfryzacji w Polsce. Naszym zdaniem, aby poprawić cyberbezpieczeństwo polskich sieci, warto wziąć pod uwagę ustalenie obiektywnych i jasnych kryteriów oceny ryzyka, opierając się na zasadzie transparentności oraz upewnienie się, że wyniki zastosowanych kryteriów oceny są prawidłowe. Warto rozważyć ustanowienie wspólnego unijnego mechanizmu certyfikacji dla krytycznego sprzętu i oprogramowania, który obowiązywałby dla wszystkich, niezależnie od kraju pochodzenia. Wierzymy, że takie podejście wpłynęłoby na zwiększenie poziomu cyberbezpieczeństwa w Polsce. Proponujemy, aby Ministerstwo Cyfryzacji zorganizowało otwartą debatę i zaprosiło zainteresowane strony do pochylenia się i pełnego omówienia kwestii poruszonych w Projekcie. Rząd powinien w pełni ocenić wpływ Projektu, w tym koszty i straty, konkurencję handlową, legalność, społeczno-gospodarcze i międzynarodowe stosunki handlowe oraz klimat inwestycyjny w Polsce. Wyrażamy nadzieję, że nasza opinia zostanie wzięta pod uwagę | **Wyjasnienie**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | TEP Doradztwo Biznesowe | Uwaga ogólna | Jako jeden z podmiotów szczególnie zainteresowanych nowymi regulacjami chcieliśmy wyrazić swoje obawy w kilku kwestiach, takich jak choćby:   1. naruszanie przez projekt zasad uczciwej konkurencji i równego traktowania podmiotów; 2. wpływanie przez Kolegium w sposób niejasny i bez szczegółowych wytycznych (technicznych) na podmioty w branży; 3. pozbawienie prawa do odwołania od decyzji Kolegium w przypadku ocen określających średnie i niskie ryzyko; 4. Relatywnie krótki termin wycofania z rynku sprzętu, oprogramowania i usług w przypadku wydania niekorzystnej oceny przez Kolegium oraz wysokie koszty wycofywania z rynku sprzętu i oprogramowania   **Naruszanie przez projekt zasad uczciwej konkurencji i równego traktowania podmiotów.**  Polski rynek jest obecnie jednym z najbardziej atrakcyjnych przestrzeni inwestycyjnych dla branży. Dzisiaj jesteśmy państwem, z którym handluje się w sposób wolny i przejrzysty, mamy przepisy gwarantujące inwestorom uczciwą konkurencję, wolny rynek i sprawiedliwe traktowanie. Proponowany kształt nowych przepisów znacząco wpływa na te atuty, które  stanowią podstawowe przymioty w każdym demokratycznym państwie. Zagraniczny kapitał jest bardzo wrażliwy na tego rodzaju regulacje. Jesteśmy pewni, że w przypadku wprowadzenia przepisów w proponowanym kształcie przełożą się one na rozwój zarówno polskiego przemysłu, sektora usług ale także na życie polskich obywateli  **Wpływanie przez Kolegium** w sposób niejasny oraz bez szczegółowych wytycznych (technicznych) na podmioty w branży. W myśl projektu Kolegium dostałoby bardzo szerokie, niejasne, niekontrolowane przez żaden zewnętrzny podmiot uprawnienia do wpływania na konkretnego dostawcę. To z kolei w dalszej kolejności przekłada się na inne podmioty gospodarcze, a na samym końcu na konsumenta. Postępowanie które pozbawia prawa do możliwości składania wyjaśnień wydaje się wysoce niesprawiedliwe. Natomiast pozbawienie możliwości odwołania (w niektórych przypadkach) zgodnie z przepisami KPA wyraźnie narusza porządek prawny oraz zasady równego traktowania zagwarantowane w Konstytucji. Proponowane przepisy stworzą potencjalne ryzyko wpływania w sposób nieuczciwy i niezgodny z prawem na podejmujących decyzję w sprawie oceny. Powstanie szczegółowych wytycznych-jasnych, obiektywnych kryteriów oceny powinno zminimalizować to ryzyko.  **Pozbawienie prawa do odwołania od decyzji Kolegium w przypadku ocen określających średnie i niskie ryzyko.** Każdy podmiot - zarówno w przypadku oceny określającej wysokie ryzyko, jak i ocen określających średnie i niskie ryzyko - powinien mieć takie same możliwości odwoławcze od oceny. Blokowanie możliwości odwoławczych niektórych z nich wpływa przede wszystkim na równość podmiotów względem innych. Każdy zasługuje na możliwość odwołania od oceny, która w założeniu nowych przepisów ma się odbywać bez udziału zainteresowanego podmiotu. Odwołanie powinno zawieszać postępowanie do czasu wydania prawomocnego wyroku w sprawie przez sąd powszechny w myśl przepisów KPA. Taki stan rzeczy byłby w sposób oczywisty najbardziej sprawiedliwy.  Relatywnie krótki termin wycofania z rynku sprzętu, oprogramowania i usług w przypadku wydania niekorzystnej oceny przez Kolegium oraz wysokie koszty wycofywania z rynku sprzętu i oprogramowania. Pięcioletni termin wycofania z rynku jest bardzo krótkim terminem na wycofanie z rynku całego sprzętu, oprogramowania i usługi z rynku. Proponujemy termin 10-cio letni, który jest dużo bardziej adekwatny do sytuacji. Należy pamiętać o tym, że operatorzy poniosą również gigantyczne koszty związane wprost z nowymi przepisami i w żaden sposób przez siebie nie zawinione. Dlatego też rząd powinien wprowadzić rekompensaty dla tych podmiotów, które takie koszty będą musiały ponieść. Oczywistym jest, że każdy podmiot który poniesie takie straty będzie szukał możliwości ich odrobienia. To z kolei wprost przełoży się na ceny usług dla końcowego odbiorcy, czyli obywatela. Sam termin 5-cio letni jest tak krótki, że może również wpłynąć na stabilność sieci, która będzie miała również szeroko idące konsekwencje. | **Uwaga częściowo uwzględniona**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | TILT | Uwaga ogólna | Martwimy się, że ocenianie dostawców na podstawie nietechnicznych czynników nie zapewni zwiększenia poziomu cyberbezpieczeństwa w Polsce, a co więcej, wpłynie negatywnie na zatrudnienie i rozwój branży ICT.  W związku z powyższym, w celu zapewnienia obiektywnych standardów, sugerujemy wprowadzenie ściśle określonych wymogów technicznych dotyczących sprzętu w kluczowych sektorach, które powinny być spełnione przez wszystkich dostawców sprzętu niezależnie od kraju pochodzenia. Uważamy, że takie rozwiązanie wpłynęłoby pozytywnie i kompleksowo na poziom cyberbezpieczeństwa w Polsce. Sugerujemy przeprowadzić pełną analizę skutków płynących z Projektu nowelizacji ustawy oraz konsultacji społecznych, co pozwoliłoby obywatelom brać aktywny udział w debatach dotyczących ich rzeczywistych interesów, a także pozwoliłoby Ministerstwu na opracowanie projektu ustawy pozbawionego ryzyka negatywnego wpływu na branżę teleinformatyczną i bezpośrednio na społeczeństwo.  Dziękujemy za wysłuchanie naszych opinii. | **Uwaga nieuwzględniona**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | Związek Cyfrowa Polska | Uwaga ogólna  Uwaga ogólna | Jako Związek Cyfrowa Polska wyrażamy poparcie dla nowelizowanej ustawy o krajowym systemie cyberbezpieczeństwa (dalej: projekt UKSC). Jest ona potrzebna i wyczekiwana przez rynek cyfrowy i nowoczesnych technologii. Cyberbezpieczeństwo musi stać się najważniejszym elementem cyfrowej gospodarki, a bez jednoznacznych, jasno sprecyzowanych regulacji prawnych byłoby to niemożliwe. Niewątpliwie należy pamiętać, że mówiąc o cyberbezpieczeństwie nie wskazujemy interesu jednego czy innego dostawcy usług, ale całościowo określamy bezpieczeństwo narodowe. I właśnie z tej perspektywy należy ocenić narzędzia, jakie daje nowelizacja ustawy dla cyberbezpieczeństwa kraju. Jest to dziś tym bardziej istotne, że w perspektywie czeka nas wdrożenie sieci piątej generacji, która zmieni funkcjonowanie całego rynku nowoczesnych technologii i która da nowe możliwości do rozwoju innowacji. Jednak by w pełni wykorzystać dobrodziejstwa, jakie przyniesie sieć 5G, trzeba przede wszystkim zadbać o jej właściwą cyfrową ochronę, które przełoży się na bezpieczeństwo i konkurencyjność polskiej gospodarki.  **Mając na uwadze cyberbezpieczeństwo oraz szeroki rozwój sieci 5G w Polsce Związek Cyfrowa Polska za najbardziej pożądany model budowy sieci uznaje ten, w którym w maksymalnym stopniu wykorzystany zostanie potencjał polskich firm i działających w Polsce firm światowych vendorów, ośrodków B&R, fabryk, zatrudnionych inżynierów, w tym opowiada się za szerokim wykorzystaniem technologii Open RAN -** rozwiązanie to jest bardziej efektywne, które może obniżyć koszty wykorzystania technologii przez przedsiębiorców i administrację publiczną we wdrażaniu sieci 5G. **Popieramy również to, że projekt UKSC uwzględnia unijne narzędzia 5G Toolbox, które mają za zadanie ograniczenie cyber-ryzyk dla europejskich sieci 5G.**  Rozumiemy, że dla utrzymania cyberbezpieczeństwa dla rynku telekomunikacyjnego i komunikacji elektronicznej, Ustawa musi dawać instrumenty, które pozwalają państwu na eliminowanie z obrotu rozwiązań zarówno sprzętowych jak i oprogramowania stanowiące zagrożenia dla bezpieczeństwa państwa, przedsiębiorców, jak i obywateli. Uważamy, że metoda regulacji oparta na analizie ryzyk i wykorzystująca wspólne instrumenty Unii Europejskiej z tzw. Toolbox 5 G jest właściwa - projektowane w art. 66 a-c rozwiązanie bazuje na podmiotowej ocenie ryzyka, która odbywa się przez pryzmat dostawcy sprzętu lub oprogramowania. Jest to podejście trafne, jeśli chodzi o ryzyko opisane jak *„R.5 State interference through 5G supply chain”,* zgodnie z analizą ryzyk opracowaną na poziomie EU w dokumencie 5G Toolbox. Podejście to ma jednak zasadniczą wadę - w dzisiejszym zglobalizowanym świecie przynależność geograficzna dostawców nie jest stała, więc również oparcie się wyłącznie na kryterium kraju pochodzenia może okazać się nieskuteczne już w perspektywie kilku lat. Niedawno jeszcze nikt nie przypuszczał, że cały brytyjski przemysł samochodowy znajdzie się w rękach inwestorów spoza UE i NATO. Tak samo niewielu spodziewało się, że największy grecki port w Pireusie będzie własnością chińskich inwestorów. **Tak więc kryterium geopolityczne, jakkolwiek ważne dla bezpieczeństwa (w tym także cyberbezpieczeństwa), powinno zostać wzmocnione dodatkowymi mechanizmami.**  Jednocześnie należy wskazać, że ryzyka opisane w diagnozie 5G Toolbox są znacznie szersze i bardziej różnorodne. Jednym z najbardziej jaskrawych jest *„R4. Dependency on a single supplier”.* Stan obecny w Polsce wskazuje, że sprzęt i oprogramowanie od jednego dostawcy stanowią dziś ok. 65 proc, całej infrastruktury LTE i 5G na terenie kraju, a w przypadku niektórych operatorów jest to ponad 80 proc, ich zasobów sieciowych. Jest to zjawisko głęboko niepożądane, gdyż problem z jednym tylko dostawcą stawia pod znakiem zapytania cyberbezpieczeństwo około 2/3 sieci LTE/5G w kraju, a pozostała część sieci nie ma szans obsłużyć nawet najbardziej niezbędnego ruchu. Z punktu widzenia bezpieczeństwa sieci, a także bezpieczeństwa państwa, należałoby w UKSC wprowadzić środki zaradcze, które adresują to właśnie zjawisko.  Zgodnie z przyjętym również przez Polskę na szczeblu europejskim dokumentem 5G Toolbox  rozwiązaniami adresującymi to ryzyko są:   * dywersyfikacja dostawców, * zrównoważony i zróżnicowany łańcuch dostaw i wartości 5G.   Ich skuteczność w opracowanym 5G Toolbox *{tabela 3)* określono jako „bardzo wysoką” *{Very High)* i one jako jedyne adresują to właśnie ryzyko. W naszej opinii UKSC jest odpowiednim aktem prawnym, aby stosowanie tych środków zaradczych wprowadzić. Nie ma na nie miejsca w projektowanej ustawie Prawo Komunikacji Elektronicznej, natomiast zawarcie ich w przyszłych aktach wykonawczych, a więc na poziomie rozporządzeń Ministerstwa Cyfryzacji może w przyszłości wzbudzać wątpliwości legislacyjne.  Wdrożenie dywersyfikacji oraz zrównoważonego łańcucha dostaw i wartości do proponowanego projektu jest możliwe, ale wymagałoby spojrzenia przez pryzmat podmiotów budujących sieć, a nie dostawców sprzętu i oprogramowania. Oczywistym adresatem będą operatorzy sieci (obecni oraz przyszli), w tym narodowy operator sieci 5G, ale także podmioty budujące sieci lokalne w modelu Private Networks, Smart City i podobnych. Kluczowym elementem takiej oceny będzie więc nie tyle kraj pochodzenia danego sprzętu lub oprogramowania, co parytet sprzętu i oprogramowania pochodzącego od jednego dostawcy w całej sieci krajowej (danego operatora/ operatora lokalnego). Oczywiście ze inne ryzyka także musza być mitygowane. Wydaje się, że obowiązek dywersyfikacji powinien zostać wprowadzony przede wszystkim dla sieci o zasięgu krajowym, a także dla sieci o znaczeniu strategicznym dla bezpieczeństwa państwa. Przykładem mogą być sieci prywatne 5G, które powstaną w kluczowych zakładach i obiektach (typu rafinerie, gazoporty, lotniska).  **Podejście do tego tematu powinno uwzględniać zarówno dywersyfikację horyzontalną (ilościową, geograficzną), jak i wertykalną (zróżnicowanie na poziomie różnych elementów sieci).**  Dywersyfikacja horyzontalna oznacza, że żaden podmiot posiadający sieć lub ją budujący nie opiera się na jednym dostawcy, a więc np. maksymalnie połowa infrastruktury może pochodzić od jednego dostawcy. Rozwiązanie zbliżone do tego podejścia wdraża Wielka Brytania. W tym modelu wystąpienie incydentu poważnie zagrażającego cyberbezpieczeństwu państwa jest siłą rzeczy ograniczone terytorialnie oraz podmiotowo (ponieważ działa kilka konkurujących  sieci).  Dywersyfikacja wertykalna oznacza, że łańcuch wartości w sieci jest zróżnicowany, a więc różne elementy sieci kompatybilne ze sobą nawzajem pochodzą od różnych dostawców. Dzięki temu podejściu możliwe jest budowanie sieci z uwzględnieniem obszarów infrastruktury krytycznej (tylko bezpieczni dostawcy) oraz pozostałych (większa swoboda zakupowa, bo mniejsze ryzyko). Podejście to również jest stosowane w kilku krajach budujących swoje sieci 5G. Dzięki temu podejściu sieci budowane w modelu *non-stand-alone* łatwiej jest dostosować do nowych wymagań cyberbezpieczeństwa, ponieważ urządzenia peryferyjne nie generujące ryzyka mogą pozostać na swoim miejscu, a właściciele sieci zbudowanej na komponentach od jednego, ryzykownego dostawcy muszą zadbać o wymianę infrastruktury krytycznej, a nie całej sieci. Oczywiście jest to możliwe przy założeniu, że dostawcy Ci udostępnią interfejsy swoich urządzeń i oprogramowania w taki sposób, aby była możliwa konfiguracja całego zestawu ze sprzętu i oprogramowania różnych dostawców.  Rozwiązaniem najlepiej adresującym problem dywersyfikacji wertykalnej są otwarte (z definicji) interfejsy, oparte o powszechnie przyjęte międzynarodowe standardy. Przykładem takiego rozwiązania jest model Open RAN, w którym poszczególne elementy infrastruktury aktywnej mogą pochodzić od różnych dostawców i żaden dostawca nie ma kontroli nad całością sieci. Powstają już pierwsze komercyjne sieci oparte na tym modelu (np. amerykański Dish lub japoński Raku ten).  Podsumowując, wdrożenie do porządku prawnego dywersyfikacji horyzontalnej i jednocześnie wertykalnej daje szanse na uodpornienie infrastruktury na zależność od jednego dostawcy i jest to znakomite rozwiązanie uzupełniające do zaproponowanych w projekcie ustawy środków zabezpieczających o charakterze geopolitycznym. | **Uwaga częsciowo uwzględniona**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. |
|  | Signum Edward Kuś Marcin Kuś | Uwaga ogólna | Po zapoznaniu się z tym projektem stwierdzamy, że proponowane zmiany nie przyniosą pozytywnych skutków dla bezpieczeństwa cybernetycznego w Polsce. Poniżej wskazujemy na braki zaproponowanych w Projekcie przepisów:   1. **Naruszenie zasad uczciwej konkurencji:, Jeśli** zostanie przyjęty, Projekt nada Kolegium prawo wyboru dostawców, a rynek komercyjny będzie podlegał politycznej ingerencji, która nie będzie sprzyjać konkurencji rynkowej. Obecnie jest tylko trzech głównych dostawców sprzętu 5G. Ograniczenie ich liczby do jednego, spowoduje stłumienie konkurencji na rynku ICT i negatywnie wpłynie na rozwój branży. 2. **Wyraźna dyskryminacja:** Kryteria oceny ryzyka dostawcy to wyłącznie czynniki nietechniczne, takie jak relacje między dostawcą a ich krajem macierzystym, przepisy dotyczące praw człowieka w kraju macierzystym, przepisy dotyczące ochrony danych osobowych w kraju macierzystym, struktura własności dostawcy i możliwości kraju macierzystego dotyczące ingerencji w działania dostawców. 3. **Projekt wyraźnie dyskryminuje dostawców z niektórych regionów:** Kryteria oceny ryzyka dostawcy to jedynie czynniki nietechniczne, w tym związek między dostawcami a krajem macierzystym, przepisy dotyczące praw człowieka w kraju macierzystym, przepisy dotyczące ochrony danych osobowych w kraju macierzystego, struktura własności dostawcy i możliwości kraju macierzystego w ingerowanie w działania dostawców.   **4. Brak technicznych kryteriów oceny:** Rząd będzie podejmował interwencje w zakresie wyboru dostawcy, wskazując na dostawców wysokiego/ średniego ryzyka, zamiast ustanowić jednolite standardy techniczne i wskazać sprzęt objęty nowymi regulacjami. Operatorzy będą zobowiązani do zaprzestania kupowania sprzętu od dostawców wysokiego / średniego ryzyka oraz do wymiany całego sprzętu od dostawców wysokiego ryzyka w ciągu pięciu lat.  5. **Brak metod weryfikacji bezpieczeństwa cybernetycznego:** Projekt nic zawiera wystarczających środków do weryfikacji bezpieczeństwa cybernetycznego, aby zapewnić bezpieczeństwo i niezawodność sieci w czasie rzeczywistym.  6 **Opóźnienie we wdrożeniu 5G wpłynie na wyniki gospodarcze i zatrudnienie:** Według badania przeprowadzonego przez Komisję Europejską szacuje się, że ie5G zapewni łącznie 141 miliardów euro i 2,3 miliona miejsc pracy w 27 państwach członkowskich Unii Europejskiej.  7. **Projekt ogranicza dywersyfikację technologii i przyszły rozwój:** Każdy sprzedawca samodzielnie ocenia rynek i wyznacza własny kierunek rozwoju. Daje to nieograniczony potencjał dywersyfikacji technologicznej i przyczynia się do przyszłego rozwoju branży. =Wykluczenie jednego z najważniejszych dostawców będzie miało negatywny wpływ na badania naukowe w Polsce, różnorodność technologii i przyszły rozwój.  Podsumowując, przyjęcie Projektu nie wpłynie pozytywnie na bezpieczeństwo cybernetyczne w Polsce. | **Wyjasnienie**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | Signum Edward Kuś Marcin Kuś | Uwaga ogólna | W odpowiedzi na problemy wkazane powyżej, proponujemy, co następuje:   1. Należy przestrzegać unijnego zestawu narzędzi 5G (5G EU toolbox), nieskierowanego do określonych krajów lub dostawców oraz przyjąć ujednolicone standardy techniczne i weryfikacyjne. 2. Cyberbezpieczeństwem w zakresie 5G należy zarządzać za pomocą jasnych specyfikacji technicznych i ujednoliconych standardów, a niewykluczać dostawców z określonych krajów. Model większości krajów UE, takich jak Niemcy, na którym można się z powodzeniem wzorować, to standard bezpieczeństwa cybernetycznego opracowany przez Federalną Agencję Bezpieczeństwa Informacji (BSI) oraz plan zapewnienia bezpieczeństwa sprzętu sieciowego (NESAS) opracowany przez GSMA, zgodnie, z którymi wszyscy dostawcy są traktowani jednakowo. 3. Należy przyjąć kompromisowe (hierarchiczne) rozwiązanie w kwestii zarządzania bezpieczeństwem cybernetycznym i ograniczenie do elementów krytycznych (sieć rdzeniowa), odwołując się do definicji unijnego zestawu narzędzi 5G. Stacje bazowe 5G nie są komponentami podstawowymi, więc nie wymagają żadnych ograniczeń.   a)Model niemiecki: Przyjęcie NESAS, opracowanego przez GSMA, jako standard bezpieczeństwa cybernetycznego; certyfikowanie sprzętu wszystkich dostawców oraz przyjęcie strategii wielu dostawców.  b) Model w Szwecji i Finlandii: operatorzy zarządzają bezpieczeństwem cybernetycznym, przyjmują strategię wielu dostawców i dokonują przeglądu podstawowych komponentów sieci.   1. Należy przeprowadzić pełną analizę skutków płynących z projektu nowelizacji ustawy oraz konsultacji publicznych. 2. Należy wysłuchać zdecydowanego sprzeciwu ze strony branży teleinformatycznej i opinii publicznej wobec projektu, zaangażować ekspertów w celu pełnego przedstawienia Projektu, zorganizować debatę i wysłuchać opinii wszystkich stron. 3. Należy zmienić przepisy dyskryminujące ze względu na kraj pochodzenia danego dostawcy na przepisy, które będą zgodne z prawem konkurencji UE i zasadami WTO. Należy ustanowić prawa i regulacje sprzyjające cyfrowej przyszłości kraju, wolnej konkurencji operatorów i wysokiej, jakości usług sieciowych dla obywateli kraju. | **Wyjaśnienie**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostałty określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | PKN Orlen | Uwaga ogólna | 1.1 W pierwszej kolejności PKN wskazuje na potrzebę przyznania organowi właściwemu do spraw cyberbezpieczeństwa w rozumieniu *Ustawy z dnia 5 lipca 2018r. o krajowym systemie cyberbezpieczeństwa* (Dz.U. z 2018r. poz. 1560 - dalej jako **„Ustawa o KSC")** prawa do ustanowienia *„CSIRT grupy kapitałowej”* czyli *„Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego działającego w* ***ramach oraz na poziomie*** *grupy kapitałowej ustanowionego przez organ właściwy do spraw cyberbezpieczeństwa.”*  1.2 Powyższe prawo w/w organu do ustanowienia *„CSIRT grupy kapitałowej”* dotyczyłoby  takich grup kapitałowych, do których należy **więcej niż jeden operator usługi kluczowej** z określonego sektora. W konsekwencji *„CSIRT grupy kapitałowej"* zachowałby swój sektorowy charakter z tym jednak zastrzeżeniem, że posiadałby **status równorzędny** wobec *„CSIRT-ów sektorowych"*  w rozumieniu Projektu. Szczegółowe propozycje wybranych zmian w Projekcie dotyczące powyższego zagadnienia zawarto w **Tabeli numer 1 poniżej.**  1.3 Uzasadnieniem powyższego jest sposób funkcjonowania dużych i strategicznych Grup Kapitałowych:  1.3.1 wspólna infrastruktura wymuszająca efektywne zarządzanie incydentami, możliwe wyłącznie dzięki scentralizowanemu zarządzaniu cyberbezpieczeństwem,  1.3.2 posiadanie niezbędnych zasobów ludzkich i technicznych do skutecznego, centralnego zarządzania cyberbezpieczeństwem Grupy Kapitałowej, w tym realizacji zadań CSIRT  1.4 W myśl powyższej koncepcji organ właściwy do spraw cyberbezpieczeństwa  zapewniałby funkcjonowanie *„CSIRT sektorowego”* dla operatorów usług kluczowych w danym sektorze lub podsektorze wymienionym w załączniku nr 1 do Ustawy o KSC (zgodnie z Projektem),  a dodatkowo byłby uprawniony ustanowić *„CSIRT grupy kapitałowej"*. Organ właściwy do spraw cyberbezpieczeństwa mógłby powierzyć realizację zadań:  1.4.1 *„CSIRT sektorowego”* m.in. jednostkom podległym lub nadzorowanym (zgodnie z Projektem), a także  1.4.2 *„CSIRT grupy kapitałowej"* temu podmiotowi danej grupy kapitałowej, który spełnia warunki, o których mowa w projektowanym art. 44 ust. 6 Projektu, a także po zasięgnięciu opinii Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa.  1.5 Ponadto, w myśl preambuły do *Dyrektywy NIS: „(...) Państwa członkowskie* ***powinny zatem zapewnić dobrze funkcjonujące*** *CSIRT, zwane również zespołami reagowania na*  *incydenty komputerowe (zwane dalej „CERT"), które spełniają zasadnicze wymogi w celu zagwarantowania efektywnych i kompatybilnych zdolności w zakresie postępowania*  *z incydentami i ryzykiem oraz zapewnienia skutecznej współpracy na poziomie Unii (...)"* **(motyw 34)** oraz *„Odpowiedzialność za zapewnienie bezpieczeństwa sieci i systemów informatycznych*  ***w dużym stopniu spoczywa na operatorach usług kluczowych* (motyw 44).** | **Uwaga nieuwzględniona.**  Nie jest konieczna tworzenie nowego rodzaju CSIRT. Zadania doskonale wypełni podmiot w ramach grupy kapitałowej świadczący usługę SOC dla operatorów usługi kluczowej w ramach grupy kapitałowej. |
|  | Skandynawsko-Polska Izba Gospodarcza | Uwaga ogólna | Wyrażamy poparcie dla wprowadzenia do polskiego prawodawstwa opracowanego przez państwa członkowskie EU unijnego zestawu narzędzi na potrzeby cyberbezpieczeństwa sieci 5G ("5G Toolbox"), zgodnie z propozycją zawartą w projekcie ustawy z dnia 7. września 2020 roku o zmianie ustawy o krajowym systemie cyberbezpieczeństwa. Wraz ze zmianami technologicznymi będącymi konsekwencjami wprowadzenia sieci 5G i możliwościami rozwoju tej technologii w szerokim obszarze zastosowań, jak przemysł ochrona zdrowia, telekomunikacja, transport, wzrosną zagrożenia i poszerzy  się pole do ataków cybernetycznych.  Naszym zdaniem proponowana zmiana ustawy o krajowym systemie  cyberbezpieczeństwa i wdrożenie unijnego zestawu narzędzi 5G jest krokiem we właściwym kierunku, co pozwoli na zapewnienie ochrony przedsiębiorstwom i pozwoli za zabezpieczenie ich praw własności intelektualnej.  Proponowana zmiana stanowi dobrą odpowiedz na wymóg identyfikacji potencjalnych luk w istniejących ramach legislacyjnych i mechanizmach egzekwowania prawa, w tym roli nadzorczej organów publicznych w zakresie krajowego systemu cyberbezpieczeństwa przed pełnym wprowadzeniem 5G w Polsce.  Oczekując na dalsze procedowanie proponowanego projektu, pragniemy jeszcze raz zaznaczyć, ze projekt w obecnej formie jest krokiem we właściwym kierunku, pozwalającym na zapewnienie bezpiecznego i przewidywalnego środowiska biznesowego przedsiębiorcom stowarzyszonych w naszej organizacji | **Wyjaśnienie**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | Liquid Systems | Uwaga ogólna | Wiele planowanych zmian narusza zasadę niedyskryminacji i uczciwej konkurencji przedsiębiorstw, co wpłynie negatywnie na branżę ICT. Przyjęcie Projektu w aktualnym brzmieniu oznacza:  1. Naruszenie zasad uczciwej konkurencji: Jeśli nowe przepisy zostaną przyjęte, Kolegium uzyska de facto prawo wyboru dostawców, a rynek komercyjny będzie podlegał politycznej ingerencji, która nie sprzyja konkurencji rynkowej. Obecnie jest tylko trzech głównych dostawców sprzętu 5G. Ograniczenie do tylko jednego z nich spowoduje stłumienie konkurencji na rynku ICT i negatywnie wpłynie na rozwój branży.  2. Wyraźna dyskryminacja: Kryteria oceny ryzyka dostawcy to wyłącznie czynniki nietechniczne, w tym relacje między dostawcami a krajem macierzystym, przepisy dotyczące praw człowieka w kraju  macierzystym, przepisy dotyczące ochrony danych osobowych w kraju macierzystym, struktura własności dostawcy i możliwości kraju macierzystego dotyczące ingerencji w działania dostawców.  3. Brak technicznych kryteriów oceny: Rząd ingeruje w wybór dostawcy zamiast ustanowić jednolite standardy techniczne. Nie określa również sprzętu objętego zakresem nowych przepisów. Operatorzy zobowiązani do zaprzestania kupowania sprzętu od dostawców wysokiego / średniego ryzyka oraz do wymiany całego sprzętu od dostawców wysokiego ryzyka w ciągu pięciu lat.  4. Wzrost kosztów budowy sieci zostanie ostatecznie przeniesiony na konsumentów, prowadząc do zastosowania wyższych cen dla usług telekomunikacyjnych. Wyłączanie dostawców doprowadzi do  zniesienia konkurencji, zwiększając koszty zaopatrzenia operatorów, co z kolei będzie prowadzi to do wyższych cen usług telefonii komórkowej dla użytkowników. Koszty budowy infrastruktury IT dla rządów i przedsiębiorstw mogą znacznie wzrosnąć. Na przykład, brytyjskie media podały, ze po wykluczeniu  Huawei koszt budowy sieci w Wielkiej Brytanii wzrósł o 30%.Taryfy w Polsce są obecnie jednymi unijnego zestawu narzędzi 5G. Stacje bazowe 5G nie są komponentami podstawowymi, więc nie wymagają  żadnych ograniczeń.  a) Model niemiecki: Przyjcie NESAS, opracowanego przez GSMA jako standard bezpieczeństwa cybernetycznego; certyfikowanie sprzętu wszystkich dostawców oraz przyjęcie strategii wielu dostawców.  b) Model w Szwecji i Finlandii: operatorzy zarządzają bezpieczeństwem cybernetycznym, przyjmują strategię wielu dostawców i dokonują przeglądu podstawowych komponentów sieci.  5. Należy przeprowadzić pełną analizę skutków płynących z projektu nowelizacji ustawy oraz konsultacji publicznych.  6. Należy wysłuchać zdecydowanego sprzeciwu ze strony branży teleinformatycznej i opinii publicznej wobec Projektu, zaangażować ekspertów w celu pełnego przedstawienia Projektu, zorganizować debaty i wysłuchać opinii wszystkich stron.  7. Należy zmienić przepisy dyskryminujące kraj pochodzenia danego dostawcy na klauzule 0 niedyskryminacji, zgodnie z prawem konkurencji UE i zasadami WTO. Należy ustanowić prawa i regulacje  sprzyjające cyfrowej przyszłości kraju, wolnej konkurencji operatorów i wysokiej jakości usług sieciowych dla obywateli kraju. | **Uwaga nieuwzględniona**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | Instytut Staszica | Uwaga ogólna | Projekt może naruszać istotne regulacje unijne, a co za tym idzie – być powodem do kolejnego sporu między polskim rządem a Komisją Europejską.  Jest kwestią oczywistą, która nie powinna budzić sporów niezależnie od partyjnych barw, że priorytetem jest budowa w naszym kraju możliwie najnowocześniejszego systemu komunikacji na możliwie najbardziej dogodnych warunkach. Te warunki to nie tylko kwestie finansowe, ale także szczegóły związane z obsługą systemu, dostępem do kolejnych, nowych rozwiązań, które pojawią się w następnych latach, możliwość rozwijania przez polskie firmy współpracy z dostawcą technologii. Telekomunikacja, a zwłaszcza technologia 5G, stanowią fundament cyfrowej transformacji oraz ścieżkę powrotu do ożywienia gospodarczego, w szczególności w kontekście aktualnej sytuacji epidemicznej. Sprawne wdrożenie sieci 5G w Polsce może stanowić istotny potencjał gospodarczy w ciągu najbliższych kilku lat. Bez wątpienia jest to czynnik napędzający konkurencyjność i innowacyjność państwa na arenie międzynarodowej, zrównoważony rozwój i transformację cyfrową. Niezależnie od tego, czy jest to transport, energetyka, opieka zdrowotna czy rolnictwo, technologia 5G położy podwaliny pod zieloną i cyfrową transformację gospodarki Rzeczypospolitej  Nie można udawać, że całe przedsięwzięcie nie ma kontekstu geopolitycznego. Budowa sieci 5G w krajach europejskich odbywa się w cieniu rywalizacji amerykańsko-chińskiej. Sytuacja ta pokazuje, niestety, słabość Europy, która nie jest już podmiotem w takiej rywalizacji, a jedynie przedmiotem zabiegów pozaeuropejskich koncernów.  Polska, podejmując kierunkową decyzję w sprawie budowy sieci 5G, musi znaleźć równowagę między interesami gospodarczymi, politycznymi i pozycją w Unii Europejskiej. Jest to niezwykle trudne zadanie, wymagające współpracy ponad politycznymi podziałami. To zadanie, którego sami politycy, bez ekspertów, nie będą w stanie udźwignąć.  Kwestia uwzględnienia powyższych interesów w przyszłej ustawie to jedno, a kwestia przygotowania regulacji w taki sposób, by nie stały w sprzeczności z prawem europejskim i międzynarodowymi umowami, to drugie. Nie kwestionując faktu, że rząd i sejmowa większość przy tak strategicznym projekcie nie tylko mogą, lecz wręcz muszą zagwarantować w jak najlepszy sposób narodowe interesy, eksperci Instytutu Staszica zwracają uwagę, że nie można przy tym lekceważyć podstawowych zasad prawa europejskiego. Niestety, istnieją bardzo poważne obawy, że projekt ustawy w obecnym kształcie te regulacje narusza.  **Cele projektu i polityczne kryteria oceny**  W założeniu projekt ów ma na celu zapewnienie odpowiedniego poziomu cyberbezpieczeństwa. Właściwy poziom cyberbezpieczeństwa ma natomiast zostać zrealizowany poprzez przeprowadzenie postępowania ocennego w stosunku do dostawców sprzętu i oprogramowania w oparciu o takie czynniki jak: stopień i rodzaj powiązań tego dostawcy z państwem jego pochodzenia, prawodawstwo tego państwa w zakresie ochrony praw obywatelskich i praw człowieka, strukturę własnościową tego dostawcy oraz zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy. Nie kwestionując tego, że kwestia ochrony praw człowieka powinna być brana pod uwagę przy podejmowaniu strategicznych decyzji o współpracy z zagranicznymi partnerami, to nie może stanowić nietransparentnego kryterium. Według jakich bowiem zasad i przez kogo ta kwestia miałaby być oceniana? Warto przypomnieć, że również Polska bywa obiektem oskarżeń o naruszanie praw obywatelskich m.in. w kontekście reformy sądownictwa i sporu wokół „ideologii LGBT”. Zasadnicze obawy budzi uznaniowość rozstrzygnięcia, które będzie prowadzić do natychmiastowego wykluczenia z polskiego rynku dowolnego podmiotu dostarczającego sprzęt lub usługi elektroniczne.  **Sposób oceny, oparty na kryteriach kraju pochodzenia dostawcy, z pominięciem aspektów technicznych dostarczanych produktów, może spowodować oskarżenia o dyskryminację, skutkującą naruszeniem wartości porządku UE oraz prawa międzynarodowego.**  **Regulacje UE, które projekt ustawy może naruszać:**  1. Dyrektywa o konkurencji i zasada swobodnego przepływu towarów. Dyrektywa w sprawie konkurencji (2002/77/WE) wyłącza możliwość przyznawania jakichkolwiek specjalnych praw w sektorze łączności elektronicznej. W tym przypadku dostawcy z Unii Europejskiej nie znajdują się na pozycji uprzywilejowanej. Polski projekt daje narzędzie do uznaniowego wykluczenia z postępowania dostawców spoza UE, w oparciu o nieostre kategorie ocenne, o czym wspomniano wyżej. Ze wspomnianą dyrektywą wiąże się także fundamentalna dla Wspólnego Rynku zasada swobodnego przepływu towarów. Zasada ta jest w orzecznictwie unijnych instytucji i sądów traktowana rozszerzająco; uznaje się, że zakaz używania produktu na terenie jednego z państw unijnych wpływa na postawy nabywców. Przepisy skutkujące wyłączeniem dostawcy z łańcucha dostaw w jednym lub kilku państwach unijnych mogą bowiem powstrzymać klientów przed kupowaniem produktów tego dostawcy.  2. Zasady niedyskryminacji i ograniczeń swobody przedsiębiorczości, zapisane w Traktacie o Funkcjonowaniu Unii Europejskiej. Przedmiotowy projekt posługuje się bardzo ogólnymi, umożliwiającymi swobodną interpretację przez urzędników kategoriami wyłączającymi dostawców technologii 5G. W dodatku procedury administracyjne i możliwość odwołania się od wykluczającej decyzji są ujęte w sposób wyjątkowo mało przejrzysty. Jest niemal pewne, że wykluczone podmioty będą się powoływać na naruszenie art. 34 i 49 TFUE (zakaz ograniczeń ilościowych w przywozie, zakaz ograniczania swobody przedsiębiorczości). 3. Zasada niedyskryminacji, ujęta w Karcie Praw Podstawowych. Równość wobec prawa i wynikające z tego równe traktowanie podmiotów prawa, niezależnie od narodowości i kraju pochodzenia, to jeden z kluczowych zapisów Karty Praw Podstawowych UE. Zapisy krajowego prawa, które umożliwią zablokowanie dostępu do rynku dostawcom z wybranych krajów w sposób uznaniowy, tę zasadę naruszają.  **Potencjalne naruszenie GATT:**  Układ Ogólny w sprawie Taryf Celnych i Handlu (GATT) przewiduje, że członek Światowej Organizacji Handlu (jakim jest Polska) nie może dyskryminować indywidualnych partnerów handlowych, dając przywileje określonym krajom. Wynika stąd obowiązek równego traktowania podobnych produktów i technologii z różnych krajów i z kraju własnego. Kryterium pochodzenia produktu bądź technologii z danego kraju, na co położono nacisk w projekcie polskiej ustawy, może być uznane za jaskrawe naruszenie GATT.  **Europejskie rozwiązania – przykłady regulacji przyjętych w wybranych państwach członkowskich UE:**  Rządzący nie powinni tracić z pola widzenia rozwiązań przyjętych w pozostałych państwach, zarówno Unii Europejskiej, jak i poza naszym kontynentem. W tym kontekście całkowicie niezrozumiały jest brak dokonania przez autorów projektu analizy prawno-porównawczej w obrębie krajów OECD/EU. Tymczasem podejście zastosowane w Niemczech, Szwecji, Francji czy Finlandii, jak również w Korei Południowej, pozwala na zastosowanie kryteriów technicznych sprzętu i oprogramowania wykorzystywanego do budowy sieci 5G. W tych państwach to operatorzy są zobowiązani do analizy ryzyka sprzętu i oprogramowania. Weryfikacja bezpieczeństw dokonywana jest w oparciu o mechanizmy certyfikacji, wydawane przez niezależne centra naukowe, które stosują wyłącznie kryteria techniczne do oceny bezpieczeństwa stosowanych produktów. Zaostrzone kryteria oceny stosowane są wyłącznie w przypadku infrastruktury uznanej za kluczową dla bezpieczeństwa państwa, np. w branży energetycznej, transportowej, czy też ze względu na potrzeby militarne.  W opinii ekspertów Instytutu Staszica rząd i sejmowa większość mają pełne prawo decydować o kwestiach kluczowych dla pozycji Polski na arenie międzynarodowej. Jednak przyjmowane regulacje nie mogą stać w sprzeczności z porządkiem Unii Europejskiej i z traktatami międzynarodowymi. Taki sposób rozwiązywania skomplikowanych kwestii przynosi więcej problemów, niż korzyści, a finalnie może narazić Polskę na zapłatę ogromnych sum z tytułu kar i odszkodowań. Złe prawo, zakwestionowane przez Komisję Europejską oraz Europejski Trybunał Sprawiedliwości, może znacznie opóźnić proces budowy systemu 5G w Polsce, a tym samym znacząco osłabić polską innowacyjność i konkurencyjność.  Instytut Staszica stoi na stanowisku, że kwestia wyboru dostawcy sprzętu i technologii 5G powinna być uregulowana prawnie w sposób, który z jednej strony nie skrępuje rządowi rąk w zakresie wyboru odpowiedniej technologii, a z drugiej – będzie zgodny z prawem międzynarodowym i prawem UE. Obecny projekt ustawy tych warunków nie spełnia. Wzorem innych Państw UE warto skupić się na kryteriach technicznych, gdyż tylko takie podejście przyczyni się do rzeczywistego zabezpieczenia interesów Państwa zarówno z perspektywy cyberbezpieczeństwa, jak i geopolitycznej. | **Uwaga nieuwzględniona**  Projekt nie narusza przepisów unijnych oraz innych przepisów międzynarodowych.  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały 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 nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. |
|  | Transition Software | Uwaga ogólna do PZP | Należy zmodyfikować poniższe artykuły, tj. umieścić w nim jasne i rozwiewające wszelkie wątpliwości zapisy, że postępowania zakupowe prowadzone przez podmioty IK, a dotyczące szczególnie infrastruktury ICT, w tym zwłaszcza systemów bezpieczeństwa, są wyłączone z przepisów Ustawy Pzp.  Z jednej strony są napisane wyraźnie, z drugiej strony, praktyka i pragmatyka zamówień publicznych prowadzonych przez ostatnie lata przez instytucje w naszym kraju, pokazują co innego (pełne stosowanie zakupów w formie przetargu nieograniczonego, nadmierna otwartość i informacyjność, nadmiernie szeroka pula potencjalnych wykonawców, nieuzasadniona, nadmierna obawa przed potencjalnymi zarzutami z powodu naruszenia dyscypliny finansów publicznych, etc. etc.).  Jest zrozumiałe, że procesy zakupowe IT w dużych jednostkach budżetowych powinny być należycie kontrolowane, gdyż ryzyka zarówno:  - zakupu niewłaściwych rozwiązań, niespełniających kryteriów (ustawianie przetargów),  - marnotrawstwa środków publicznych,  - korupcji,  nie są pomijalne, to jednak chęć nadmiernej otwartości wprost powoduje ryzyka dla bezpieczeństwa infrastruktury ICT podmiotu świadczącego usługę kluczową (choćby targetowanie exploitów, spear phishing, celowane ataki APT, skoro stosowana infrastruktura i oprogramowanie jest możliwe do łatwego poznania, etc.).  Poprzez bezkrytyczne, nadmiernie przezroczyste stosowanie obowiązującej Ustawy Prawo zamówień publicznych przez piony, departamenty i wydziały odpowiedzialne za procesy zamówień publicznych w jednostkach organizacyjnych podmiotów wchodzących w skład Infrastruktury Krytycznej RP, jest ona w niewystarczający sposób chroniona przez wypływem informacji dość wrażliwych z punktu widzenia cyberbezpieczeństwa RP, tj. dotyczących stosowanej w podmiotach i obiektach IK infrastruktury ICT, oprogramowania, wersji, systemów bezpieczeństwa, etc.  Wg mojej oceny sytuacji prawnej obowiązującej w Polsce, informacje dotyczące infrastruktury ICT - w tym w szczególności systemów bezpieczeństwa - stosowanej w podmiotach wchodzących w skład IK są dalece niewystarczająco chronione, m.in. z poniższych powodów:   1. Najczęściej nie wchodzą w skład systemów przetwarzających informacje niejawne, więc nie są chronione obejmującą je ustawą. 2. Nie są też stricte systemami przetwarzającymi dane osobowe, więc nie obowiązuje je również w wystarczającym stopniu ochrona poprzez zapisy RODO. 3. Nie wszystkie podmioty IK wchodzą w skład wojska, resortów siłowych, służb specjalnych, więc nie obowiązuje je możliwa do zastosowania przez ww. instytucje niemalże domyślna ochrona wszelkich informacji dotyczących ich infrastruktury, możliwości i procedur. 4. Analogicznie j.w. – nie wszystkie podmioty i obiekty IK wchodzą w skład sektorów, więc nie obowiązuje je obszar zamówień sektorowych i pewnej ochrony z nimi związanej. 5. Bardzo często, z obawy przed sankcjami spowodowanymi potencjalnym naruszeniem dyscypliny finansów publicznych, jednostki organizacyjne resortów publicznych, a w szczególności pracownicy i decydenci pionów zamówień publicznych, przeprowadzają wszystkie organizowane przez siebie zamówienia wyłącznie w formie przetargu nieograniczonego. Bardzo często dochodzi do tego nadmierna, swoiście rozumiana chęć zapewnienia wysokiej konkurencyjności rynkowej, która – podczas przeprowadzania procesu zakupowego - często prowadzi do: 6. Zaznajamiania się z informacjami dot. zamówienia bardzo szerokiego grona odbiorców (w przypadku przetargu nieograniczonego jest to w zasadzie cały świat, wystarczy znajomość jęz. polskiego, ogłoszenia są publikowane na stronach internetowych); 7. Konieczności wypisania/ujawniania wykorzystywanej infrastruktury ICT, w niektórych przypadkach już w ogłoszeniu, w niektórych przypadkach w formie odpowiedzi na zapytania przetargowe, gdyż jest to wymuszone przez zastosowaną formę zakupu, tj. przetarg nieograniczony (pytania są publiczne, odpowiedzi również muszą takie być, więc odpowiedzi są zamieszczane w formie otwartej, na stronach internetowych Zamawiającego lub BIP); 8. Uczestnictwie w procesie przetargowym czasem nie do końca wiarygodnych i zweryfikowanych wykonawców, którzy czasami zadają pytania przetargowe w celu ujawnienia wrażliwych z punktu widzenia technologicznego i bezpieczeństwa, informacji dot. stosowanej u Zamawiającego infrastruktury. 9. Braku możliwości ograniczania proponowanych rozwiązań ICT (a zwłaszcza rozwiązań i systemów bezpieczeństwa), z powodu np. ujawnionych, ogólnie znanych doniesień medialnych nt. potencjalnie niepożądanych powiązań produkujących je firm, wątpliwości dot. faktycznej wydajności lub stopnia zabezpieczeń, etc. zwłaszcza, jeżeli wg. dokumentacji produktowej, rozwiązania te spełniają wymogi, etc. 10. Dodatkowo to zjawisko jest wzmagane przez bezkrytyczny trend stosowania w znaczącej wadze kryterium ceny, do wyliczenia ostatecznej wyceny rozwiązania. Reputacja producenta produktu, jego uczestnictwo w UE, NATO, etc. nie ma najmniejszego znaczenia. Powoduje to pewne ryzyka w bezpieczeństwie łańcucha dostaw, mogące zostać wykorzystane. 11. etc. etc.   Poniższe artykuły są zapisane w sposób niewystarczająco nakazowy, a także jest – patrząc obiektywnie – niewielki objętościowo w stosunku do wielu artykułów Ustawy, nakazujących bezwzględne jej stosowanie i opisujących różne warianty. Ustawa w ogóle nie wspiera tego, co tak ewidentnie jest zapisane w *Strategii Cyberbezpieczeństwa RP na lata 2019-2024*, tj. tego, że obszar obronności państwa obejmuje również cyberprzestrzeń, a ta przecież powstaje poprzez uruchamianie i łączenie infrastruktur ICT, stąd postępowania zakupowe dot. infrastruktury ICT i bezpieczeństwa IT powinny być w szczególności chronione przed nieuzasadnionym szerokim wypływem informacji, przy zachowaniu kontroli nad finansami publicznymi.  Dodatkowo, możliwości oferowane przez Art. 131e ust.1 (ograniczanie potencjalnych Wykonawców) należałoby rozszerzyć o zapisy proponowane przez Państwa projekt zmian Ustawy o ksc. Są bardzo sensowne z punktu widzenia cyberbezpieczeństwa. Na razie obecnie obowiązująca Ustawa Prawo Zamówień publicznych nie wspiera w wystarczający sposób możliwość wykluczenia potencjalnego Wykonawcy z postępowania, wskutek obiektywnie wiarygodnych informacji na jego temat, dotyczących bezpieczeństwa, które w wystarczający sposób uzasadniają podjęcie daleko idącej ostrożności w stosunku do niego. | **Wyjaśnieni**  Zrezygnowano z przepisów zmieniających Prawo Zamówień Publicznych |
|  | SayF | Art. 1 ust. 1 pkt 4) | Ustawa określa organizację krajowego systemu cyberbezpieczeństwa oraz zadania i obowiązki podmiotów wchodzących w skład tego systemu, sposób sprawowania nadzoru i kontroli w zakresie stosowania przepisów ustawy, zakres Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej.  Projekt nowelizacji tej ustawy rozszerza zakres regulacji ustawy o krajowym systemie cyberbezpieczeństwa, dalej „KSC”, o zadania i obowiązki przedsiębiorców komunikacji elektronicznej wykraczające poza obszar cyberbezpieczeństwa.  Pojęcie bezpieczeństwa w komunikacji elektronicznej jest znacznie szerszy niż tylko sprawy określone w ustawie o KSC to znaczy sprawy związane z cyberbezpieczeństwem.    **Proponujemy wykreślić art. 1 ust. 1 pkt 4 lub przeredagować treść art. 1 ust 1 pkt 4 i nadając mu treść:**  **„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;”**  **Po wykreśleniu art. 1 ust. 2 pkt 1 KSC będzie odnosiła się również do przedsiębiorców komunikacji elektronicznej w takim samym zakresie jak do innych podmiotów.** | **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 przez ustawę wprowadzającą PKE.  Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowym.  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. |
|  | KIGEIT | Art. 1 ust. 1 pkt 4 | **Propozycja zmiany:** wykreślenie:  ~~„4) 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;”,~~  **Uzasadnienie:**  Zgodnie z dyrektywą NIS wymogi w zakresie sprawozdawczości dotyczące bezpieczeństwa i incydentów wynikające z przedmiotowej dyrektywy nie mają zastosowania do przedsiębiorstw telekomunikacyjnych. Obowiązki związane z kwestiami cyberbezpieczeństwa podlegają wymogom Art. 13a i 13b dyrektywy 2002/21/WE. | **Uwaga nieuwzględniona**  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 przez ustawę wprowadzającą PKE.  Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowym.  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. |
|  | PIIT | Art. 1 | 1. **Art. 1 ustawy o krajowym systemie cyberbezpieczeństwa (dalej, jako KSC).**   Projekt zakłada bardzo istotną, systemową zmianę w sposobie regulacji obecnych obowiązków przedsiębiorców telekomunikacyjnych, a w przyszłości przedsiębiorców komunikacji elektronicznej. Celem projektu jest, bowiem włączenie tej kategorii podmiotów do krajowego systemu cyberbezpieczeństwa, a także określenie nowych obowiązków, w tym w zakresie – przekraczającym postanowienia aktualnej ustawy – Prawo telekomunikacyjne oraz projektowanej ustawy – Prawo komunikacji elektronicznej. Tym samym, podmioty dotychczas wyłączone tj. m.in. przedsiębiorcy telekomunikacyjni mieliby zostać objęci wymaganiami ustawy KSC w zakresie wymogów dot. bezpieczeństwa i zgłaszania incydentów.  Rozwiązanie to, jako rodzące daleko idące wątpliwości wymaga przynajmniej istotnej modyfikacji. Należy, bowiem zwrócić uwagę na podstawowe ramy nadawane w tym zakresie przez prawodawstwo unijne:   * Zgodnie z art. 1 ust. 3 dyrektywy Parlamentu Europejskiego I Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. *w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii,* który stanowi, że: „3.*Wymogi dotyczące bezpieczeństwa i zgłaszania incydentów przewidziane w niniejszej dyrektywie* ***nie mają zastosowania do przedsiębiorstw, które podlegają wymogom art. 13a i 13b dyrektywy*** *2002/21/WE,* ***ani do dostawców usług zaufania****, którzy podlegają wymogom art. 19 rozporządzenia (UE) nr 910/2014.”.* * Zmiany w zakresie bezpieczeństwa i integralności sieci i usług w Dyrektywie Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiającej Europejski kodeks łączności elektronicznej, wobec dotychczasowych przepisów art. 13a i 13 b dyrektywy ramowej sprowadzają się do:   + rozszerzenia zakresu regulacji z przedsiębiorców telekomunikacyjnych, na przedsiębiorców komunikacji elektronicznej;   + uelastycznienia w zakresie możliwości określenia organu właściwego poprzez zastąpienie odwołania do właściwości organu regulacyjnego odwołaniem do „właściwego organu”;   + doprecyzowania parametrów dla kryteriów zgłoszenia incydentów;   + dodania możliwości zwracania się o pomoc CSIRT.   Niepodważalne jest więc wyłączenie m.in. przedsiębiorców telekomunikacyjnych spod regulacji dyrektywy NIS. Tym samym nie jest możliwe wprowadzenie w polskich przepisach regulacji odmiennej, która mogłaby skutkować w przyszłości objęciem tego kręgu podmiotów regulacjami odnoszącymi się np. do usług kluczowych lub cyfrowych. Z drugiej strony implementacja EKŁE nie wymaga tak daleko idących zmian jak te przedstawione w ustawie. Do zakresu proponowanych regulacji odnosimy się jednak w kolejnych punktach stanowiska.  **Postulat**  W zakresie art. 1 pkt 1 należy wprowadzić następujące zmiany:   * przywrócić wyłączenie przewidziane w art. 1 ust. 3 dyrektywy NIS oraz aktualnym art. 1 ust. 2 pkt 1 i 2 KSC; | **Uwaga niewuzględniona**  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 przez ustawę wprowadzającą PKE.  Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowym.  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. |
|  | KIGEIT | Art 1 ust. 2 pkt 1) | **1)nałożenie obowiązków** wynikających z KSC na przedsiębiorców komunikacji elektronicznej)  **Propozycja zmiany:** przywrócenie wyłączenia podmiotowego przedsiębiorców komunikacji elektronicznej o następującej treści:  *2. Ustawy nie stosuje się do:*  *1) przedsiębiorców komunikacji elektronicznej, o których mowa w ustawie z dnia ….Prawo komunikacji elektronicznej (Dz.U. z 2017 r., pozycje 1907 i 2201; 2018, pozycje 106, 138, 650 i 118) w zakresie wymogów dotyczących powiadamiania o zdarzeniach i bezpieczeństwa;*  *2) 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 dla transakcji elektronicznych na rynku wewnętrznym i uchylające dyrektywę 1999/93/WE (Dz.U. L 25) 2005, s. 7, 28.08.2014, s. 73);*  **Uzasadnienie:**  Zgodnie z dyrektywą NIS wymogi w zakresie sprawozdawczości dotyczące bezpieczeństwa i incydentów wynikające z przedmiotowej dyrektywy nie mają zastosowania do przedsiębiorców komunikacji elektronicznej. Obowiązki związane z kwestiami cyberbezpieczeństwa podlegają wymogom Art. 13a i 13b dyrektywy 2002/21/WE | **Uwaga nieuwzględniona**  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 przez ustawę wprowadzającą PKE.  Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowym.  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. |
|  | Izba Gospodarcza Gazownictwa/PGNIG SA Oddział w Zielonej Górze | Art. 1 pkt 10) | Projekt ustawy zakłada znaczne spłaszczenie struktur poprzez wskazanie SOC ( zespół pełniący funkcję operacyjnego centrum bezpieczeństwa w danym podmiocie) zamiast uprzednio wskazywanych „wewnętrznych struktur” odpowiedzialnych za cyberbezpieczeństwo. Takie podejście przy rozległych strukturach terytorialnych przedsiębiorstwa ma znaczny wpływ na ograniczenie zdolności operacyjnych zespołu. W naszej opinii powinno się uwzględnić włączenie w wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo przedsiębiorstwa SOC jako organu operacyjnego. | **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.  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. |
|  | Polska Izba Handlu | Art. 1 ust. 1 pkt 4 KSC | **Propozycja zmiany:** Należy wykreślić  **Uzasadnienie:**  Zgodnie z dyrektywą NIS wymogi w zakresie sprawozdawczości dotyczące bezpieczeństwa i incydentów wynikające z przedmiotowej dyrektywy nie mają zastosowania do przedsiębiorstw telekomunikacyjnych. Obowiązki związane z kwestiami cyberbezpieczeństwa podlegają wymogom Art. 13a i 13b dyrektywy 2002/21 / WE | **Uwaga nieuwzględniona**  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 przez ustawę wprowadzającą PKE.  Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowym.  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. |
|  | KIGEIT | Art. 2 pkt 3b | **Propozycja zmiany:** wykreślenie  *„~~3b) CSIRT Telco – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na rzecz przedsiębiorców komunikacji elektronicznej~~;”*  **Uzasadnienie:**  Zgodnie z dyrektywą NIS wymogi w zakresie sprawozdawczości dotyczące bezpieczeństwa i incydentów wynikające z przedmiotowej dyrektywy nie mają zastosowania do przedsiębiorstw telekomunikacyjnych. Obowiązki związane z kwestiami cyberbezpieczeństwa podlegają wymogom Art. 13a i 13b dyrektywy 2002/21 / WE.  Nawet w wypadku nieuwzględnienia powyższego argumentu, za wykreśleniem definicji przemawia jej nadmiarowość – w projektowanym art. 2 pkt 3a) przewidziana została definicja CSIRT sektorowego, która obejmuje między innymi CSIRT dla sektora telekomunikacyjnego. | **Uwaga nieuwzględniona**  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 przez ustawę wprowadzającą PKE.  Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowym.  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. |
|  | Fundacja Bezpieczna Cyberprzestrzeń | Art. 2 pkt 3b | 1)W art. 2 pkt 3b tworzy się CSIRT Telco. Z jakiego powodu wybrano już nazwę dla CSIRT-u i czemu jest szczególnie wskazany w ustawie, a nie został dodany jako kolejny CSIRT sektorowy - zespół zakresem działania obejmujący usługi telekomunikacyjne.  2)W propozycji nowelizacji nie jest jasne kto pełni rolę organu właściwego dla CSIRT Telco? Czy jest w ogóle organ właściwy dla CSIRT Telco? Projekt nie wskazuje tego jednoznacznie. | CSIRT Telco nie jest CSIRT sektorowym ponieważ w ustawie nie ma sektora telekomunikacja. Organem zapewniającym funkcjonowanie CSIRT Telco jest minister właściwy do spraw informtyzacji |
|  | Fundacja Bezpieczna Cyberprzestrzeń | Art. 2 pkt 3c | Nie jest jasne dlaczego zadania ISAC zostały ograniczone do wymiany i analizy informacji na temat podatności, zagrożeń i incydentów? Z reguły ISAC świadczą usługi w zależności od potrzeb swoich członków, nie ograniczając się tylko do zadań wskazanych w ustawie. Proponuje się następujące brzmienie przepisu: „centrum wymiany i analizy informacji świadczące wybrane usługi z zakresu cyberbezpieczeństwa na rzecz swoich członków lub funkcjonujące w celu wspierania podmiotów krajowego systemu cyberbezpieczeństwa”. Przepisy projektu zmiany ustawy nie wyjaśniają również sensu powoływania i korzyści z powoływania ISAC, proponowany zakres działalności ISAC można zlecić np. CSIRT-om sektorowym bez uszczerbku dla wymiany informacji w ramach KSC. Trudno o jednoznaczne wskazanie wartości dodanej dla wprowadzenia tego rozwiązania. | **Wyjaśnienie**  ISAC nie są jednostkami operacyjnymi. Są to centra wymiany informacji. |
|  | Związek Banków Polskich | Art. 2 pkt 3c | 3c) ISAC – centrum wymiany i analizy informacji na temat podatności, zagrożeń i incydentów funkcjonujące w celu wspierania**, w szczególności** podmiotów krajowego systemu cyberbezpieczeństwa**, a także podmiotów w ramach danego sektora, sektorów lub podsektorów;**  ISAC powinien również wspomagać podmioty z danego sektora, sektorów lub podsektorów niezależnie od wydania decyzji o uznaniu za OUK – zapewni to szczelność systemu. Szczególnym przypadkiem jest tutaj sektor bankowy, w którym bezpieczeństwo jednego banku zależy również od innych podmiotów – pozostałych banków, dostawców usług płatniczych, izb rozliczeniowych itd. | **Uwaga nieuwzględniona**  ISAC mogą przekazywać informacje wszystkim podmiotom KSC. |
|  | Fundacja Bezpieczna Cyberprzestrzeń | Art. 2 pkt 3d | Proponuje się następujące brzmienie tłumaczenia Security Operation Center: „centrum operacji bezpieczeństwa” lub „centrum operacji cyberbezpieczeństwa”. Jeśli natomiast przewidywana jest możliwość outsourcingu SOC to w definicji powinien być zapis „zespół pełniący funkcję centrum operacji cyberbezpieczeństwa w danym podmiocie lub na rzecz tego podmiotu”. | **Uwaga nieuwzględniona**  Obecna definicja SOC zapewnia możliwość funkcjonowania takich zespołów wewnątrz operatorów usług kluczowych jak i mogą być te zespoły prowadzone przez podmioty zewnętrzne na rzecz OUK. |
|  | PKP Energetyka | Art. 2 pkt 3d | Projekt wprowadza definicję Operacyjne Centrum Bezpieczeństwa (SOC) i określa szereg obowiązków, które ma ten podmiot wykonywać. Należy zwrócić uwagę na ust. 6 art. 14 Projektu zgodnie z którym SOC na swojej stronie internetowej ma udostępnić szereg informacji na temat swojej działalności. Podsumowując kwestie związane z ujawnianiem danych chronionych – wielość tych danych oraz  obowiązek wskazany w Projekcie w kontekście przekazywania ich różnym podmiotom, przy braku konkretnego celu ich wykorzystania – wydaje się nadmiernym obowiązkiem.  Wątpliwości rodzi budowanie złożonej siatki przekazywania informacji i wielu chronionych danych (np. osobowych lub o incydentach) pomiędzy podmiotami CSIRT-y centralne, sektorowe, Biuro Pełnomocnika, Kolegium ds. Cyberbezpieczeństwa oraz ISAC-e (takich podmiotów może być  kilkadziesiąt), np. kiedy, do kogo aby spełnić wymagania 24 godzin. W zaproponowanych regulacjach brakuje klucza według którego podmioty miałyby się dzielić takimi informacjami. Mając na uwadze powyższe, proponujemy dla danego obszaru (branży) stworzenie jednego punktu kontaktu. Takie rozwiązanie (stosowane na wzór np. single point of contact w telekomunikacji, one stop shop w  branży kolejowej) pozwoli na transparentność procesu w kontekście zbierania informacji. | **Wyjaśnienie**  Projekt nawiązuje do praktyki rynkowej – udostępniania informacji według wzoru dokumentu RFC 2350.  Skuteczną komunikację zapewni podłączenie podmiotu krajowego systemu cyberbezpieczeństwa do systemu o którym mowa w art. 46. |
|  | SayF | Art. 2 pkt 3e | Proponuje się wykreślić wyraz „oznacza”. Wyraz ten użyto już w zdaniu wprowadzającym do wyliczania w art. 2. | **Wyjaśnienie**  Definicja została zmieniona |
|  | Związek Banków Polskich | Art. 2 pkt 3e | W pierwszym zdaniu mowa jest o dostawcy sprzętu lub oprogramowania, a rozwinięcie w podpunkcie a) mówi dodatkowo o usługach ICT. Jest to znacznie szerszy zakres. | **Wyjaśnienie**  Definicja została zmieniona |
|  | PKP Energetyka | art. 2 pkt. 3e | Projekt przewiduje w art. 2 pkt 3e) dodanie definicji *„dostawcy sprzętu lub oprogramowania”* (w tym definicje produktów, usług i procesów ICT) które jak rozumiemy, zostało wprowadzone w związku z  uprawnieniem Kolegium do oceny Dostawców oraz objęciem ustawą rynku telekomunikacyjnego. Takie ujęcie ww. definicji może mieć negatywny wpływ na rozwój rynku, nie tylko informatycznego poprzez ustalanie listy Dostawców. Zgodnie z Projektem, centralizacja na szczeblu rządowym szeregu decyzji właściwych dla firm, podejmowanych na poziomie operacyjnym, takich jak np. wybór odpowiedniego dla danej organizacji Dostawcy lub korekty analizy ryzyka (poprzez polecenie zabezpieczające) i  wdrożenie zabezpieczeń, ogranicza decyzyjność i niezależność biznesową tych podmiotów. | **Wyjaśnienie**  Definicja została zmieniona |
|  | KIGEIT | Art. 2 pkt 8a | **Propozycja zmiany:** wykreślenie  *~~8a) incydent telekomunikacyjny – incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi komunikacji elektronicznej;~~*  **Uzasadnienie:**  Incydenty dotyczące wszystkich pozostałych sektorów nie zostały ujęte w definicjach. Brak jest również określenia mechanizmów oznaczania incydentów, np. dla operatora usługi komunikacji elektronicznej, sklasyfikowanej jako usługa kluczowa, pojawia się wątpliwość – czy incydent może być: telekomunikacyjny, istotny i poważny, czy tylko kluczowy (niejasne jest stopniowanie typów ryzyk). | **Uwaga nieuwzględniona**  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 przez ustawę wprowadzającą PKE.  Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowym.  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.  Dlatego potrzebne jest przeniesienie odpowiednich definicji z PKE do ustawy KSC. |
|  | SayF | Art. 2 pkt 8a | Proponuje się wykreślić tę definicję lub zmienić definicję na odnoszącą się do bezpieczeństwa systemów informacyjnych wykorzystywanych w komunikacji elektronicznej – do cyberbezpieczeństwa w komunikacji elektronicznej.  Incydent telekomunikacyjny nie dotyczy innego bezpieczeństwa jak tylko bezpieczeństwa w cyberprzestrzeni.  Definicja incydentu (art. 2 pkt 5) odnosi się do wszystkich incydentów bez względu na podmiot, u którego wystąpi.  **Jeśli jednak powinien autorzy projektu uznają, że należy zdefiniować pojęcie „incydent telekomunikacyjny” to proponuję:**  **„incydent telekomunikacyjny – zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo w komunikacji elektronicznej, w szczególności może spowodować lub spowoduje obniżenie; jakości lub przerwanie ciągłości świadczenia usługi komunikacji elektronicznej**; | **Uwaga nieuwzględniona**  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.  Dlatego potrzebne jest przeniesienie odpowiednich definicji z PKE do ustawy KSC. |
|  | KIGEIT | art. 2 pkt 8f | **Propozycja zmiany:**  *8f) bezpieczeństwo sieci i usług – zdolność sieci telekomunikacyjnych lub usług komunikacji elektronicznej do odpierania lub minimalizowania skutków wszelkich działań naruszających dostępność, autentyczność, integralność lub poufność:*  *a) tych sieci lub usług,*  *b) przetwarzanych danych i treści objętych tajemnicą komunikacji elektronicznej,*  *c) innych świadczonych przez przedsiębiorcę komunikacji elektronicznej usług związanych z usługami komunikacji elektronicznej lub sieciami telekomunikacyjnymi tego przedsiębiorcy;*  **Uzasadnienie:**  Z praktycznego punktu widzenia nie jest możliwe zagwarantowanie absolutnej skuteczności stosowanych zabezpieczeń, zapewniających w każdym przypadku uniknięcie naruszenia. | **Uwaga nieuwzględniona**  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 przez ustawę wprowadzającą PKE.  Zaproponowana definicja jest wyczerpująca. |
|  | SayF | Art. 2 pkt 8f | Konsekwencją przeredagowania art. 1 ust. 1 pkt 4 będzie usunięcie art. 1 pkt 8f. Definicja zawarta w art. 2 pkt 4 (i nie tylko ta definicja) dotyczy również systemów informacyjnych wykorzystywanych przez przedsiębiorców komunikacji elektronicznej. | **Uwaga nieuwzględniona**  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 przez ustawę wprowadzającą PKE.  Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowym.  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.  Dlatego potrzebne jest przeniesienie odpowiednich definicji z PKE do ustawy KSC. |
|  | KIGEIT | art. 2 pkt 8g | **Propozycja zmiany:** wykreślenie  *~~8g) sytuacja szczególnego zagrożenia – sytuacja, o której mowa w art. 2 pkt 65 ustawy z dnia … – Prawo komunikacji elektronicznej;~~*  **Uzasadnienie:**  Art. 2 pkt 8g przedmiotowego projektu definiuje sytuację szczególnego zagrożenia jako sytuację, o której mowa w art. 2 pkt 65 ustawy z dnia … – Prawo komunikacji elektronicznej. Jednakże zgodnie z powołanym przepisem projektowanego Prawa komunikacji elektronicznej, sytuacja szczególnego zagrożenia oznacza: *stan nadzwyczajny, sytuację kryzysową, w rozumieniu ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. 2019 r. poz. 1398 oraz z 2020 r. poz. 148, 284, 374 i 695) lub bezpośrednie zagrożenie dla bezpieczeństwa sieci i usług*. Definicja sytuacji szczególnego zagrożenia określona została w Prawie komunikacji elektronicznej na potrzeby planowania działań przedsiębiorcy telekomunikacyjnego na wypadek wystąpienia stanu nadzwyczajnego (wojennego, wyjątkowego lub klęski żywiołowej), sytuacji kryzysowej lub szeroko rozumianego zagrożenia dla bezpieczeństwa sieci i usług, w tym również zagrożenia terrorystycznego, awarii sprzętu, przerwy w dostawie energii elektrycznej i innych. Przepisy ustawy o krajowym systemie cyberbezpieczeństwa nie odnoszą się do tak szeroko rozumianych sytuacji szczególnego zagrożenia. Przepisy te odnoszą się wyłącznie do zagrożenia dla bezpieczeństwa sieci i usług w zakresie cyberataków. W tej sytuacji definicja sytuacji szczególnego zagrożenia nie ma zastosowania w ustawie o krajowym systemie cyberbezpieczeństwa. Problematyka sytuacji szczególnego zagrożenia została wystarczająco uregulowana w Prawie telekomunikacyjnym oraz będzie uregulowana w Prawie komunikacji elektronicznej, którego przepisy odnoszą się również do cyberbezpieczeństwa.  Co więcej, pojęcie sytuacji szczególnego zagrożenia w ogóle nie występuje na gruncie ustawy o KSC poza projektowanym art. 20a, który, jak wspomniano powyżej, stanowi powtórzenie art. 39 projektu PKE i z tego powodu winien zostać usunięty z Projektu. | **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 przez ustawę wprowadzającą PKE.  Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowym.  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.  Dlatego potrzebne jest przeniesienie odpowiednich definicji z PKE do ustawy KSC. |
|  | SayF | Art. 2 pkt 15 | Zła odmiana. Proponujemy zamienić „usługę świadczoną drogą elektroniczną” na „usługa świadczona drogą elektroniczną” | **Uwaga uwzględniona** |
|  | SayF | Art. 2 pkt 16 | Definicja niejasna. Proponujemy zmienić definicję na „usługa kluczowa – usługa wymieniona w wykazie usług kluczowych, o którym mowa w Art. 6 pkt 1; | **Uwaga nieuzględniona**  Uwaga nie dotyczy projektu nowelizacji.  Definicja usługi kluczowej nawiązuje do art. 5 ust. 2 dyrektywy NIS. |
|  | SayF | Art. 2 pkt 18 | Definicja niejasna. Proponujemy rozwinięcie definicji lub dodanie do definicji „o którym mowa w Art. 48” | **Uwaga nieuzględniona**  Uwaga nie dotyczy projektu nowelizacji.  Definicja usługi kluczowej nawiązuje do art. 2 pkt 8 dyrektywy NIS. |
|  | SayF | Art. 2 pkt 19 | Definicja niejasna. Proponujemy rozwinięcie definicji lub dodanie do definicji „o którym mowa w Art. 61 ust 1” | **Uwaga nieuzględniona**  Uwaga nie dotyczy projektu nowelizacji. |
|  | Związek Pracodawców Mediów Elektronicznych i Telekomunikacji MEDIAKOM | Art. 4 | **Mediakom postuluje, by ograniczyć grono przedsiębiorców komunikacji elektronicznej będących częścią systemu cyberbezpieczeństwa do tych tylko, którzy zobowiązani są sporządzać plany działań w sytuacjach szczególnych zagrożeń, o którym mowa w art. 47 ust. 1 PKE.** Jak wskazano powyżej – plany mają obowiązek sporządzać przedsiębiorcy o dużej skali działalności, świadczący własne usługi, z wykorzystaniem własnej sieci i osiągający przychody przekraczające 10 mln złotych. Mają oni realne znaczenie dla krajowego systemu cyberbezpieczeństwa, zaś incydenty bezpieczeństwa, które mogą ich dotknąć z zasady będą miały istotne znaczenie z uwagi na ilość abonentów i obszar, który incydent może dotknąć. Inaczej jest w przypadku mniejszych przedsiębiorców, których liczba jest bardzo znacząca, a jednocześnie znaczenie z uwagi na ilość obsługiwanych abonentów i obszar działania – niewielkie. Przedsiębiorcy ci nie mają realnego znaczenia dla krajowego systemu cyberbezpieczeństwa. Jak pokazała praktyka przedsiębiorcy osiągający przychody do 10 mln złotych nie mieli istotnego znaczenia z punktu widzenia lokalnych podmiotów odpowiedzialnych za zarządzanie kryzysowe – stąd zwolnienie ich z obowiązku tworzenia i uzgadniania z właściwymi podmiotami planów działania, o których mowa w art. 47 ust. 1 PKE. Jednocześnie wielość przedsiębiorców prowadzących działalność na mniejszą skalę jest tak duża – sięgająca aż 6.000 podmiotów, że sama obsługa zgłoszeń incydentów bezpieczeństwa będzie wymagała ogromnej pracy logistycznej.  Dodanie do niego pkt 2a i tym samym włączenie do krajowego systemu cyberbezpieczeństwa wszystkich podmiotów komunikacji elektronicznej  „2a) przedsiębiorców komunikacji elektronicznej sporządzający plan, o którym mowa w art. 47 ust. 1 ustawy Prawo komunikacji elektronicznej” | **Wyjaśnienie**  W sytuacji gdy tak duża liczba różnych usług kluczowych dla bezpieczeństwa państwa i obywateli jest zależna od niezakłóconego świadczenia usług komunikacji elektronicznej niezbędne jest włączenie wszystkich przedsiębiorców komunikacji elektronicznej do jednolitego systemu cyberbezpieczeństwa. |
|  |  |  | **3.** Art. 4 pkt 2a dot. włączenia przedsiębiorców komunikacji elektronicznej do krajowego systemu cyberbezpieczeństwa  Tak jak wskazaliśmy w części ogólnej, w naszej ocenie proponowane przepisy KSC wykraczają poza zakres niezbędny dla wdrożenia EKŁE. Jednocześnie zakres proponowanych zmian jest tak szeroki i budzi tak daleko idące wątpliwości, że nie będzie możliwe wykonanie nowych obowiązków w przewidywanych  w projekcie ustawy terminach. Co więcej dublowanie obowiązków raportowych uważamy za nieproporcjonalne i nieefektywne rozwiązanie.  Nie negując na tym etapie ewentualnej potrzeby wzmocnienia aspektów cyberbezpieczeństwa w dotychczasowym modelu raportowym postulujemy przeniesienie dyskusji w tym zakresie na okres po wdrożeniu PKE, tak aby zarówno model raportowania jak i przepisy w tym zakresie, zostały odpowiednio dopracowane, spójne, a przede wszystkim dawały odpowiedni czas na podjęcie organizacyjnego i finansowego wysiłku w zakresie dostosowania się do nowych wymagań.  Postulat:  o Art. 4 ust. 2a oraz 5a należy usunąć z obecnego projektu. Dyskusję nad przepisami w tym zakresie powinna poprzedzić rzetelna debata nad realnymi potrzebami, przeprowadzona z udziałem zainteresowanych partnerów społecznych, w tym podmiotów, które miałyby zostać objęte tymi wymaganiami. | **Uwaga nieuwzględniona**  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 przez ustawę wprowadzającą PKE.  Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowym.  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. |
|  | KIGEIT | Art. 4 pkt 2a i 5a | **Propozycja zmiany:** wykreślenie  *~~2a) przedsiębiorców komunikacji elektronicznej;~~*  *~~5a) CSIRT Telco~~;*  **Uzasadnienie:**  Zgodnie z dyrektywą NIS wymogi w zakresie sprawozdawczości dotyczące bezpieczeństwa i incydentów wynikające z przedmiotowej dyrektywy nie mają zastosowania do przedsiębiorstw telekomunikacyjnych. Obowiązki związane z kwestiami cyberbezpieczeństwa podlegają wymogom Art. 13a i 13b dyrektywy 2002/21/WE. | **Uwaga nieuwzględniona**  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 przez ustawę wprowadzającą PKE.  Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowym.  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.  Dlatego potrzebne jest przeniesienie odpowiednich definicji z PKE do ustawy KSC. |
|  | ISSA Polska | Art. 4 pkt 6 | Proponujemy dla art. 14 dla punktu 6 zastosować terminologię przyjętą w ustawie w zakresie określania deklaracji działania SOC. W związku z powyższym proponujemy punkt 6. zamienić na: 6) posiadać i udostępniać w języku polskim i angielskim deklarację polityki działania w zakresie określnym w dokumencie RFC 2350 publikowanym przez organizację Internet Engineering Task Force (IETF); | **Wyjaśnienie**  Przywoływany przepis prawa dotyczy jedynie SOC prowadzonych podmioty nie będące operatorami usług kluczowych. |
|  | ISSA Polska | Art. 4 pkt 16 | **Propozycja zmiany**  SOC i podmioty świadczące usługi z zakresu cyberbezpieczeństwa;”  Wykreślenie podmiotów świadczących usługi mogłoby spowodować naruszenie równowagi rynku oraz wyrzucić dostawców usług np. specjalizowanej usługi forensic poza ustawę. W naszej ocenie nie każdy podmiot świadczący usługi z zakresu cyberbezpieczeństwa jest lub będzie SOC. | **Wyjaśnienie**  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.  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. |
|  | Związek Banków Polskich | Art. 4 pkt 16 | Przepis budzi wątpliwości.  Aktualna treść tego punktu to: „podmioty świadczące usługi z zakresu cyberbezpieczeństwa;” – jest to znacznie szersze określenie dotyczące wielu podmiotów. Zmiana zapisu na SOC jest niejasna, niejednoznaczna i wskazuje na pojedynczą komórkę jakiegoś podmiotu. | **Wyjaśnienie**  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.  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. |
|  | Naczelna Organizacja Techniczna. Federacja Stowarzyszeń Naukowo-Technicznych | Art. 4a | art. 4a *„(…) 4. 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. Wniosek zawiera dane, o których mowa w ust. 3 pkt 1-5. (…)”.* W związku z tym, że do zakresu zadań ISAC ma należeć m.in. wymiana informacji, dobrych praktyk i doświadczeń dotyczących zagrożeń cyberbezpieczeństwa, podatności oraz incydentów rekomendujemy, aby we wskazanym katalogu organów uprawnionych do wydania opinii pozytywnej na temat ISAC włączyć również CSIRT sektorowy oraz CSIRT Telco | **Wyjaśnienie**  Przepis został zmieniony. ISAC będzie opiniowany przez organy właściwe do spraw cyberbezpieczeństwa. |
|  | Izba Gospodarcza Gazownictwa/Polska Spółka Gazownictwa Sp. z.o.o. | Art. 4a. 1. | **Nowy rodzaj podmiotu ISAC - brak zdefiniowanych kryteriów i wymagań, które ISAC powinny spełniać**  ISAC powinno podlegać i spełniać wymagania ustawy na poziomie nie mniejszym niż OUK | **Uwaga nieuwzględniona**  ISAC są inicjatywą dobrowolną i nie są jednostkami operacyjnymi. Ich zadaniem ma być gromadzenie i dzielenie się przydatnymi informacjami z zakresu cyberbezpieczeństwa. 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. |
|  | Izba Gospodarcza Gazownictwa/Polska Spółka Gazownictwa Sp. z.o.o. | Art. 4.a | **Zespoły ISAC**  Nie zostały doprecyzowane : funkcja, miejsce i rola ISAC, co rodzi m.in. poniższe pytania:  Czy w ramach CSiRT mogą być powołane ISAC?  Czy ISAC będzie pełnił role wymiany informacji z podmiotami OUK i DUC, czy też komercyjne.  Na jakich zasadach OUK, DUC będą mogły korzystać z usług lub pomocy ISAC – na zasadach komercyjnych czy nieodpłatnych ? | **Wyjaśnieni**  ISAC są inicjatywą dobrowolną i nie są jednostkami operacyjnymi. Ich zadaniem ma być gromadzenie i dzielenie się przydatnymi informacjami z zakresu cyberbezpieczeństwa. 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. |
|  | Związek Banków Polskich | Art. 4a ust. 1 | „Art. 4a. 1. W ramach krajowego systemu cyberbezpieczeństwa może funkcjonować ISAC **realizujący zadania dla podmiotów z danego sektora, sektorów lub podsektorów**, w szczególności związane z wymianą informacji, dobrych praktyk i doświadczeń dotyczących zagrożeń cyberbezpieczeństwa, podatności lub incydentów;**”**  ISAC (centra wymiany i analizy informacji), tworzone jako inicjatywy sektorowe lub dziedzinowe, mają być jednostkami wspierającymi podmioty krajowego systemu cyberbezpieczeństwa. ISAC powinien jednak wspomagać również podmioty z danego sektora lub sektorów, niezależnie od wydania decyzji o uznaniu za OUK – zapewni to szczelność systemu. Szczególnym przypadkiem jest tutaj sektor bankowy, w którym bezpieczeństwo jednego banku zależy również od innych podmiotów – pozostałych banków, dostawców usług płatniczych, izb rozliczeniowych itd. | **Uwaga nieuwzględniona**  ISAC są inicjatywą dobrowolną i nie są jednostkami operacyjnymi. Ich zadaniem ma być gromadzenie i dzielenie się przydatnymi informacjami z zakresu cyberbezpieczeństwa. 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. Nic nie broni, aby ISAC świadczyły swoje usługi podmiotom spoza KSC. |
|  | Fundacja Bezpieczna Cyberprzestrzeń | art. 4a ust. 1 | w przepisie powinna być zastosowana liczba mnoga tj. „mogą funkcjonować ISAC”, ponadto zakres zadań wskazanych w tym artykule jest odmienny od wskazanego w definicji ISAC w art. 2 pkt 3c | **Wyjaśnienie**  W technice legislacyjnej używa się liczby pojedynczej dla określenia podmiotów, które będą spełniać cechy określone w ustawie. |
|  | Fundacja Bezpieczna Cyberprzestrzeń | art. 4a ust. 2 | Nie jest jasne w jakim celu minister prowadzi wykaz ISAC? Czy jest to forma wyrażenia zgody na prowadzenie tego typu działalności, wbrew ust. 7? Nie są również podane żadne zadania jakie miałby realizować ISAC, poza celem jego funkcjonowania. Z uzasadnienia wynika, że celem jest dostęp do wiedzy eksperckiej dotyczącej cyberzagrożeń, ale ustawodawca nie określił na jakie konkretne zadania należy ten cel przełożyć | **Wyjaśnienie**  ISAC są inicjatywą dobrowolną i nie są jednostkami operacyjnymi. Ich zadaniem ma być gromadzenie i dzielenie się przydatnymi informacjami z zakresu cyberbezpieczeństwa. 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. |
|  | Związek Banków Polskich | Art. 4a ust. 2 | Nowe brzmienie ust. 2 – **dalsze ustępy art. 4a uległyby przenumerowaniu.**  **2)ISAC może wykonywać zadania powierzone SOC, w szczególności związane z zarządzaniem, koordynowaniem i obsługą incydentów (bezpieczeństwa) zagrażających bezpieczeństwu podmiotów, o których mowa w ust. 1 lub ich klientom.**  Taka propozycja podniesie efektywność wymiany informacji o incydentach, będzie zgodna z formą działania ISAC praktykowaną w Europie polegającą na tworzeniu zespołów zadaniowych w celu reagowania na incydenty (Ad hoc investigative working group). Umożliwi również realne wsparcie podmiotów krajowego systemu cyberebzpieczeństwa oraz podmiotów z danego sektora, sektorów lub podsektorów.  <https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models/at_download/fullReport>  Np. Luxemburg CERT jest jednocześnie ISAC. | **Uwaga nieuwzględniona**  ISAC są inicjatywą dobrowolną i nie są jednostkami operacyjnymi. Ich zadaniem ma być gromadzenie i dzielenie się przydatnymi informacjami z zakresu cyberbezpieczeństwa. 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. |
|  | Fundacja Bezpieczna Cyberprzestrzeń | art. 4a ust. 4 | Konieczne jest doprecyzowanie w jakim zakresie opiniowany jest wniosek o wpisanie do wykazu ISAC. Dodatkowo przepis wymaga uszczegółowienia kwestia czy bez uzyskania pozytywnej opinii wszystkich CSIRT-ów poziomu krajowego można zostać wpisanym do wykazu oraz czy bez takiej opinii nie można zaprzestać prowadzenia ISAC. Sama idea ISAC zakłada samoorganizację podmiotów (najczęściej danego sektora) w celu wymiany istotnych informacji z zakresu cyberbezpieczeństwa. Podmioty te działają na własną rzecz i we własnym zakresie się finansują. Z założenia ISAC nie są tworzone w celach komercyjnych (choć ten cel nie jest wykluczony). Z uzasadnienia wynika, że celem jest dostęp do wiedzy eksperckiej dotyczącej cyberzagrożeń. Prowadzenie rejestru, konieczność uzyskania opinii CSIRT-u poziomu krajowego oraz obowiązek przedkładania sprawozdania z realizacji zadań za poprzedni rok kalendarzowy na pewno nie są czynnikami sprzyjającymi i zachęcającym do tworzenia ISAC, co jest zaprzeczeniem idei przedstawionej w uzasadnieniu projektu. | **Wyjasnienie**  ISAC są 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.  W nowej wersji projektu zrezygnowano z opiniowania ISAC przez CSIRT poziomu krajowego natomiast będą opiniować wszystkie organy właściwe do spraw cyberbezpieczeństwa. |
|  | Fundacja Bezpieczna Cyberprzestrzeń | art. 4a ust. 9 | Istnieje konieczność doprecyzowania jaki jest cel przedstawiania sprawozdania oraz jaki miałby być zakres informacji przedstawianych w sprawozdaniu, biorąc pod uwagę brak precyzyjnie określonych dla ISAC zadań. | **Wyjaśnienie**  ISAC są inicjatywą dobrowolną i nie są jednostkami operacyjnymi. Ich zadaniem ma być gromadzenie i dzielenie się przydatnymi informacjami z zakresu cyberbezpieczeństwa. 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. Sprawozdanie jest niezbędne dla oceny funkcjonowania ISAC w ramach KSC. |
|  | Związek Banków Polskich | Art. 4a ust. 9 | **4a. ust. 9. ISAC** współpracują ze sobą oraz z CSIRT MON, CSIRT NASK, CSIRT GOV **i CSIRT sektorowymi, w szczególności w zakresie wymiany wiedzy i informacji o podatnościach, zagrożeniach i zidentyfikowanych incydentach oraz ich obsługi i koordynacji.**  **Propozycja nowego ust. 10 w brzmieniu:**  4a. ust. 10.ISAC przedkładają ministrowi spraw informatyzacji w terminie do dnia 31 marca każdego roku sprawozdanie z realizacji zadań za poprzedni rok kalendarzowy.  Dotychczasowy ust. 10 uległby przenumerowaniu.  Zapewnienie wymiany informacji między sektorami.  Proponujemy również rozdzielić kwestię współpracy z CSIRTami od kwestii przedkładania sprawozdań i zawarcie tej kwestii w kolejnym ustępie (dalsze ustępy uległy by przenumerowaniu). | **Uwaga częściowo uwzględniona**  ISAC nie ma kompetencji operacyjnych. Nie bierze udziału w obsłudze i reagowaniu na incydenty. Może uczestniczyć w wymianie informacji o zagrożeniach, podatnościach czy zaobserwowanych incydentach. |
|  | Fundacja Bezpieczna Cyberprzestrzeń | art. 4a ust. 10 | Istnieje konieczność doprecyzowania w jakim zakresie działalność ISAC może być niezgodna z prawem oraz zasad współpracy obowiązujących w ramach KSC. | **Wyjaśnienie**  Chodzi o przypadki naruszenia ustawy ksc lub prawa karnego albo nie respektowanie warunków zawartych w porozumieniu ws. korzystania z systemu z art. 46. |
|  | Home.pl | Art. 5 ustawy zmieniającej | Zgodnie z przepisem art. 5  ustawy zmieniającej, nowelizacja ma wejść w życie 21 grudnia 2020 r. to jest wraz z PKE.    **Uwagi w ramach konsultacji:**  - do art. 5 ustawy zmieniającej:  ustawodawca planuje, aby nowelizacja i ustawa Prawo komunikacji elektronicznej, weszły w życie z dniem 21 grudnia 2020 r. Biorąc pod uwagę, dalszą pracę w ramach komisji sejmowych, procedurę głosowania nad projektami w parlamencie oraz podpis pod projektami Prezydenta RP, przewiduję iż ustawy zostaną opublikowana na przełomie listopada i grudnia. W obliczu znacznej ilości zmian, które projekty zawierają okres vacatio legis wynoszący być może niecały miesiąc jest zdecydowanie za krótki. Należy w związku z tym zasugerować przesunięcie daty wejścia w życie przepisów, aby zapewnić adresatom ustawy niezbędny okres na wdrożenie zmian. | **Wyjaśnienie**  Wejście w życie ustawy jest wstępnie planowane na II kwartał 2021 r. |
|  | ISSA Polska | Art. 8 pkt 2 lit. e | Modyfikacja  Objęcie systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej systemem monitorowania cyberbezpieczeństwa w trybie ciągłym w sposób umożliwiający wykrycie i prowadzenie natychmiastowych czynności reakcji na incydent lub zagrożenie. | **Uwaga nieuwzględniona**  Operator usługi kluczowej będzie wprowadzać proporcjonalne do oszacowanych ryzyk środki bezpieczeństwa w tym organizacyjne oraz techniczne. |
|  | ISSA Polska | Art. 8 pkt 3 | Modyfikacja  adekwatne do oceny ryzyka reagowanie na zagrożenia cyberbezpieczeństwa i ujawnione podatności w systemach informacyjnych wykorzystywanych do świadczenia usługi kluczowej; | **Uwaga nieuwzględniona**  Operator usługi kluczowej będzie wprowadzać proporcjonalne do oszacowanych ryzyk środki bezpieczeństwa w tym organizacyjne oraz techniczne. |
|  | ISSA Polska | Art. 8 pkt 5 lit. e | Dodanie zapisu  Przeprowadzania okresowej oceny parametrów konfiguracyjnych systemów wpływających na cyberbezpieczeństwo zgodnie z uznanymi standardami i praktykami. | **Uwaga nieuwzględniona**  Operator usługi kluczowej będzie wprowadzać proporcjonalne do oszacowanych ryzyk środki bezpieczeństwa w tym organizacyjne oraz techniczne. |
|  | ISSA Polska | Art. 8 pkt 5 lit. b | w art. 8 w pkt 5 lit. b otrzymuje brzmienie:  „b) regularne przeprowadzanie aktualizacji oprogramowania, stosownie do zaleceń  producenta, z uwzględnieniem poziomu krytyczności poszczególnych aktualizacji,”;  Na:  „b) regularne przeprowadzanie aktualizacji oprogramowania, stosownie do zaleceń  producenta, na podstawie analizy ryzyka wpływu podatności zawartych w aktualizacjach,”;  Zapis jest adekwatny do czynności przeprowadzanych w ramach procesy zarządzania podatnościami oraz wydaniami. | **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. |
|  | ISACA Warsaw Chapter | Ustawa KSC  ustęp 7) w art. 8 w pkt 5 lit. b | b) regularne przeprowadzanie aktualizacji oprogramowania, stosownie do zaleceń producenta, z uwzględnieniem poziomu krytyczności poszczególnych aktualizacji,”;  **Propozycja treści:**  „b) regularne przeprowadzanie aktualizacji oprogramowania z wykorzystaniem zweryfikowanych aktualizacji; wersjonowanie oprogramowania,” | **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. |
|  | SayF | Art. 10 ust 2 | Brakuje CSIRT Telco | **Uwaga 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 ksc przez ustawę wprowadzającą PKE. |
|  | Transition Software | Art. 11, ust.1, pkt. 4,5 oraz powiązane z nim art.12 i zwłaszcza art. 13, ust.1, pkt.2 (o elektronicznym kanale przesyłu), jak również wszystkie powiązane z nimi analogiczne artykuły na przestrzeni całej ustawy (np. Art. 18, ust. 5, Art.20, Art. 20c, ust.1., pkt 3) i ust2 i ust.3 pkt1),2),3), Art.22, ust.1 i 2, Art.23, Art.24, 24a pkt 1), etc. | Należy w ustawie dodać artykuł, który ma zawierać jedną ogólną zbiorczą informację (na poziomie ustawy), że wymiana informacji (rozumiana w sposób całościowy) musi odbywać się w sposób bezpieczny, tj. z zastosowaniem bezpiecznych sposobów organizacyjnych oraz minimalnych mechanizmach technicznych/technologicznych (bezpieczny tunel, szyfrowanie, IPSec, PKI, etc.), ogólnouznawanych (rynek, branża IT) za bezpieczne, w okresie ich wdrożenia (np. w obecnym okresie, ogólnouznawany w branży IT za taki jest minimum AES256, etc.).  Jest obecnie w *Rozporządzeniu Ministra Cyfryzacji z dn. 4 grudnia 2019 r. w sprawie warunków organizacyjnych i technicznych dla podmiotów (…)* opisane to ogólnie w §2, ust. 1 pkt. d) oraz pkt. 2), ale w obecnej formie jest niewystarczający (bez konkretnych wymogów technicznych, które należy traktować jako wymagane niezbędne minimum), dlatego ten paragraf w tej formie powinien zostać przeniesiony do ustawy.  Natomiast w ww. Rozporządzeniu należy go zastąpić artykułem, który będzie precyzował i podawał konkretne minimalne technologie (np. AES256, IPSec, PKI, etc.), na jakich muszą się opierać wdrażane środki bezpieczeństwa. Analogicznie, jak jest to podane chociażby w przypadku stopnia ochrony stropu, drzwi, ścian w §2 ust. 2 tegoż rozporządzenia.  Podane mechanizmy zabezpieczeń powinny być przez podmiot zapewnione i wdrożone, niezależnie od wyniku przeprowadzonej przez dane przedsiębiorstwo analizy ryzyka, która zawsze ma charakter subiektywny w obrębie danej organizacji. | **Uwaga nieuwzględniona**  Operator usługi kluczowej będzie wprowadzać proporcjonalne do oszacowanych ryzyk środki bezpieczeństwa w tym organizacyjne oraz techniczne. |
|  | Związek Banków Polskich | Art. 11 ust. 3 pkt 1-3 | 3. W przypadku ustanowienia CSIRT sektorowego **lub ISAC działającego w danym sektorze, sektorach lub podsektorach** operator usługi kluczowej niezależnie od zadań określonych w ust. 1:  1) przekazuje jednocześnie właściwemu CSIRT sektorowemu oraz **właściwemu ISAC** w postaci elektronicznej zgłoszenie, o którym mowa w ust. 1 pkt 4;  2) współdziała z właściwym CSIRT sektorowym na poziomie sektora lub podsektora oraz **właściwym ISAC** podczas obsługi incydentu**, w tym incydentu** poważnego lub incydentu krytycznego, przekazując niezbędne dane, w tym **informacje stanowiące tajemnice** **prawnie chronione oraz dane osobowe**;  3 )zapewnia właściwemu CSIRT sektorowemu oraz **właściwemu ISAC** dostęp do informacji o rejestrowanych incydentach w zakresie niezbędnym do realizacji jego zadań.  ISAC to centra wymiany i analiz informacji tworzone jako inicjatywy sektorowe lub dziedzinowe. W celu prawidłowej realizacji zadań powierzonych ISAC, OUK powinni przekazywać mu informacje analogiczne jak przekazywane CSIRT sektorowemu. Zgodnie z uzasadnieniem projektu zadaniem ISAC jest wspieranie podmiotów krajowego systemu cyberbezpieczeństwa – nie byłoby to możliwe bez zapewnienia możliwości pozyskiwania informacji o incydentach przez ISAC. Należy również zapewnić możliwość przekazywania informacji stanowiących informacje prawnie chronione. | **Uwaga nieuwzględniona**  Nie przewiduje się właściwości ISAC. To nie są jednostki operacyjne. ISAC wymieniają informacje z podmiotami, z którymi porozumieją się. |
|  | SayF | Art. 12 ust 1 pkt,  Art. 14a ust 2 pkt 3 | Jaki „właściwy rejestr”? | **Wyjaśnienie**  Chodzi przede wszystkim o numer KRS. |
|  | Fundacja Bezpieczna Cyberprzestrzeń | Art. 14 | Wydaje się, że przypisanie realizacji wszystkich zadań, o których mowa w art. 8, art. 9, art. 10 ust. 1-3, art. 11 ust. 1-3, art. 12 i art. 13 w zakresie cyberbezpieczeństwa do struktury zwanej SOC jest nieuzasadnione. Zespoły SOC są powoływane do realizacji usług związanych z zarządzaniem zdarzeniami i incydentami, rzadziej prowadzenia systematycznego szacowania ryzyka wystąpienia incydentu oraz zarządzania tym ryzykiem czy zbierania informacji o zagrożeniach cyberbezpieczeństwa i podatnościach – tym samym w projekcie dokonano nieuzasadnionego połączenia działań operacyjnych z działaniami typowo zarządczymi. Nawet sam projektodawca w OSR posługuje się pojęciami „usługi tzw. CERTowe (analityczne) oraz SOCowe (reagowania na incydenty)”. Proponuje się wyłączenie zadań nieoperacyjnych z obowiązków zespołu SOC, pozostawiając OUK możliwość zawierania umów z podmiotami świadczącymi usługi z zakresu bezpieczeństwa inne niż SOC (zarzadzanie zdarzeniami i incydentami). Jako alternatywę można przyjąć wyodrębnienie katalogu usług z zakresu cyberbezpieczeństwa (np. na bazie tłumaczenia katalogu CSIRT Services Framework FIRST) do załącznika do ustawy lub odrębnego rozporządzenia i przypisanie konkretnego zestawu tych usług do poszczególnych rodzajów podmiotów krajowego systemu cyberbezpieczeństwa tj. SOC, ISAC, CSIRT sektorowy czy CSIRT poziomu krajowego. Pozwoli to na wyraźny podział pomiędzy tymi podmiotami oraz uniknięcie nakładających się kompetencji i obowiązków. | **Wyjaśnienie**  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.  Definicja SOC odnosi się do wieloletniej praktyki rynkowej, a skrót jest powszechnie rozpoznawalny.  Wskazany 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. |
|  | Naczelna Organizacja Techniczna. Federacja Stowarzyszeń Naukowo-Technicznych | Art. 14 | „*art. 14 (…) 5. W przypadkach, kiedy to niezbędne dla zapewnienia cyberbezpieczeństwa, podmiot prowadzący SOC zapewnia bezpieczny zdalny dostęp do swoich systemów dla obsługiwanego operatora usługi kluczowej przez co najmniej: 1) ustalenie zasad dostępu do systemu; 2) stosowanie środków zapewniających bezpieczne przetwarzanie danych i komunikację; 3) minimalizację przechowywanych danych poza bezpiecznym środowiskiem*”. Biorąc pod uwagę krytyczność danych do których dostęp w związku ze świadczonymi usługami może posiadać podmiot prowadzący SOC rekomendujemy wykreślenie punktu 3, ponieważ w opinii Federacji wszelkie dane powinny być przechowywane wyłącznie w bezpiecznym środowisku. | **Uwaga nieuwzględniona**  Obowiązkiem operatora usługi kluczowej prowadzącego SOC lub podmiotów zewnętrznych prowadzących SOC na rzecz OUK jest zapewnienie takich technicznych i organizacyjnych środków bezpieczeństwa, proporcjonalnych do oszacowanego ryzyka. |
|  | ISSA Polska | Art. 14 pkt 5 | Proponujemy dla art. 14 dla punktu 5 doprecyzować zapis umożliwiający realizacje obowiązku bezpiecznego dostępu zdalnego. Proponujemy następujący zapis:  5. W przypadkach, kiedy jest to niezbędne podmiot prowadzący SOC zapewnia kryptograficznie zabezpieczony, rozliczany dostęp pomiędzy swoimi systemami realizującymi usługi SOC, a monitorowanymi systemami informacyjnych operatora usługi kluczowej. | **Uwaga nieuwzględniona**  Obowiązkiem operatora usługi kluczowej prowadzącego SOC lub podmiotów zewnętrznych prowadzących SOC na rzecz OUK jest zapewnienie takich technicznych i organizacyjnych środków bezpieczeństwa, proporcjonalnych do oszacowanego ryzyka. |
|  | KGHM/Związek Pracodawców Polska Miedź | 14.1 | Zgodnie z nowym brzmieniem art. 14.1 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).  Obarczenie SOC zadaniami innymi niż operacyjne, tj. odpowiedzialność za wdrożenie SZB odpowiedzialność za wdrożenie środków tech/org 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.  Art. 14. 1. Zadania operatora usługi kluczowej, o których mowa w art. 8.3, 8.4, 8.5, 8.6 art. 9 <i dalej bez zmian> | **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.  Definicja SOC odnosi się do wieloletniej praktyki rynkowej, a skrót jest powszechnie rozpoznawalny.  Wskazany 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. |
|  | Federacja Przedsiębiorców Polskich | Art. 14 ust. 1 (w zw. z art. 8) | Przepis art. 14 ust. 1 ustawy o cyberbezpieczeństwie w nowym, projektowanym brzmieniu przewiduje, że zespół operacyjnego centrum bezpieczeństwa (SOC) ma m.in. wdrażać system zarządzania bezpieczeństwem oraz wdrażać odpowiednie i proporcjonalne do oszacowanego ryzyka środki techniczne i organizacyjne (w tym zapewniać bezpieczeństwo fizyczne i środowiskowe).  Nałożenie na SOC obowiązku wdrażania systemu zarządzania bezpieczeństwem, a nie tylko wykonywanie działalności operacyjnej, będzie trudne lub nawet niemożliwe. Zwłaszcza w dużych podmiotach, w których odpowiedzialność za szeroko rozumiane bezpieczeństwo spoczywa na różnych pionach, skupienie tych zadań w SOC utrudni wykonywanie zadań operacyjnych. W związku z powyższym uprzejmie zwracam się o odstąpienie od zmiany art. 14 ust. 1. | **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.  Definicja SOC odnosi się do wieloletniej praktyki rynkowej, a skrót jest powszechnie rozpoznawalny.  Wskazany 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. |
|  | PIIT |  | 1. **Art. 14 - SOC**   Kluczowe zmiany przewidziano w art. 14 ustawy KSC, gdzie dotychczasowe wewnętrzne struktury bezpieczeństwa zastępowane są SOC. Jednocześnie popieraną przez nas zmianą jest przeniesienie na strukturę operatora usługi kluczowej dokonania oceny ryzyka i uzależnienie od niej zakresu wdrażanych środków technicznych i organizacyjnych. Stanowi to realizację naszego podstawowego postulatu przedstawianego w toku prac nad dwoma kolejnymi iteracjami rozporządzeń w tym zakresie.  W zakresie zmiany nazewnictwa i wskazania na konieczność powołania SOC, w naszej ocenie przyjęta w tym przepisie konstrukcja realizacji przez operatora usługi kluczowej zadań wskazanych w ustawie w ramach SOC opiera się na błędnym założeniu, że wszystkie zadania realizowane są w ramach SOC. W strukturach dużych i rozproszonych nałożone na operatora usługi kluczowej obowiązki mogą i często są realizowane przez wiele komórek organizacyjnych, które wspólnie tworzą system bezpieczeństwa całej organizacji. Ponadto warto zwrócić uwagę, że nawet sam projektodawca definiując SOC podkreślił jego operacyjny charakter - SOC to zespół pełniący funkcję operacyjnego centrum bezpieczeństwa w danym podmiocie. Zadania przypisane strukturze bezpieczeństwa OUK nie zawsze jednak mają charakter operacyjny i nie zawsze będą one pozostawały w zakresie odpowiedzialności już istniejących w firmach SOC, które dzisiaj nie zajmują się wyłącznie usługą kluczową i na pewno nie jej pełnym spektrum (np. SOC, jako jednostka operacyjna nie powinna, co do zasady zarządzać ryzykiem, nie zawsze też jest odpowiedzialna za obszar utrzymania i eksploatacji systemów teleinformatycznych). W praktyce w ramach całościowego zarządzania bezpieczeństwem angażowane są różne obszary, dla których odpowiedzialność za część zadań związanych z usługą kluczową jest jedynie ułamkiem działalności. Tym samym nie jest powoływany SOC, jako jednolita struktura dedykowana wyłącznie usłudze kluczowej. Takie rozwiązanie, w przypadku wielości usług i dużej skali działania byłoby rażąco nieefektywne i nieskuteczne.  Wprowadzenie powyższego wymagania może się wiązać w praktyce z koniecznością reorganizacji i przebudowy przyjętego modelu zarządzania usługą kluczową i jej bezpieczeństwem. Nie znajdujemy racjonalnego uzasadnienia dla tak daleko idącej ingerencji państwa w strukturę podmiotów.  **Postulaty:**   * Zwrot SOC jest powszechnie używanym określeniem dla centrów operacyjnych bezpieczeństwa, również w zdecydowanie szerszym niż cyberbezpieczeństwo zakresie. W naszej ocenie na potrzeby usługi kluczowej należy pozostawić dotychczasowe nazewnictwo dla struktury wewnętrznej, a wobec usług zewnętrznych użyć innego, bardziej precyzyjnego określenia, jak np. SOC-OUK lub podobnego akronimu, który jasno wskaże, że chodzi o SOC dla Operatora Usługi Kluczowej. * Ewentualnie należy doprecyzować, że SOC w rozumieniu art. 14 może mieć również formułę opisanej w dokumentacji wewnętrznej, rozproszonej struktury bezpieczeństwa. * Należy rozwiązać potencjalny problem, jaki będzie występował w przypadku powołania (np. w formie zamówienia publicznego) zewnętrznego SOC. Dopiero taki zewnętrzny SOC dokona oceny potrzeb w zakresie środków technicznych i organizacyjnych i tym samym w zależności od dokonanej oceny będzie potrzebował środków na ich wdrożenie, które powinien zapewnić zamawiający usługę OUK. Na tym tle mogą występować konflikty i różnice zdań, które mogą być problematyczne również z uwagi na budżetowanie w ramach zamówień publicznych i jego ograniczoną elastyczność. * W art. 14 ust. 3 pkt 4 słowo „jakością” proponujemy zastąpić słowem „skutecznością”. * W art. 14 ust. 5 proponujemy doprecyzować, że dostęp jest zapewniany w „uzasadnionych przypadkach”, a także postulujemy dodanie zwrotu, że: „*Dostęp operatora usługi kluczowej do systemów podmiotu świadczącego usługę SOC nie może prowadzić do naruszenia tajemnic prawnie chronionych, do których przestrzegania podmiot świadczący usługę SOC jest zobowiązany na podstawie przepisów prawa lub zawartych umów.*” | **Wyjaśnienie**  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.  Definicja SOC odnosi się do wieloletniej praktyki rynkowej, a skrót jest powszechnie rozpoznawalny.  Wskazany 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. |
|  | Federacja Przedsiębiorców Polskich | Art. 14 ust. 2 | Projektowany przepis art. 14 ust. 2 budzi wątpliwość, czy możliwe będzie powierzanie (zawieranie umów) poszczególnych zadań rożnym podmiotom. Projektowane obecnie brzmienie sugeruje, że zlecenie może dotyczyć tylko całość zadań SOC. W związku z powyższym powyższy przepis powinien być zmieniony, aby nie pozostawiać wątpliwości, że możliwe będzie zlecanie różnych zadań, z jednoczesnym utrzymaniem SOC w ramach własnej struktury. | **Wyjaśnienie**  Operator usługi kluczowej może zawrzeć umowę z kilkoma podmiotami realizujących inne zadania o których mowa w art. 14 ust.1. |
|  | KGHM/Związek Pracodawców Polska Miedź | 14. 2 | W 14.2 daje się możliwość realizacji zadań SOC poprzez zlecenie ich innemu podmiotowi.  Zapis nie precyzuje, że jest możliwe częściowe wyotsourcowanie niektórych jedynie zadań SOC. Wg opiniodawcy konieczne jest doprecyzowanie – umożliwienie częściowego outsourcingu. Operator usługi kluczowej powołuje SOC wewnątrz swojej struktury lub zawiera umowę dotyczącą prowadzenia SOC w zdefiniowanym przez niego zakresie działań i na jego zlecenie z innym podmiotem. | **Wyjaśnienie**  Operator usługi kluczowej może zawrzeć umowę z kilkoma podmiotami realizujących inne zadania o których mowa w art. 14 ust.1. |
|  | Bank Handlowy  Pan Szymon Kurnicki | Art 14 2. | Z uwagi na szerokie spektrum działania SOC, częstą praktyką jest model mieszany, w którym część zadań wykonywanych jest w ramach wewnętrznych struktur cyberbezpieczeństwa a część zlecana podmiotom zewnętrznym. Rozumiemy, że zgodnie z brzmieniem cytowanego ust. 2 ustawodawca dopuszcza model hybrydowy działania SOC tj. SOC działający w ramach organizacji OUK przy jednoczesnym powierzeniu wykonaniu części zadań SOK podmiotom zewnętrznym. Zasadnym jest potwierdzenie, że taki model jest dopuszczalny. Jeśli tak, to celem uniknięcia wątpliwości zwracamy się z prośbą o potwierdzenie, czy w takiej sytuacji należy rozróżnić jednoczesne funkcjonowanie dwóch SOC tj. wewnętrznego oraz zewnętrznego. | **Wyjaśnienie**  Operator usługi kluczowej może zawrzeć umowę z kilkoma podmiotami realizujących inne zadania o których mowa w art. 14 ust.1. |
|  | Związek Banków Polskich | Art. 14 ust. 3 | 3. **SOC**, 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 **[ucięte w uwagach – uwaga DC KPRM].**  SOC to zgodnie z definicją „zespół pełniący funkcję operacyjnego centrum bezpieczeństwa w danym Podmiocie”. Odpowiedzialność za wprowadzanie konkretnych zabezpieczeń powinno zostać przypisane do OUK a nie do pojedynczego zespołu w ramach OUK, ponieważ SOC może nie mieć odpowiednich umocowań do wprowadzania konkretnych zabezpieczeń.  Niezależnie zakres zadań który stawiany jest przed SOC może wykraczać poza ramy zadań SOC u konkretnego OUK co może powodować trudności związane z dopasowaniem struktury organizacyjnej do wymogów ustawy. W szczególności zadania związane z projektowaniem konkretnych zabezpieczeń mogą być realizowane przez role Architektów bezpieczeństwa które nie muszą być umieszczone w SOC.  **Proponujemy uchylić ust. 3** | **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.  Definicja SOC odnosi się do wieloletniej praktyki rynkowej, a skrót jest powszechnie rozpoznawalny.  Wskazany 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. |
|  | Krajowy Depozyt Papierów Wartościowych | Art. 14 ust. 3 | Zgodnie z propozycją treści ust. 3 *„SOC, na podstawie przeprowadzonego szacowania ryzyka, wprowadza zabezpieczenia zapewniające poufność, integralność, dostępność i autentyczność przetwarzanych informacji…”* Mając na względzie pierwszy wariant funkcjonowania SOC przewidziany we wcześniejszym ust. 2 (*„Operator usługi kluczowej powołuje SOC wewnątrz swojej struktury”*), niewłaściwym wydaje się założenie, że taki SOC będzie mógł sam wprowadzić jakiekolwiek zabezpieczenia czy też podejmować inne tego rodzaju decyzje. Jako część struktury organizacyjnej operatora usługi kluczowej może raczej posiadać te zabezpieczenia, których wprowadzenia dokonać może wyłącznie sam operator. W związku z tym proponujemy, aby art. 14 ust. 3 ustawy o krajowym systemie cyberbezpieczeństwa brzmiał: *„SOC, na podstawie przeprowadzonego szacowania ryzyka, posiada zabezpieczenia zapewniające poufność, integralność, dostępność i autentyczność przetwarzanych informacji…”* | **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.  Definicja SOC odnosi się do wieloletniej praktyki rynkowej, a skrót jest powszechnie rozpoznawalny.  Wskazany 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. |
|  | KIGEIT | art. 14 ust. 3 | **Propozycja zmiany:**  *3. SOC, ~~na podstawie przeprowadzonego szacowania ryzyka, wprowadza zabezpieczenia zapewniające~~ nadzoruje i uczestniczy we wprowadzaniu zabezpieczeń zapewniających poufność, integralność, dostępność i autentyczność przetwarzanych informacji, z uwzględnieniem bezpieczeństwa osobowego, eksploatacji i architektury systemów, w celu:*  *1) monitorowania i wykrywania incydentów;*  *2) reagowania na incydenty;*  *3) zapobiegania incydentom;*  *4) zarządzania jakością zabezpieczeń systemów, informacji i powierzonych aktywów;*  *5) aktualizowania ryzyk ~~w przypadku zmiany struktury organizacyjnej, procesów i technologii~~, które mogą wpływać na reakcję na incydent.*  **Uzasadnienie:**  Propozycja zmian w celu zapewnienia elastycznej pracy SOC i możliwości reagowania na bieżące zagrożenia niezależnie od procesu szacowania ryzyka i zmian w strukturze organizacyjnej | **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.  Definicja SOC odnosi się do wieloletniej praktyki rynkowej, a skrót jest powszechnie rozpoznawalny.  Wskazany 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. |
|  | Bank Handlowy  Pan Szymon Kurnicki | Art. 14 4. | Z uwagi na nowe obowiązki wynikające z nowelizacji ustawy, w szczególności związane z obowiązkiem powołania przez OUK operacyjnych centrów bezpieczeństwa koniecznym wydaje się doprecyzowanie w jakim terminie OUK zobowiązani są do ich powołania. Biorąc pod uwagę wskazany termin wejścia ustawy w życie tj. 21 grudnia 2020 r. rozumiemy, że dotyczy on SOC działających w ramach struktury wewnętrznej OUK. Nie jest jednak jasne w jakim terminie należy powołać SOC zewnętrzny jeżeli OUK zdecyduje się na podpisanie umowy z innym podmiotem. Tym samy koniecznym jest doprecyzowanie i wyjaśnienie jaki jest termin na powołanie SOC oraz jaki jest termin na podpisanie umowy z zewnętrznym SOC. Dodatkowo, z uwagi na brak ustalonego trybu komunikacji z organem właściwym ds. Cyberbezpieczeństwa tj. z Ministrem Cyfryzacji należy określić w jaki sposób OUK ma dokonać zgłoszenia takiej umowy do Ministerstwa cyfryzacji. | **Uwaga nieuwzględniona**  Zespoły SOC są doprecyzowaniem aktualnie funkcjonującym „wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo” oraz zastępuje określenie „podmioty świadczące usługi na rzecz cyberbezpieczeństwa”. |
|  | Transition Software | Art.14 ust. 5 pkt 3 | Przestawić miejscami słowa „przechowywanych” i „danych”. Zdanie powinno mieć docelowe brzmienie: „minimalizację danych przechowywanych poza bezpiecznym środowiskiem”. | **Uwaga nieuwzględniona**  Szyk zdania jest właściwy. |
|  | Krajowy Depozyt Papierów Wartościowych | Art. 14 ust. 6 | Zgodnie z propozycją treści ust. 6 *„Podmiot niebędący operatorem usługi kluczowej, prowadzący SOC udostępnia na swojej stronie internetowej co najmniej następujące informacje na temat swojej działalności…”* W naszej opinii niniejszy przepis powinien brać pod uwagę również sytuację często spotykaną w grupach kapitałowych, w których dany podmiot świadczy określone usługi, np. informatyczne czy w zakresie cyberbezpieczeństwa, ale wyłącznie na potrzeby podmiotów należących do tej grupy kapitałowej. Taki podmiot, sam niebędący operatorem usługi kluczowej, ale świadczący usługi operatorowi wchodzącemu w skład grupy kapitałowej, nie zamierza ani nie jest przygotowany do tego, aby świadczyć takie usługi szerokiemu odbiorcy, co uzasadniałoby potrzebę udostępniania na stronie internetowej informacji na temat jego działalności jako SOC. Zaistniała sytuacja, w której podmiot ten świadczy usługi SOC, wynika wyłącznie ze sposobu zorganizowania procesów wewnętrznych w ramach powiązanych kapitałowo podmiotów, które organizacyjnie stanowią wspólną całość (a SOC działa wyłącznie wewnątrz tej całości, której integralną częścią jest operator usługi kluczowej). Naszym zdaniem w takim przypadku obowiązek publikowania na stronie internetowej informacji na temat działalności SOC nie powinien mieć zastosowania. | **Uwaga nieuwzględniona**  W tym zakresie ustawa nawiązuje do praktyki rynkowej – udostępniania informacji według dokumentu RFC2350. |
|  | Fundacja Bezpieczna Cyberprzestrzeń | Art. 14 ust. 6 | proponuje się pozostawienie obecnego wymogu dla podmiotu świadczącego usługi z zakresu cyberbezpieczeństwa, jakim jest publikacja RFC2350. Publikacja RFC2350 była wymogiem w akcie wykonawczym do zmienianej ustawy i w większości przypadków został on zrealizowany, ponadto RFC2350 stanowi uznany standard w społeczności zespołów reagowania na incydenty komputerowe i warto ten standard utrzymać, nie nakładając na te podmioty dodatkowych obciążeń związanych z publikacją odmiennego zakresu informacji lub tych samych informacji w różnych formach. Trudno o wyjaśnienie i wskazanie uzasadnienia czemu SOC-i mają publikować informacje takie jak np. wymagana w pkt 2 lit. c polityka komunikacji i uwierzytelnienia informacji. Rozsądnym wydaje się powrót do obecnie obowiązującego wymogu publikacji dokumentu RFC2350 | **Wyjaśnienie**  W tym zakresie ustawa nawiązuje do praktyki rynkowej – udostępniania informacji według dokumentu RFC2350. |
|  | Polskie Centrum Badań i Certyfikacji | Art. 14 ust. 6 | Proponujemy zmienić zapisy art. 14 ust. 6 KSC na następujące:  „6. Podmiot niebędący operatorem usługi kluczowej, prowadzący SOC udostępnia na swojej stronie internetowej co najmniej następujące informacje na temat swojej działalności:   1. nazwa SOC; 2. dane kontaktowe, w tym: 3. adres ze wskazaniem strefy czasowej, 4. numer telefonu, adres poczty elektronicznej oraz wskazanie innych dostępnych środków komunikacji z SOC.   **Komentarz** **(uzasadnienie) do art. 14 ust. 6 nowelizacji KSC**  W uzasadnieniu poszczególnych przepisów materialnych, ustawodawca wskazuje, iż cyt.:*„Nawiązując do praktyki obecnej na rynku podmioty trzecie świadczące funkcje SOC udostępniają na stronie internetowej podstawowej informacje o swojej działalności.”.*  Konsekwencją powyższego, jest zaproponowanie regulacji art. 14 ust. 6 KSC, w którym ustawodawca wymienia elementy jakie SOC winien udostępnić na swojej stronie internetowej, przy czym w części „uzasadnienie poszczególnych przepisów materialnych” nie wyjaśnia przesłanek, którymi kierował się formułując wyszczególniony w niniejszym przepisie katalog. W opinii komentatora katalog ten jest nieprecyzyjny i zbyt szeroki. Dla przykładu – w projektowanym art. 14 ust. 6 pkt 2 lit. b i lit. c oraz pkt 3 ustawodawca wskazuje następująco:  Podmiot niebędący operatorem usługi kluczowej, prowadzący SOC udostępnia na swojej stronie internetowej posiadane przez siebie kompetencje (art. 14 ust. 6 pkt 1 KSC), zasady współpracy i wymiany informacji (art. 14 ust. 6 pkt 2 lit. b KSC), politykę komunikacji i uwierzytelniania informacji (art. 14 ust. 6 pkt 2 lit. c KSC), oferowane usługi, w tym politykę obsługi incydentów i koordynacji incydentów (art. 14 ust. 6 pkt 3 KSC) oraz (art. 14 ust. 6 pkt 4 lit. c i lit. d KSC). Ujawnienie w/w zakresu informacji nie odpowiada zasadom cyberbezpieczeństwa, gdyż ujawnia zastosowane zabezpieczenia, metody szyfrowania, metodologię pracy, środki techniczne i organizacyjne w podmiotach obsługiwanych przez SOC, oraz nie odpowiada zasadom konkurencyjności wolnego rynku, a wręcz ujawnia tajemnicę przedsiębiorstwa oraz zastosowane know-how. Przedstawienie w/w informacji pozwala zidentyfikować słabe punkty zabezpieczeń oraz ich metod zastosowanych przez SOC względem operatorów usług kluczowych, których *de facto i de iure* ma chronić i zabezpieczać. Dostęp cyberprzestępców do wiadomości o stosowanych metodach zabezpieczeń jest niczym nieskrępowany i pozwalający już od razu przejść do poszukiwanie sposobów ich przełamania, zamiast ewentualnej początkowo identyfikacji technologii, a następnie poszukiwania sposobów jej obejścia.  Powyższe elementy winny pozostawać tajemnicą SOC działającego wewnątrz struktury operatora usługi kluczowej lub tajemnicą przedsiębiorstwa działającego w ramach SOC, w tym umowy z operatorem usługi kluczowej na rzecz którego świadczona jest usługa, ewentualnie pozostawać podawane do wiadomości podczas kontroli dokonywanej przez organ nadzorczy – organ właściwy do spraw cyberbezpieczeństwa. Ograniczony dostęp do w/w informacji jest uzasadniony tym bardziej, że wskazuje się w „uzasadnieniu poszczególnych przepisów materialnych”:  *„Do wykazu* [od komentatora: prowadzonego przez ministra właściwego do spraw informatyzacji] *mogą być wpisane SOC, które nie są częścią krajowego systemu cyberbezpieczeństwa, a zajmują się reagowaniem na incydenty, ich zapobieganiem, zarządzaniem jakością zabezpieczeń jak również aktualizowaniem ryzyk.”.*  Cytowany fragment, jak i przepisy nowelizacji KSC, wskazują wyraźnie na dopuszczenie podmiotów wolnorynkowych do krajowego systemu cyberbezpieczeństwa, w związku z czym również ze względów tajemnicy przedsiębiorstwa w zakresie dotyczącym ich metodologii pracy, umiejętności, zasobów kadry pracowniczej, elementy o których mowa w art. 14 ust. 1, ust. 6 pkt 2 lit. b i lit. c, pkt 3 oraz pkt 4 lit. c i lit. KSC nie mogą być powszechnie dostępne. Powszechna, łatwo dostępna wiedza w zakresie wskazanymi przepisami pozwoli kopiować stosowane metody, „podkupować” kadrę pracowniczą (tj. dopuszczać się czynów nieuczciwej konkurencji), a tym samym dopuszczać do rynku podmioty nieodpowiednio przygotowane do pełnienia funkcji SOC, których eliminacja przez operatora usługi kluczowej na etapie wyboru kontrahenta będzie de facto niemożliwa. Wpłynie to negatywnie na podmiot i sam sektor mający być rzekomo poddany ochronie przepisami KSC. | **Wyjaśnienie**  W tym zakresie ustawa nawiązuje do praktyki rynkowej – udostępniania informacji według dokumentu RFC2350. |
|  | Transition Software | Art.14 ust.7, pkt 2), Art. 26, ust. 3, pkt 9) | Bezpieczeństwo osobowe osób pracujących/świadczących usługi w podmiotach SOC/CSIRT obsługujących podmioty infrastruktury krytycznej powinno być zweryfikowane i potwierdzone przez odpowiednie służby przed faktycznym rozpoczęciem świadczenia przez nich obowiązków pracy/usług w SOC/CSIRT. Zaleca się przeprowadzenie przynajmniej postępowania podstawowego wobec każdej osoby rozpoczynającej świadczenie obowiązków. Również z uwagi na potencjalną klauzulę informacji stanowiących tajemnicę przedsiębiorstwa (tj. może się zdarzyć, że informacja stanowiąca tajemnicę danego przedsiębiorstwa będzie jednocześnie oklauzulowana jako niejawna). Personel SOC/CSIRT musi być wcześniej zweryfikowany i przygotowany na taką okoliczność, tj. posiadać poświadczenie bezpieczeństwa osobowego przynajmniej równe klauzulą, jaki mogą posiadać potencjalne otrzymywane dane.  Przy uwzględnieniu outsourcingu również należy sprawdzić - przez dedykowane służby – bezpieczeństwo osobowe personelu, który będzie miał wykonywać powierzone prace. Przed rozpoczęciem świadczenia obowiązków, musi on posiadać aktualne poświadczenie bezpieczeństwa, o stopniu przynajmniej równym do klauzuli potencjalnych otrzymywanych informacji niejawnych.  Powinien zostać zachowany bezpieczny łańcuch dostaw sprzętu i oprogramowania dla SOC/CSIRT, w obszarze ICT (PC, data center, storage, laptopy, telefony i inne urządzenia mobilne).  Jeżeli weryfikacja pod kątem bezpieczeństwa każdego egzemplarza sprzętu wykorzystywanego przez SOC/CSIRT nie jest to możliwa - np. z powodów logistycznych, w kontekście skali i ilości podmiotów – to dedykowane służby (np. trzy główne CSIRT: MON, GOV, NASK) we współpracy powinny przekazać wytyczne/standardy (np. w sposób niepubliczny, wyłącznie do wskazanych podmiotów), jakie musi spełniać sprzęt i oprogramowanie wykorzystywane w SOC/CSIRT i sposoby ich konfiguracji/zabezpieczenia. Wdrożenie i stosowanie tych wytycznych musi podlegać okresowemu audytowi przez ww. główne CSIRTy lub ich podwykonawców, związanych odpowiednimi umowami poufnościowymi.  Powinno to być wprowadzone w ramach wdrażania Narodowych Standardów Cyberbezpieczeństwa, wzmiankowanych w *Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024* (Uchwała nr 125 Rady Ministrów z dn. 22 października 2019r.) | **Wyjaśnienie**  O dostępie do informacji wrażliwych np. tajemnicy przedsiębiorstwa decyduje dany przedsiębiorca. |
|  | ISSA Polska | Art. 14a pkt 7 | Proponujemy dla projektowanego artkułu „14a.” w zakresie punku 7. o treści: „7. Minister właściwy do spraw informatyzacji może na wniosek zainteresowanego przedsiębiorcy lub z urzędu, wpisać do wykazu, o którym mowa w ust. 1, SOC inny …” | **Uwaga nieuwzględniona**  Dotychczasowa redakcja jest poprawna. |
|  |  |  | Przyjęta w art. 14a ust. 7 konstrukcja wpisania przez ministra danego SOC z urzędu budzi wątpliwości. Czy przesłanki wskazane w ust. 2 mają być spełnione łącznie? Prośba o uzasadnienie wymagania dotyczącego przedstawienia dokumentu potwierdzające zdolność do ochrony informacji niejawnych przez ten podmiot – w odniesieniu do SOC-ów takiego wymagania (słusznie!) nie zdefiniowano. | **Wyjaśnienie**  Przesłanki mają być spełnione łącznie. Chodzi o możliwość dodania do KSC takiego SOC, który nie świadczy usług na rzecz operatora usługi kluczowej. |
|  | Fundacja Bezpieczna Cyberprzestrzeń | Art. 14a | Nie jest jasny cel w jakim został wprowadzony. Po pierwsze informacja o SOC, z którymi OUK zawarł umowę jest przekazywana przez OUK organowi właściwemu, nie jest zatem konieczne tworzenie kolejnych obciążeń administracyjnych w postaci wnioskowanie o ujęcie w wykazie (art. 14a ust. 3), wystarczającym wydaje się przekazanie tej informacji ministrowi właściwemu do spraw informatyzacji. Po drugie, nie jest jasny cel wpisywania SOC „z urzędu” oraz czy ten przepis dotyczy SOC, z którymi OUK zawarł umowę czy SOC powołany wewnątrz swojej struktury. Po trzecie przepis w ust. 7 pkt 1 tworzy kolejny zestaw usług dla SOC z niecodzienną usługą „aktualizowania ryzyk w przypadku zmiany struktury organizacyjnej, procesów i technologii, które mogą wpływać na reakcję na incydent”, a w pkt. 2 wymóg, który nie ma zastosowania do innych SOC-ów niż wpisywane z urzędu, przy czym wyraźnie należy zaznaczyć, że zdolność do ochrony informacji niejawnych zgodnie z ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych jest wymogiem nadmiarowym i nieuzasadnionym, gdyż taka zdolność powinna wynikać z faktu lub przewidywanego przetwarzania informacji niejawnych. | **Wyjaśnienie**  Przepis jest niezbędny, aby minister właściwy do spraw informatyzacji mógł wypełniać swoje uprawnienia nadzorcze wobec SOC. |
|  | Home.pl | Art. 14  Art. 14a | Do krajowego systemu cyberbezpieczeństwa planuje się wprowadzić pojęcie operacyjnych centrów bezpieczeństwa, zwane dalej: ,,SOC” (Security operations center). Zastąpią one dotychczasowe struktury odpowiedzialne za cyberbezpieczeństwo operatora usług kluczowych. Do tej pory operator usługi kluczowej mógł powołać wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo lub zawierał umowę z podmiotem świadczącym usługi z zakresu cyberbezpieczeństwa (art. 14). Po nowelizacji operator usługi kluczowej może powołać SOC wewnątrz swojej struktury lub zawrzeć umowę prowadzenia SOC z innym podmiotem. Minister właściwy do spraw informatyzacji będzie prowadził wykaz, do którego będą wpisywane podmioty SOC (art. 14a). Dotychczasowe centra SOC w ocenie ustawodawcy posiadają ugruntowaną na rynku pozycję struktur realizujących wszystkie funkcje związane z monitorowaniem i zarządzaniem cyberbezpieczeństwem, zarówno w strukturze wewnętrznej, jak i usług świadczonych na rzecz innych jednostek.    **Uwagi w ramach konsultacji:**  - do art. 14a ust. 3: w sposób nieprecyzyjny wskazują, czy każdy SOC będzie musiał zostać ujęty w wykazie SOC, czy tylko te SOC, które w ramach outsourcingu świadczą usługi na rzecz operatora usługi kluczowej – należy w trybie konsultacji publicznych zwrócić się o korektę przepisów precyzującą tę kwestię  - do art. 14 ust. 1-3: zmiany dot. wymogów związanych z wdrożeniem SOC. Jeżeli wdrożenie zmian będzie się wiązało z istotnymi kosztami dla OUK, należy rozważyć zgłoszenie w trybie konsultacji publicznych postulatu zawarcia w ustawie nowelizującej przepisów dot. rekompensat dla operatorów usługi kluczowej, bądź zmianę przepisów umożliwiającą redukcję kosztów wdrożenia zmian. | **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.  Definicja SOC odnosi się do wieloletniej praktyki rynkowej, a skrót jest powszechnie rozpoznawalny.  Wskazany 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.  Operator usługi kluczowej może zawrzeć umowę z kilkoma podmiotami realizujących inne zadania o których mowa w art. 14 ust.1. |
|  | ISSA Polska | Art. 14a ust 7 | Proponujemy dla projektowanego artkułu „14a.” w zakresie ustępu 7. dodać punkt 4) „złożyć oświadczenie w zakresie spełniania warunków technicznych określonych w rozporządzeniu Ministra właściwego do spraw informatyzacji” | **Uwaga nieuwzględniona**  W związku z całkowitym nowym brzmieniem nie będzie już obowiązywało rozporządzenie z art. 14 ksc |
|  | Politechnika Wrocławska. Wrocławskie Centrum Sieciowo-Superkomputerowe | Art. 14a ust. 7 | Zawarta w Projekcie zmiana w **pkt. 11)** wprowadzająca **art. 14a ust. 7** do Ustawy o KSC, stawia warunek na uzyskanie przez SOC dostępu do systemu teleinformatycznego, o którym mowa w art. 46 Ustawy o KSC, w postaci dokonania wpisu przez Ministra właściwego do spraw informatyzacji do wykazu SOC. Z kolei dokonanie wpisu do ww. wykazu dla SOC innego niż określony w art. 14a ust. 3, warunkowane jest m.in. przez **art. 14a ust. 7 pkt. 2**, zgodnie z którym SOC:  *„2) przedstawi dokument potwierdzający 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) oraz; „*  Zapis ten nie precyzuje o jakiej klauzuli tajności informacji niejawnych jest mowa (zastrzeżone, poufne, tajne, ściśle tajne). Równocześnie, ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych w art. 54. [Zdolność do ochrony informacji niejawnych] mówi o przeprowadzeniu audytu przemysłowego w podmiocie, nie części podmiotu, jaką stanowiłby SOC działający w strukturach Uczelni. Jeżeli Uczelnia posiada kancelarię tajną uprawnioną do przetwarzania informacji niejawnych o klauzuli tajności „zastrzeżone”, to zgodnie z art. 54 ust. 9 oraz art. 55 ust. 1 nie posiada świadectwa bezpieczeństwa, gdyż dla tej klauzuli tajności takowe nie jest przez ABW wydawane. Skoro w omawianym **art. 14a ust. 7 pkt. 2**. dokument jest wymagany, wydaje się, że oznaczałoby to konieczność wydania Uczelni przez ABW świadectwa o zdolności do ochrony informacji niejawnych o klauzuli tajności „poufne” lub wyższej. Nie jest jasne czy taka była intencja autora omawianego punktu. Proponuje się doprecyzowanie zapisu w odniesieniu do charakteru wymaganego dokumentu i/lub dopuszczenie przedstawiania przez SOC poświadczeń bezpieczeństwa osób stanowiących jego personel. | **Wyjaśnienie**  Przepis ten dotyczy SOC znajdujących się poza krajowym systemem cyberbezpieczeństwa, które mogą być włączone w jego skład. |
|  | SayF | Art. 14a ust 10 | Proponujemy odwołać się do artykułów w ustawach dotyczących konkretnej służby., np. art. 20c ust 2 ustawy o policji, art. 10b ust 2 ustawy o służbie granicznej, art. 30 ust 2 ustawy o żandarmerii wojskowej itd. | **Uwaga nieuwzględniona**  Przepis opiera się o dotychczasową sprawdzoną praktykę z art. 7 ust.8. |
|  | Santander | Strona 8 pkt. 10 | Określenie „*niezbędnym*” jest mało precyzyjne i rodzi ryzyko nadużyć. Adresy, gdzie prowadzony jest SOC powinny być ściśle strzeżone, gdyż mają wpływ na bezpieczeństwo tych podmiotów jak również całego rynku, w naszym przypadku finansowego, oraz Państwa. Przykładowo nie widać silnego uzasadnienia dostępu dla KAS. | **Uwaga nieuwzględniona**  Przepis opiera się o dotychczasową sprawdzoną praktykę z art. 7 ust.8. |
|  | Transition Software | Art. 15, ust. 2, pkt 3 | Należy rozważyć, czy CSIRT sektorowy lub podsektorowy powinien w interwale 2 letnim, audytować system, który sam zabezpiecza i/lub nadzoruje, jako jednostka cyberbezpieczeństwa dedykowana do ochrony danego sektora/podsektora?  Czy nie powinna raz na dwa lata tego jednak robić jednostka nadrzędna, adekwatny do obszaru jeden z trzech głównych CSIRTów (NASK, GOV, MIL), NIK, lub jednostka akredytowana, o której mowa w tym samym art. w ust. 2 pkt 1)? | **Uwaga nieuwzględniona**  Uwaga nie jest do projektu nowelizacji. |
|  | Transition Software | Art. 15, ust. 2, pkt 3 | Rozporządzenie Ministra Cyfryzacji z dn. 12 października 2018r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu powinno również zawierać punkt wymieniający poświadczenie bezpieczeństwa osobowego o klauzuli nie niższej niż audytowany system.  Ww. punkt miałby zastosowanie wszędzie tam, gdzie system świadczący usługę kluczową przetwarza również informacje niejawne. Potencjalnie taka sytuacja może mieć miejsce (np. w MON, w służbach, etc.).  Częściowo jest to wzmiankowane w pkt.4) tego samego ustępu, jednak jest to ujęte w kontekście nie ujawniania wyników audytu, a nie w kontekście spełniania wymogów do jego przeprowadzenia. | **Uwaga nieuwzględniona**  Uwaga nie jest do projektu nowelizacji. |
|  | SayF | Art. 15 ust 4  Art. 37 ust 4  Art. 40 ust 3 | W naszej ocenie zapis jest niepotrzebny. Kwestie zachowania określonych informacji w tajemnicy regulują odrębne ustawie np. ustawa o ochronie informacji niejawnych, ustawa o ochronie danych osobowych, ustawa o zwalczaniu nieuczciwej konkurencji itd. | **Uwaga nieuwzględniona**  Uwaga nie jest do projektu nowelizacji. |
|  | Transition Software | Art. 15 ust. 6 | Czy należy to rozumieć tak, że w przypadku posiadania przez danego operatora kluczowego zespołu audytorów wewnętrznych i przeprowadzania przez niego okresowego (co 2 lata) audytu wewnętrznego własnymi siłami, nie jest on zobowiązany do przechodzenia - w zasadzie nigdy w takim razie – jakichkolwiek audytów zewnętrznych, tj. przez jakąkolwiek jednostkę nadrzędną/nadzorującą, lub akredytowaną jednostkę uprawnioną do wykonywania tego typu audytów? | **Uwaga nieuwzględniona**  Uwaga nie jest do projektu nowelizacji. |
|  | Transition Software | Art. 15, ust. 7 | Jest tu jasno opisane, że kopia raportu jest przedstawiana wymienionym trzem podmiotom, na ich wyraźny i uzasadniony wniosek.  Należy rozważyć wprowadzenie obligatoryjnego przesyłania co 2 lata kopii tego raportu bezpiecznym kanałem do wskazanych odbiorców oraz – ew. – NIK?  Wtedy istniałaby możliwość jakiejś, wyrywkowej nawet, okresowej weryfikacji poszczególnych raportów lub zbioru raportów, co powinno dać możliwość uzyskania jakiegoś zbiorczego obrazu sytuacji, choćby bardzo zgrubnego.  Może zaistnieć sytuacja, że nawet przez kilka kolejnych interwałów żaden z wymienionych podmiotów nie zwróci się ze wspomnianym uzasadnionym wnioskiem odnośnie raportów np. danych konkretnych organizacji (banków, energetyki, administracji, produkcji, w tym produkcji specjalnej, etc.) i kolejne audyty – przeprowadzane przez operatorów kluczowych własnymi siłami, w ramach struktury własnej organizacji i na własnym obszarze – nie będą w żaden sposób weryfikowane przez instytucje nadrzędne/wyznaczone, etc. | **Uwaga nieuwzględniona**  Uwaga nie jest do projektu nowelizacji. |
|  | SayF | Art. 17 ust 1 | Dlaczego wyklucza się mikro i małych przedsiębiorców? | **Uwaga nieuwzględniona**  Uwaga nie jest do projektu nowelizacji. |
|  | Związek Pracodawców Mediów Elektronicznych i Telekomunikacji MEDIAKOM  Reprezentowany przez adw. Annę Gąsecką | art. 39 PKE i art. 20a ustawy o krajowym systemie cyberbezpieczeństwa,  art.43 ust. 2 i 3 PKE i art. 20e ustawy o krajowym systemie cyberbezpieczeństwa  art. 44 ust.1 PKE i art. 20f ustawy o krajowym systemie cyberbezpieczeństwa | Niejasny jest stosunek projektowanych przepisów do zapisów projektu Prawa Komunikacji Elektronicznej (dalej PKE). Oba akty regulują tę samą materię, a część projektowanych przepisów jest tożsama. | **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 przez ustawę wprowadzającą PKE.  Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowym.  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.  Dlatego potrzebne jest przeniesienie odpowiednich definicji z PKE do ustawy KSC. |
|  | PIIT | Art. 20a | **Art. 20a, art. 2 pkt 8f, 8g**  Proponowany przepis stanowi kopię projektowanego art. 39 ustawy PKE. Aktualne są więc uwagi przedstawione w tym zakresie do projektu PKE, w szczególności w zakresie upoważnienia ustawowego do wydania rozporządzenia dot. warunków technicznych i organizacyjnych, w tym wyjaśnienia statusu obowiązującego rozporządzenia do art. 175d PT, którego moc obowiązująca nie jest w projekcie PKE utrzymywana. Jedyna zmiana art. 20a to dodanie odwołań niezbędnych, aby wprowadzić ten przepis do ustawy KSC.  Jednocześnie zupełnie niezrozumiała jest intencja powtarzania tego samego przepisu w dwóch projektowanych aktach prawnych, a tym bardziej utrzymywanie dwóch podstaw prawnych do wydania rozporządzenia w potencjalnie tym samym zakresie.  **Postulaty:**  W zakresie art. 20a należy:   * Wykreślić przepis z projektu ustawy nowelizującej KSC i zachować go w PKE ze zmianami zaadresowanymi w stanowisku PIIT przekazanym w konsultacjach projektu PKE. * W przypadku zamiaru dodatkowego podkreślenia potrzeby uwzględniania incydentów w rozumieniu KSC, tj. incydentów cyberbezpieczeństwa można podkreślić ten aspekt w projekcie PKE. * Wykreślić z KSC związane z art. 20a definicje, które miałyby być dodane w art. 2 pkt 8f-g, czyli definicje bezpieczeństwa sieci i usług oraz sytuacji szczególnego zagrożenia. W przypadku braku usunięcia ww. definicji z projektu KSC definicję bezpieczeństwa sieci i usług (8f) należy zapisać tak jak definicję sytuacji szczególnego zagrożenia (8g) tj. przez odwołanie do definicji PKE. * W zakresie brzmienia definicji bezpieczeństwa sieci i usług ponawiamy uwagę przedstawioną w tym zakresie do stanowiska do PKE, tj. jej niespójności z EKŁE:   *Definicja bezpieczeństwa sieci i usług w projekcie PKE różni się od definicji wskazanej w EKŁE*  Definicja z PKE:  *„bezpieczeństwo sieci i usług – zdolność sieci telekomunikacyjnych lub usług komunikacji elektronicznej do odpierania wszelkich działań naruszających dostępność, autentyczność, integralność lub poufność:*  *a) tych sieci lub usług,*  *b) przetwarzanych danych i treści objętych tajemnicą komunikacji elektronicznej,*  *c) innych świadczonych przez przedsiębiorcę komunikacji elektronicznej usług związanych z usługami komunikacji elektronicznej lub sieciami telekomunikacyjnymi tego przedsiębiorcy”*  Definicja z EKŁE  „*bezpieczeństwo sieci i usług” oznacza zdolność sieci i**usług łączności elektronicznej do odpierania,* ***na danym poziomie pewności****, wszelkich działań naruszających dostępność, autentyczność, integralność lub poufność tych sieci i usług, przechowywanych, przekazywanych lub przetwarzanych danych lub związanych z nimi usług oferowanych przez te sieci lub usługi łączności elektronicznej lub dostępnych za ich pośrednictwem*;  Prośba o wskazanie argumentacji leżącej u podstaw pominięcia w definicji określenia „na danym poziomie pewności”. Naszym zdaniem wskazanie przez europejskiego prawodawcę w ww. definicji określenia jest celowe i koresponduje z koncepcją dostosowania zabezpieczeń do wyników analizy ryzyka – motyw 94 „Środki te powinny zapewniać poziom bezpieczeństwa sieci i usług proporcjonalny do istniejącego ryzyka z uwzględnieniem aktualnego stanu wiedzy i technologii”. Kategoryczne sformułowanie zdolności do odpierania wszelkich działań oznaczałoby de facto obowiązek zapewnienia 100% odporności. Taki poziom wydaje się nierealny do osiągnięcia nie tylko dla operatorów telekomunikacyjnych, ale i nawet dla najbardziej zabezpieczonych systemów służb  i organów państwowych. Stąd niezbędne jest doprecyzowanie zgodne z EKŁE | **Uwaga nieuwzględniona**  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 przez ustawę wprowadzającą PKE.  Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowym.  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.  Dlatego potrzebne jest przeniesienie odpowiednich definicji z PKE do ustawy KSC. |
|  | PIIT | Art. 20b-d | * 1. **Art. 20b-d, art. 2 pkt 8a**   Proponowane przepisy art. 20b-d wraz ze związanymi z nimi definicjami: incydentu telekomunikacyjnego i CSIRT Telco stanowią znaczącą modyfikację dotychczasowego sposobu działania przedsiębiorców telekomunikacyjnych w zakresie obsługi incydentów, w tym w zakresie incydentów cyberbezpieczeństwa.  Zgodnie z obowiązującym prawem telekomunikacyjnym, system, który miał być przeniesiony również na grunt PKE jest następujący. Przedsiębiorca, zgodnie z art. 175a ma obowiązek niezwłocznego poinformowania Prezesa UKE o naruszeniu bezpieczeństwa lub integralności, podjętych działaniach zapobiegawczych i środkach naprawczych oraz innych działaniach w tym zakresie. W części IV.4 obowiązującego formularza raportowego przedsiębiorca określa przyczynę zaistniałego naruszenia, przy czym jedną z opcji jest wskazanie, że przyczyną był cyberatak. Jeśli natomiast zdarzenie miało charakter incydentu w rozumieniu KSC, tj. incydentu w zakresie cyberbezpieczeństwa wówczas Prezes UKE przekazywał informację właściwemu CSIRT. Prezes UKE jest też uprawniony do korzystania z systemu teleinformatycznego tworzonego na potrzeby krajowego systemu cyberbezpieczeństwa, o którym mowa w art. 46 KSC. Jednocześnie określone w rozporządzeniu progi są uniwersalne i odnoszą się de facto do ciągłości działania usługi (czasu niedostępności) w relacji do zakresu objętych użytkowników. Tym samym aktualny stan prawny, jak i ten, który miał zostać wprowadzony w projekcie PKE zapewniają, że po pierwsze naruszenia/incydenty związane z cyberprzestrzenią będą raportowane, a po drugie informacja ta zostanie przekazana właściwym CSIRT. W projektowanym art. 45 ust. 3 PKE przewidziano również możliwość zwrócenia się przez UKE o pomoc do właściwego CSIRT, co implementuje w pełni art. 41 ust. 4 EKŁE.  Należy więc wskazać, że pod kątem pełnej zgodności z przepisami unijnymi oraz z uwagi na wieloletnią już i zasadniczo bezproblemową praktykę raportowania za pożądane rozwiązanie należy uznać utrzymanie istniejącego rozdziału między regulacją właściwą przedsiębiorcom telekomunikacyjnym/komunikacji elektronicznej i ich relacji z UKE, a regulacjami właściwymi dla krajowego systemu cyberbezpieczeństwa w jego dotychczasowym zakresie. Szczególnie biorąc pod uwagę bardzo bliskie terminy wejścia w życie projektowanych obecnie przepisów oraz skalę wątpliwości i praktycznych problemów, jakie mogą wyniknąć z nakładania się na siebie obowiązków.  W tym miejscu **należy spróbować zrekonstruować podstawowe elementy docelowego stanu prawnego, jaki wystąpiłby po jednoczesnym wejściu w życie nowego PKE oraz zmian KSC**, które jak zakładamy zostałyby wprowadzone do ustawy wprowadzającej PKE. Poniższe porównanie jest również istotne dla przedstawienia różnic, szczególnie w zakresie definicji incydentu, dla scenariusza w którym obowiązki raportowe miałyby zostać przeniesione z UKE do CSIRT.  **[Tabela usunięta ze względu na brak miejsca – dostępna na stronie Rządowego Procesu Legislacyjnego – DC KPRM)**  **Podsumowując powyższe zestawienie odrębnych reżimów raportowych wyraźnie widoczne są istotne różnice na poziomie podstawowych definicji, zakresu objętych podmiotów, organów właściwych. Brak jest również aktów wykonawczych do realizacji nowych obowiązków,** o których mowa w projekcie ustawy KSC. Obowiązki wobec CSIRT Telco będą niemożliwe do realizacji w istotnym okresie obowiązywania przepisów, albowiem jego powołanie ma nastąpić dopiero w okresie 18 miesięcy od wejścia w życie ustawy. Nie przewidziano w tym zakresie odpowiednich regulacji intertemporalnych. Poza powyższym, należy wskazać, że przedsiębiorcy komunikacji elektronicznej nie będą mieli możliwości przygotowania się do realizacji nowych obowiązków raportowych, a w szczególności wdrożenia odpowiednich zmian organizacyjnych i technicznych pod kątem nowych (jeszcze nieznanych) progów incydentów.  **Postulaty:**   * **Art. 20b-d projektu KSC powinny zostać usunięte z projektu.**   Nie jest zasadne utrzymanie propozycji zakładającej dwa nakładające się reżimy zgłaszania incydentów bezpieczeństwa (PKE) i incydentów telekomunikacyjnych (KSC). Nie jest również zasadne przeniesienie przedsiębiorstw komunikacji elektronicznej pod reżim KSC.  Obowiązki raportowe przedsiębiorców komunikacji elektronicznej powinny zostać utrzymane jedynie wobec Prezesa UKE, a w każdym razie powinien istnieć wyłącznie jeden kanał zgłoszeń.   * **Definicja incydentu, jaki ma zgłaszać przedsiębiorca komunikacji elektronicznej musi być jedna, podobnie jak spójne muszą być kryteria dokonywania zgłoszeń** – nawet, jeśli miałyby dotyczyć szerokiego spektrum sytuacji. **Ewentualne dodatkowe potrzeby w zakresie incydentów w rozumieniu ustawy KSC można zaspokoić przez odpowiednie uzupełnienie ustawy PKE lub dostosowanie praktyki działania**. Jeśli podmioty krajowego systemu potrzebują szerszej informacji, także dot. samego przerwania ciągłości bez związku z przyczyną, nie widzimy istotnych przeszkód, aby takie informacje były przekazywane przez UKE do odpowiednich CSIRT. Możliwe wydaje się również, aby te informacje były dostępne w ramach budowanego systemu S46. Ewentualnie, w przypadkach, w których przedsiębiorca kwalifikuje incydent, jako wpływający na cyberbezpieczeństwo, mógłby zostać zobowiązany do przekazywania tej samej informacji zarówno do UKE jak i właściwego CSIRT krajowego. * Ponadto, w celu potwierdzenia możliwości komunikowania o zagrożeniach postulujemy wprowadzenie do projektu PKE przepisu art. 175c ust. 5 PT, który nie został przeniesiony do PKE, a który wskazuje *przedsiębiorca telekomunikacyjny może informować innych przedsiębiorców telekomunikacyjnych i podmioty zajmujące się bezpieczeństwem teleinformatycznym o zidentyfikowanych zagrożeniach, o których mowa w ust. 1. Informacja może zawierać dane niezbędne do identyfikacji oraz ograniczenia zagrożenia.* W nowym brzmieniu przepis powinien odnosić się do przedsiębiorstw komunikacji elektronicznej oraz do podmiotów krajowego systemu cyberbezpieczeństwa. * Niezależnie od przyjętego finalnie sposobu regulacji, kluczowe pozostaje, że konkretny **przedsiębiorca komunikacji elektronicznej może odpowiadać jedynie za bezpieczeństwo i integralność swoich usług i swojej infrastruktury**. Tym samym projektowane przepisy nie mogą ingerować w tą sferę skutkując nałożeniem na tych przedsiębiorców szerszych obowiązków. Byłaby to bardzo istotna ingerencja w konkurencyjny rynek rozwiązań bezpieczeństwa teleinformatycznego. | **Uwaga nieuwzględniona**  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 przez ustawę wprowadzającą PKE.  Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowym.  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. |
|  | Home.pl | Art. 20a-d | Nowelizacja nawiązuje w swej treści do nowej ustawy – Prawo komunikacji elektronicznej (dalej również jak PKE), która obecnie jest w fazie prac legislacyjnych, a docelowo ma wejść w życie 21 grudnia 2020 r. Prawo komunikacji elektronicznej ma zastąpić dotychczasową ustawę z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne. Wprowadzenie nowej ustawy wynika z konieczności wdrożenia do polskiego porządku prawnego przepisów Dyrektywy Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiającej Europejski kodeks łączności elektronicznej (dalej: Dyrektywa).    Ustawa o KSC posługuje się pojęciami zdefiniowanymi w PKE, w tym między innymi: pojęciem „przedsiębiorca komunikacji elektronicznej”, który jest w rozumieniu projektu ustawy prawo komunikacji elektronicznej - przedsiębiorcą telekomunikacyjnym lub podmiotem świadczącym usługę komunikacji interpersonalnej niewykorzystującą numerów. Ze względu na brak jasnej definicji pojęcia „komunikacji interpersonalnej niewykorzystującej numerów nie można mieć pewności, czy  podmiot będzie posiadać status przedsiębiorca komunikacji elektronicznej i w konsekwencji – czy będą do niego miały zastosowania przepisy PKE oraz nowelizacji dotyczące tej kategorii przedsiębiorców (nowy rozdział 4a „ Obowiązki przedsiębiorców komunikacji elektronicznej” wprowadzany do ustawy o KSC nowelizacją, przepisy o tzw. incydencie telekomunikacyjnym: nowy art. 2 pkt 8a ustawy o KSC itd.    **Uwagi w ramach konsultacji:**  - do nowego art. 20a ust. 1 ustawy o KSC: doprecyzowanie kto dokładnie jest adresatem nowelizacji w zakresie dot. przedsiębiorcy komunikacji elektronicznej. | **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 przez ustawę wprowadzającą PKE.  Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowym.  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.  Dlatego potrzebne jest przeniesienie odpowiednich definicji z PKE do ustawy KSC. |
|  | PIIT | Art. 20c | * 1. Art. 20c ust. 4 wprowadza upoważnienie do wydania rozporządzenia określające progi, które jest identyczne z tym przewidzianym w art. 42 ust. 2 PKE.   Uwagi w zakresie braku zrozumienia dla takiego zabiegu legislacyjnego zostały sformułowane już powyżej. Dodatkowo aktualne są poniższe uwagi przedstawione w stanowisku przekazanym do projektu PKE:  W proponowanym przepisie znacznemu rozbudowaniu uległ katalog przesłanek, jakie będą brane pod uwagę przy określaniu progów istotności incydentów. W pierwszej kolejności, tak jak w uwagach ogólnych wskazujemy, że do czasu przedstawienia projektu rozporządzenia lub chociaż jego założeń nie jest możliwe dokonanie oceny wpływu zmiany upoważnienia ustawowego na działalność przedsiębiorców. Tym samym postulujemy pilne przedstawienie, przynajmniej jego założeń.  Postulujemy, aby doprecyzować art. 42 ust. 2 pkt 1 lit. e, że progi mogą zostać ustalone dla „sieci telekomunikacyjnych” oraz „usług komunikacji elektronicznej”. Obecnie wskazano jedynie na „sieci i usługi”, co wydaje się niewystarczająco precyzyjne.  Poza tym, katalog ten został określony w sposób zmodyfikowany wobec zapisów EKŁE, w szczególności poprzez nieuwzględnienie wskazanej w EKŁE przesłanki „wpływu na działalność ekonomiczną i społeczną”.  W to miejsce wprowadzono szeroki katalog okoliczności tj.:   * 1. *wpływ incydentu bezpieczeństwa na zachowanie tajemnicy komunikacji elektronicznej,*   2. *wpływ incydentu bezpieczeństwa na świadczenie usług kluczowych w rozumieniu ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa oraz funkcjonowanie infrastruktury krytycznej w rozumieniu ustawy  z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym,*   3. *wpływ incydentu bezpieczeństwa na połączenia do numerów alarmowych,*   4. *wpływ incydentu bezpieczeństwa na wykonywanie obowiązków, o których mowa w art. 46-56 ustawy;*   Przede wszystkim postulujemy usunięcie lit. f odnoszącej się do wpływu na usługi kluczowe oraz infrastrukturę krytyczną. W przypadku gdyby w rozporządzeniu określono odrębne progi odnoszące się wyłącznie do tego zakresu, wykonanie obowiązku zgłoszenia mogłoby być niemożliwe. Z perspektywy operatora obowiązanego do dokonania zgłoszenia trudne do ustalenia byłoby bowiem czy dany incydent miał wpływ na usługi kluczowe (lista takich operatorów nie jest jawna) tudzież infrastrukturę krytyczną (lista obiektów jest zastrzeżona). Ewentualne zgłoszenie incydentu mającego wpływ w tym zakresie byłoby faktycznie możliwe jedynie w przypadku, gdy operator posiada wiedzę w zakresie takiego wpływu lub sam jest operatorem usługi kluczowej lub posiadaczem infrastruktury krytycznej.  W zakresie lit. g) podobnie jak w ramach pre-konsultacji projektu PKE postulujemy następujące doprecyzowanie:  *g) wpływ incydentu na funkcjonowanie systemów alarmowania, powiadamiania ratunkowego, numery alarmowe ustawowo powołane do niesienia pomocy 997, 998, 998 i numer 112*  Odnośnie lit. h) tj. odniesienia do wykonywania obowiązków, o których mowa w art. 45-56 sygnalizujemy, że daleko idące wątpliwości budzi zasadność wprowadzenia tej przesłanki. Przepisy, do których się odwołano to np. obowiązki Prezesa UKE (45-46), posiadanie planu (47), nakładania dodatkowych obowiązków (48), radioamatorów (49), zawieszania obowiązków przez Prezesa UKE (52), upoważnienia do wydania rozporządzenia (54), czy zakresu obowiązków retencyjnych (56). W naszej ocenie lit. h) powinna zostać usunięta z projektu ustawy.  **Postulat:**   * Art. 20c należy usunąć z projektu i przenieść dyskusję na jego temat na okres po implementacji 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 przez ustawę wprowadzającą PKE.  Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowym.  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. |
|  | PIIT | Art. 20d | * 1. Zgodnie z ust. 3-5 przedsiębiorca miałby przekazywać CSIRT, w tym CSIRT Telco informacje stanowiące prawnie chronione.   Podobne przepisy zawarto w projekcie PKE w art. 42 ust. 8, które budziły nasze istotne wątpliwości w przypadku przekazywania takich informacji do Prezesa UKE.  W naszej ocenie przepis ten zbyt szeroko określa uprawnienia CSIRT. Tajemnice prawnie chronione to bardzo szeroki katalog, dalece wykraczający poza samą tajemnicę przedsiębiorstwa czy tajemnicę telekomunikacyjną. Kwestii tych dotyczy kilkadziesiąt ustaw znajdujących się obecnie w obrocie prawnym i może dochodzić do sytuacji, w których przedsiębiorca telekomunikacyjny nie jest zobowiązany do ich zachowania. Nie zawsze bowiem będzie on w pełni dysponentem danej informacji, tj. nie w każdym przypadku będzie dotyczyła ona wyłączenie jego samego i tym samym będzie mógł przekazać ją CSIRT bez ryzyka naruszenia praw innych podmiotów. W niektórych przypadkach, aby możliwe było przekazanie takich informacji potrzebne byłoby uzyskanie zgody sądu. Ponadto już nawet przekazanie pełnych informacji w zakresie tajemnicy komunikacji elektronicznej budzi wątpliwości, pod kątem określenia czy np. treść indywidualnych komunikatów jest niezbędna CSIRT do wykonywania jego zadań.  W przypadku braku utrzymania przepisów w projekcie ustawy postulujemy proporcjonalne ograniczenie uprawnienia CSIRT. W każdym jednak wypadku to CSIRT powinien być odpowiedzialny za precyzyjne wskazanie, jakie informacje, w tym ewentualne tajemnice mają zostać przekazane. Określanie tego katalogu nie może być obowiązkiem i odpowiedzialnością przedsiębiorcy.  Ponadto należy określić minimalny termin na udzielenie odpowiedzi przez przedsiębiorcę, który powinien być proporcjonalny do zakresu wniosku.  **Postulat:**   * Art. 20d należy usunąć z projektu i przenieść dyskusję na jego temat na okres po implementacji PKE. | **Wyjaśnienie**  Przedsiębiorca komunikacji elektronicznej będzie mógł a nie musiał przekazać informacje prawnie chronione.  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 przez 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. |
|  | PIIT | Art. 20e | 1. **Art. 20e**   Proponowany art. 20e stanowi kopię projektowanego art. 43 ust. 2 i 3 PKE. Nie widzimy zasadności powtarzania tych samych przepisów w dwóch aktach prawnych, które odnosiłyby się do potencjalnie wspólnych zakresów incydentów.  W przypadku utrzymania przepisów w projekcie aktualne pozostają uwagi przedstawione w tym zakresie do PKE w pkt 19-20 zestawienia uwag do PKE dot. bezpieczeństwa.  **Postulat:**   * Art. 20e należy usunąć z projektu. | Uwaga nieuwzględniona  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 przez ustawę wprowadzającą PKE.  Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowym.  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. |
|  | PIIT | Art. 20f | 1. **Art. 20f**   Proponowany art. 20f stanowi powtórzenie przepisu art. 44 ust. 1 projektu PKE, przy czym pominięto bardzo istotny dla możliwości jego realizacji ust. 2, który w projekcie PKE wskazuje, że „*2. Zastosowanie środków, o których mowa w ust. 1, nie wyklucza zastosowania środków, o których mowa w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2015/2120 z dnia 25 listopada 2015 r. ustanawiającego środki dotyczące dostępu do otwartego internetu i dotyczące opłat detalicznych za uregulowane usługi łączności wewnątrzunijnej oraz zmieniającego dyrektywę 2002/22/WE, a także rozporządzenie (UE) nr 531/2012.”*  **Postulat:**   * Art. 20f należy usunąć z projektu. Aktualne pozostają również uwagi przedstawione w pkt 21-22 zestawienia uwag do PKE dot. Bezpieczeństwa. | **Uwaga nieuwzględniona**  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 przez ustawę wprowadzającą PKE.  Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowym.  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. |
|  | PIIT | Art. 26 ust 2 i 32 ust 4 | 8. Art. 26 ust. 2 i art. 32 ust. 4 dot. współpracy CSIRT i przedsiębiorców  Proponowany przepis daje możliwość wnioskowania do CSIRT MON, NASK, GOV o wsparcie w zakresie obsługi incydentów. W związku z powyższymi uwagami proponujemy, aby tą propozycję utrzymać w projekcie, przy czym z uwagi na postulowane wykreślenie przedsiębiorców komunikacji elektronicznej z KSC, w projektowanym przepisie należałoby odwołać się bezpośrednio do przedsiębiorców komunikacji elektronicznej, o których mowa w PKE (podobnie jak odwołano się do dysponentów infrastruktury krytycznej). Podobne rozwiązanie proponujemy przyjąć dla projektowanego art. 32 ust. 4 dot. wymiany informacji.  Postulat:  • Proponowane modyfikacje należy wprowadzić poprzez odwołanie do przedsiębiorców komunikacji elektronicznej, o których mowa w 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 przez ustawę wprowadzającą PKE.  Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowym.  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. |
|  | PIIT | Art. 26 ust. 3 | 9. Art. 26 ust 3 - zadania CSIRT  Prowadzenie działań na rzecz podnoszenia poziomu Cyberbezpieczeństwa podmiotów krajowego systemu cyberbezpieczeństwa, w szczególności przez:  a) wykonywanie testów bezpieczeństwa w porozumieniu z organami właściwymi i właściwymi podmiotami,  b) identyfikowanie podatności systemów dostępnych w otwartych sieciach teleinformatycznych, a także powiadamianie właścicieli tych systemów o wykrytych podatnościach oraz zagrożeniach cyberbezpieczeństwa  W kontekście uprawnienia wskazanego w lit. a i b – prośba o wyjaśnienie rozumienia użytego w tym punkcie określenia „właściwych podmiotów”? Jeżeli to podmioty krajowego systemu cyberbezpieczeństwa, to czy należy rozumieć, że CSIRT-y będą uprawnione do wykonywania testów bezpieczeństwa rozwiązań poszczególnych podmiotów wchodzących w skład systemu, np. SOC? | **Wyjaśnienie**  CSIRT będą mogły dokonywać testów bezpieczeństwa za zgodą podmiotu nadzorującego. |
|  | PIIT | Art. 34a | 10. Art. 34a dot. współpracy CSIRT i UKE  Tak jak już wskazywaliśmy, na obecnym etapie i w zakładanym terminie nie jest zasadne wprowadzanie dodatkowego mechanizmu raportowego.  Postulat:  • W związku z powyższymi uwagami, postulujemy, aby przepis dotyczył możliwej współpracy w zakresie incydentów, które zgłaszane są do Prezesa UKE. | **Uwaga nieuwzględniona**  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 przez ustawę wprowadzającą PKE.  Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowym.  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. |
|  | PIIT | Art. 44a | 11. Art. 44a dot. CSIRT Telco  Zgodnie z powyższym stanowiskiem, na tym etapie postulujemy usunięcie z projektu ustawy CSIRT Telco. Wprowadzenie regulacji dotyczących włączenia sektora komunikacji elektronicznej do krajowego systemu cyberbezpieczeństwa powinno być poprzedzone odpowiednią dyskusją z podmiotami objętymi tą regulacją. Brak wcześniejszej debaty w tym zakresie, bliski termin wejścia w życie oraz nakładanie się z regulacjami PKE byłyby w naszej ocenie bardzo szkodliwe dla takiego dialogu i wypracowania konstruktywnych rozwiązań.  Ewentualne wprowadzenie CSIRT Telco wymaga pogłębionej dyskusji, której dotychczas nie mieliśmy możliwości przeprowadzić. Jednocześnie tempo prac nie jest uzasadnione żadnymi szczególnymi zdarzeniami.  Postulat:  • Na obecnym etapie należy wykreślić przepisy z projektu.  • W ramach dyskusji o docelowym rozwiązaniu należy rozważyć możliwość wzmocnienia UKE i powołanie zespołu cyberbezpieczeństwa w jego strukturze, jako dodatkowego elementu już istniejącej struktury bezpieczeństwa. W tym celu należałoby wprowadzić możliwość powierzenia realizacji tego zadania także organowi nadzorowanemu lub wprost wskazać, że podmiotem odpowiedzialnym za realizację jest Prezes UKE. | **Uwaga nieuwzględniona**  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 przez ustawę wprowadzającą PKE.  Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowym.  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. |
|  | PIIT | Art. 46 | 12. Art. 46 ust. 2b  W celu wprowadzenia rozwiązania pośredniego proponujemy w ust. 2b. wskazać, że do takiego porozumienia w sprawie dostępu do systemu informatycznego może przystąpić również przedsiębiorca komunikacji elektronicznej. W razie potrzeby możliwe jest doprecyzowanie kryteriów, jakie powinien spełniać. | **Wyjaśnienie**  Docelowo przedsiębiorcy komunikacji elektronicznej mają stać się podmiotami krajowego systemu cyberbezieczeństwa. Jako podmioty ksc będą mogły być dołączone do systemu z art. 46. |
|  | ISACA Warsaw Chapter | Art. 20a 1. | Art. 2. Użyte w ustawie określenia oznaczają:  …  17) zagrożenie cyberbezpieczeństwa – potencjalną przyczynę wystąpienia incydentu;…  19) zarządzanie ryzykiem – skoordynowane działania w zakresie zarządzania cyberbezpieczeństwem w odniesieniu do  oszacowanego ryzyka  Art. 20a. 1. Przedsiębiorca komunikacji elektronicznej, w celu zapewnienia  ciągłości świadczenia usług komunikacji elektronicznej lub dostarczania sieci  telekomunikacyjnej, jest obowiązany uwzględniać możliwość wystąpienia sytuacji  szczególnego zagrożenia.  Problem generalny związany z niespójnością nazewnictwa. Podaję tu jeden przykład, warto jednak, skoro mamy ustawę o PKN i mamy w Polsce polskie normy, stosować nazewnictwo i definicje w nich istniejące, a nie wymyślać kolejne znaczenia. Tym bardziej, że projekt przedmiotowej ustawy w art.42 ust. 8 mówi również o uwzględnianiu w dziedzinie cyberbezpieczeństwa polskich norm.  **Przykłady:**  Określenie: zagrożenie cyberbezpieczeństwa z rozdz. 2 a opis „szczególne zagrożenie z Art.20 – co znaczy szczególne?  W projekcie ustawy jest definicja: szacowanie ryzyka – całościowy proces identyfikacji, analizy i oceny ryzyka;  W ISO 31000 definicja jest następująca: ocena ryzyka – całościowy proces identyfikacji, analizy i ewaluacji ryzyka;  W ISO 27005: szacowanie ryzyka to analiza ryzyka i jego ocena ryzyka, natomiast analiza ryzyka składa się z identyfikowania, estymowania.  Problem obejmuje również podstawową dla ustawy definicję „cyberbezpieczeństwa”, która nie wskazuje szerszego spektrum jakim jest bezpieczeństwo informacyjne oparte na systemach zarządzania ale mówi o odporności systemów teleinformatycznych.  Podobnie jest z incydentem poważnym, wielokrotnie zgłaszanym w dyskusji jako zdefiniowanym nieczytelnie. Zarówno incydent poważny jak i krytyczny w swojej interpretacji praktycznej nie mogą budzić wątpliwości. | **Uwaga nieuwzględniona**  Ustawa KSC uwzględnia Polskie Normy, m. in. definicja zarządzania ryzykiem nawiązuje do Normy ISO 27005. |
|  | SayF | Art. 20a ust 2 pkt 1 | Proponuje się doprecyzować pojęcie „systematyczną”. Proponuje się wyraz „ocenę” zastąpić wyrazami „wykonuje szacowanie ryzyka wystąpienia incydentu co najmniej raz w roku oraz każdorazowo po wystąpieniu incydentu ……… „ | **Uwaga nieuwzględniona**  Ocena ryzyka musi być dokonywana przed uruchomieniem sieci i usług a następnie ponawiana w przypadku zmian organizacyjnych i technicznych mogących mieć wpływ na bezpieczeństwo sieci i usług. Systematyczna ocena ryzyka powinna być prowadzona z uwzględnieniem faktu wystąpienia nowych zagrożeń, które mogą mieć wpływ na poziom oceny ryzyka.  Ponadto należy wziąć pod uwagę postęp technologiczny, najbardziej aktualny stan prawny i normy techniczne. |
|  | SayF | Art. 20a ust 3 pkt (nie podano) | Czy zapis ten należy rozumieć, że należy uwzględnić ust 2 pkt 1 i 2 w systematycznej ocenie ryzyka, która wynika z planu?  Jeżeli przedsiębiorca nie ma obowiązku sporządzenia planu, gdzie… | **Uwaga nieuwzględniona**  Przedsiębiorca ma prowadzić dokumentację zastosowanych środków technicznych i organizacyjnych a także wyników oceny ryzyka. |
|  | SayF | Art. 20a ust 3 | Proponuje się wykreślić art. 20a ust. 3 KSC.  Rekomendujemy nie łączyć dokumentacji dotyczącej cyberbezpieczeństwa z planem działań przedsiębiorcy telekomunikacyjnego.  Dokumentacja związana z cyberbezpieczeństwem powinna być  - dostępna wyłącznie osobom upoważnionym zgodnie z realizowanymi przez nie zadaniami;  - chroniona przed przypadkowym zniszczeniem, utratą, nieuprawnionym dostępem, niewłaściwym użyciem lub utratą integralności;”;  Do planów działań powinny mieć dostęp również inne osoby niż związane z cyberbezpieczeństwem. Ponadto każda zmiana zawartości planu wymaga jego aktualizacji i uzgodnienia po aktualizacji. Oznacza to, że po udokumentowaniu incydentu należy plan poddać aktualizacji i ponownie uzgodnić jego treść z właściwym organem administracji publicznej. | **Uwaga nieuwzględniona**  Dokumentacja o której mowa w art. 20a ust 3 dotyczy wszystkich aspektów bezpieczeństwa, w tym także bezpieczeństwa fizycznego co wynika z obowiązków związanych z wdrożeniem proporcjonalnych do oszacowanego ryzyka środków bezpieczeństwa. |
|  | SayF | Art. 20a ust 4 | Proponuje się w ustawie doprecyzować obowiązki przedsiębiorców komunikacji elektronicznej w zakresie zastosowania środków bezpieczeństwa, o których mowa w art. 20a ust. 2 pkt 2 KSC.  W rozporządzeniu (obligatoryjnym a nie fakultatywnym) ministra właściwego do spraw informatyzacji określić wyłącznie sposób dokumentowania stosowania tych środków bezpieczeństwa. | **Wyjaśnienie**  Przedsiębiorcy komunikacji elektronicznicznej będą stosować wspomniane środki po przeprowadzeniu systematycznej oceny ryzyka. To wyniki oceny wskażą jakie środki należy zastosować aby zapewnić bezpieczeństwo sieci lub usług komunikacji elektronicznej.  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. |
|  | KIGEIT | Art. 20a,  20e,  20f | **Propozycja zmiany:** wykreślenie w całości  *~~Art. 20a. 1. Przedsiębiorca komunikacji elektronicznej, w celu zapewnienia ciągłości świadczenia usług komunikacji elektronicznej lub dostarczania sieci telekomunikacyjnej, jest obowiązany uwzględniać możliwość wystąpienia sytuacji szczególnego zagrożenia.~~*  *~~2. Przedsiębiorca komunikacji elektronicznej:~~*  *~~1) przeprowadza systematyczną ocenę ryzyka wystąpienia sytuacji szczególnego zagrożenia;~~*  *~~2) podejmuje środki techniczne i organizacyjne zapewniające poziom bezpieczeństwa adekwatny do poziomu zidentyfikowanego ryzyka, minimalizujące w szczególności wpływ, jaki na sieci telekomunikacyjne, usługi komunikacji elektronicznej lub podmioty korzystające z tych sieci lub usług może mieć wystąpienie sytuacji szczególnego zagrożenia, dotyczące następujących obszarów:~~*  *~~a) zapewnienia bezpieczeństwa infrastruktury telekomunikacyjnej, o której mowa w art. 2 pkt 14 ustawy z dnia … – Prawo komunikacji elektronicznej,~~*  *~~b) postępowania w przypadku wystąpienia sytuacji szczególnego zagrożenia,~~*  *~~c) odtwarzania dostarczania sieci telekomunikacyjnych lub przywracania świadczenia usług komunikacji elektronicznej,~~*  *~~d) monitorowania, kontroli i testowania sieci telekomunikacyjnych lub usług komunikacji elektronicznej~~*  *~~– przy uwzględnieniu aktualnego stanu wiedzy technicznej oraz kosztów wprowadzenia tych środków;~~*  *~~3) dokumentuje czynności, o których mowa w pkt 1 i 2.~~*  *~~3. Przedsiębiorca komunikacji elektronicznej, o którym mowa w art. 2 pkt 42 ustawy – Prawo komunikacji elektronicznej, sporządzający plan, o którym mowa w art. 47 ust. 1 tej ustawy, dokumentuje w tym planie czynności, o których mowa w ust. 2 pkt 1 i 2.~~*  *~~4. Minister właściwy do spraw informatyzacji może, w drodze rozporządzenia, określić dla danego rodzaju działalności, biorąc pod uwagę skalę działalności, wykonywanej przez przedsiębiorcę komunikacji elektronicznej minimalny zakres środków, o których mowa w ust. 2 pkt 2, lub sposób ich dokumentowania, biorąc pod uwagę rekomendacje międzynarodowe o charakterze specjalistycznym oraz mając na uwadze potrzebę podejmowania przez tego przedsiębiorcę działań zapewniających bezpieczeństwo sieci i usług.~~*  *~~Art. 20e. 1. Przedsiębiorca komunikacji elektronicznej wykonujący działalność na rynku detalicznym, w przypadku szczególnego i znacznego zagrożenia wystąpienia incydentu telekomunikacyjnego, informuje o nim swoich użytkowników, na których takie zagrożenie może mieć wpływ, w tym o możliwych środkach, które użytkownicy ci mogą podjąć, oraz związanych z tym kosztach.~~*  *~~2. Przedsiębiorca komunikacji elektronicznej, o którym mowa w ust. 1, informuje, w tym na swojej stronie internetowej, o incydencie telekomunikacyjnym i jego wpływie na dostępność świadczonych usług, jeżeli w jego ocenie ten wpływ jest istotny.~~*  *~~Art. 20f. W przypadku stwierdzenia przesyłania komunikatów zagrażających bezpieczeństwu sieci i usług, przedsiębiorca komunikacji elektronicznej, z uwzględnieniem art. 349 ust. 2 ustawy z dnia … – Prawo komunikacji elektronicznej, może zastosować środki polegające na:~~*  *~~1) zablokowaniu przesłania takiego komunikatu,~~*  *~~2) ograniczeniu albo przerwaniu świadczenia usługi komunikacji elektronicznej na zakończeniu sieci, z którego następuje wysyłanie takiego komunikatu w zakresie niezbędnym dla zapobiegnięcia zagrożeniu i nie dłużej niż do czasu ustania przyczyny stwierdzenia zagrożenia~~*  **Uzasadnienie:**  Przepisy art. 20a konsultowanego projektu stanowią powielenie przepisów zawartych w art. 39 projektu z dnia 29 lipca 2020 ustawy – Prawo komunikacji elektronicznej, przepisy art. 20e – przepisów art. 42 ust. 2 i 3 projektu ustawy – Prawo komunikacji elektronicznej, a przepis art. 20f – przepisu art. 44 ust. 1 projektu ustawy – Prawo komunikacji elektronicznej.  Delegacja dla ministra właściwego do spraw informatyzacji ujęta w art. 20a ust. 4 przedmiotowego projektu jest tożsama z delegacją zawartą w art. 39 projektowanej ustawy – Prawo komunikacji elektronicznej, a ujęta w art. 20c ust. 4 – z art. 42 ust. 2 projektowanej ustawy – Prawo komunikacji elektronicznej.  Ujmowanie tych samych przepisów w różnych aktach prawnych jest niezgodne z zasadami techniki legislacyjnej. Zapewne nie było również intencją ustawodawcy, aby w systemie prawnym miały funkcjonować dwa rozporządzenia tej samej treści, wydane na podstawie upoważnień przewidzianych w dwóch różnych ustawach. W tej sytuacji proponuje się usunięcie tych przepisów z niniejszego Projektu.  Na wypadek nieuwzględnienia niniejszej uwagi należy wskazać na błąd w ujętym w art. 20a ust. 3 odwołaniu do ustawy Prawo komunikacji elektronicznej – definicja przedsiębiorcy komunikacji elektronicznej ujęta jest w art. 2 pkt 41, a nie pkt 42 | **Uwaga nieuwzględniona**  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 przez ustawę wprowadzającą PKE.  Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowym.  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.  Dlatego potrzebne jest przeniesienie odpowiednich definicji z PKE do ustawy KSC. |
|  | Signum Edward Kuś Marcin Kuś | Art. 20a-f | **Przedmiot**  Projekt nie powinien mieć zastosowania bezpośrednio do operatorów telekomunikacyjnych  **Ustawa**  Ustawa o KSC jest transpozycją dyrektywy NIS (Dyrektywa Parlamentu Europejskiego i Rady (UE) w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii), a dyrektywa NIS nie ma zastosowania do operatorów telekomunikacyjnych. Prawa i obowiązki operatorów telekomunikacyjnych zostały szczegółowo określone w projekcie ustawy Prawo Komunikacji Elektronicznej (PKE), który implementuje Europejski Kodeks Łączności Elektronicznej (EECC).  **Uzasadnienie**  Dodanie przedsiębiorstwa komunikacji elektronicznej, jako podmiotu, do którego stosuje się KSC, powoduje potencjalny konflikt przepisów o randze ustawowej. Operator telekomunikacyjny jest zazwyczaj istotnym dostawcą usług dla operatorów infrastruktury kluczowej.. Dlatego PKE ma kompleksowe i szczególne wymagania wobec operatorów telekomunikacyjnych. Nakładanie się na siebie KSC i PKE spowoduje wątpliwości interpretacyjne.  **Przepisy**  art. 1 KSC art. 20a-f KSC  **Sugestie**   1. Postępowanie zgodnie z logiką prawną dyrektywy NIS i EECC. 2. KSC nie ma zastosowania do przedsiębiorstw komunikacji elektronicznej. | **Uwaga nieuwzględniona**  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 przez ustawę wprowadzającą PKE.  Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowym.  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.  Dlatego potrzebne jest przeniesienie odpowiednich definicji z PKE do ustawy KSC. |
|  | SayF | Art. 20b pkt 1 | Art. 20b pkt 1 nadać brzmienie: „zapewnia zarządzanie incydentem”  Pojęcie „zarządzanie incydentem” jest pojęciem szerszym, obejmującym więcej elementów działalności związanej z postępowaniem po wystąpieniu incydentu: wyszukiwanie powiązań między incydentami, usuwanie przyczyn ich wystąpienia oraz opracowywanie wniosków wynikających z obsługi incydentu; | **Uwaga nieuwzględniona**  Przedsiębiorca komunikacji elektronicznej zapewnia obsługę incydentu telekomunikacyjnego. Natomiast koordynacją obsługi incydentu zajmuje się CSIRT poziomu krajowego.  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. |
|  | SayF | Art. 20b pkt 2 | Doprecyzowania wymaga na czym ma polegać zapewnienie dostępu udostępnianie informacji o incydentach właściwemu CSIRT. Zapewnienie dostępu słownikowo oznacza, że podmiot, któremu umożliwia się dostęp ma możliwość skorzystania z tych danych. Czy warunek ten będzie spełniony, jeśli przedsiębiorca umożliwi skorzystanie z tych danych jedynie w swojej siedzibie i z informacji zgromadzonych np. w formie papierowej? Ponadto zauważyć należy, że informacje dotyczące incydentów cyberbezpieczeństwa powinna być chroniona a tym samym kanał komunikacyjny służący do ich przesyłania powinien być zabezpieczony. Przedsiębiorca komunikacji elektronicznej nie ma obowiązku spełniania wymogu posiadania narzędzi bezpiecznej komunikacji. | **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 przez ustawę wprowadzającą PKE.  Aby właściwy CSIRT mógł wesprzeć przedsiębiorcę komunikacji elektronicznej w obsłudze incydentu, musi mieć dostęp do danych o incydencie. |
|  | Związek Banków Polskich | Art. 20b pkt 2 | Art. 20b pkt 2: zapewnia dostęp do informacji o rejestrowanych incydentach właściwemu CSIRT MON, CSIRT NASK, CSIRT GOV lub **właściwym** **CSIRT sektorowym** w zakresie niezbędnym do realizacji jego zadań, a także **właściwemu ISAC, jeżeli dotyczą one incydentów, które mogą mieć wpływ na bezpieczeństwo podmiotów danego sektora, sektorów lub podsektorów lub ich klientów**.  Zapewnienie wymiany informacji między sektorami i w ramach sektora. Włączenie CSIRT sektorowego i ISACów w proces wymiany informacji. | **Uwaga nieuwzględniona**  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 przez ustawę wprowadzającą PKE.  CSIRT sektorowe nie obsługują przedsiębiorców komunikacji elektronicznej. |
|  | KIGEIT | Art. 20c ust. 1,2,3,4 | **Propozycja zmiany:**  *Art. 20c. 1. Przedsiębiorca komunikacji elektronicznej, ~~sporządzający plan, o którym mowa w art. 47 ust. 1 ustawy – Prawo komunikacji elektronicznej~~:*  *1) klasyfikuje incydent jako incydent telekomunikacyjny na podstawie progów uznania incydentu za telekomunikacyjny;*  *2) zgłasza incydent telekomunikacyjny niezwłocznie, nie później niż w ciągu 24 godzin od momentu jego wykrycia, do właściwego CSIRT ~~MON, CSIRT NASK lub CSIRT GOV~~ Telco;*  *3) współdziała podczas obsługi incydentu telekomunikacyjnego i incydentu krytycznego z właściwym CSIRT ~~MON, CSIRT NASK lub CSIRT GOV~~ Telco, przekazując niezbędne dane, w tym dane osobowe.*  *4) zapewnia CSIRT Telco dostęp do informacji o rejestrowanych incydentach w zakresie niezbędnym do realizacji jego zadań.*  *2. Zgłoszenie, o którym mowa w ust. 1 pkt 2, przekazywane jest w postaci elektronicznej, a w przypadku braku możliwości przekazania go w postaci elektronicznej - przy użyciu innych dostępnych środków komunikacji.*  *~~3. Przedsiębiorca komunikacji elektronicznej niezależnie od zadań określonych w ust. 1:~~*  *~~1) przekazuje jednocześnie CSIRT Telco w postaci elektronicznej zgłoszenie, o którym mowa w ust. 1 pkt 2;~~*  *~~2) współdziała z CSIRT Telco podczas obsługi incydentu telekomunikacyjnego lub incydentu krytycznego, przekazując niezbędne dane, w tym dane osobowe;~~*  *~~3) zapewnia CSIRT Telco dostęp do informacji o rejestrowanych incydentach w zakresie niezbędnym do realizacji jego zadań.~~*  *~~4~~.3 Minister właściwy do spraw informatyzacji określi, w drodze rozporządzenia, progi uznania incydentu za incydent telekomunikacyjn~~ego~~y, ~~których przekroczenie powoduje powstanie obowiązku zgłoszenia incydentu,~~ uwzględniając:*  **Uzasadnienie:**  W celu zapewnienia efektywności podejmowanych działań stosowne wydaje się ustalenie jednego podmiotu, któremu przedsiębiorca komunikacji elektronicznej przekazywać będzie zgłoszenie i który będzie koordynować działania w ramach obsługi incydentu. CSIRT Telco winien pełnić taką wiodącą rolę w powyższym zakresie, a działać niejako równolegle w stosunku do pozostałych CSIRT, powodując konieczność dublowania działań podejmowanych przez przedsiębiorcę komunikacji elektronicznej. CSIRT Telco może być umiejscowiony w Urzędzie Komunikacji Elektronicznej.  Upoważnienie przewidziane w ust. 4 odpowiada treścią art. 42 ust. 2 projektowanej ustawy Prawo komunikacji elektronicznej. Nie wydaje się więc zasadne tworzenie dodatkowego pojęcia incydentu telekomunikacyjnego.  Niezależnie od powyższego, w projekcie przewidziano obowiązek klasyfikowania przez przedsiębiorcę incydentu na podstawie progów uznania za incydent telekomunikacyjny, wobec czego delegacja powinna przewidywać określenie tych progów. Z kolei określanie progów pozwalających na podział incydentów telekomunikacyjnych na podlegające oraz na niepodlegające obowiązkowi zgłoszenia jest zbędne, bowiem w ust. 1 pkt 2) przewidziano obowiązek zgłaszania wszystkich incydentów telekomunikacyjnych.  Zgodnie z projektowanym art. 1 ust. 1 pkt 4, ustawa ma określać zadania i obowiązki wszystkich przedsiębiorców komunikacji elektronicznej, o których mowa w ustawie Prawo komunikacji elektronicznej, w zakresie wymogów dotyczących bezpieczeństwa i zgłaszania incydentów, natomiast zgodnie z projektowanym art. 4 pkt 2a, Krajowy system cyberbezpieczeństwa ma obejmować wszystkich przedsiębiorców komunikacji elektronicznej. W związku z tym w wypadku objęcia przedsiębiorców komunikacji elektronicznej zakresem ustawy, obowiązki określone w przepisie powinny zostać nałożone na wszystkich przedsiębiorców komunikacji elektronicznej, bez ograniczenia do przedsiębiorców sporządzających plan, o którym mowa w art. 47 ust. 1 ustawy – Prawo komunikacji elektronicznej. | **Uwaga nieuwzględniona**  Jeżeli przedsiębiorcy komunikacji elektronicznej zawrą porozumienie w sprawie podłączenia się do systemu z art. 46 to uzyskają prosty sposób przekazywania informacji o incydentach.  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 przez ustawę wprowadzającą PKE. |
|  | Związek Pracodawców Mediów Elektronicznych i Telekomunikacji MEDIAKOM | Art. 20c KSC  Art. 42 PKE  Art. 20c KSC  Art. 42 PKE | Ustawa o krajowym systemie cyberbezpieczeństwa, równolegle do PKE reguluje obowiązek zgłaszania incydentów bezpieczeństwa, przy czym różny jest krąg podmiotów zobowiązanych i organ właściwy do przyjmowania zgłoszeń:  PKE nakłada obowiązek na wszystkich przedsiębiorców telekomunikacyjnych i nakazuje zgłaszać incydenty do UKE (art. 42) , zaś  ustawa o krajowym systemie bezpieczeństwa nakłada obowiązki jedynie na tych przedsiębiorców, którzy mają obowiązek sporządzania planów działania w sytuacjach szczególnych zagrożeń i nakazuje zgłaszać incydenty do właściwego CSIRT (art. 20c).  Ponadto, wobec wyżej wskazanych rozbieżności pomiędzy projektowanymi art. 42 PKE i art. 20c ustawy o krajowym systemie cyberbezpieczeństwa **Mediakom postuluje, by pozostać przy rozwiązaniu przyjętym w art. 20c – tak, by obowiązek zgłaszania incydentów obciążał wyłącznie tych przedsiębiorców telekomunikacyjnych, którzy są zobowiązani do sporządzania planów działania w sytuacjach szczególnych zagrożeń.** Są to podmioty duże, osiągające ponad 10 mln przychodów, często posiadające rozbudowane sieci i dużą liczbę abonentów. To właśnie incydenty bezpieczeństwa dotykające tych podmiotów, z uwagi na skalę ich działalności, winny być raportowane. Natomiast mniejsi przedsiębiorcy, działający na mniejszą skalę, o znacznie mniejszym zasięgu sieci i liczbie abonentów nie powinni być objęci obowiązkiem raportowania incydentów bezpieczeństwa. | **Uwaga nieuwzględniona**  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 przez ustawę wprowadzającą PKE.  Przedsiębiorcy komunikacji elektronicznej będą zgłaszać te incydenty telekomunikacyjne, które będą spełniać progi określone w rozporządzeniu. |
|  | ISSA Polska | Art. 20c ust. 2 | Art 20c ust 2. wymaga uszczegółowienia w kontekście realiów rynkowych. Czy niniejszy zapis należy rozważyć w taki sposób, że jeżeli przykładowo przedsiębiorca telekomunikacyjny zauważy „niestandardowy” ruch do podmiotu nadzorowanego przez  CSIRT MON to ma obowiązek w przeciągu 24h o tym poinformować mil.cert?  Przedsiębiorcy telekomunikacyjni często udostępniają klientom usługi SOC w formie komercyjnej usługi, taki przedsiębiorca nie powinien mieć nakładanych żadnych obowiązków w zakresie monitorowania bezpieczeństwa podmiotom, które nie wykupiły  specjalistycznej usługi SOC. Podobnie sam fakt „niestandardowego” ruchu mógłby wyłącznie zostać zarejestrowany w systemach telekomunikacyjnych a niekoniecznie zostałby zidentyfikowany. Zapisy punktu należy doprecyzować biorąc pod uwagę, że jakiekolwiek usługi na rzecz podmiotów nie będących klientami SOC mogą być realizowane jedynie fakultatywnie. | **Uwaga nieuwzględniona**  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.  Przedsiębiorca komunikacji elektronicznej ma zgłosić incydent telekomunikacyjny do tego CSIRT, który zgodnie z art. 26 będzie właściwy dla danego przedsiębiorcy. |
|  | Digital Poland | Art. 20c | Warto w tym miejsce jeszcze zwrócić uwagę na pewną terminologiczną niedbałość w stworzeniu projektu KSC. Art. 20c ustawy o KSC przywołuje pojęcie „przedsiębiorcy komunikacji elektronicznej” z art. 47 ust. 1 projektu PKE, podczas gdy przepis ten odnosi się do przedsiębiorcy telekomunikacyjnego, a zatem nie do całej kategorii przedsiębiorców komunikacji elektronicznej.  Podsumowując to zagadnienie, ujęcie w rozdziale 4a usług komunikacji interpersonalnej niewykorzystującej numerów wymaga korekty, bowiem jest całkowicie nieuzasadnione. Ponadto, projekt zmiany ustawy o KSC zawiera w rozdziale 4a nieścisłości terminologiczne, które mają olbrzymie znaczenie i także wymagają korelacji w innymi aktami prawnymi. | **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.  Wszyscy przedsiębiorcy komunikacji elektronicznej będą zgłaszać incydenty telekomunikacyjne przekraczające progi ustalone w rozporządzeniu. |
|  | SayF | Art. 20c ust 1 | Skoro nadrzędnym celem przepisów dotyczących bezpieczeństwa, a cyberbezpieczeństwa w szczególności, jest stworzenie systemu stwarzające warunki do szczelnego systemu bezpieczeństwa, to przepisy określają w bardzo różny sposób obowiązek realizacji tych obowiązków. W inny sposób określono obowiązki operatora usługi kluczowej, dostawców usług cyfrowych i w inny sposób przedsiębiorcy komunikacji elektronicznej.  Dodatkowo podzielono przedsiębiorców komunikacji elektronicznej na dwie grupy tych, którzy sporządzają plany działań oraz tych, którzy nie mają takiego obowiązku.  Kryterium obowiązku posiadania planu działań przez przedsiębiorcę telekomunikacyjnego nie będzie w każdym przypadku właściwą granicą podziału przedsiębiorców na grupy o różnych obowiązkach zapewnienia cyberbezpieczeństwa.  Zdarza się, że przedsiębiorca telekomunikacyjny świadczący usługi np. w technologii VoIP dla kilkudziesięciu tysięcy abonentów, nieposiadający własnej infrastruktury telekomunikacyjnej, jest zwolniony z obowiązku posiadania planu działań. Oznacza to, że również jego działania w zakresie bezpieczeństwa usług będą ograniczone jak dla przedsiębiorców nie mających obowiązku wykonania planu działań, czyli będzie wykonywał te zadania w ograniczonym zakresie.  Ponadto należy podkreślić, że projektowanie przepisów regulujących w odmienny sposób te same zagadnienie (obowiązki) wykonywane przez różne podmioty powoduje lub może powodować różne interpretacje i też różne wykonanie tych obowiązków. . | **Wyjaśnienie**  Przepisy zostały zmienione  Przedsiębiorca komunikacji elektronicznej ma zapewnić obsługę każdego incydentu telekomunikacyjnego. Zgłaszać będzie takie incydenty telekomunikacyjne, które będą spełniały progi określone w rozporządzeniu.  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. |
|  | SayF | Art. 20c ust 1 pkt 1 | Dlaczego tylko wybrany przedsiębiorca kwalifikuje incydent jako incydent telekomunikacyjny. Czy incydent jest lub nie jest incydentem telekomunikacyjnym decyduje charakter incydentu i jego skutki a nie rodzaj podmiotu, u którego taki incydent zaistnieje? | **Wyjaśnienie**  Przepisy zostały zmienione  Przedsiębiorca komunikacji elektronicznej ma zapewnić obsługę każdego incydentu telekomunikacyjnego. Zgłaszać będzie takie incydenty telekomunikacyjne, które będą spełniały progi określone w rozporządzeniu.  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 przez ustawę wprowadzającą PKE. |
|  | Związek Banków Polskich | Art. 20c ust. 1 pkt 2 | Art.20c ust. 1 pkt 2: zgłasza incydent telekomunikacyjny niezwłocznie, nie później niż w ciągu 24 godzin od momentu jego wykrycia, do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV i **właściwych CSIRT sektorowych,** a także **właściwego ISAC, jeżeli incydent telekomunikacyjny może mieć wpływ na bezpieczeństwo podmiotów danego sektora, sektorów lub podsektorów lub ich klientów**;  Zapewnienie skutecznej wymiany informacji w ramach sektora. Włączenie CSIRT sektorowego oraz ISAC w proces wymiany informacji | **Uwaga nieuwzględniona**  CSIRT sektorowe nie będą obsługiwać incydentów telekomunikacyjnych. W ich właściwości nie jest obsługa przedsiębiorców komunikacji elektronicznej.  ISAC nie jest jednostką operacyjną.  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 przez ustawę wprowadzającą PKE. |
|  | SayF | Art. 20c ust 3 | Czy ten przepis dotyczy tylko przedsiębiorców telekomunikacyjnych zobowiązanych do posiadania planu działań czy dotyczy wszystkich przedsiębiorców komunikacji elektronicznej? | **Wyjaśnienie**  Według nowego brzmienia przepisów będzie dotyczył wszystkich przedsiębiorców komunikacji elektronicznej.  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 przez ustawę wprowadzającą PKE. |
|  | Związek Banków Polskich | Art. 20c ust. 1 pkt 3 | 1. współdziała podczas obsługi incydentu telekomunikacyjnego i incydentu krytycznego z właściwym CSIRT MON, CSIRT NASK lub CSIRT GOV i **właściwym CSIRT sektorowym, a także** **właściwym** **ISAC jeżeli incydent telekomunikacyjny może mieć wpływ na bezpieczeństwo podmiotów danego sektora, sektorów lub podsektorów lub ich klientów**, przekazując niezbędne dane, w tym dane osobowe.   Zapewnienie skutecznej wymiany informacji w ramach  sektora. Włączenie CSIRT sektorowego oraz ISAC w  proces wymiany informacji. | **Uwaga nieuwzględniona**  CSIRT sektorowe nie będą obsługiwać incydentów telekomunikacyjnych. W ich właściwości nie jest obsługa przedsiębiorców komunikacji elektronicznej.  ISAC nie jest jednostką operacyjną.  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 przez ustawę wprowadzającą PKE. |
|  | Związek Banków Polskich | Art. 20d ust. 3 | **Art.20d ust. 3:Przedsiębiorca komunikacji elektronicznej może przekazać, w niezbędnym zakresie, w zgłoszeniu, o którym mowa w art. 20c ust. 1 pkt 2, informacje stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa, gdy jest to konieczne do obsługi incydentu przez właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV oraz CSIRT Telco i inny właściwy CSIRT sektorowy, a także właściwy ISAC, jeżeli incydent może mieć wpływ na bezpieczeństwo podmiotów danego sektora, sektorów lub podsektorów lub ich klientów.**  Zapewnienie wymiany informacji między sektorami w celu skutecznej obsługi incydentu. | **Uwaga nieuwzględniona**  CSIRT sektorowe nie będą obsługiwać incydentów telekomunikacyjnych. W ich właściwości nie jest obsługa przedsiębiorców komunikacji elektronicznej.  ISAC nie jest jednostką operacyjną.  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 przez ustawę wprowadzającą PKE. |
|  | SayF | Art. 20e ust. 1 | Czy warto ten obowiązek do przedsiębiorcy komunikacji elektronicznej wykonującego działalność na rynku detalicznym?  Ponadto art. 20e ust. 1 zobowiązuje przedsiębiorcę komunikacji elektronicznej do informowania swoich użytkowników o szczególnym i znacznym zagrożeniu wystąpienia incydentu telekomunikacyjnego.  Wątpliwości nasze dotyczą:  1)W jaki sposób przedsiębiorca może wiedzieć o zagrożeniu wystąpienia incydentu telekomunikacyjnego. Takie zdarzenie wydarzy się w przyszłości. Przedsiębiorca może stwierdzić (i to nie zawsze) wystąpienie incydentu. Natomiast zagrożenie wystąpienia incydentu istnieje zawsze, w każdej chwili istnieje zagrożenie wystąpienia incydentu.  2)W jaki sposób przedsiębiorca będzie mógł stwierdzić istnienie szczególnego i znacznego zagrożenia. | **Uwaga nieuwzględniona.**  Obecnie już funkcjonuje analogiczny przepis w art. 175e Prawa telekomunikacyjnego. |
|  | SayF | Art. 20f | Spójnik „i” we frazie „sieci i usług” proponuje się zastąpić spójnikiem „lub”. Może się zdarzyć, że przesyłany komunikat może zagrozić tylko bezpieczeństwu sieci albo tylko bezpieczeństwu usług. | **Uwaga nieuwzględniona**  Spójnik „i” pełni tutaj funkcję wyliczenia. Poza tym należy czytać to zgodnie z definicją bezpieczeństwa sieci i usług komunikacji elektronicznej |
|  | Związek Banków Polskich | Art. 20f | Art. 20f  W przypadku stwierdzenia przesyłania komunikatów zagrażających bezpieczeństwu sieci i usług, przedsiębiorca komunikacji elektronicznej, z uwzględnieniem art. 349 ust. 2 ustawy z dnia ... – Prawo komunikacji elektronicznej, może zastosować środki polegające na:  1) zablokowaniu przesłania takiego komunikatu,  2) ograniczeniu albo przerwaniu świadczenia usługi komunikacji elektronicznej na zakończeniu sieci, z którego następuje wysyłanie takiego komunikatu  **3) w sytuacji przesłania już komunikatu przed podjęciem działań zapobiegawczych poinformowaniu odbiorcy o zagrożeniu i jego skutkach wynikających z przesłanego komunikatu, a także sposobie jego neutralizacji**  - w zakresie niezbędnym dla zapobiegnięcia zagrożeniu i nie dłużej niż do czasu ustania przyczyny stwierdzenia zagrożenia.  Pierwotny zapis zakłada, że zagrożenie będzie niwelowane przed jego dystrybucją. Brak jest wskazówek co powinno nastąpić, gdy zagrożenie zostało zidentyfikowane w trakcie trwania incydentu. | **Uwaga nieuwzględniona**  Obecne Prawo telekomunikacyjne zawiera analogiczny przepis i nie ma potrzeby jego rozszerzania. |
|  | ISACA Warsaw Chapter | Art. 20f | „Art. 20f. W przypadku stwierdzenia przesyłania komunikatów zagrażających bezpieczeństwu sieci i usług, przedsiębiorca komunikacji elektronicznej, z uwzględnieniem art. 349 ust. 2 ustawy z dnia … – Prawo komunikacji elektronicznej, może zastosować środki polegające na:  1) zablokowaniu przesłania takiego komunikatu,  2) ograniczeniu albo przerwaniu świadczenia usługi komunikacji elektronicznej na zakończeniu sieci, z którego następuje wysyłanie takiego komunikatu  - w zakresie niezbędnym dla zapobiegnięcia zagrożeniu i nie dłużej niż do czasu ustania przyczyny stwierdzenia zagrożenia”  Propozycja rozszerzenia zapisu o to, kto będzie miał upoważnienie do stosowania wymienionych działań. | **Uwaga nieuwzględniona**  Obecne Prawo telekomunikacyjne zawiera analogiczny przepis i nie ma potrzeby jego rozszerzania. |
|  | SayF | Art. 20f pkt 1 i 2 | Proponuje się wykreślić art. 20f pkt 1, ponieważ w celu określenia jaki komunikat powoduje zagrożenie bezpieczeństwu sieci lub usług przedsiębiorca będzie musiał wykonać kontrolę i analizę tego komunikatu. Ponadto w celu zrealizowania tego przepisu będzie musiał zablokować przesłania tylko tego komunikatu, który zagraża bezpieczeństwu. W naszej ocenie prawnie jest to niedopuszczalne a technicznie bardzo trudne do wykonania.  Pkt 2 w art. 20f w pełni obejmuje również zakres określony w pkt1 | **Uwaga niewuzględniona**  Analogiczny przepis jest w art. 175c Prawa telekomunikacyjnego. |
|  | SayF | Art. 20f myślnik po punkcie 2 | Wzorem przepisów ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne proponuje się uzupełnić ten zapis o przepisy zwalniające przedsiębiorcę z odpowiedzialności za skutki działań, o których mowa w art. 20f. (chyba, że przepisy te znajdą się w PKE) | **Uwaga nieuwzględniona**  W chwili obecnej nie są planowane zmiany w projekcie, o których mowa w uwadze. |
|  | Liquid Systems | Art. 20a-f | Projekt nie powinien mieć zastosowania bezpośrednio do operatorów telekomunikacyjnych.  Ustawa KSC jest transpozycją dyrektywy NIS (Dyrektywa  Parlamentu Europejskiego i Rady (UE) w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii), a dyrektywa NIS nie ma zastosowania do operatorów telekomunikacyjnych, ponieważ prawa i obowiązki operatorów telekomunikacyjnych zostały  szczegółowo określone w ustawie Prawo Komunikacji Elektronicznej,  implementującej do prawa polskiego Europejski Kodeks  łączności Elektronicznej (EECC).  Dodanie przedsiębiorstwa komunikacji elektronicznej jako podmiotu, do którego stosuje się KSC, powoduje nakładanie się przepisów i potencjalny konflikt między nimi. Operator telekomunikacyjny jest zazwyczaj bardzo ważnym dostawcą usług operatora infrastruktury krytycznej..  Dlatego PKE ma kompleksowe i szczególne wymagania wobec operatorów telekomunikacyjnych. Nakładanie się na siebie KSC i PKE  powoduje wątpliwości w zakresie interpretacji przepisów.  **Sugestie:**  1.Postępowanie zgodnie z logiką prawną dyrektywy NIS i EECC .  2.KSC nie powinno mie6 zastosowania do przedsiębiorstw  Komunikacji elektronicznej. | **Uwaga nieuwzględniona**  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 przez ustawę wprowadzającą PKE.  Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowym.  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.  Dlatego potrzebne jest przeniesienie odpowiednich definicji z PKE do ustawy KSC. |
|  | Izba Gospodarcza Gazownictwa/Polska Spółka Gazownictwa Sp. z.o.o. | Art. 22 ust. 1 pkt 2a | **Pominięte słowo**  będący jednostką samorządu terytorialnego, niezależnie od obowiązku, o którym mowa w punkcie 2, zgłasza incydent w podmiocie publicznym niezwłocznie, nie później niż w ciągu 24 godzin od momentu wykrycia, do właściwego wojewody | **Uwaga uwzględniona** |
|  | Transition Software | Art.24 pkt.3 ppkt c) i d) | Podmioty świadczące usługę kluczową oraz inne podmioty wchodzące w skład systemu cyberbezpieczeństwa powinny obligatoryjnie przeprowadzać - minimum wśród personelu pełniącego obowiązki w procesie świadczenia usługi kluczowej – cykliczne (minimum raz w roku kalendarzowym) szkolenia z zakresu świadomości zagrożeń cyberbezpieczeństwa (tzw. *Security Awareness*).  Zalecane jest natomiast cykliczne szkolenie całego personelu przedsiębiorstwa/podmiotu, z powodu minimalizacji ryzyka poprzez minimalizację powierzchni potencjalnego ataku (zasada *„najsłabszego ogniwa łańcucha*). | **Uwaga nieuwzględniona**  Operator usługi kluczowej odpowiada za swój personel. |
|  | Fundacja Bezpieczna Cyberprzestrzeń | Art. 24a | Należy rozważyć powołanie CSIRT-u sektorowego dla “sektora administracji samorządowej” z organem właściwym przy ministrze właściwym do spraw administracji. Zakres obowiązków i zadań w stosunku do jednostek samorządu terytorialnego uzasadnia taką propozycję. | **Uwaga nieuwzględniona**  Podmioty publiczne w tym jednostki samorządu terytorialnego są specyficzną kategorią podmiotów ksc i nie mogą być traktowane jak operatorzy usługi kluczowej. Wsparciem w obsłudze incydentu dla JST zajmuje się CSIRT NASK. |
|  | Związek Banków Polskich | Art. 24a | 24a. Wojewoda:  1) zapewnia wymianę informacji na temat zagrożeń cyberbezpieczeństwa, podatności oraz incydentów dotyczących podmiotów publicznych w województwie;  2)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 oraz właściwym CSIRT sektorowym i właściwym ISAC;  3)we współpracy z Pełnomocnikiem oraz właściwymi CSIRT MON, CSIRT NASK lub CSIRT GOV oraz właściwym CSIRT sektorowym i właściwym ISAC przekazuje marszałkowi województwa, starostom, wójtom, burmistrzom, prezydentom miast w informacje dotyczące: (…)  Włączenie CSIRT sektorowych oraz ISAC w kanał informacyjny. | **Uwaga nieuwzględniona**  CSIRT sektorowe nie będą obsługiwać incydentów w podmiocie publicznym. W ich właściwości nie jest obsługa podmiotów publicznych.  ISAC nie jest jednostką operacyjną. |
|  | Transition Software | Art.26, ust. 3, pkt 14 | Rozważyć wprowadzenie zapisów umożliwiających zastosowania outsourcingu/body leasingu w przypadku braku zasobów kadrowych. Przy uwzględnieniu outsourcingu/body leasingu również należy sprawdzić - przez dedykowane służby – bezpieczeństwo osobowe personelu, który będzie miał wykonywać powierzone prace. W przypadku istnienia potencjalnej możliwości odbioru informacji niejawnych jako danych niezbędnych do świadczenia obowiązków, przed rozpoczęciem świadczenia obowiązków musi on posiadać aktualne poświadczenie bezpieczeństwa, o stopniu przynajmniej równym do klauzuli potencjalnych otrzymywanych informacji niejawnych. | **Uwaga nieuwzględniona**  Uwaga nie dotyczy projektowanej ustawy. |
|  | Transition Software | Art. 26, ust. 3, pkt 15 | Wprowadzić zapis, który jednoznacznie wskazuje, że „obsługa” musi obejmować również to, że ta potencjalna platforma i kanały przekazu zgłoszeń muszą być zawsze bezpieczne, z bieżącymi aktualizacjami i regularnie przeglądane pod kątem istnienia ew. luk/podatności. | **Uwaga nieuwzględniona**  Uwaga nie dotyczy projektowanej ustawy. |
|  | ISSA Polska | Art. 26 ust. 3 pkt 21 | Prosimy o informacje, w jaki sposób regulator rozgranicza otwarte sieci teleinformatyczne od tych, w zakresie których sieci mają niezamierzone błędy konfiguracji lub są wynikiem ujawnionej podatności itp. w kontekście ustawowej zgody na skanowanie sieci wyrażoną w punkcie 21 ustępu 3 artykułu 26.  Nie został przedstawione konsekwencje w zakresie regresji i odszkodowań na skutek skanowania lub dostępu do informacji na systemach informacyjnych osoby fizycznej, podmiotów gospodarczych czy międzynarodowych podmiotów będących uczestnikami sieci teleinformatycznych.  Prosimy dodatkowo prosimy o określenie czasu retencji informacji pozyskanych w ramach skanowania - prawo do bycia zapomnianym / zatarcie. | **Wyjaśnienie**  Zespoły CSIRT poziomu krajowego takie działania będą mogły prowadzić jedynie w porozumieniu z podmiotem. |
|  | Transition Software | Art. 32 ust.4, Art.35, ust.4 | 3 główne CSIRTy nie „mogą”, tylko POWINNY się informować wzajemnie o zagrożeniach bezpieczeństwa oraz POWINNY wspomagać merytorycznie inne wzmiankowane podmioty.  POWINNY oznacza nakaz wykonania danej czynności, tj. w tym przypadku ww. wsparcia/współpracy, chyba, że istnieją okoliczności, obiektywnie i wysoce uzasadniające odstąpienie od tych czynności informacyjnych/współpracy (decyduje Kierownik Jednostki Organizacyjnej danego CSIRT, decyzja ta podlega ew. późniejszej analizie/audytowi). | **Uwaga nieuzwględniona**  Taki przepis doprowadziłby do chaosu informacyjnego – CSIRT poziomu krajowego musiałyby informować o każdym cyberzagrożeniu. |
|  | Związek Banków Polskich | Art. 34 ust. 1 | 1)CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT sektorowy i CSIRT Telco oraz SOC i **ISAC** **współpracują między sobą** oraz z organami ścigania i wymiaru sprawiedliwości i służbami specjalnymi przy realizacji ich ustawowych zadań.”;  Włączenie do wymiany również ISAC. Zapewnienie wymiany informacji między sektorami w celu skutecznej obsługi działań zmierzających do wyjaśnienia incydentu. | **Uwaga nieuzględniona**  ISAC nie pełnią funkcji operacyjnej. |
|  | Fundacja Bezpieczna Cyberprzestrzeń | Art. 34a pkt 3 | ten artykuł wprowadza rozmytą odpowiedzialność. Należy odpowiedzialność ustanowić jasno, tzn. sprawozdanie, o którym mowa w tym artykule powinien przygotowywać CSIRT Telco we współpracy z CSIRTami poziomu krajowego | **Wyjaśnienie**  Wynika to z obecnej praktyki, czyli że sprawozdanie przygotowuje i przekazuje Prezes UKE. |
|  | Transition Software | Rozdział 7, Art.37, ust. 1 | Bardzo dobry artykuł. Zapisy należy dodatkowo rozszerzyć, tj. uwzględnić i dodatkowo zapisać wyjęcie również spod zapisów Ustawy o dostępie do informacji publicznej, wykorzystywaną przez dany podmiot infrastrukturę ICT, tj. sprzęt (modele, firmware, numery seryjne, licencje, wersje oprogramowania), stosowane systemy i oprogramowanie infrastrukturalne/usługowe oraz – w szczególności - oczywiście stosowane systemy i oprogramowanie bezpieczeństwa, zarówno te biorące bezpośrednio udział w świadczeniu usługi kluczowej, jak i wchodzące w skład infrastruktury ICT ogólnej, funkcjonującej w ramach organizacji podmiotu, a wspomagającej świadczenie usługi lub tworzącej jej szkielet (minimalizacja ryzyka poprzez minimalizację udzielanych informacji dot. infrastruktury ICT). | **Uwaga nieuwzględniona**  Uwaga nie dotyczy projektowanej ustawy. |
|  | SayF | Art. 39 ust. 5 i 6 | Proponujemy zastąpienie słowa „lub” na „albo”. Warto też się zastanowić, czy jest sens zanonimizowania danych, skoro są już niepotrzebne? | **Uwaga nieuwzględniona**  Uwaga nie dotyczy projektowanej ustawy. |
|  | SayF | Art. 39 ust. 9 | Warto przeanalizować Czy zapisy w tym ustępie nie są powielone przez ustawę o ochronie danych osobowych oraz RODO? jeżeli tak to proponujemy wykreślić | **Uwaga nieuwzględniona**  Uwaga nie dotyczy projektowanej ustawy. |
|  | SayF | Art. 41 | Brak organu odpowiedzialnego za przedsiębiorców komunikacji elektronicznej | **Wyjaśnienie**  Organem regulacyjnym wobec przedsiębiorców komunikacji elektronicznej będzie Prezes Urzędu Komunikacji Elektronicznej |
|  | SayF | Art. 41 pkt 8 i 9 | Brak definicji infrastruktury cyfrowej. | **Uwaga nieuwzględniona**  Uwaga nie dotyczy projektowanej ustawy., w załączniku nr 1 znajduje się pojęcie infrastruktury cyfrowej |
|  | ISSA Polska | Art. 44 ust. 6 pkt 4 | Proponujemy dodać do zapisu nowo proponowanego ustępu 6 artykułu 44 punktu 4)  obecności na wykazie podmiotów realizujących zadania SOC. | **Uwaga nieuwzględniona**  CSIRT sektorowe będą mogły przyjmować zgłoszenia nawet zwykłych incydentów. |
|  | Związek Banków Polskich | Art. 44 ust. 1 | 1. Organ właściwy do spraw cyberbezpieczeństwa zapewnia funkcjonowanie CSIRT sektorowego dla operatorów usług kluczowych w danym sektorze lub podsektorze wymienionym w załączniku nr 1 do ustawy, do którego zadań należy:  1) przyjmowanie zgłoszeń **o incydentach poważnych**;  W aktualnym brzmieniu ustawy mowa jest jedynie o przyjmowaniu przez SZC zgłoszeń o incydentach poważnych.  Jeżeli celem projektowanego przepisu jest zwiększenie ilości incydentów, które będą notyfikowane należy przede wszystkim rozważyć zmianę kryteriów kwalifikowania incydentów jako incydenty poważne lub krytyczne. W innym przypadku dojdzie do powstania szumu informacyjnego, w szczególności poprzez przekazywanie informacji o bardzo drobnych incydentach. | **Uwaga nieuwzględniona**  **Przygotowane zapisy ustawy nie spowodują powstania szumu informacyjnego. CSIRTy będą w stanie skutecznie odsiać otrzymywane informacje. Ponadto im więcej informacji CSIRTy otrzymają tym lepiej będą znać zagrożenia w swoim sektorze.** |
|  | Fundacja Bezpieczna Cyberprzestrzeń | Art. 44 ust. 1 | Należy uzupełnić przepis o obowiązek ustanowienia CSIRT-ów sektorowych np. poprzez dodanie zdanie pierwszego: „Organy właściwe do spraw cyberbezpieczeństwa tworzą CSIRT sektorowe.”. W art. 3 ust. 1 ustawy zamieniającej jest bowiem przepis wskazujący termin na ustanowienie takiego zespołu. Przede wszystkim jednak należy poddać analizie zasadność obowiązkowego powoływania takich zespołów. W uzasadnieniu czytamy bowiem: „Mimo ustawowej możliwości, sektorowe zespoły cyberbezpieczeństwa nie były dotychczas powoływane. Dla podniesienia skuteczności reagowania na incydenty zachodzi konieczność ustanowienia CSIRT sektorowych dla każdego z sektorów. Dzięki temu operatorzy usług kluczowych będą w stanie szybciej i efektywniej radzić sobie z incydentami”. Czy została przeprowadzona analiza jaki był powód niepowoływania zespołów sektorowych oraz analiza rzeczywistego podniesienia skuteczności reagowania na incydenty w przypadku funkcjonowania zespołu sektorowego? Na jakiej podstawie wysunięto wniosek, że dzięki funkcjonowaniu CSIRT sektorowego operatorzy usług kluczowych będą w stanie szybciej i efektywniej radzić sobie z incydentami? W przypadku istnienia takiej analizy naszą uwagę prosimy uznać za nieważną i jednocześnie prosimy o wskazanie wyników tych analiz lub ich źródła. | **Wyjaśnienie**  CSIRT sektorowe efektywnie wspomogą podmioty krajowego systemu cyberbezpieczeństwa w obsłudze incydentów. |
|  | PKN Orlen | Art. 44 ust. 1 | Propozycja zmiany art. 44 ust. 1 Ustawy o KSC jak poniżej:  „ Organ właściwy do spraw cyberbezpieczeństwa zapewnia funkcjonowanie CSIRT sektorowego dla operatorów usług kluczowych w danym sektorze lub podsektorze wymienionym w załączniku nr 1 do ustawy, **a także może ustanowić CSIRT grupy kapitałowej do** których zadań należy:   1. przyjmowanie zgłoszeń o incydentach; 2. reagowanie na incydenty; 3. gromadzenie   informacji o  podatnościach i zagrożeniach, które mogą mieć negatywny wpływ na cyberbezpieczeństwo;   1. współpraca z operatorami usług kluczowych w zakresie wymiany dobrych praktyk oraz informacji o podatnościach i zagrożeniach, organizację i uczestniczenie w ćwiczeniach oraz wspieranie inicjatyw szkoleniowych; 2. współpraca z CSIRT   MON, CSIRT NASK i CSIRT GOV w zakresie wymiany informacji i reagowania na incydenty poważne i krytyczne oraz wymianę informacji o  zagrożeniach. ”,  2. Ponadto w projektowanym:   * art. 44 ust. la) Projektu   należy zastąpić pojęcie: „CSIRT sektorowy”  użytymi w odpowiedniej liczbie i odpowiednim przypadku pojęciami: „CSIRT sektorowy oraz CSIRT grupy kapitałowej”',  art. 44 ust. 5 Projektu należy dodać: „(...) a w przypadku CSIRT grupy kapitałowej podmiotowi wchodzącemu w jej skład, który spełnia warunki o których mowa w art. 44 ust. 6, a także po zasięgnięciu opinii Pełnomocnika. ”  W przypadku zawarcia w krajowym systemie cyberbezpieczeństwa „CSIRT grupy kapitałowej” **niezbędne jest wskazanie sposobu ustanowienia takiego podmiotu.** | **Uwaga nieuwzględniona.**  Nie jest konieczne tworzenie nowego rodzaju CSIRT. Zadania doskonale wypełni podmiot w ramach grupy kapitałowej świadczący usługę SOC dla operatorów usługi kluczowej w ramach grupy kapitałowej. |
|  | Związek Banków Polskich | Art. 44 ust. 1 pkt 5 | 5) współpraca z CSIRT MON, CSIRT NASK i CSIRT GOV **oraz innymi właściwymi CSIRT sektorowymi, a także właściwym ISAC, jeżeli incydent może mieć wpływ na bezpieczeństwo podmiotów danego sektora, sektorów lub podsektorów lub ich klientów,** w zakresie wymiany informacji i reagowania na incydenty poważne i krytyczne oraz wymianę informacji o **podatnościach i** zagrożeniach.”,  Zapewnienie wymiany informacji między sektorami i w ramach sektora. Włączenie CSIRT sektorowego oraz ISAC w proces wymiany informacji z innymi CSIRT. Nadrzędnym celem dla instytucji jest pozyskiwanie wszelkich informacji i wsparcia pochodzącego od innych uczestników krajowego systemu cyberbezpieczeństwa, w tym innych CSIRT sektorowych i ISAC. | **Uwaga częściowo uwzględniona**  Została dodana możliwość współpracy między CSIRT sektorowymi. |
|  | Związek Banków Polskich | Art. 44 po ustępie 1 dodaje się ustęp 1a | „1a. CSIRT sektorowy może, w szczególności:  1)zapewniać dynamiczną analizę ryzyka i incydentów oraz wspomagać w podnoszeniu świadomości zagrożeń cyberbezpieczeństwa;  2)koordynować w uzgodnieniu z operatorami usług kluczowych obsługę incydentów, które dotyczą różnych podmiotów w danym sektorze lub podsektorze.”,  **3)nawiązywać współpracę z innymi CSIRT sektorowymi oraz ISAC w celu wymiany informacji o zagrożeniach i incydentach.**  Wymiana informacji powinna mieć charakter poziomy i pionowy. | **Uwaga nieuwzględniona.**  Współpraca CSIRT sektorowych została ujęta w poprzednim stanowisku. ISAC nie jest jednostką operacyjną. |
|  | Związek Banków Polskich | Art. 44a pkt 5 | 4. Do zadań CSIRT Telco należy:  …..  5)współpraca z CSIRT MON, CSIRT NASK i CSIRT GOV **oraz innymi właściwymi CSIRT sektorowymi, a także właściwym ISAC, jeżeli incydent może mieć wpływ na bezpieczeństwo podmiotów danego sektora, sektorów lub podsektorów lub ich klientów,** w zakresie wymiany informacji i reagowania na incydenty telekomunikacyjne i krytyczne oraz wymianę informacji **o podatnościach** i zagrożeniach.”.  Zapewnienie wymiany informacji między sektorami i w ramach sektora. Włączenie CSIRT sektorowego oraz ISAC w proces wymiany informacji z innymi CSIRT. Nadrzędnym celem dla instytucji jest pozyskiwanie wszelkich informacji i wsparcia pochodzącego od innych uczestników krajowego systemu cyberbezpieczeństwa, w tym innych CSIRT sektorowych i ISAC. | **Uwaga nieuwzględniona**  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 przez ustawę wprowadzającą PKE. |
|  | PKN Orlen | Art. 53 ust. 1 | Propozycja zmiany aktualnego art. 53 ust. 1 punkt 1 Ustawy o KSC, w myśl której w/w przepis miałby następujące brzmienie:  „Nadzór w zakresie stosowania przepisów ustawy sprawują:   1. minister właściwy do spraw informatyzacji w zakresie spełniania przez **podmioty prowadzące SOC,** wymogów, o których mowa w art. 14 ust. 2; (...). ”   Zmiana wynika z zawartej w Projekcie propozycji zastąpienia w art. 4 punkt 16 pojęcia ,podmioty świadczące usługi z zakresu cyberbezpieczeństwa” pojęciem SOC. | **Uwaga uwzględniona** |
|  | SayF | Art. 53 ust 1 pkt 2 | Kto sprawuje nadzór w zakresie przedsiębiorców komunikacji elektronicznej? Wymaga uzupełnienia | **Wyjaśnienie**  Nadzór nad przedsiębiorcami komunikacji elektronicznej sprawuje Prezes UKE.  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. |
|  | ISACA Warsaw Chapter | Art. 62 ust. 1 pkt 6 | Art. 62. 1. W ramach koordynowania działań i realizowania polityki rządu w zakresie zapewnienia cyberbezpieczeństwa do zadań Pełnomocnika należy:  wydawanie rekomendacji dotyczących stosowania urządzeń informatycznych lub oprogramowania na wniosek CSIRT.  Art. 62 ust. 6 upoważnia pełnomocnika do „wydawania  „rekomendacji dotyczących sprzętu lub oprogramowania na wniosek CSIRT MON, CSIRT NASK lub CSIRT GOV”  Cóż ta rekomendacja lub raczej jej brak może oznaczać? Ustawa tego nie reguluje, a powinna. Co gdy podmiot nie zastosuje się do rekomendacji pełnomocnika?  Problem jednak jest dużo poważniejszy. Mamy już bardzo dobrą regulację dotycząca certyfikacji w zakresie cyberbezpieczeństwa. Jest ona budowana w ramach ENISA, oparta miedzy innymi o:  „DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union”  “REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity)”  Ostatni akt ma dwa podstawowe cele:  “objectives, tasks and organisational matters relating to ENISA,  a framework for the establishment of European cybersecurity certification schemes.”  I właśnie schematy certyfikacji cybersecurity powinny być podstawą do klasyfikacji sprzętu, oprogramowania i usług jako bezpieczne.  Dokument ten w artykule 54 mówi:  “54 certification schemes will include at least:  \* 54(1a) Scope (type and categories of ICT products, ICT services and ICT processes),  \* 54(1c) References to international standards”.  Zatem to nie CSIRTy i pełnomonik rządu mają rekomendować produkty, usługi czy procesy, a niezależne podmioty certyfikujące.  Przypomnę obowiązki z tego wynikające dla RP:  “58(1) Each member state shall designate one or more national cybersecurity certification authorities.  62(1) European Cybersecurity Certification Group shall be established, composed by national cybersecurity certification authorities representatives.  58(7a) enforce rules of cybersecurity certification schemes in cooperation with marked surveillance authorities” | **Wyjaśnienie**  Przepis ten dotyczy rekomendacji z art. 33.  Uwaga nie dotyczy nowelizacji ustawy. |
|  | SayF | Art. 65 | Brak CSIRT Telco | **Uwaga uwzględniona** |
|  | SayF | Art. 66 | Czemu w skład kolegium nie wchodzi Prezes Urzędu Komunikacji Elektronicznej? | **Wyjaśnienie**  Przewodniczący Kolegium może zaprosić na posiedzenie Kolegium przedstawicieli instytucji których udział uzna za niezbędny. |
|  | Pracodawcy RP | Art. 66a | 1. **Naruszenie polskich przepisów** 2. Naruszenie prawa konstytucyjnego 3. Zasada proporcjonalności   Proponowane kryteria procedury ocennej, której efektem może być zakaz prowadzenia działalności gospodarczej w Polsce zostały określone w sposób nieprecyzyjny. Przepisy Projektu przyznają Kolegium, które nie jest kompetencyjnie i ustrojowo umocowane, inwazyjną, niczym nieograniczoną, opartą na niejasnych kryteriach, pozbawioną kontroli sądowej kompetencję do prowadzenia jednostronnego postępowania ocennego. Konsekwencje tego postępowania mogą wywrzeć olbrzymi wpływ na sytuację ekonomiczną danego dostawy, ale również operatorów telekomunikacyjnych oraz konsumentów. Postępowanie przed Kolegium do spraw cyberbezpieczeństwa ma się w całości odbywać bez udziału ocenianego dostawcy, który dopiero z komunikatu w Monitorze Polskim dowie się, o przeprowadzonej ocenie. Dlatego też przyjęte rozwiązania legislacyjne są sprzeczne z zasadą proporcjonalności wyprowadzoną z zasady demokratycznego państwa prawnego (Art. 2 Konstytucji). | **Uwaga nieuwzględniona**  Projekt jest zgodny z Konstytucją, która umożliwia ograniczenie prawa swobody działalności gospodarczej ze względu na ważny interes publiczny. |
|  | Pracodawcy RP | Art. 66a | Projektowane przepisy w rażący sposób podważają zaufanie obywateli do Państwa. Projekt zakłada rażąco niekonstytucyjny obowiązek usunięcia z rynku przejawów dotychczasowej działalności dostawcy. W związku z powyższym analizowany zakaz należy poddać kontroli w zakresie zgodności z zasadą lex retro non agit (niedziałania prawa wstecz). W związku z tym, że demokratyczne państwo prawne oznacza państwo w którym chroni się zaufanie obywatela do państwa i stanowionego przez nie prawa, ustawodawca dokonując kolejnych zmian stanu prawnego nie może stracić z pola widzenia interesów podmiotów, jakie ukształtowały się przed dokonaniem zmiany stanu prawnego . | **Uwaga nieuwzględniona**  Projekt jest zgodny z Konstytucją, która umożliwia ograniczenie prawa swobody działalności gospodarczej ze względu na ważny interes publiczny. |
|  | Pracodawcy RP | Art. 66a | **Naruszenie zasady równości wobec prawa**  Projektowane rozwiązania w zakresie wyboru dostawcy sprzętu i oprogramowania sieci 5G pozwalają na arbitralne wykluczenie dostawców z udziału we wdrożeniu sieci 5G w oparciu o dowolne, nieokreślone kryteria. Nie przyznają przy tym dostawcom środków prawnych pozwalających na wniesienie odwołania od decyzji wykluczających. Wobec tego uznać je należy za sprzeczne z konstytucyjnymi zasadami równości wobec prawa (art. 32 Konstytucji). | **Uwaga nieuwzględniona**  Projekt jest zgodny z Konstytucją, która umożliwia ograniczenie prawa swobody działalności gospodarczej ze względu na ważny interes publiczny. |
|  | Pracodawcy RP | Art. 66a | a) Istotne braki przy ocenie skutków regulacji  Zmiany zawarte w projekcie nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa mogą wiązać się z daleko idącymi negatywnymi skutkami społecznymi (likwidacja miejsc pracy, obniżenie dostępności nowoczesnych usług, wzrost wykluczenia cyfrowego), gospodarczymi (obniżenie konkurencyjności polskiej gospodarki, spadek zaufania inwestorów oraz wzmocnienie oligopoli) i politycznymi (uderza w harmonizację europejską oraz relacje międzynarodowe z krajami dotkniętymi sankcjami). Wynika to z konieczności wymiany sprzętu oraz aplikacji, które są obecnie w użyciu, na alternatywne, pochodzące od innych dostawców. Tymczasem w uzasadnieniu Projektu na s. 33 poświęconym skutkom gospodarczym i finansowym w ogóle nie ma o tym mowy. Wspomina się tylko o kosztach związanych z powoływaniem nowych struktur administracyjnych z zakresu cyberbezpieczeństwa (s. 49-52 uzasadnienia Projektu). Jest to istotne naruszenie procesu legislacyjnego (§ 28 Regulamin Pracy Rady Ministrów, t.j. M.P. z 2016 r. poz. 1006) świadczące o niekonstytucyjnym charakterze Projektu. | **Uwaga częściowo uwzględniona**  OSR został uzupełniony. |
|  | Pracodawcy RP | Art. 66a | b) Naruszenie przepisów procedury administracyjnej  W projektowanych przepisach nie przewidziano prawa strony do udziału w postępowaniu ocennym, prowadzonym przez Kolegium. Proponowane rozwiązania naruszają więc podstawowe zasady postępowania administracyjnego wyrażone w ogólnych przepisach Kodeksu postępowania administracyjnego., m.in. zasadę pogłębiania zaufania obywateli do władzy publicznej (art. 8 kpa), zasadę udzielenia informacji przez organ (art. 9), zasadę wysłuchania stron (art. 10). Wprowadzone przepisy naruszają więc podstawowe prawo jednostki do czynnego udziału w postępowaniu. | **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. |
|  | Pracodawcy RP | Art. 66a | **Naruszenie prawa konkurencji w Polsce**  Uregulowanie kwestii wykluczenia dostawców w ustawie KSC narusza również podstawowe zasady prawa konkurencji. Zasady i tryb postępowania w stosunku do pomiotów działających na konkurencyjnym rynku, jeżeli podmioty te naruszają przepisy reguluje inna ustawa tj. ustawa z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów, Dz. U. nr 50, poz. 331 ze zm. Zgodnie z art. 1 ust. 2 tej ustawy, reguluje ona w szczególności zasady i tryb postępowania w stosunku do pomiotów działających na konkurencyjnym rynku, jeżeli podmioty te naruszają przepisy tej ustawy. Oznacza to faktyczne naruszenie przez Kolegium kompetencji właściwego organu administracyjnego, jakim jest Prezes Urzędu Ochrony Konkurencji i Konsumentów. | **Uwaga nieuwzględniona**  Projekt jest zgodny z Konstytucją, która umożliwia ograniczenie prawa swobody działalności gospodarczej ze względu na ważny interes publiczny. |
|  | Pracodawcy RP | Art. 66a | Istotnym argumentem, który należy podnieść jest kwestia obowiązku notyfikacji uregulowanego na poziomie prawa krajowego w Rozporządzeniu Rady Ministrów z dnia 23 grudnia 2002 r. (w szczególności w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych). Przedmiotowy obowiązek jest także uregulowany w Dyrektywie 2015/1535 Parlamentu Europejskiego i Rady z dnia 9 września 2015 r. ustanawiającej procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego. | **Uwaga uwzględniona**  Projekt zostanie notyfikowany. |
|  | Pracodawcy RP | Art. 66a | **Naruszenie praw człowieka regulowane przez EKPC**  ECHR(Europejska konwencja praw człowieka) stwierdza, że: „Każda osoba fizyczna i prawna ma prawo do poszanowania swego mienia. Nikt nie może być pozbawiony swojej własności, chyba że w interesie publicznym i na warunkach przewidzianych przez ustawę oraz zgodnie z ogólnymi zasadami prawa międzynarodowego". | **Uwaga nieuwzględniona**  Projekt jest zgodny z EKPCz. |
|  | Pracodawcy RP | Art. 66a | 1. **Naruszenie zasad TFUE**   Każda ocena ryzyka lub decyzja o wprowadzeniu ograniczeń rynkowych i pozataryfowych barier w handlu na podstawie niejednoznacznych kryteriów (np. kraj pochodzenia dostawców zawarty w projekcie) i nietransparentne procedury administracyjne, naszym zdaniem, są sprzeczne z podstawowymi zasadami równego traktowania/niedyskryminacji, które znajdują odzwierciedlenie w art. 18 (zakaz dyskryminacji ze względu na narodowość), Art. 34 (zakaz ograniczeń ilościowych w przywozie oraz wszystkich środków o skutku równoważnym), Art. 49 (zakaz ograniczeń swobody przedsiębiorczości) TFUE. | **Uwaga nieuwzględniona**  Projekt jest proporcjonalny i zgodny z prawem europejskim. |
|  | Pracodawcy RP | Art. 66a | **d) Naruszenie zasady niedyskryminacji w prawie UE**  Kluczową zasadą praworządności jest to, że prawo musi mieć zastosowanie do wszystkich i być stosowane jednakowo i w sposób konsekwentny. Jest to powtórzone w Karcie Praw Podstawowych Unii Europejskiej (art. 20), w której "każdy jest równy wobec prawa”. Karta (art. 21 ust. 2) zabrania „wszelkiej dyskryminacji ze względu na narodowość”. Europejski Trybunał Sprawiedliwości zauważył, że „zakaz dyskryminacji ustanowiony w prawie UE. jest szczególnym wyrazem ogólnej zasady równości, która jest jedną z podstawowych zasad prawa wspólnotowego”. Jest zatem zgodne z zasadą praworządności, że wymogi bezpieczeństwa powinny być powszechnie stosowane do wszystkich dostawców, a nie dotyczyć wybranych dostawców lub dostawców z określonych krajów. | **Uwaga nieuwzględniona**  Projekt jest proporcjonalny i zgodny z prawem europejskim. |
|  | Pracodawcy RP | Art. 66a | **Naruszenie zasady proporcjonalności określonej przez ETS**  Pkt 13 w sprawie C-331/88 Fedesa odnosi się do zasady proporcjonalności: Po wprowadzeniu środka dyskryminującego Trybunał przyjrzy się proporcjonalności środka w odniesieniu do jego celu. Innymi słowy, środek taki musi być (1) konieczny do osiągnięcia celu i nie może wykraczać poza to, co jest konieczne do osiągnięcia celu, (2) najmniej restrykcyjny środek do osiągnięcia tego celu, oraz (3) spowodowane niedogodności nie mogą być nieproporcjonalne do zamierzonych celów. | **Uwaga nieuwzględniona**  Projekt jest proporcjonalny i zgodny z prawem europejskim. |
|  | Pracodawcy RP | Art. 66a | **Naruszenie zasady swobodnego przepływu towarów**  Zasada ta może być nadal naruszona, nawet jeśli państwo członkowskie nie ustanawia wyraźnego przepisu zakazującego przywozu produktów od niektórych dostawców. Jak wyjaśnił Europejski Trybunał Sprawiedliwości, każdy zakaz używania produktu na terytorium państwa członkowskiego UE wpłynie na zachowanie nabywców i wpłynie na dostęp tego produktu na rynku tego państwa członkowskiego. Przepisy mające na celu odsunięcie określonego dostawcy od łańcucha dostaw w niektórych państwach członkowskich UE powstrzymają potencjalnych klientów przed kupowaniem produktów/technologii danego dostawcy. | **Uwaga nieuwzględniona**  Projekt jest proporcjonalny i zgodny z prawem europejskim. |
|  | Pracodawcy RP | Art. 66a | **Naruszenie postanowień umów międzynarodowych**  Naszym zdaniem ustawodawca koncentruje się na ocenie cech dotyczących dostawców, a nie na bezpieczeństwie sprzętu czy oprogramowania, jakie zapewnia. Jedną z istotnych cech ocenianych w profilu dostawcy jest kryterium pochodzenia dostawcy z danego kraju. Rodzi to zagrożenie, że Polska naruszy umowy międzynarodowe zakazujące dyskryminacji ze względu na pochodzenie. Kryteria powinny opierać się o ustandaryzowane metody weryfikacji i certyfikacji w oparciu o normy międzynarodowe, takie jak normy ISO, branżowe standardy NESAS i europejskie schematy certyfikacji przewidziane w Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. | **Uwaga nieuzwględniona**  Projekt jest zgodny z prawem międzynarodowym.  Porozumienie o Wolnym Handlu GATT w art. XXI pozwala na stosowanie przez strony porozumienia wszelkich działań, jakie uważają one za niezbędne do ochrony swych żywotnych interesów bezpieczeństwa. Projektowane przepisy wpisują się wobec tego w środki opisane w art. XXI GATT. |
|  | Pracodawcy RP | Art. 66a | Istotne braki przy ocenie skutków regulacji oraz negatywne skutki dla gospodarki  Zmiany zawarte w projekcie nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa mogą wiązać się z daleko idącymi negatywnymi skutkami społecznymi (likwidacja miejsc pracy, obniżenie dostępności nowoczesnych usług, wzrost wykluczenia cyfrowego), gospodarczymi (obniżenie konkurencyjności polskiej gospodarki, spadek zaufania inwestorów oraz wzmocnienie oligopoli) i politycznymi (uderza w harmonizację europejską oraz relacje międzynarodowe z krajami dotkniętymi sankcjami). Wynika to z konieczności wymiany sprzętu oraz aplikacji, które są obecnie w użyciu, na alternatywne, pochodzące od innych dostawców. Tymczasem w uzasadnieniu Projektu na s. 33 poświęconym skutkom gospodarczym i finansowym w ogóle nie ma o tym mowy. Wspomina się tylko o kosztach związanych z powoływaniem nowych struktur administracyjnych z zakresu cyberbezpieczeństwa (s. 49-52 uzasadnienia Projektu). Jest to istotne naruszenie procesu legislacyjnego (§ 28 Regulamin Pracy Rady Ministrów, t.j. M.P. z 2016 r. poz. 1006) świadczące o niekonstytucyjnym charakterze Projektu.  W zakresie skutków Projektu na budżet Polski i gospodarkę krajową wskazać należy, iż Projekt będzie miał negatywny wpływ na gotowość podmiotów do składania ofert na pasma częstotliwości 5G. Fakt niemożności wybrania dostawcy sprzętu lub usług odroczy uruchomienie sieci 5G oraz rozwój Przemysłu 4.0. Według analizy wymiarów strat (aktywów, dodatkowych kosztów migracji, zwiększonej niestabilności OPEX oraz sieci), bezpośrednie straty operatorów przekroczą 2,5 mld euro.  Nie bez znaczenia dla polskiej gospodarki pozostaje również fakt, iż wykluczone podmioty gospodarcze będą uprawnione do dochodzenia odszkodowania od Skarbu Państwa. Roszczenia odszkodowawcze operatorów i dostawców wobec Skarbu Państwa zostaną ostatecznie wypłacone przez podatników i konsumentów. Budżet państwa będzie zasilał operatorów i producentów zamiast ułatwiać życie obywatelom, szczególnie po pandemii.  W zakresie skutków społecznych należy opisać wpływ Projektu na likwidację miejsc pracy, obniżenie dostępności nowoczesnych usług, wzrost wykluczenia cyfrowego wynikający z wyższego kosztu usług dla konsumentów i przedsiębiorstw: w szczególności w obszarach pracy zdalnej, zdalnej edukacji, telemedycyny, rozwoju inteligentnych usług samorządowych (smart cities) oraz nowoczesnych rozwiązań w rolnictwie, ochronie środowiska czy energetyce. | **Uwaga częsciowo uwzględniona**  OSR został uzupełniony.  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 przekazanym 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. |
|  | Pracodawcy RP | Art. 66a | 1. Kryteria powinny być neutralne technologicznie, i dotyczyć wyłącznie zagadnień mających rzeczywisty wpływ na bezpieczeństwo podmiotów krajowego systemu cyberbezpieczeństwa:  1) Przedmiotem oceny ryzyka powinien być sprzęt i oprogramowanie uznane za krytyczne (takie jak sieć rdzeniowa 5G, kluczowe systemy kontroli przemysłowej), a nie charakterystyka dostawcy;  2) Kryteria powinny mieć charakter techniczny, być obiektywne, rozsądne i proporcjonalne, oraz opierać się na standardach weryfikacji odpowiednich dla poszczególnych rodzajów sprzętu i oprogramowania, w szczególności normach ISO, branżowych standardach NESAS i europejskich schematach certyfikacji przewidzianych w Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. | **Uwaga nieuwzględniona**  Zgodnie z Toolbox 5G ocena powinna dotyczyć dostawcy i jego powiązań z państwem pochodzenia. |
|  | Polska Izba Handlu | Art. 66a | **Projekt:** brak środków odwoławczych w ramach postępowania administracyjnego  Propozycja zmiany: W Art. 66a Projektu należy dodać nowy ust. 10: „*Postępowanie przed Kolegium prowadzone jest zgodnie z przepisami ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego”*  **Uzasadnienie**  Postanowienia k.p.a. regulują tryb postępowania i wydawanie decyzji przez organy i podmioty państwowe. Obecnie projektowane przepisy odrębnie regulują te kwestie za pomocą zaledwie kilku przepisów, które posiadają charakter proceduralny. Przepisy te nie mogą zastąpić odpowiednich regulacji k.p.a. Uwagi te dotyczą także projektowanego postanowienia w zakresie wymogów jakie elementy powinna zawierać ocena Kolegium (art. 66a ust. 5 Projektu). | **Uwaga uwzględniona**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowanoz oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | PIIT | Art. 66a | 1. Art. 66a  1.1. Art. 66a ust. 1 – uprawnienie Kolegium do dokonania oceny  W myśl projektowanych przepisów organem uprawnionym do dokonywania oceny byłoby Kolegium, które jest działającym przy Radzie Ministrów organem opiniodawczo-doradczym. W jego skład wchodzą przedstawiciele administracji publicznej, tj. Pełnomocnik Rządu ds. Cyberbezpieczeństwa, określeni Ministrowie, Szef BBN, minister koordynator służb specjalnych. Oznacza to, że de facto Kolegium jest w wysokim stopniu gremium polityczno-administracyjnym. W jego składzie brakuje natomiast organów lub jednostek posiadających dogłębną wiedzę techniczną oraz doświadczenie w certyfikacji i ocenie urządzeń i oprogramowania. Takich można szukać dopiero wśród jednostek i organów podległych lub nadzorowanych, których udział w ocenie nie został jednak zaakcentowany w projekcie ustawy.  Postulaty:  • W naszej ocenie niezbędne jest, aby skład Kolegium, przynajmniej na potrzeby dokonywania ocen, o których mowa w art. 66a uzupełniany był o jednostki stricte techniczne, w tym certyfikacyjne, które w oparciu o przyjęte międzynarodowe standardy, mogłyby przedstawiać ocenę techniczno-inżynierską ocenianych dostawców. Jednostki te mogłyby być zarówno laboratoriami publicznymi, jak i prywatnymi niekoniecznie posiadającymi siedzibę na terytorium Polski. Taki element oceny byłby w naszej ocenie korzystny również dla bezpieczeństwa i trwałości samej decyzji, która posiadając wyraźne podstawy techniczne byłaby trudniejsza do późniejszego kwestionowania, w tym ramach ewentualnych postępowań w zakresie roszczeń.  • Należy dodać możliwość zgłoszenia wniosku przez kilku członków Kolegium wspólnie. Zagadnienia w zakresie cyberbezpieczeństwa mają charakter międzysektorowy. W związku z tym, należy dopuścić możliwość składania wniosku, którego inicjatorem może być więcej podmiotów, niż jeden.  • W związku z postulowanym brakiem włączania przedsiębiorców komunikacji elektronicznej do zakresu krajowego systemu cyberbezpieczeństwa, art. 66a ust. 1 należy uzupełnić o odwołanie do przedsiębiorców komunikacji elektronicznej, o których mowa w PKE.  • W zakresie dokonywanych ocen należy uwzględniać także zagrożenia związane z aplikacjami. Warto bowiem zauważyć, że proponowana nowelizacja będzie nakładała na dostawców sprzętu czy operatorów telekomunikacyjnych bardzo wygórowane wymagania i środki wpływu/kontroli, natomiast pomijana jest zupełnie kwestia aplikacji, która ma fundamentalne znaczenie dla cyberbezpieczeństwa. Aplikacje mogą mieć dostęp do GPS/mikrofonu/wiadomości/plików. Już dziś są na rynku aplikacje, które w jawny sposób stosują podsłuch, umożliwiają nagrywanie nie tylko rozmów telefonicznych, ale i całego otoczenia, a same śledzą użytkownika włączając GPS-a. To zagrożenie dla cyberbezpieczeństwa powinno być adresowane w szerszym nawet zakresie niż ryzyko związane z samą siecią.  • Niezbędne jest wprowadzenie przepisu wskazującego, że podmioty zobowiązane do dostosowania się do opinii Kolegium są zwolnione z wszelkiej odpowiedzialności cywilnoprawnej wobec dostawcy, którego urządzenia lub oprogramowanie zostały wskazane w ocenie ryzyka. | **Wyjaśnienie**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3.  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 przekazanym 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. |
|  | PIIT |  | 1.2. Art. 66a ust. 1 – przedmiot oceny  W projektowanym ust. 1 wskazano, że ocena może dotyczyć „ryzyka dostawcy sprzętu lub oprogramowania istotnego dla cyberbezpieczeństwa podmiotów krajowego systemu cyberbezpieczeństwa”.  Poza powyższymi uwagami zauważamy, że przepis nie jest wystarczająco precyzyjny. W szczególności nie jest jasne czy zwrot „istotnego” odnosi się do „ryzyka”, „dostawcy” czy do „sprzętu lub oprogramowania”. W naszej ocenie, powinien on wyraźnie referować do samego sprzętu lub oprogramowania.  Tym samym postulujemy nadanie ust. 1 następującego brzmienia:  1. Kolegium może sporządzić, na wniosek członka lub członków Kolegium, ocenę ryzyka dostawcy dotyczącą sprzętu lub oprogramowania istotnego dla cyberbezpieczeństwa podmiotów krajowego systemu cyberbezpieczeństwa lub przedsiębiorców komunikacji elektronicznej.  Ponadto zakres „istotnego sprzętu lub oprogramowania” powinien być w zakresie sieci telekomunikacyjnych, rozumiany zgodnie z koncepcją „kluczowych aktywów/zasobów” do których referuje 5G Toolbox (essential assets) oraz koncepcją kluczowej infrastruktury, której wykaz należy sporządzić zgodnie z par. 2 pkt 2 rozporządzenia do art. 175d PT także w odniesieniu do sieci 5G. Do tego samego zakresu powinny referować ewentualne restrykcje opisane w dalszej części projektu. W projekcie ustawy należy wyraźnie doprecyzować podstawę na której określany będzie zakres kluczowych zasobów, pod katem których dokonywana jest ocena ryzyka oraz nakładane restrykcje.  W tym kontekście zwracamy bowiem uwagę na konkretne zapisy 5G Toolbox gdzie wskazano, że działanie to ma polegać na:  • SM03 - Ocena profilu ryzyka dostawców i stosowanie ograniczeń dla dostawców uznawanych za obarczonych wysokim ryzykiem - w tym niezbędne wyłączenia w celu skutecznego ograniczenia ryzyka - dla kluczowych aktywów.  o Ustanowić ramy z jasnymi kryteriami, biorąc pod uwagę czynniki ryzyka określone w pkt 2.37 skoordynowanej oceny ryzyka UE i dodając informacje specyficzne dla danego kraju (np. Ocena zagrożenia przeprowadzona przez krajowe służby bezpieczeństwa itp.), Dla właściwych organów krajowych i operatorów sieci ruchomej  o Przeprowadzać rygorystyczne oceny profilu ryzyka wszystkich odpowiednich dostawców na poziomie krajowym i / lub UE (na przykład wspólnie z innymi państwami członkowskimi lub innymi operatorami sieci ruchomej);  o Na podstawie oceny profilu ryzyka zastosować ograniczenia - w tym niezbędne wyłączenia w celu skutecznego ograniczenia ryzyka - dla kluczowych aktywów określonych jako krytyczne lub wrażliwe w skoordynowanym sprawozdaniu z oceny ryzyka UE (np. Funkcje sieci bazowej, funkcje zarządzania siecią i orkiestracji oraz funkcje dostępu do sieci);  o Podjęcie kroków w celu zapewnienia, że operatorzy sieci ruchomej mają odpowiednie mechanizmy kontrolne i procesy zarządzania potencjalnym ryzykiem szczątkowym, takie jak regularne audyty łańcucha dostaw i oceny ryzyka, solidne zarządzanie ryzykiem  Stąd uważamy, że ocena dostawcy nie może być oderwana od oferowanych przez niego urządzeń lub oprogramowania, które mogą lecz nie muszą stanowić kluczowych zasobów/aktywów i tym samym stanowić lub nie stanowić istotnego zagrożenia dla bezpieczeństwa.  Wcześniejsze określenie, np. w rozporządzeniu zakresu aktywów uznawanych za kluczowe byłoby bardzo istotnym narzędziem również dla samych użytkowników, którzy dla takich przypadków mogliby kierować się szczególnymi wymaganiami bezpieczeństwa. Zapewniłoby to również nieporównywalnie większą przewidywalność skutków potencjalnych wykluczeń. | **Wyjaśnienie**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne, tak jak wymaga tego Toolbox 5G. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3.  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 przekazanym 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. |
|  | PIIT | Art. 66a ust 2 i 3 | 1.3. Art. 66a ust. 2 i 3 – zakres oceny i wniosku  W ust. 2 zbyt ogólnie wskazano obligatoryjny zakres wniosku, który de facto mógłby być ograniczony do wskazania, że należy ocenić dostawcę X, który działa w zakresie np. telekomunikacji. Tymczasem spektrum oferowanych urządzeń lub oprogramowania może być tak szerokie, że skutki ewentualnego wydania oceny wobec całości działalności mogą prowadzić do całkowitego zablokowania telekomunikacji w Polsce, w tym w zakresie terminali abonenckich. W przypadku, więc gdyby ocenie miały podlegać urządzenia lub oprogramowanie dla sieci telekomunikacyjnych należałoby wyraźnie wskazać już we wniosku, że ocenie podlega dostawca w zakresie oferowanych urządzeń lub oprogramowania dla sieci 5G Stand Alone, lub core 5G, a nie np. dla sieci 4G, sieci fix, czy terminali abonenckich. Jednocześnie wniosek nie powinien w naszej ocenie pozostawać bez uzasadnienia.  Ponadto warto zauważyć, że projektowany system oceny będzie miał zastosowanie uniwersalne, nie tylko do dotychczas dyskutowanego obszaru sieci 5G, ale także wobec wszelkich innych zastosowań u podmiotów krajowego systemu cyberbezpieczeństwa, w tym operatorów usług kluczowych, tj. m.in. sektora energetyki, finansowego, ochrony zdrowia, wody, transportu. Tym samym brak precyzji wniosku może skutkować tym, że np. wykluczenie dokonane wobec danego dostawcy, będzie potencjalnie uzasadnione wobec jednego sektora, ale w drugim spowoduje istotne, niezbadane i nieoczekiwane reperkusje, które trudno będzie naprawić.  Teoretyczny brak możliwości przedstawienia takich doprecyzowań na etapie wniosku nie powinien być argumentem przeciwko doprecyzowaniu przepisów. Ocena i jej skutki będą potencjalnie bardzo brzemienne w skutkach i nie mogą być realizowane bez odpowiedniego przygotowania, które powinno być wymagane od wszystkich członków Kolegium, a w szczególności od wnioskodawcy.  Docelowo wniosek o wydanie opinii przez Kolegium powinien już w całości przedstawiać zagadnienie do rozstrzygnięcia przez Kolegium.  Postulaty:  • W ust. 2 postulujemy dodanie, jako obligatoryjnych elementów wniosku:  o Identyfikacja urządzeń lub oprogramowania dostawcy, stanowiących kluczowe zasoby/aktywa, które mają podlegać ocenie ryzyka, a w przypadku dokonywania oceny w zakresie sieci lub usług komunikacji elektronicznej wskazanie konkretnych typów sieci i jej warstw lub usług, których ocena ryzyka i jej konsekwencje mają dotyczyć. Podobnie jak w przypadku procedur certyfikacji należy wyraźnie określać, co jest oceniane. Inne ryzyko rodzi wykorzystywanie Security Gateway, inne BTS’a, inne radiolinii, a inne anteny pasywne danego producenta.  o Identyfikacja podmiotów, które wykorzystują lub mogą wykorzystywać urządzenia lub oprogramowanie dostawcy, które mają podlegać ocenie ryzyka, w tym wskazanie czy są to podmioty krajowego systemu cyberbezpieczeństwa czy przedsiębiorcy komunikacji elektronicznej, o których mowa w PKE.  o Identyfikacja poziomu wykorzystania sprzętu lub oprogramowania w realizacji przez przedsiębiorców telekomunikacyjnych obowiązków wynikających ze stanów nadzwyczajnych i stanu wojny.  o Identyfikacja poziomu zobowiązań przedsiębiorców telekomunikacyjnych i użytkowników końcowych wobec dostawcy.  o Identyfikacja innych podmiotów działających na tym samym rynku co oceniany dostawca, w zakresie urządzeń i oprogramowania, w którego zakresie ma zostać dokonana ocena.  o Określenie, jakiego zakresu dotyczy ocena, tj. czy np. powszechnego użycia (usługa masowa) czy np. użycia w określonych systemach czy usługach (np. rejestry państwowe, określone kategorie przemysłu, określone strategiczne lokalizacje).  o Uzasadnienie wniosku, w tym przedstawienie potencjalnych ryzyk związanych z wykorzystaniem urządzeń lub oprogramowania danego dostawcy.  o Identyfikacja zagrożeń w zakresie:  - możliwych obszarów działalności, w których dostawca sprzętu lub oprogramowania może stanowić zagrożenie dla bezpieczeństwa narodowego.  - 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:  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, nieosobowych oraz ochronie prywatności, zwłaszcza tam gdzie nie ma porozumień 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;  - liczbę i rodzaje oraz sposób i czas eliminowania wykrytych podatności i incydentów dotyczących sprzętu lub oprogramowania danego dostawcy;  - stopień, w jakim dostawca sprzętu lub oprogramowania sprawuje nadzór nad procesem wytwarzania, dostarczania i utrzymania sprzętu lub oprogramowania oraz ryzyka dla procesu wytwarzania i dostarczania sprzętu lub oprogramowania;  - treść wydanych wcześniej rekomendacji, o których mowa w art. 33, dotyczących sprzętu lub oprogramowania danego dostawcy.  o Identyfikacja rozwiązań alternatywnych działań w stosunku do sprzętu lub oprogramowania danego dostawcy  o Ocena skutków regulacji zawierająca: identyfikację podmiotów lub grupy podmiotów ponoszących koszty ewentualnej opinii; identyfikację skali działań mających zostać podjętych przez przedsiębiorstwa telekomunikacyjne, podmioty publiczne i użytkowników końcowych, w tym kosztów  o Rekomendacje działań dla Kolegium  - zakładany czas aktualizacji opinii;  - rekomendacje działań dla Kolegium;  - czas wdrożenia do 10 lat;  - proponowany mechanizm refinansowania kosztów przedsiębiorców lub użytkowników, w tym konsumentów.  • Ust. 3 powinien zostać włączony (po dostosowaniu) do ust. 2, jako obligatoryjny element wniosku. Tym samy ust. 3 powinien zostać usunięty. | **Wyjaśnienie**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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.  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 przekazanym 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. |
|  | PIIT | Art. 66a ust.4 | 1.1. Art. 66a ust. 4 – kryteria oceny  Przedstawione kryteria oceny dostawcy wskazują, że ocena będzie dokonywana nie pod kątem technicznych zagrożeń związanych z wykorzystaniem sprzętu lub oprogramowania ocenianego dostawcy, ale pod kątem czynników ogólnych o charakterze potencjalnym i geopolitycznym. Wśród kryteriów brak jest takich, które w jasny sposób odnoszą się do sfery techniki, czy budowanego dorobku w zakresie certyfikacji, zarówno tej ogólnej, jak i tej, która będzie opierana na Cybersecurity Act, gdzie przecież bezpieczeństwo 5G jest jednym z kandydatów do wprowadzenia certyfikacji europejskiej. Decyzja o utrzymaniu takiego kształtu regulacji pozostaje oczywiście w mocy ustawodawcy. Warto jednak zaznaczyć, że ani przepisy, ani uzasadnienie nie odnoszą się do potencjalnej sytuacji, w której ocena ryzyka na poziomie wysokim lub umiarkowanym musiałaby zostać wydana np. wobec dostawcy z kraju UE lub NATO. Wydaje się, więc, że dla zapewnienia niezbędnego obiektywizmu, oraz w celu uniknięcia ryzyka i zarzutu, jaki można postawić projektowanym obecnie przepisom należałoby doprecyzować, jakie skutki i jakie reguły kolizyjne będą stosowane w przypadku wpływu wydania oceny i np. faktycznego zablokowania wymiany handlowej w jakimś zakresie, na prawo międzynarodowe i zawarte umowy, traktaty czy porozumienia.  Postulaty:  • Za zasadne uznajemy (tak jak w pkt 1.1 powyżej) uzupełnienie zakresu oceny o dokonanie weryfikacji technicznej przez certyfikowane w odpowiednim zakresie laboratorium. Taka ocena będzie niezbędna także dla określenia poziomu ryzyka oraz możliwości wdrożenia odpowiednich środków technicznych i organizacyjnych na podstawie art. 66a ust. 5.  • Prowadzona ocena ryzyka powinna zostać skorelowana z istniejącymi już schematami certyfikacji oraz odnosić się do ew. wykrytych niezgodnościami z dokumentacją standaryzacyjną dla danego typu urządzenia (np. 3GPP czy ITU). Ponadto należy w ramach mechanizmów oceny uwzględnić budowany na bazie rozporządzenia Cybersecurity Act system certyfikacji europejskiej, który ma dotyczyć również 5G.  • Badaniu powinien również podlegać wpływ na konkurencję i konsumentów, a także możliwość utrzymania ciągłości usług, systemów i produktów, w których stosowane jest dane oprogramowanie lub urządzenie. Ocenie należy poddać czy wydanie oceny nie będzie skutkowało ograniczeniem możliwości świadczenia usług oraz faktycznym powstaniem na krajowym rynku monopoli lub duopoli oraz związanym z tym realnym ryzykiem dla przedsiębiorstw i konsumentów.  • Obowiązkiem Kolegium powinno być zidentyfikowanie podmiotów, których ocena ryzyka będzie dotyczyła (posiadających lub mogących planować zakup urządzeń lub oprogramowania ocenianego dostawcy) oraz zapoznanie się z ich opinią w sprawie dokonywanej oceny.  • Należy rozważyć, czy w art. 66a ust. 4 nie uzupełnić zakresu o EOG/EFTA. Ponadto, należy odnieść się do faktu, że przynajmniej w zakresie sieci 5G istnieją, jeszcze nieobecni na polskim rynku dostawcy, którzy nie są formalnymi członkami NATO, ale z Sojuszem współpracują w ramach inicjatyw partnerskich. Kwestia ta może mieć fundamentalne znaczenie dla poziomu konkurencyjności rynku. | **Uwaga nieuzwględniona**  Kryteria oceny są zgodne z Toolbox 5G. |
|  | PIIT | Art. 66a ust. 5 | 1.5. Art. 66a ust. 5 – poziomy ryzyka  Projektowany ust. 5 zawiera generalne wytyczne do sposobu określania poziomu ryzyka. Zastosowane sformułowania ogólne, tj. „poważne”, „niewielkie”, „znikome”, a także brak informacji, w jaki sposób ma być dokonywana ocena czy możliwe jest wdrożenie środków technicznych i organizacyjnych w zasadzie uniemożliwiają dokonanie faktycznej oceny przepisu i jego potencjalnych skutków. Wynika to przede wszystkim z faktu, że kryteria te będą mogłyby być bardzo elastycznie stosowane i dopasowywane przez samo Kolegium w toku oceny. Tym samym, wydaje się, że niemal każda decyzja mogłaby w ich świetle znaleźć uzasadnienie formalnie odpowiadające kryteriom.  Postulaty:  • Należy doprecyzować kryteria, np. poprzez odwołanie się kategorii ryzyka wystąpienia incydentów o określonych poziomach istotności, w tym ciągłości działania lub naruszenia bezpieczeństwa danych u podmiotów krajowego systemu cyberbezpieczeństwa oraz przedsiębiorstw komunikacji elektronicznej.  • Wnioskujmy o dodanie doprecyzowania, które będzie mówiło, iż Kolegium wystawia ocenę ryzyka dostawcy tylko w obszarze, który został przeanalizowany i nie blokuje to możliwości współpracy w innych obszarach z takim dostawcą. Przykładowo np. telefony komórkowe dopuszczone standardami międzynarodowymi albo elementy pasywne jak anteny, światłowody, etc. – nie powinny podlegać restrykcjom. | **Wyjaśnienie**  Zrezygnowano z poziomów ryzyka umiarkowany, niski, brak zidentyfikowanego poziomu ryzyka. |
|  | PIIT | Art. 66a ust.6-8 | * 1. **Art. 66a ust. 6 -8 - forma oceny**   Proponowane rozwiązanie polega na nadaniu ocenie Kolegium formy „Komunikatu” publikowanego w Monitorze Polskim.  Jednocześnie, dostawca w zależności od poziomu oceny ma możliwość przedstawienia środków zaradczych i planu naprawczego (niejasne, czym się faktycznie różnią) albo odwołania. Abstrahując od tego, że dotychczas nieupowszechniona jest praktyka procedury odwoławczej od publikacji Komunikatu w oficjalnym publikatorze (stosowanie KPA, dwuinstancyjność, właściwość sądu) należy szczegółowo rozpatrzyć ewentualne skutki tych środków „negocjacyjnych” i odwoławczych na podmioty obowiązane do stosowania się do treści Komunikatu i poziomu dokonanej oceny. Nie może bowiem dochodzić do sytuacji, w których ocena ryzyka wskazuje na ryzyko wysokie, a więc od publikacji Komunikatu nie jest możliwe np. wdrażanie urządzeń danego dostawcy (co ma swoje skutki organizacyjne, finansowe, techniczne i dla ciągłości usług), ale po rozpatrzeniu odwołania decyzja i treść Komunikatu się zmieniają. Tak doniosłe w skutkach dokumenty muszą być wydawane w formie ostatecznej i w pełni skutecznej.  **Postulaty:**   * Publikowany Komunikat musi mieć formę ostateczną. Wszelkie ustalenia, wymiana stanowisk, negocjacje i badanie stanu faktycznego muszą nastąpić w toku postępowania oceniającego. Finalny Komunikat musi mieć stabilną formułę i być zmieniany wyłącznie w przypadkach szczególnej wagi tj. trybie, o którym mowa w ust. 9. * Odpowiednią dla ogłoszenia oceny formą działania powinna być forma decyzji administracyjnej. * Komunikat powinien określać termin wejścia w życie oceny i jej skuteczności wobec konkretnych podmiotów, o których mowa w art. 66b ust. 1. Termin ten powinien być odpowiedni na dostosowanie się przedsiębiorców do jego treści, tj. być nie krótszy niż 12 miesięcy. * Podmiotem uprawnionym do odwołania od oceny powinien być również podmiot, którego dotyczą jego postanowienia, w tym ewentualnie przedsiębiorca telekomunikacyjny szczególnie, że jego skutki oceny będą dotyczyły w bardzo zbliżonym zakresie. | **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. |
|  | PIIT | 66b ust 1 | 1. **Art. 66b ust. 1 – wysokie ryzyko**   **Postulaty:**   * W zdaniu pierwszym należy odwołać się do daty wejścia w życie Komunikatu, a nie „sporządzenia oceny”. Moment sporządzenia oceny nie jest równoznaczny z upublicznieniem Komunikatu, ani jego wejściem w życie. * W zdaniu pierwszym zwrot „podmioty krajowego systemu cyberbezpieczeństwa” należy uzupełnić o słowa „oraz przedsiębiorcy komunikacji elektronicznej”. * Ocena nie powinna odwoływać się do „usług” które wg wcześniejszych przepisów nie są objęte oceną. * Skutki oceny powinny odnosić się do kluczowych zasobów/aktywów, zgodnie z naszymi wcześniejszymi uwagami. * Pkt 1) powinien otrzymać brzmienie:   „*nie dokonują zakupów sprzętu lub oprogramowania określonych w ocenie danego dostawcy sprzętu lub oprogramowania, z wyjątkiem sytuacji, kiedy dokonanie zakupów lub wdrożeń jest niezbędne dla funkcjonowania ich sieci, infrastruktury lub zapewnienia poziomu jakości oraz ciągłości świadczonych usług zgodnie z zapotrzebowaniem, w tym naprawy awarii lub uszkodzeń oraz następuje to w okresie nie dłuższym niż określony w opinii Kolegium;”.*  Propozycja ma na celu uniknięcie bardzo negatywnych skutków gospodarczych, w których ocena byłaby wydana i weszła w życie po dokonaniu zakupu, ale przed wdrożeniem, które jest procesem ciągłym i długotrwałym. Po drugie dokonywanie pewnych zakupów lub wdrożeń (aktualizacja oprogramowania, dokończenie procesu inwestycyjnego) jest konieczne dla utrzymania ciągłości świadczenia usług, przynajmniej w okresie wyznaczonym na dokonanie całkowitej wymiany, co miałoby znaczenie gdyby dana ocena miała zastosowanie do wykorzystywanego już sprzętu lub urządzeń. Jeśli byłoby to konieczne, o takich zakupach lub wdrożeniach podmiot mógłby informować Kolegium, natomiast samo ich dopuszczenie jest niezbędne.   * Pkt 2) powinien otrzymać brzmienie:   „*wycofują z użytkowania sprzęt lub oprogramowanie określone w ocenie danego dostawcy sprzętu lub oprogramowania nie później niż w okresie określonym w opinii Kolegium, który nie może być jednak krótszy niż 10 lat od dnia wejścia w życie ogłoszenia komunikatu o ocenie*”.  Przewidziany w pierwotnej propozycji przepisu 5 letni okres na wycofanie jest zdecydowanie krótszy niż podobne rozwiązania przyjmowane w innych krajach, np. we Francji licencje wydawane są na okres do 8 lat, a w Wielkiej Brytanii czas na wycofanie od momentu ogłoszenia decyzji ma wynieść ponad 7 lat. Jednocześnie realne okresy amortyzacji urządzeń są zdecydowanie dłuższe i sięgają okresu 9-10 lat, przy czym to i tak nie odpowiada technicznej użyteczności, która co do zasady jest dłuższa niż okres amortyzacji. Stąd postulujemy przyjęcie okresu 10 letniego, a w każdym przypadku efektywnie nie krótszego niż 8 lat.  Dodatkowo w tym zakresie wyjaśniamy, że praktyczna realizacja opinii Kolegium:   * oznacza przeprowadzenie szerokich plac analitycznych oraz planistycznych po stronie przedsiębiorców telekomunikacyjnych, w zakresie przygotowania procedury wyboru nowego dostawcy i wdrożenia nowych elementów sieciowych lub oprogramowania **– niezbędny jest czas na wdrożenie opinii!**; * oznacza przeprowadzenie procedury przetargowej i dodatkowych negocjacji przeprowadzenia wyboru nowego dostawcę sprzętu lub oprogramowania **– niezbędny jest czas na wdrożenie opinii!**; * oznacza przeprowadzenie procesu wdrożenia sprzętu lub oprogramowania oraz przeprowadzenia procesu odtwarzania dodatkowych funkcjonalności, w tym dodatkowych szkoleń pracowników **– niezbędny jest czas na wdrożenie opinii!**; * istnieje ryzyko kumulacji przetargów zmiany dostawcy sprzętu lub oprogramowania po stronie wielu przedsiębiorców telekomunikacyjnych (w kraju i za granicą), przekraczających możliwości dostawców w danym okresie i w konsekwencji opóźnienia   **– niezbędny jest czas na wdrożenie opinii!**; * istnieje ryzyko kumulacji działań po stronie dostawców przedsiębiorców telekomunikacyjnych w zakresie integracji nowego sprzętu lub oprogramowania, co będzie powodować opóźnienia **– niezbędny jest czas na wdrożenie opinii!**; * oznacza poniesienie dodatkowych opłat administracyjnych np. pozwoleń radiowych. Niezbędny jest czas na minimalizowanie nieprzewidzianych obciążeń przedsiębiorców telekomunikacyjnych; * oznacza poniesienie dodatkowej marży dla dostawców „nowego” sprzętu i oprogramowania, którzy będą tworzyć i wykorzystywać presję czasową na przedsiębiorców telekomunikacyjnych **– niezbędny jest czas na wdrożenie opinii!** * oznacza poniesienia dodatkowej marży dla dostawców „starego” sprzętu lub oprogramowania, którzy będą wykorzystywać wszelkie nieprzewidziane działania po stronie przedsiębiorców telekomunikacyjnych **– niezbędny jest czas na wdrożenie opinii!** * oznacza kumulację dodatkowych kosztów przez przedsiębiorców telekomunikacyjnych związanych z utrzymywaniem sprzętu lub oprogramowania „starego” i „nowego” dostawcy, w okresie przejściowym; * w przypadku złożonych usług telekomunikacyjnych na rynku B2B, zmiana dostawcy sprzętu lub oprogramowania oznaczać będzie przeprowadzenia dodatkowych ustaleń z klientami B2B w zakresie integracji; * istnieje uzasadnione ryzyko pogorszenia jakości usług telekomunikacyjnych w okresie przejściowym, co może powodować dodatkowe finansowe reperkusje w stosunku do użytkowników końcowych;   Podsumowując, oceniamy iż istnieje uzasadnione ryzyko, iż zmiana dostawcy sprzętu lub oprogramowania spowoduje kumulację zamówień do dostawców „nowego” sprzętu, co w konsekwencji prowadzić będzie do opóźnień. Z reguły rynek telekomunikacyjny w Polsce w okresie 2 – 3 lat osiąga zdolność techniczną porównywalną do najbardziej wartościowych rynków telekomunikacyjnych (USA, Korea, Niemcy, Wlk Brytania). Czynnik ten musi być brany pod uwagę przy określaniu terminu wdrożenia opinii, w porównaniu do innych bogatszych rynków.  Jednocześnie opinia Kolegium może mieć wpływ na konkurencyjność rynku telekomunikacyjnego, ponieważ przedsiębiorcy telekomunikacyjni w różnym stopniu będą posiadać sprzęt lub oprogramowanie określonego dostawcy. W celu uniknięcia tak dalece idących konsekwencji opinii Kolegium, niezbędne jest zastosowanie wydłużonego czasu na jej realizację. | **Wyjaśnienie**  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest 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.  Zmieniony został 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 został dołączony do ustawy jako załącznik nr 3.  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 przekazanym 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. |
|  | PIIT | Art. 66b ust 2 | * 1. Art. 66b ust. 2 – umiarkowane ryzyko   Postulaty:   * W zdaniu pierwszym należy odwołać się do daty wejścia w życie Komunikatu, a nie „sporządzenia oceny”. Moment sporządzenia oceny nie jest równoznaczny z upublicznieniem Komunikatu ani jego wejściem w życie. * W zdaniu pierwszym zwrot „podmioty krajowego systemu cyberbezpieczeństwa” należy uzupełnić o słowa „oraz przedsiębiorcy komunikacji elektronicznej”. * Ocena nie powinna odwoływać się do „usług” które wg wcześniejszych przepisów nie są objęte oceną. * Skutki oceny powinny odnosić się do kluczowych zasobów/aktywów, zgodnie z naszymi wcześniejszymi uwagami. * Pkt 1) powinien otrzymać brzmienie:   *„nie dokonują zakupów sprzętu lub oprogramowania określonych w ocenie danego dostawcy sprzętu lub oprogramowania”*  Uzasadnienie jak wyżej dla ryzyka wysokiego.   * Pkt 2 powinien otrzymać brzmienie:   *„mogą kontynuować użytkowanie dotychczas posiadanych egzemplarzy sprzętu lub oprogramowania wykorzystywanych przed opublikowaniem komunikatu o ocenie danego dostawcy sprzętu lub oprogramowania, w tym dokonywać zakupów lub wdrożeń jest to niezbędne dla funkcjonowania ich sieci, infrastruktury lubzapewnienia poziomu jakości oraz ciągłości świadczonych usług zgodnie z zapotrzebowaniem, w tym naprawy awarii i uszkodzeń.”*  Uzasadnienie jak wyżej dla ryzyka wysokiego. | **Wyjaśnienie**  Zrezygnowano z umiarkowanego poziomu ryzyka, do procedury zastosowane zostanie KPA. |
|  | Nanocoder | Art. 66a | Przepisy art. 66a niniejszego projektu nie zapewniają pełnych i równych praw dla podmiotów objętych postępowaniem oceniającym ryzyko, które gwarantuje chociażby Kodeks Postępowania Administracyjnego. Niniejsze przepisy nie umożliwiają odwołania się od decyzji kolegium dotyczącej oceny określającej średnie i niskie ryzyko, co jest niedopuszczalne. Nielogicznym jest umożliwienie podmiotom odwołania się jedynie od oceny określającej ryzyko wysokie. Ponadto niespotykanym rozwiązaniem jest fakt, że odwołanie nie zawiesza wykonalności decyzji. Obecne zapisy pozbawiają stronę zainteresowaną obiektywnej i niezależnej ochrony podstawowych praw w postępowaniu | **Uwaga uwzględniona**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | T-Mobile Polska | Art. 66a | **Propozycja zmiany:**  *Art. 66a. 1. Kolegium może sporządzić, na wniosek jednego lub kilku członków Kolegium, ocenę ryzyka dostawcy sprzętu lub oprogramowania istotnego dla cyberbezpieczeństwa podmiotów krajowego systemu cyberbezpieczeństwa.*  **Uzasadnienie:**  Zagadnienia w zakresie cyberbezpieczeństwa mają charakter międzysektorowy. W związku z tym, należy dopuścić możliwość składania wniosku, którego inicjatorem może być więcej podmiotów, niż jeden. | **Wyjaśnienie**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | Signum Edward Kuś Marcin Kuś | Art. 66a ust. 1 | **Przedmiot**  Metody Kontroli Cyberbezpieczeństwa  **Ustawa**  Ustanowienie warunków dla oceny ryzyka  **Uzasadnienie**  Zestaw narzędzi UE dla działań ograniczających ryzyka dotyczy analizy ryzyka dla kluczowych aktywów, a nie wszystkich aktywów.  Podejście UE wymaga wzięcia pod uwagę planu ograniczenia ryzyka celem kontroli realnego, zidentyfikowanego ryzyka a niezakładanego ryzyka. § 2 pkt 13 Rozporządzenia Ministra Cyfryzacji z dnia 22 czerwca 2020 r. w sprawie minimalnych środków technicznych i organizacyjnych (...) przewiduje, że przedsiębiorcy telekomunikacyjni przeprowadzą okresową analizę ryzyka w zakresie naruszenia bezpieczeństwa sieci i podatności  **Przepisy**  Art. 66a ust. 1  **Sugestie**  Ocenę ryzyka przeprowadza się wyłącznie:  1) W odniesieniu do krytycznego sprzętu lub oprogramowania, które stwarzają wysokie ryzyko dla bezpieczeństwa lub integralności kluczowych usług na poziomie krajowym o znaczącym wpływie.  2) , Gdy wystąpiły poważne naruszenia bezpieczeństwa lub podatności, których nie można załagodzić. | **Uwaga nieuwzględniona**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | GBX Soft | Art. 66a ust. 1 | Szczególnie kontrowersyjny w mojej ocenie jest art. 66a, który w ustępie 1 stanowi, że Kolegium może sporządzić, na wniosek członka Kolegium, ocenę ryzyka dostawcy sprzętu lub oprogramowania istotnego dla cyberbezpieczeństwa podmiotów krajowego systemu cyberbezpieczeństwa. Przy czym podejście UE wymaga wzięcia pod uwagę planu ograniczenia ryzyka celem kontroli realnego zidentyfikowanego ryzyka, a nie zakładanego ryzyka. Ust. 13 regulacji z dnia 6 kwietnia 2020 w zakresie minimalnych zasad technicznych i organizacyjnych oraz metod zakłada że spółki telekomunikacyjne przeprowadzą okresową analizę ryzyka w zakresie naruszenia bezpieczeństwa sieci i podatności wykrycia, to wymaga pokrycia większości scenariuszy oceny ryzyka. W związku z powyższym celowym wydaje się wprowadzenie zmiany zapisów, zgodnie z którymi ocenę ryzyka przeprowadza się wyłącznie w odniesieniu do krytycznego sprzętu lub oprogramowania, które stwarzają wysokie ryzyko dla bezpieczeństwa lub integralności kluczowych usług na poziomie krajowym o znaczącym wpływie lub w sytuacji gdy wystąpiły poważne naruszenia bezpieczeństwa lub wysokie podatności, których nie można złagodzić | **Uwaga nieuwzględniona**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | Polsko-Chińska Główna Izba Gospodarcza SinoCham | Art. 66a ust. 1 | **Uzasadnienie:**  1) Zestaw narzędzi UE dla działań ograniczających ryzyka dla skupienia analizy ryzyka na kluczowych aktywach zamiast wszystkich aktywach.  2) Podejście UE wymaga wzięcia pod uwagę planu ograniczenia ryzyka celem kontroli realnego zidentyfikowanego ryzyka a nie zakładanego ryzyka.  3) ust. 13 regulacji z dnia 6 kwietnia 2020 w zakresie minimalnych zasad technicznych i organizacyjnych oraz metod zakłada że spółki telekomunikacyjne przeprowadzą okresową analizę ryzyka w zakresie naruszenia bezpieczeństwa sieci i podatności wykrycia, to wymaga pokrycia większości scenariuszy oceny ryzyka.  **Propozycja zmiany:** Ocenę ryzyka przeprowadza się wyłącznie:  1) W odniesieniu do krytycznego sprzętu lub oprogramowania, które stwarzają wysokie ryzyko dla bezpieczeństwa lub integralności kluczowych usług na poziomie krajowym o znaczącym wpływie.  2) Wystąpiły poważne naruszenia bezpieczeństwa lub wysokie podatności, których nie można złagodzić. | **Uwaga nieuwzględniona**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | Excogitate | Art. 66a ust. 1 | Metody Kontroli Cyberbezpieczeństwa  Ustanowienie warunków dla oceny ryzyka   1. Zestaw narzędzi UE dla działań ograniczających ryzyka dotyczy analizy ryzyka dla kluczowych aktywów, a nie dla wszystkich aktywów. 2. Podejście UE wymaga wzięcia pod uwagę planu ograniczenia ryzyka celem kontroli realnego zidentyfikowanego ryzyka a nie zakładanego ryzyka.   ust. 13 regulacji z dnia 6 kwietnia 2020 w zakresie minimalnych zasad technicznych i organizacyjnych oraz metod zakłada, że spółki telekomunikacyjne przeprowadzą okresową analizę ryzyka w zakresie naruszenia bezpieczeństwa sieci i podatności wykrycia, to wymaga pokrycia większości scenariuszy oceny ryzyka.  Ocenę ryzyka przeprowadza się wyłącznie:   1. W odniesieniu do krytycznego sprzętu lub oprogramowania, które stwarzają wysokie ryzyko dla bezpieczeństwa lub integralności kluczowych usług na poziomie krajowym o znaczącym wpływie.   Wystąpiły poważne naruszenia bezpieczeństwa lub wysokie podatności, których nie można złagodzić | **Uwaga nieuwzględniona**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | KIGEIT | Art. 66a ust. 1 | **Propozycja zmiany**:  **„***Kolegium, a w stosunku do przedsiębiorców komunikacji elektronicznej Prezes UKE, może sporządzić, ~~na wniosek członka Kolegium,~~ ocenę ryzyka ~~dostawcy~~ związaną ze sprzęt~~u~~em lub oprogramowani~~a~~em ~~istotnego dla cyberbezpieczeństwa podmiotów krajowego systemu cyberbezpieczeństwa~~ o znaczeniu krytycznym, decydującym o sposobie zarządzania: przetwarzaniem informacji i przesyłania danych, mechanizmami kryptograficznymi, mechanizmami zarządzania wirtualizacją oraz interfejsami zapewniającymi uprawnionym podmiotom dostęp do przekazów nadawanych lub odbieranych w sieci podmiotów krajowego systemu bezpieczeństwa cybernetycznego. Ocena ta jest dokonywana:*  ***a)*** *po**stwierdzonym istotnym naruszeniu bezpieczeństwa lub integralności usług kluczowych o istotnym wpływie na funkcjonowanie tych usług na poziomie krajowym i spowodowanym przez sprzęt i oprogramowanie danego dostawcy, w zakresie objętym naruszeniem, lub*  ***b)*** *wykryciu wysokiej podatności sprzętu lub oprogramowania zwiększającej istotnie poziom ryzyka wystąpienia naruszenia bezpieczeństwa lub integralności usług kluczowych o istotnym wpływie na funkcjonowanie tych usług na poziomie krajowym, w zakresie objętym wykrytą podatnością i kiedy operator usługi kluczowej, którego dotyczy podatność oraz dostawca tego sprzętu i oprogramowania, poinformują Kolegium lub odpowiednio Prezesa UKE w przypadku przedsiębiorców komunikacji elektronicznej o braku możliwości ograniczenia ryzyka.”*  **Uzasadnienie:**  1) Jak zostało wskazane we wstępie, sektor powszechnych usług komunikacji elektronicznej z uwagi na specyfikę powinien pozostać kompleksowo regulowany w osobnych przepisach jego dotyczących (tj. w ustawie Prawo komunikacji elektronicznej, które zastąpi ustawę Prawo telekomunikacyjne) i poddany kompleksowemu nadzorowi jednego organu regulacyjnego (Prezes Urzędu Komunikacji Elektronicznej - UKE), z zastrzeżeniem realizowanych przez niektórych przedsiębiorców zadań kluczowych z punktu widzenia bezpieczeństwa publicznego, podobnie jak ma to miejsce obecnie. Dlatego proponujemy, by w stosunku do przedsiębiorców telekomunikacyjnych ocenę przeprowadzał Prezes UKE. Rozwiązanie to jest zgodne z postanowieniami tytułu V EKŁE, zatytułowanego „Bezpieczeństwo” (art. 40-41 EKŁE). Zgodnie z motywem 5 EKŁE, celem tej dyrektywy jest stworzenie ram prawnych dla zapewnienia swobody w zakresie dostarczania sieci i usług łączności elektronicznej, podlegających wyłącznie warunkom określonym w niniejszej dyrektywie oraz ograniczeniom zgodnie z art. 52 ust. 1 Traktatu o funkcjonowaniu Unii Europejskiej, a w szczególności środkom podejmowanym w związku z polityką państwową, bezpieczeństwem publicznym oraz zdrowiem publicznym, oraz spójne z art. 52 ust. 1 Karty praw podstawowych Unii Europejskiej. Zgodnie z art. 1 ust. 3 lit c) EKŁE, postanowienia tej dyrektywy pozostają bez uszczerbku dla działań podejmowanych przez państwa członkowskie do celów zachowania porządku publicznego i bezpieczeństwa publicznego oraz obronności. Nie mogą być jednak sprzeczne z art. 1 ust. 3 dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii Europejskiej (Dz. Urz. UE L Nr 194, s. 1), który stanowi, że wymogi dotyczące bezpieczeństwa i zgłaszania incydentów przewidziane w niniejszej dyrektywie nie mają zastosowania do przedsiębiorstw, 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. UE. L Nr 108, str. 33), ani do dostawców usług zaufania, którzy podlegają wymogom art. 19 rozporządzenia (UE) nr 910/2014. Zgodnie więc z tymi przepisami problematyka dotycząca realizacji bezpieczeństwa powinna być uregulowana w odpowiednim akcie prawnym, regulującym rynek sieci i usług łączności elektronicznej, którym obecnie jest ustawa Prawo telekomunikacyjne a przyszłości będzie ustawa Prawo komunikacji elektronicznej.  Organem właściwym na rynku usług łączności elektronicznej w zakresie spraw dotyczących m.in. bezpieczeństwa, zgodnie z art. 192 ust. 1 pkt 9 obowiązującej ustawy Prawo telekomunikacyjne, jest Prezes Urzędu Komunikacji Elektronicznej. Zgodnie z tym przepisem, do zakresu działania Prezesa UKE należy w szczególności wykonywanie obowiązków na rzecz obronności, bezpieczeństwa państwa i porządku publicznego (w tym dział VIIA Bezpieczeństwo i integralność sieci i usług telekomunikacyjnych – art. 175-175e).  Analogiczne rozwiązania przewiduje projekt ustawy Prawo komunikacji elektronicznej. Wprost o kompetencji Prezesa UKE w zakresie zapewnienia bezpieczeństwa publicznej sieci telekomunikacyjnej stanowi art. 375 ust. 2 pkt 5 lit f) PKE. Rozdział 5 PKE zatytułowany jest Bezpieczeństwo sieci i usług oraz zadania i obowiązki na rzecz obronności, bezpieczeństwa państwa i porządku publicznego. W rozdziale 5 znajduje się oddział 1, w którym uregulowane zostały kwestie dotyczące obowiązku stosowania przez przedsiębiorców telekomunikacyjnych środków zapewniających bezpieczeństwo sieci lub usług oraz obowiązku sporządzania planu działań w sytuacjach szczególnych zagrożeń (art. 39-49 PKE). Organem kompetencyjnym w zakresie spraw tam wymienionych jest Prezes UKE. W szczególności to Prezes UKE dokonuje oceny podjętych przez przedsiębiorcę komunikacji elektronicznej środków technicznych i organizacyjnych, o których mowa w art. 39 ust. 2 pkt 2 PKE, kierując się rekomendacjami Agencji Unii Europejskiej do spraw cyberbezpieczeństwa (art. 40 ust. 1 PKE). Następnie, „może, w drodze decyzji, nałożyć na przedsiębiorcę komunikacji elektronicznej obowiązek: 1) zastosowania dodatkowych środków technicznych i organizacyjnych lub 2) w przypadku powstania uzasadnionych wątpliwości co do stosowania właściwych środków bezpieczeństwa, poddania się, na własny koszt, audytowi bezpieczeństwa przeprowadzanemu przez wykwalifikowany, wybrany przez przedsiębiorcę podmiot i udostępnienia Prezesowi UKE wyników takiego audytu” (art. 40 ust. 3 PKE). Szczegółowe wymagania dla podmiotu, który mógłby przeprowadzić wskazany audyt oraz podstawowe obowiązki audytora określa art. 41 PKE. W uzasadnieniu PKE, dotyczącym art. 40 ust. 3 wyjaśniono, że art. 40 ust. 3 pkt 1 PKE stanowi właśnie implementację art. 41 ust. 1 EKŁE, a art. 40 ust. 3 pkt 2 PKE stanowi implementację art. 41 ust. 2 lit b PKE.  Kompetencje Prezes UKE w zakresie dokonywania ocen jest więc zbieżna w zakresie kompetencji z dotychczasowymi postanowieniami obowiązującej ustawy Prawo telekomunikacyjnej, opartej na europejskich dyrektywach w zakresie łączności elektronicznej oraz obowiązujący już EKŁE oraz projektowanej ustawy PKE, stanowiącej wdrożenie do polskiego porządku prawnego EKŁE.  2) Zgodnie z Toolbox 5G, (str. 12)."Ocena profilu ryzyka dostawców i zastosowanie ograniczeń do dostawców uznanych za wysokiego ryzyka — ma następować w odniesieniu do kluczowych aktywów”, projekt nie bierze pod uwagę kategorii aktywów z punktu widzenia bezpieczeństwa, wraz z poziomem wrażliwości i listą kluczowych elementów (kategorie elementów i funkcji). Niewłaściwe jest nakładanie takich samych zobowiązań na wszystkie aktywa.  3) Niezgodność ze środkiem SM03 Toolbox (strony 12 i 21 Toolbox), również dlatego, że przewiduje całościowe wyłączenie dostawcy, np. z wyłączeniem określonego dostawcy. Toolbox 5G SM03 przewiduje możliwość wyłączenia, ale z wyłączeniem dostaw określonej infrastruktury (aktywa kluczowe). Innymi słowy, polskie propozycje zawarte w projekcie wykraczają poza wymagania zawarte w Toolbox’ie | **Uwaga nieuwzględniona**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | KIGEIT | Art. 66a ust 2-3 | **Propozycja** zmiany:  *2. Wniosek o ~~sporządzenie~~ wydanie opinii ~~oceny~~ zawiera wskazanie:*  *1) danych identyfikujących dostawcę sprzętu lub oprogramowania;*  *2) możliwych obszarów działalności, w których ~~dostawca~~ sprzęt~~u~~ lub oprogramowani~~a~~e może stanowić zagrożenie dla bezpieczeństwa narodowego.*  *3) ocena skutków regulacji zawierająca:*  *a) identyfikację podmiotów lub grupy podmiotów ponoszących koszty ewentualnej opinii;*  *b) identyfikacja skali działań mających zostać podjętych przez przedsiębiorstwa komunikacji elektronicznej, podmioty publiczne i użytkowników końcowych, w tym kosztów związanych ze skutkami ewentualnej opinii;*  *c) oczekiwany harmonogram działań;*  *4) rekomendacje działań dla Kolegium lub odpowiednio Prezesa UKE w stosunku do przedsiębiorców komunikacji elektronicznej*  *5) proponowany mechanizm refinansowania kosztów przedsiębiorców komunikacji elektronicznej lub użytkowników końcowych;*  *6) czas wdrożenia nie krótszy niż 10 lat,*  *7) zakładany czas aktualizacji opinii;*  *3. Wniosek o sporządzenie oceny może określać:*  *1) rodzaje sieci telekomunikacyjnych i systemów teleinformatycznych lub produktów, usług i procesów, o których mowa w art. 2 pkt 3e lub,*  *2) kategorie podmiotów wchodzących w skład krajowego systemu cyberbezpieczeństwa*  *- które uwzględnia się przy sporządzeniu oceny ~~dostawcy~~ sprzętu lub oprogramowania.*  **Uzasadnienie:**  Z punktu widzenia bezpieczeństwa sieci i usług głównym źródłem ryzyka są konkretne rozwiązania techniczne oferowane przez tych dostawców. W konsekwencji ocena ryzyka powinna być przeprowadzana dla danego typu sprzętu lub oprogramowania, ale nie charakterystyki dostawcy. Z kolei ocenę bezpieczeństwa dostawcy należy oceniać z punktu widzenia bezpieczeństwa procesu produkcji i zapewnienia ciągłości dostaw.  Należy podkreślić, że na obecnym rynku wielu dostawców funkcjonuje w modelu zintegrowanym pionowo (np. Samsung, Huawei), w którym dostarczane przez nich rozwiązania funkcjonują w różnych obszarach sieci i maja zróżnicowany wpływ na bezpieczeństwo sieci i usług. Przykładowo jeden dostawca może być producentem zarówno terminali użytkownika, jak również inwerterów elektrycznych w instalacjach fotowoltaicznych przy stacjach bazowych, infrastruktury radiowej oraz oprogramowania w sieci szkieletowej. Każdy z tych elementów powinien być oceniany z punktu widzenia roli, jaką pełni w świadczeniu usług telekomunikacyjnych, a nie z punktu widzenia rodzaju dostawcy | **Uwaga nieuwzględniona**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | T-Mobile Polska | Art. 66a ust. 3, 8 | **Propozycja zmiany zakresu wniosku art. 66a ust. 3 [opis w nawiasach ma wyjaśnić cel zapisu]**  *2. Wniosek o sporządzenie oceny zawiera wskazanie:*  ***[cel: identyfikacja dostawcy]***   1. *danych identyfikujących dostawcę sprzętu lub oprogramowania;*   ***[cel: identyfikacja produktu]***   1. *produktu lub grupy produktów dostawcy, w tym obszar ich lokalizacji, realizowanych funkcji w sieciach teleinformatycznych, świadczonych usługach w oparciu sprzęt lub oprogramowanie;*   ***[cel: identyfikacja odbiorców]***   1. *odbiorców sprzętu lub oprogramowania*   ***[cel: identyfikacja poziomu wykorzystywania w sektorze prywatnym i publicznym]***  *3) poziomu wykorzystania sprzętu lub oprogramowania przez przedsiębiorstwa telekomunikacyjne, podmioty publiczne i użytkowników końcowych;*  *5) poziomu wykorzystania sprzętu lub oprogramowania w realizacji przez przedsiębiorców telekomunikacyjnych obowiązków wynikających ze stanów nadzwyczajnych i stanu wojny;*  *4) poziom zobowiązań przedsiębiorców telekomunikacyjnych i użytkowników końcowych wobec dostawcy;*  ***[cel: identyfikacja zagrożeń]***  *6) możliwych obszarów działalności, w których dostawca sprzętu lub oprogramowania może stanowić zagrożenie dla bezpieczeństwa narodowego.*  *7) analizę zagrożeń bezpieczeństwa narodowego o charakterze ekonomicznym, kontrwywiadowczym i terrorystycznym oraz zagrożeń dla realizacji zobowiązań sojuszniczych i europejskich, jakie stanowi dostawca sprzętu i oprogramowania;*  *8) 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, nieosobowych oraz ochronie prywatności, zwłaszcza tam gdzie nie ma porozumień 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;*  *9) liczbę i rodzaje oraz sposób i czas eliminowania wykrytych podatności i incydentów dotyczących sprzętu lub oprogramowania danego dostawcy;*  *10) stopień, w jakim dostawca sprzętu lub oprogramowania sprawuje nadzór nad procesem wytwarzania, dostarczania i utrzymania sprzętu lub oprogramowania oraz ryzyka dla procesu wytwarzania, dostarczania i utrzymania sprzętu lub oprogramowania;*  *11) treść wydanych wcześniej rekomendacji, o których mowa w art. 33, dotyczących sprzętu lub oprogramowania danego dostawcy.*  ***[cel: identyfikacja rozwiązań alternatywnych]***  *12) rozwiązań alternatywnych działań w stosunku do sprzętu lub oprogramowania danego dostawcy*  ***[cel: ocena skutków opinii]***  *13) ocena skutków regulacji zawierająca:*  *a) identyfikację podmiotów lub grupy podmiotów ponoszących koszty ewentualnej opinii;*  *b) identyfikacja skali działań mających zostać podjętych przez przedsiębiorstwa telekomunikacyjne, podmioty publiczne i użytkowników końcowych, w tym kosztów związanych ze skutkami ewentualnej opinii;*  *c) oczekiwany harmonogram działań;*  ***[cel: rekomendowane działania dla Kolegium]***  *14) rekomendacje działań dla Kolegium*  *15) proponowany mechanizm refinansowania kosztów przedsiębiorców telekomunikacyjnych lub użytkowników końcowych;*  *16) czas wdrożenia nie krótszy niż 10 lat,*  *17) zakładany czas aktualizacji opinii;*  Uzasadnienie:  Zgodnie z uwagami przedstawionymi w części ogólnej, wniosek o wydanie opinii powinien już w całości przedstawiać w pełnym wymiarze zagadnienie dla Kolegium, w tym konsekwencje jakie będą związane z podjęciem decyzji przez Kolegium i wdrożeniem w życie jej postanowień.  Uzasadnienia dla przyjęcia okresu „10 lat” na wdrożenie opinii. Praktyczna realizacja opinii Kolegium:   1. oznacza przeprowadzenie szerokich plac analitycznych oraz planistycznych po stronie przedsiębiorców telekomunikacyjnych, w zakresie przygotowania procedur wyboru nowego dostawcy i wdrożenia nowych elementów sieciowych lub oprogramowania; 2. oznacza przeprowadzenia procedur przetargowych i dodatkowych negocjacji oraz przeprowadzenia wyboru nowego dostawcy sprzętu lub oprogramowania; 3. oznacza przeprowadzenie procesu wdrożenia sprzętu lub oprogramowania oraz przeprowadzenia procesu odtwarzania dodatkowych funkcjonalności (tzw. ‘features’), w tym dodatkowych szkoleń pracowników. W tym miejscy zaznaczamy, iż oferta dostawców sprzętu i oprogramowania jest zazwyczaj zróżnicowana w zakresie dostępności różnych funkcjonalności dla operatora. Zazwyczaj dostępność konkretnych funkcjonalności na ‘roadmapach’ poszczególnych dostawców jest na tyle różna, że ponowne ich odtworzenie w sieci operatora – po usunięciu sprzętu innego dostawcy – może zająć nawet kilka lat, a niektóre z funkcjonalności mogą okazać się trwale niedostępne dla operatora, powodując brak możliwości świadczenia niektórych usług; 4. istnieje ryzyko kumulacji przetargów zmiany dostawcy sprzętu lub oprogramowania po stronie wielu przedsiębiorców telekomunikacyjnych (w kraju i za granicą), przekraczających możliwości dostawców w danym okresie i w konsekwencji opóźnienia daleko większe niż standardowo możliwe do akceptacji na rynku; 5. istnieje ryzyko kumulacji działań po stronie dostawców przedsiębiorców telekomunikacyjnych w zakresie integracji nowego sprzętu lub oprogramowania, co będzie powodować opóźnienia; 6. oznacza poniesienie dodatkowych opłat administracyjnych np. konieczność sfinansowania przez operatora opłat związanych z wydaniem nowych pozwoleń radiowych. Niezbędny jest czas na minimalizowanie nieprzewidzianych obciążeń przedsiębiorców telekomunikacyjnych; 7. oznacza poniesienie dodatkowej marży dla dostawców „nowego” sprzętu i oprogramowania, którzy traktując tę sytuację jako szansę rynkową będą podwyższać ceny i wykorzystywać presję czasową na przedsiębiorców; 8. oznacza poniesienia dodatkowej marży dla dostawców „starego” sprzętu lub oprogramowania, którzy będą wykorzystywać wszelkie nieprzewidziane działania po stronie przedsiębiorców telekomunikacyjnych; 9. oznacza kumulację dodatkowych kosztów przez przedsiębiorców telekomunikacyjnych związanych z utrzymywaniem i integracją sprzętu lub oprogramowania „starego” i „nowego” dostawcy, w okresie przejściowym; 10. w przypadku złożonych usług telekomunikacyjnych na rynku B2B, zmiana dostawcy sprzętu lub oprogramowania oznaczać będzie przeprowadzenia dodatkowych ustaleń z klientami B2B w zakresie integracji; 11. istnieje uzasadnione ryzyko pogorszenia jakości usług telekomunikacyjnych w okresie przejściowym, co może powodować dodatkowe finansowe reperkusje w stosunku do użytkowników końcowych; 12. w ramach cyklu życia danego produktu/usługi, zdolność sieci musi być stale rozwijana, przynajmniej pod kątem pojemności, aby zapewnić zdolność do bieżącego reagowania na wzrastające zapotrzebowanie. Oznacza to, iż w okresie przejściowym operator będzie musiał realizować inwestycje z obecnym dostawcą. Wydatek inwestycyjny może mieć związek z np. zakupem dodatkowej pojemności/funkcjonalności, aż do ostatecznego wycofania danego elementu sieciowego. Oznacza to, iż należy rozszerzyć okres 5 lat o dodatkowy czas (tj. w sumie do 8-10 lat), uwzględnić okres amortyzacji funkcjonowania elementu sieciowego, wraz z dodatkową pojemnością/funkcjonalnością, która została zakupiona w pierwszym okresie 5 lat.   Podsumowując, oceniamy iż istnieje uzasadnione ryzyko, iż zmiana dostawcy sprzętu lub oprogramowania spowoduje kumulację zamówień do dostawców „nowego” sprzętu, co w konsekwencji prowadzić będzie do opóźnień i wzrostu cen. Z reguły rynek telekomunikacyjny w Polsce w okresie 2 – 3 lat osiąga zdolność techniczną porównywalną do najbardziej wartościowych rynków telekomunikacyjnych (USA, Korea, Niemcy, Wlk Brytania). Czynnik ten musi być brany pod uwagę przy określaniu terminu wdrożenia opinii, w porównaniu do innych bardziej rozwiniętych rynków.   1. Propozycja uwzględnienie procesu konsultacji   *2a Wniosek przed złożeniem do Kolegium jest konsultowany z przedsiębiorcami telekomunikacyjnymi, stosuje się przepisy o ochronie informacji niejawnych.*  Uzasadnienie:  Z uwagi na daleko idące konsekwencje dla gospodarki, niezbędne jest konsultacja wniosku przed przedłożeniem do Kolegium, aby uwzględnić istotne zagadnienia w procesie decyzyjnym, zwiększyć pewność prawną zaangażowanych stron.  Proponujemy zmianę ust. 8  *8. Dostawca sprzętu lub oprogramowania oraz przedsiębiorca komunikacji elektronicznej, 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 wstrzymuje działań określonych w art. 66b.*  Uzasadnienie:  Koszty wdrożenia opinii Kolegium ponosi dostawca sprzętu lub oprogramowania, ponieważ traci potencjalne przychody z tytułu sprzedaży sprzęty lub oprogramowania. Dodatkowo koszty ponosi też przedsiębiorca telekomunikacyjny, który będzie musiał ponieść dodatkowe koszty związane ze zmianą dostawy sprzętu lub oprogramowania. W związku z tym, zarówno dostawca sprzętu lub oprogramowania oraz przedsiębiorstwa komunikacji elektronicznej ponoszą koszty opinii Kolegium. Oznacza to, iż powinni mieć uprawnienie do weryfikacji decyzji Kolegium. | **Uwaga nieuwzględniona**  Przepisy art. 66a-66c został zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | Związek Cyfrowa Polska | Art. 66a ust. 4 | W art. 66a ust 4 (kryteria oceny ryzyka) dodanie punktów 6 i 7 w brzmieniu:  *6) udział danego dostawcy sprzętu lub oprogramowania przekraczający 50% w:*  *a)krajowym rynku infrastruktury telekomunikacyjnej, w tym w szczególności LTE i 5G*  *b)infrastrukturze sieci telekomunikacyjnych poszczególnych operatorów*  *7) stosowanie rozwiązań uniemożliwiających dywersyfikację, interoperacyjnośći kompatybilność z innymi dostawcami*  *na pozostawienie w sieci już zbudowanej elementów infrastruktury niekrytycznej, pod*  *warunkiem otwarcie interfejsów przez ich dostawców i wycofania elementów infrastruktury*  *krytycznej w celu zastąpienia ich dostawcą o niskim lub zerowym poziomie ryzyka.*  3. Przyznanie Ministrowi właściwemu do spraw informatyzacji, po zasięgnięciu opinii  Kolegium, kompetencji do określania, w drodze rozporządzenia, maksymalnego parytetu udziału jednego dostawcy w sieci publicznej (czyli w skali sieci jednego operatora lub sieci narodowej), przynajmniej w zakresie infrastruktury krytycznej.  4. Wskazanie wprost w art. 66a ust. 7 stosowania otwartych interfejsów dla poszczególnych elementów infrastruktury sieciowej jako środka pozytywnie wpływającego na ocenę ryzyka. | **Uwaga nieuwzględniona**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | Związek Banków Polskich | Art. 66a ust. 4 | Poprawka językowa.  Art. 66a ust. 4  Przy sporządzaniu oceny przeprowadza się w szczególności:  (…) | **Uwaga uwzględniona** |
|  | KIGEIT | art. 66a ust. 4 pkt 1 | **Propozycja** zmiany:  *„4. W ramach 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~~ dany typ sprzętu ~~i~~ lub oprogramowania*”.  **Uzasadnienie:**  Analiza winna mieć charakter przedmiotowy, a nie podmiotowy – dotyczyć samego sprzętu i oprogramowania zamiast ich dostawcy. Pod względem podmiotowym ewentualne zagrożenie jest bardziej uzależnione od tego, kto używa sprzętu w taki sposób, aby stwarzać takie zagrożenie niż od tego, kto ten sprzęt sprzedaje. | **Uwaga nieuwzględniona**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | Polska Izba Handlu | art. 66a ust. 4 pkt 1 | **Propozycja zmiany:** W art. 66a ust. 4 pkt 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”) usunąć słowa „jakie stanowi dostawca sprzętu i oprogramowania”:  *„analizę zagrożeń bezpieczeństwa narodowego o charakterze ekonomicznym, kontrwywiadowczym i terrorystycznym oraz zagrożeń dla realizacji zobowiązań sojuszniczych i europejskich.*  **Uzasadnienie:**  Polska Izba Handlu jako organizacja branżowa współpracująca podmiotami, które na co dzień konkurują ze sobą doskonale rozumie jak ważna jest etyka konkurencji. Z drugiej strony zachowanie różnorodności tak zakresie obszarów, którymi zajmujemy się bezpośrednio jak i dostawców innych usług z których zarówno handel jak i inne branże będą szeroko korzystać jest niezbędne dla zapobiegania działaniom quasi monopolistycznym.  Jako, że naszym mottem **jest zachowanie różnorodności handlu i usług na rynku wewnętrznym** wierzymy, że zapewnienie równych możliwości prowadzenia walki konkurencyjnej wszystkim podmiotom rynku jest kluczowe dla jego rozwoju. Pozwalamy sobie mieć nadzieję iż jedyne kryteria według jakich oceniane są lub będą oferty to spójność z oczekiwaniami biznesowymi inwestora oraz warunki współpracy, co wynika z zasad swobody prowadzenia działalności gospodarczej. Podsumowując liczymy, że ocena proponowanych rozwiązań oparta będzie na tym czym rozwiązania są, a nie czym mogłby być gbyby korzystano z nich w złej woli, ponieważ żadne usługi ani produkty nie są ze swej natury dobre ani złe. | **Uwaga nieuwzględniona**  Przepisy art. 66a-66c został zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | KIGEIT | Art. 66a ust. 4 pkt 2 | **Propozycja**: przepis powinien zostać usunięty  *~~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)~~*  **Uzasadnienie:**  1) Ocena musi być przeprowadzana na podstawie jasno określonych, jednoznacznych i możliwych do zweryfikowania kryteriów. W przeciwnym razie nie będzie to obiektywna ocena, lecz ocena uznaniowa, bez uzasadnienia merytorycznego, prowadząca do błędnych wniosków;  2) Ocena na podstawie kraju pochodzenia niesie ze sobą istotną dyskryminację;  3) Jest to sprzeczne z przepisami §6 rozporządzenia Prezesa Rady Ministrów z dnia 20 czerwca 2002 r. w sprawie „Zasad techniki prawodawczej” (t.j. Dz.U. z 2016 r., poz. 283 z późniejszymi zmianami): „*Przepisy ustawy redaguje się tak, aby dokładnie i w sposób zrozumiały dla adresatów zawartych w nich norm wyrażały intencje prawodawcy.”* Przepisy prawa winny być tak sformułowane, aby intencje prawodawcy były dokładnie wyrażone adresatom zawartych w nich norm. Projektowane normy naruszają przepisy rozporządzenia, ponieważ są one niezrozumiałe i nie jest możliwe określenie ich treści.  Wiele niepewności i wątpliwości interpretacyjnych przewiduje przykładowo "prawdopodobieństwo wpływu dostawcy sprzętu lub oprogramowania na kraj spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego” – jest niejasne i rodzi następujące pytania:  Jaki stopień prawdopodobieństwa?  Co to znaczy „być pod wpływem państwa”?  Jak należy rozumieć "wpływ" – czy chodzi o politykę, ekonomię itp.?  Czy wpływ państwa powinien zawsze być oceniany negatywnie? | **Uwaga nieuwzględniona**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | GBX Soft | Art. 66a ust. 4 pkt 2-5 | Patrząc dalej, ten sam art. 66a, ust. 4, pkt 2)-5) powinien zawierać jasne, bezstronne i obiektywne kryteria oceny ryzyka. Co gwarantuje poprawność wyników zastosowanych kryteriów oceny, bardziej skuteczne będzie motywowanie dostawców do samodzielnego sprawdzania i składania oświadczeń o wiarygodności.  Kryteria nietechnologiczne są bardzo często nieokreślone i wykorzystują niejasne pojęcia, które są bardzo trudne do zweryfikowania i oceny. W tym wypadku celową wydaje się propozycja ustanowienia wspólnego unijnego mechanizmu certyfikacji dla krytycznego sprzętu i oprogramowania, a także wymaganie od dostawców posiadania oświadczenia o wiarygodności, ustawienia wymagań technicznych lub organizacyjnych dla dostawców sieci telekomunikacyjnej i systemu ICT oraz wprowadzenie odniesienia do modelu niemieckiego. | **Uwaga nieuwzględniona**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | Polska Izba Handlu | art. 66a ust. 4 pkt 2-5 | **Propozycja zmiany: Art. 66a ust. 4 pkt 2-5 otrzymuje następujące brzmienie:**  *„Do sporządzania oceny przeprowadza się analizę sposobu i zakres wdrożenia przez dostawców środków technicznych i organizacyjnych, zwanych dalej „środkami”, w celu zapewnienia bezpieczeństwa lub integralności sieci lub usług, a w szczególności:*  *a)uzyskanie certyfikatu dla sprzętu lub oprogramowania o znaczeniu krytycznym, o którym mowa w art. 66 a ust. 1 KSC*;  *b)posiadanie deklaracji wiarygodności od producentów i dostawców infrastruktury telekomunikacyjnej, która powinna w szczególności zawierać :*  *ba) zobowiązanie producenta lub dostawcy infrastruktury telekomunikacyjnej do współpracy z przedsiębiorcą w zakresie techniki bezpieczeństwa, a w szczególności do wczesnego informowania o nowych produktach, technologiach i aktualizacjach istniejących linii produktów;*  *bb) zapewnienie producenta lub dostawcy infrastruktury telekomunikacyjnej, że żadne informacje pochodzące z jego relacji umownych z przedsiębiorcą nie zostaną przekazane osobom trzecim;*  *bc) obowiązek producenta lub dostawcy infrastruktury telekomunikacyjnej polegający na niezwłocznym poinformowaniu przedsiębiorcy, że nie może już zagwarantować dotrzymania zadeklarowanego zobowiązania;*  *bd) zobowiązanie producenta lub dostawcy infrastruktury telekomunikacyjnej do posługiwania się wyłącznie godnymi zaufania pracownikami przy opracowywaniu i produkcji krytycznych pod względem bezpieczeństwa części infrastruktury telekomunikacyjnej;*  *be) deklaracje gotowości producenta lub dostawcy infrastruktury telekomunikacyjnej do wyrażenia zgody i odpowiedniego wsparcia w zakresie kontroli bezpieczeństwa i analiz penetracyjnych jego produktu w wymaganym zakresie;*  *bf) zapewnienie producenta lub dostawcy infrastruktury telekomunikacyjnej, że produkt, którego dotyczy składana deklaracja, nie posiada celowo wdrożonych wrażliwych pod względem bezpieczeństwa funkcjonalności i że nie zostaną one wbudowane w późniejszym czasie;*  *bg) zobowiązanie producenta lub dostawcy infrastruktury telekomunikacyjnej do niezwłocznego powiadomienia przedsiębiorcy o wszelkich znanych mu lub wykrytych zagrożeniach dla zapewnienia bezpieczeństwa.*  *c)zapewnienie integralności dostarczanych krytycznych składników infrastruktury, a w szczególności:*  *ca) zapewnienie możliwości weryfikacji integralności nabytych składników krytycznych w każdym czasie, począwszy od ich odbioru a skończywszy na uruchomieniu;*  *cb) sprawdzenie w czasie odbioru, czy dane składniki krytyczne nie zostały podczas dostawy zmanipulowane, naruszone lub w inny sposób zmienione.*  *d)prowadzenie monitoringu bezpieczeństwa w celu zidentyfikowania zagrożeń bezpieczeństwa oraz podejmowania środków zapobiegawczych;*  *e)zatrudnianie tylko przeszkolonych specjalistów w obszarach związanych z bezpieczeństwem, posiadających stosowne kompetencje i doświadczenie;*  *f)zapewnienie w odpowiednim zakresie redundacji, wskazanym w procedurze bezpieczeństwa, krytycznych składników infrastruktury;*  *g)uzyskanie przez producenta sprzętu telekomunikacyjnego międzynarodowych lub uznanych przez UE norm bezpieczeństwa cybernetycznego.*  **Uzasadnienie:**  Zaproponowany powyżej model charakteryzuje się obiektywizmem w zakresie weryfikacji kryteriów oraz bardzo wysokim stopniem profesjonalizacji weryfikacji, co zapewnia poprawność wyników stosowanych kryteriów oceny. Kryteria nietechnologiczne są często niezdefiniowane i bardzo trudno jest zweryfikować i ocenić niejasne pojęcia, ale nie powinny odgrywać kluczowej roli, gdyż mogą prowadzić do błędnych wniosków. | **Uwaga nieuwzględniona**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | Excogitate | Art. 66a ust. 4 pkt 2)-5) | Metody Kontroli Cyberbezpieczeństwa  Kryteria oceny ryzyka powinny być obiektywne, jasne i bezstronne   1. Ustalenie obiektywnych i jasnych kryteriów, gwarantujących poprawność wyników zastosowanych kryteriów oceny. 2. Bardziej skuteczne będzie motywowanie dostawców do samodzielnego sprawdzania i składania oświadczeń o wiarygodności.   Kryteria nietechnologiczne są bardzo często nieokreślone i wykorzystują niejasne pojęcia, które są bardzo trudne do zweryfikowania i oceny.   1. Ustanowienie wspólnego unijnego mechanizmu certyfikacji dla krytycznego sprzętu i oprogramowania. 2. Wymaga się od dostawców posiadania oświadczenia o wiarygodności. 3. Ustawienie wymagań technicznych lub organizacyjnych dla dostawców sieci telekomunikacyjnej i systemu ICT.   Wprowadzenie odniesienia do modelu niemieckiego | **Uwaga nieuwzględniona**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | Polsko-Chińska Główna Izba Gospodarcza  SinoCham | Art. 66a ust. 4 pkt 2-5 | **Uzasadnienie:**  1) Ustalenie obiektywnych i jasnych kryteriów, gwarantujących poprawność wyników zastosowanych kryteriów oceny.  2) Bardziej skuteczne będzie motywowanie dostawców do samodzielnego sprawdzania i składania oświadczeń o wiarygodności.  3) Kryteria nietechnologiczne są bardzo często nieokreślone i wykorzystują niejasne pojęcia, które są bardzo trudne do zweryfikowania i oceny.  **Propozycja zmiany:**  1) Ustanowienie wspólnego unijnego mechanizmu certyfikacji dla krytycznego sprzętu i oprogramowania.  2) wymaga się od dostawców posiadania oświadczenia o wiarygodności.  3) Ustawienie wymagań technicznych lub organizacyjnych dla dostawców sieci telekomunikacyjnej i systemu ICT.  4) Wprowadzenie odniesienia do modelu niemieckiego | **Uwaga nieuwzględniona**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | KIGEIT | Art. 66a ust. 4 pkt 2-5 | *„Do sporządzania oceny przeprowadza się analizę sposobu i zakres wdrożenia przez dostawców środków technicznych i organizacyjnych, zwanych dalej „środkami”, w celu zapewnienia bezpieczeństwa lub integralności sieci lub usług, a w szczególności:*  *a)uzyskanie certyfikatu dla sprzętu lub oprogramowania o znaczeniu krytycznym, o którym mowa w art. 66 a ust. 1 KSC*. *Prezes UKE ustala z odpowiednim CSRIT oraz przedsiębiorcami komunikacji elektronicznej świadczącymi usługi w ruchomej publicznej sieci telekomunikacyjnej oraz ich stowarzyszeniami, producentami i dostawcami infrastruktury telekomunikacyjnej oraz ich stowarzyszeniami, listę funkcji i składników sprzętu oraz oprogramowania o znaczeniu krytycznym, w ruchomej publicznej sieci telekomunikacyjnej, którą publikuje na swojej stronie internetowej;*  *b)posiadanie deklaracji wiarygodności od producentów i dostawców infrastruktury telekomunikacyjnej, która powinna w szczególności zawierać;*  *ba) zobowiązanie producenta lub dostawcy infrastruktury telekomunikacyjnej do współpracy z przedsiębiorcą w zakresie techniki bezpieczeństwa, a w szczególności do wczesnego informowania o nowych produktach, technologiach i aktualizacjach istniejących linii produktów;*  *bb) zapewnienie producenta lub dostawcy infrastruktury telekomunikacyjnej, że żadne informacje pochodzące z jego relacji umownych z przedsiębiorcą nie zostaną przekazane osobom trzecim;*  *bc) obowiązek producenta lub dostawcy infrastruktury telekomunikacyjnej polegający na niezwłocznym poinformowaniu przedsiębiorcy, że nie może już zagwarantować dotrzymania zadeklarowanego zobowiązania;*  *bd) zobowiązanie producenta lub dostawcy infrastruktury telekomunikacyjnej do posługiwania się wyłącznie godnymi zaufania pracownikami przy opracowywaniu i produkcji krytycznych pod względem bezpieczeństwa części infrastruktury telekomunikacyjnej;*  *be) deklaracje gotowości producenta lub dostawcy infrastruktury telekomunikacyjnej do wyrażenia zgody i odpowiedniego wsparcia w zakresie kontroli bezpieczeństwa i analiz penetracyjnych jego produktu w wymaganym zakresie;*  *bf) zapewnienie producenta lub dostawcy infrastruktury telekomunikacyjnej, że produkt, którego dotyczy składana deklaracja, nie posiada celowo wdrożonych wrażliwych pod względem bezpieczeństwa funkcjonalności i że nie zostaną one wbudowane w późniejszym czasie;*  *bg) zobowiązanie producenta lub dostawcy infrastruktury telekomunikacyjnej do niezwłocznego powiadomienia przedsiębiorcy o wszelkich znanych mu lub wykrytych zagrożeniach dla zapewnienia bezpieczeństwa.*  *c)zapewnienie integralności dostarczanych krytycznych składników infrastruktury, a w szczególności:*  *ca) zapewnienie możliwości weryfikacji integralności nabytych składników krytycznych w każdym czasie, począwszy od ich odbioru a skończywszy na uruchomieniu;*  *cb) sprawdzenie w czasie odbioru, czy dane składniki krytyczne nie zostały podczas dostawy zmanipulowane, naruszone lub w inny sposób zmienione.*  *d)prowadzenie monitoringu bezpieczeństwa w celu zidentyfikowania zagrożeń bezpieczeństwa oraz podejmowania środków zapobiegawczych;*  *e)zatrudnianie tylko przeszkolonych specjalistów w obszarach związanych z bezpieczeństwem, posiadających stosowne kompetencje i doświadczenie;*  *f)zapewnienie w odpowiednim zakresie redundacji, wskazanym w procedurze bezpieczeństwa, krytycznych składników infrastruktury;*  *g)uzyskanie przez producenta sprzętu telekomunikacyjnego międzynarodowych lub uznanych przez UE norm bezpieczeństwa cybernetycznego, takich jak ISO27001, Common Criteria, Network Equipment Security Scheme, unijny program certyfikacji cyberbezpieczeństwa.*  **Uzasadnienie:**  Zaproponowany powyżej model charakteryzuje się obiektywizmem w zakresie weryfikacji kryteriów oraz bardzo wysokim stopniem profesjonalizacji weryfikacji, co zapewnia poprawność wyników stosowanych kryteriów oceny. Kryteria nietechnologiczne są często niezdefiniowane i bardzo trudno jest zweryfikować i ocenić niejasne pojęcia, ale nie powinny odgrywać kluczowej roli, gdyż mogą prowadzić do błędnych wniosków. | **Uwaga nieuwzględniona**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | Signum Edward Kuś Marcin Kuś | Art. 66a ust. 4 pkt 2-5 | **Przedmiot**  Metody Kontroli Cyberbezpieczeństwa  **Ustawa**  Kryteria oceny ryzyka powinny być obiektywne, jasne i bezstronne  **Uzasadnienie**  Ustalenie obiektywnych i jasnych kryteriów, gwarantujących poprawność wyników zastosowanych kryteriów oceny. Bardziej skuteczne będzie motywowanie dostawców do samodzielnego sprawdzania i składania oświadczeń o wiarygodności. Kryteria nietechnologiczne są bardzo często nieokreślone i wykorzystują niejasne pojęcia, które są bardzo trudne do zweryfikowania i oceny.  **Przepisy**  Art. 66a ust. 4 pkt 2)-5)  **Sugestie**   1. Ustanowienie wspólnego unijnego mechanizmu certyfikacji dla krytycznego sprzętu i oprogramowania. 2. Wymaganie od dostawców posiadania oświadczenia o wiarygodności. 3. Ustawienie wymagań technicznych lub organizacyjnych dla dostawców sieci telekomunikacyjnej i systemu ICT.   Skorzystanie z wzorca modelu niemieckiego | **Uwaga nieuwzględniona**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostałyokreślone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | KIGEIT | art. 66a ust. 5 | **Propozycja zmiany:**  doprecyzowanie definicji w zakresie gradacji ryzyk i usunięcie odniesień do dostawców.  **Przepis art. 66a ust. 5 Projektu otrzymuje następujące brzmienie:**  **„**5.*Sporządzona ~~przez Kolegium~~ ocena ~~ryzyka dostawcy sprzętu lub oprogramowania~~ określa:*  *a) wysokie ryzyko, jeżeli ~~dostawca~~ sprzęt~~u~~ lub oprogramowanie~~a~~ stanowi bardzo poważne zagrożenia dla cyberbezpieczeństwa państwa ~~i zmniejszenie poziomu tego ryzyka przez wdrożenie środków technicznych lub organizacyjnych nie jest możliwe”.~~*  *b) umiarkowane ryzyko, jeżeli ~~dostawca~~ sprzęt~~u~~ lub oprogramowanie~~a~~ stanowi poważne zagrożenie dla cyberbezpieczeństwa państwa a zmniejszenie poziomu tego ryzyka możliwe jest przez wdrożenie środków technicznych lub organizacyjnych, albo*  *c) niskie ryzyko, jeżeli ~~dostawca~~ sprzęt~~u~~ lub oprogramowanie~~a~~ stanowi niewielkie zagrożenie dla cyberbezpieczeństwa państwa, albo*  *d) brak zidentyfikowanego poziomu ryzyka, jeżeli nie stwierdzono zagrożenia dla cyberbezpieczeństwa państwa lub jego poziom jest znikomy.*  **Uzasadnienie**  Niezgodność ze środkiem SM03 Toolbox (strony 12 i 21 Toolbox), dlatego, że przewiduje całościowe wyłączenie dostawcy bez odniesienia do konkretnych „krytycznych aktywów”. Toolbox istotnie przewiduje możliwość wyłączenia, ale to wyłączenie dotyczy określonej infrastruktury. Innymi słowy, polskie propozycje zawarte w projekcie wykraczają poza wymagania zawarte w Toolbox’ie.  Wątpliwości budzi także przyjęta w art. 66a ust. 5 Projektu gradacja ryzyk, a ściśle ich definiowanie. Chodzi o różnicę pomiędzy wysokim ryzykiem a ryzykiem umiarkowanym. W przypadku bowiem obu definicji jest to poważne zagrożenie a różnica polega na tym, że w przypadku wysokiego ryzyka zmniejszenie tego ryzyka nie jest możliwe a w przypadku umiarkowanego jest możliwe. Tymczasem powinny te definicje (art. 66a ust. 5 lit a-b Projektu) różnić się gradacją, tak jak się różnią ryzyka opisane w art. 66a ust. 5 lit b-d Projektu, a nie tym czy można to ryzyko zmniejszyć czy też nie, gdyż należy przyjąć, że zawsze można poziom takiego ryzyka zmniejszyć a przynajmniej powinno się stworzyć możliwość dla dostawcy podjęcia próby jego zmniejszenia. Poważne więc zastrzeżenia budzi przyjęcie z góry założenia, że w przypadku „wysokiego ryzyka” zmniejszenie poziomu tego ryzyka przez wdrożenie środków technicznych lub organizacyjnych nie jest możliwe. W kontekście zaproponowanych zmian polegających na bezpośrednim powiązaniu oceny z dostawcą, po raz kolejny wskazujemy, że analiza powinna mieć charakter przedmiotowy (dotyczyć sprzętu), a nie podmiotowy (dotyczyć charakterystyki samego dostawcy). | **Uwaga nieuwzględniona**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | Signum Edward Kuś Marcin Kuś | Art. 66a ust. 7 | **Przedmiot**  Metody Kontroli Cyberbezpieczeństwa  **Ustawa**  Możliwość zmiany wyniku oceny powinna mieć również zastosowanie do sprzętu lub oprogramowania wysokiego ryzyka.  **Uzasadnienie**  Dostawca sprzętu lub oprogramowania o wysokim ryzyku powinien mieć takie samo prawo i możliwość złożenia wniosku o zmianę oceny, jak dostawca o umiarkowanym i niskim ryzyku  **Przepisy**  Art. 66a ust. 7  **Sugestie**  Dostawca sprzętu lub oprogramowania wysokiego ryzyka może również przedłożyć Kolegium środki zaradcze i plan naprawczy. Jeżeli te środki zaradcze oraz plan naprawczy zostaną zaakceptowane, Kolegium może zmienić ocenę. | **Uwaga nieuwzględniona**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | KIGEIT | art. 66a ust. 7 | **Propozycja zmiany:**  **Art. 66a ust. 7 Projektu** powinien otrzymać następujące brzmienie:  7. *W przypadku określenia wysokiego, umiarkowanego lub niskiego ryzyka, dostawca ~~sprzętu lub oprogramowania~~, którego sprzętu lub oprogramowania dotyczy ~~ta~~ ocena ~~dostawcy sprzętu lub oprogramowania~~, może przedstawić Kolegium lub Prezesowi UKE w przypadku przedsiębiorców komunikacji elektronicznej* *środki zaradcze i plan naprawczy. W przypadku akceptacji tych środków zaradczych i planu naprawczego, Kolegium*, *a w stosunku do przedsiębiorców komunikacji elektronicznej Prezes UKE*,  *zmienia ~~może zmienić~~ ocenę*.  **Uzasadnienie:**  Zmiana art. 66a ust. 7 Projektu jest konsekwencją ewentualnej zmiany art. 66a ust. 5 lit a Projektu. | **Uwaga nieuwzględniona**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | GBX Soft | Art. 66a ust. 7 | Ponadto w odniesieniu do ust. 7 omawianego art. 66a należy podkreślić, że możliwość zmiany wyniku oceny powinno mieć zastosowanie również do sprzętu lub oprogramowania wysokiego ryzyka. Dostawca sprzętu lub oprogramowania o wysokim ryzyku powinien mieć takie samo prawo i możliwość złożenia wniosku o zmianę oceny, jak dostawca o umiarkowanym i niskim ryzyku. Tego rodzaju argumentacja wymagałaby zmiany zapisów, które z wyjątkiem umiarkowanego lub niskiego poziomu ryzyka umożliwią dostawcy sprzętu lub oprogramowania wysokiego ryzyka przedłożenie Kolegium środków zaradczych i planu naprawczego. Jeżeli te środki zaradcze oraz plan naprawczy zostaną zaakceptowane, Kolegium może zmienić ocenę. | **Uwaga częściowo uwzględniona**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | Polska Izba Handlu | Art. 66a ust. 7 | **Propocycja zmiany:**  **Art. 66a ust. 7 Projektu** powinien otrzymać następujące brzmienie:  7. W przypadku określenia wysokiego, umiarkowanego lub niskiego ryzyka, dostawca sprzętu lub oprogramowania, którego sprzętu lub oprogramowania dotyczy ocena dostawcy, może przedstawić Kolegium środki zaradcze i plan naprawczy. W przypadku akceptacji tych środków zaradczych i planu naprawczego, Kolegium zmienia ocenę.  **Uzasadnienie:**  Zmiana art. 66a ust. 7 Projektu jest konsekwencją ewentualnej zmiany art. 66a ust. 5 lit a Projektu. | **Uwaga nieuwzględniona**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | Liquid Systems | Art. 66a ust. 7 | Metody Kontroli Cyberbezpieczeństwa  Możliwość zmiany wyniku oceny powinna mieć zastosowane również do sprzętu lub oprogramowania wysokiego ryzyka.  Dostawca sprzętu lub oprogramowania o wysokim ryzyku powinien mieć takie samo prawo i możliwość złożenia wniosku o zmianę oceny, jak dostawca o umiarkowanym i niskim ryzyku.  Sugestie:  Z wyjątkiem umiarkowanego lub niskiego poziomu ryzyka dostawca sprzętu lub oprogramowania wysokiego ryzyka może również przedłożyć Kolegium środki zaradcze i plan naprawczy. Jeżeli te środki zaradcze oraz plan naprawczy zostaną^ zaakceptowane, Kolegium  może zmienić ocenę. | **Uwaga częściowo uwzględniona**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | Związek Banków Polskich | Art. 66a ust. 8 | **art. 66a ust. 8:** Dostawca sprzętu lub oprogramowania którego dotyczy ocena określająca wysokie ryzyko lub **podmiot krajowego systemu bezpieczeństwa użytkujący sprzęt 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 **w formie decyzji administracyjnej**. Wniesienie odwołania **wstrzymuje działania** określone w art. 66b. **Od decyzji Kolegium przysługuje skarga do sądu administracyjnego.**  Z uwagi na istotne konsekwencje organizacyjne i finansowe (konieczność wycofania użytkowanego sprzętu lub oprogramowania) prawo wniesienia odwołania powinno przysługiwać również podmiotowi użytkującemu taki sprzęt lub oprogramowanie. Wniesienie odwołania powinno wstrzymywać wskazane działania gdyż mogą one wywołać nieodwracalne skutki dla podmiotu krajowego systemu bezpieczeństwa. Postulowane byłoby również wprowadzenie wskazania, iż rozstrzygnięcie kolegium następuje w formie decyzji oraz, iż od takiej decyzji przysługuje odwołanie do sądu, co umożliwiłoby ostateczne rozstrzygnięcie sprawy przez niezależny organ. | **Uwaga uwzględniona**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | Polsko-Chińska Główna Izba Gospodarcza  SinoCham | Art. 66a ust. 8 | **Uzasadnienie:** 1) Prawo odwołania od decyzji kolegium dotyczy tylko oceny określającej wysokie ryzyko, ocena określająca średnie i niskie ryzyko nie zapewnia prawa do odwołania.  2) Odwołanie nie zawiesza wykonalności decyzji  3) Obecne postanowienie upoważnia Kolegium do działania we własnej sprawie, tym samym pozbawia strony zainteresowanej obiektywnej i niezależnej ochrony podstawowych praw stron w postępowaniu.  **Propozycja zmiany:**  1) Ocena określająca średnie i niskie ryzyko powinna również upoważniać do wniesienia odwołania.  2) Wniesienie odwołania powinno zawieszać wykonalność decyzji.  3) Wynik oceny ryzyka może być przedmiotem odwołania do sądu zgodnie z postanowieniami Kodeksu Postępowania Administracyjnego.  4) Wykonalność decyzji powinna zostać zawieszona do czasu prawomocnej decyzji sądu. | **Uwaga częściowo uwzględniona**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | SmartWeb Media | Art. 66a ust. 8 | Negatywne implikacje biznesowe niesie za sobą również projektowana regulacja art. 66a ust. 8 zd. trzecie ustawy o krajowym systemie cyberbezpieczeństwa, w myśl którego wniesienie odwołania nie wstrzymuje działań określonych w art. 66b tejże ustawy, tj. zakazu wprowadzania do użytkowania sprzętu, oprogramowania i usług określonych w ocenie danego dostawcy sprzętu lub oprogramowania oraz obowiązku wycofania z użytkowania sprzętu, oprogramowania i usług określonych w ocenie danego dostawcy sprzętu lub oprogramowania nie później niż 5 lat od dnia ogłoszenia komunikatu o tej ocenie. W celu zapewnienia stabilności gospodarczej, wykonalność decyzji powinna zostać zawieszona do czasu uprawomocnienia się oceny ryzyka | **Uwaga nieuwzględniona**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | KIGEIT | Art. 66a ust. 8 | **Propozycja zmiany:**  „*8. ~~Dostawca sprzętu lub oprogramowania którego dotyczy~~ Od ocen~~a~~y określając~~a~~ej ~~wysokie~~ ryzyko ~~może odwołać się w terminie 14 dni od publikacji komunikatu o sporządzonej ocenie do Kolegium~~ przysługuje wniosek o ponowne rozpatrzenie sprawy; do wniosku tego stosuje się odpowiednio przepisy dotyczące odwołań od decyzji. Kolegium rozpatruje ~~odwołanie~~ wniosek o ponowne rozpatrzenie sprawy w ciągu 2 miesięcy od otrzymania. ~~Wniesienie odwołania nie wstrzymuje działań określonych w art. 66b.~~*  **Uzasadnienie:**  Od rozstrzygnięcia, stanowiącego decyzję administracyjną, powinna być zapewniona możliwość wniesienia środków odwoławczych przez podmiot niezadowolony z rozstrzygnięcia (dokonanej oceny ryzyka sprzętu lub oprogramowania ocenianego dostawcy) do organów sprawujących wymiar sprawiedliwości, niezależnie do jakiej kategorii ryzyka, o którym mowa w art. 66a ust. 5 Projektu dostawca sprzętu lub oprogramowania. Nie powinna być bowiem dokonywana gradacja środków odwoławczych w zależności od tego, czy rozstrzygnięcie (ocena) jest bardziej lub mnie dotkliwa.  Obecna konstrukcja art. 66a ust. 8 Projektu w zakresie środków odwoławczych, pomimo że używa się w tym przepisie słowa „odwołanie”, nie stanowi w istocie odwołania, ale wniosek o ponowne rozpatrzenie sprawy, o którym mowa w art. 127 § 3 KPA. Z uwagi na fakt, że Kolegium nie należy do organów wskazanych w powyższym przepisie, konieczne jest ujęcie wprost odniesienia do przepisów dotyczących odwołań od decyzji, za wyjątkiem przedsiębiorców komunikacji elektronicznej, dla których organem właściwym do rozpatrywania odwołań będzie Prezes UKE.  Ostatnie zdanie winno zostać wykreślone, gdyż pozostaje w sprzeczności z art. 130 § 1 KPA. W praktyce oznaczałoby również, że przewidziane w tym przepisie „odwołanie” nie miałoby żadnego praktycznego znaczenia, skoro pomimo jego wniesienia byłyby podejmowane praktycznie nieodwracalne w swoich skutkach decyzje w zakresie np. wycofania sprzętu z sieci operatora czy utraty kontraktu na sprzedaż infrastruktury telekomunikacyjnej. | **Uwaga częściowo uwzględniona**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | Excogitate | Art. 66a ust.8 | **Mechanizm odwołań od decyzji kolegium**  Zapewnić zakres pełnych i równych praw zgodnie z Kodeksem Postępowania Administracyjnego   1. Prawo odwołania od decyzji kolegium dotyczy tylko oceny określającej wysokie ryzyko, ocena określająca średnie i niskie ryzyko nie zapewnia prawa do odwołania. 2. Odwołanie nie zawiesza wykonalności decyzji   Obecne postanowienie upoważnia Kolegium do działania we własnej sprawie, tym samym pozbawia stronę zainteresowaną obiektywnej i niezależnej ochrony podstawowych praw stron w postępowaniu.   1. Ocena określająca średnie i niskie ryzyko powinna również upoważniać do wniesienia odwołania. 2. Wniesienie odwołania powinno zawieszać wykonalność decyzji. 3. Wynik oceny ryzyka może być przedmiotem odwołania do sądu zgodnie z postanowieniami Kodeksu Postępowania Administracyjnego.   Wykonalność decyzji powinna zostać zawieszona do czasu prawomocnej decyzji sądu. | **Uwaga częściowo uwzględniona**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | Polska Izba Handlu | Art. 66a ust. 8 | **Propozycja:** Przepis art. 66a ust. 8 Projektu otrzymuje brzmienie: „*Dostawcy sprzętu lub oprogramowania, którego dotyczy ocena, przysługuje wniosek do Kolegium o ponowne rozpoznanie sprawy w zakresie oceny. Przepisy działu 2 rozdziału 10 ustawy z dnia 14 czerwca 1960 r. - Kodeks postępowania administracyjnego w zakresie odwołań od decyzji stosuje się odpowiednio. Od decyzji Kolegium wydanej po rozpoznaniu wniosku o ponowne rozpoznanie sprawy przysługuje skarga do Wojewódzkiego Sądu Administracyjnego.*  **Uzasadnienie:**  Od rozstrzygnięcia Kolegium powinna być zapewniona możliwość wniesienia środków odwoławczych przez podmiot niezadowolony z rozstrzygnięcia (dokonanej oceny ryzyka dostawcy) do organów sprawujących wymiar sprawiedliwości, niezależnie do jakiej kategorii ryzyka, o którym mowa w art. 66a ust. 5 Projektu dostawca sprzętu lub oprogramowania. Nie powinna być bowiem dokonywana gradacja środków odwoławczych w zależności od tego, czy rozstrzygnięcie (ocena) jest bardziej lub mnie dotkliwa.  Obecna konstrukcja art. 66a ust. 8 Projektu w zakresie środków odwoławczych, pomimo że używa się w tym przepisie słowa „odwołanie” jest pozorowana, pozbawiająca podstawowych praw podmiotów zainteresowanych weryfikacją dokonanej oceny przez Kolegium w sposób obiektywny i niezależny przez sąd. Przyjęta konstrukcja pozwala na to, że Kolegium będzie „sędzią we własnej sprawie” tj. będzie sprawdzało własną decyzję. W prawie przewidziana jest konstrukcja złożenia wniosku o ponowne rozpoznanie sprawy przez organ, który wydał decyzję, ale zawsze przysługują środki odwoławcze do sądu od takiego ponownego rozpoznania sprawy.  Potwierdzeniem tezy o pozorowanej konstrukcji odwołania, a wręcz o jej fikcyjności jest dodatkowo to, że zgodnie z obecnym brzmieniem art. 66a ust. 8 Projektu, zdanie ostatnie: *Wniesienie odwołania nie wstrzymuje działań określonych w art. 66b.* W praktyce oznacza to więc, że przewidziane w tym przepisie „odwołanie” nie ma żadnego praktycznego znaczenia, skoro pomimo jego wniesienia będą podejmowane praktycznie nieodwracalne w swoich skutkach decyzje w zakresie np. wycofania sprzętu z sieci operatora czy utraty kontaktu na sprzedaż infrastruktury telekomunikacyjnej. | **Uwaga uwzględniona**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | Narodowy Bank Polski | Art. 66a ust. 10 | **Dodanie w projektowanym art. 66a ust. 10 o treści:**  „10. Sporządzana przez Kolegium ocena ryzyka dostawcy sprzętu lub oprogramowania wskazująca wysokie lub umiarkowane ryzyko ma zastosowanie wobec Narodowego Banku Polskiego jedynie w zakresie w jakim nie wywiera wpływu na realizację zadań NBP. Po ogłoszeniu komunikatu, o którym mowa w ust. 6, NBP przekazuje Kolegium informację o ewentualnym ograniczeniu stosowania oceny ryzyka dostawcy sprzętu lub oprogramowania.”. | **Uwaga nieuwzględniona**  Obowiązek wycofania sprzętu lub oprogramowania pochodzących od dostawcy wysokiego ryzyka nie wpływa na konstytucyjną niezależność Narodowego Banku Polskiego. Nie dotyczy jego zadań konstytucyjnych i ustawowych. |
|  | Excogitate | Art. 66b | Operatorzy telekomunikacyjni powinni otrzymać rekompensatę za koszty poniesione w związku z wymianą sprzętu lub oprogramowania, a rekompensatę powinno obliczać się na podstawie wydatków poniesionych na zakup infrastruktury lub oprogramowania, z uwzględnieniem amortyzacji i kosztów usunięcia.  **Uzasadnienie:**  Wprowadzenie przepisów art. 66b Projektu spowoduje oczywiste dla operatorów telekomunikacyjnych koszty, niezawinione przez nich, spowodowane nowymi regulacjami, które to koszty powinny być operatorom zrekompensowane przez Skarb Państwa reprezentowany przez Prezesa UKE. |  |
|  | Business Centre Club | Art. 66b | BCC zwraca uwagę na finansowe konsekwencje projektowanej regulacji art. 66b Noweli Ustawy zarówno w przypadku oceny wysokiego, jak i umiarkowanego ryzyka. Ustawodawca wprowadzając w przypadku oceny wysokiego ryzyka nakaz wycofania z użytkowania sprzętu lub oprogramowania nie później niż w terminie 5 lat od dnia ogłoszenia komunikatu o ocenie, nie uwzględnia realiów biznesowych i technicznych, w tym amortyzacji sprzętu lub oprogramowania, zasad projektowania sieci, jej remontów, konserwacji i usuwania awarii, co często nie będzie możliwe przy użyciu innych części niż części oryginalne, a w przypadku użycia zamienników może się wiązać z utratą gwarancji na sprzęt. Brak możliwości naprawy takiego sprzętu (art. 66b ust. 1 pkt 1)) bądź obowiązek pozbycia się go przed upływem okresu amortyzacji (art. 66b ust. 1 pkt 2)) będzie skutkować w najczarniejszym scenariuszu pogorszenie działania sieci, jej czasowe wyłączenia i spadek przychodów sektora telekomunikacyjnego oraz wzrost cen usług detalicznych. Realny czas eksploatacji/zwrotu inwestycji to 10-12 lat. | **Wyjaśnienie**  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 został dołączony do ustawy jako załącznik nr 3. |
|  | KIGEIT | Art. 66b | **Propozycja: należy dodać ust. 3 oraz 4 w art. 66b po ust. 2:**  *„3. operatorzy telekomunikacyjni otrzymują odszkodowanie za koszty związane z wymianą sprzętu lub oprogramowania;*  *4. rekompensata jest obliczana na podstawie wydatków poniesionych na zakup infrastruktury lub oprogramowania, z uwzględnieniem amortyzacji i kosztów usunięcia. Rekompensata jest wypłacana w ciągu 30 dni przez Prezesa UKE na podstawie dokumentów uzupełniających”*  **Uzasadnienie:**  Wprowadzenie przepisów art. 66b Projektu spowoduje oczywiste dla operatorów telekomunikacyjnych koszty, niezawinione przez nich, spowodowane nowymi regulacjami, które to koszty powinny być operatorom zrekompensowane przez Skarb Państwa reprezentowany przez Prezesa UKE. Zaproponowane regulacje w praktyce oznaczają de facto „wywłaszczenie” operatorów z posiadanego Sprzętu, w tym znaczeniu, że muszą się pozbyć sprzętu wcześniej zakupionego, pomimo, że gdyby nie wprowadzone nowe regulacje mogliby korzystać z tego sprzętu dłużej. W konsekwencji będą musieli ponieść wydatki związane z koniecznością zakupu nowego sprzętu, a ponadto wydatki związane z usuwaniem z sieci istniejącego sprzętu | **Uwaga nieuwzględniona**  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. |
|  | T-Mobile Polska | Art. 66b ust. 1 | **Proponujemy zmianę at. 66b ust. 1**  *Art. 66b. 1. W przypadku sporządzenia oceny ryzyka określającej wysokie ryzyko dostawcy sprzętu lub oprogramowania podmioty krajowego systemu cyberbezpieczeństwa:*  *1) nie wprowadzają do użytkowania sprzętu, oprogramowania i usług określonych w ocenie danego dostawcy sprzętu lub oprogramowania;*  *2) wycofują z użytkowania sprzęt, oprogramowanie i usługi określone w ocenie danego dostawcy sprzętu lub oprogramowania nie później niż czas określony w opinii Kolegium~~; 5 lat od dnia ogłoszenia komunikatu o ocenie~~.*  **Uzasadnienie:**  Czas na wycofanie sprzętu lub oprogramowania ma być określony w opinii Kolegium, ponieważ musi uwzględniać specyficzną sytuację każdego dostawcy sprzętu, przedsiębiorców telekomunikacyjnych oraz użytkowników końcowych | **Uwaga nieuwzględniona**  Zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | Związek Banków Polskich | Art. 66b ust. 1 | Art. 66b. 1. W przypadku sporządzenia oceny ryzyka określającej wysokie ryzyko dostawcy sprzętu lub oprogramowania podmioty krajowego systemu cyberbezpieczeństwa:  1)nie wprowadzają do użytkowania sprzętu, oprogramowania i usług określonych w ocenie danego dostawcy sprzętu lub oprogramowania;  2) **w miarę istnienia możliwości organizacyjnych i finansowych** 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.  Nakazanie podmiotowi krajowego systemu bezpieczeństwa wycofanie sprzętu i oprogramowania naraża go na poniesienie istotnych kosztów finansowych. Biorąc pod uwagę wskazany okres 5 lat na wycofanie sprzętu lub oprogramowania skuteczność wskazanego instrumentu dla zapewnienia cyberbezpieczeństwa wydaje się i tak iluzoryczna. Postulowane byłoby zatem aby wskazany obowiązek był uzależniony od możliwości danego przedsiębiorcy i powiązany np. z planowanymi postępowaniami zakupowymi sprzętu i oprogramowania. | **Uwaga nieuwzględniona**  Zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | S4IT Michał Podgórski | Art. 66b ust. 1 pkt 2 | Okres 5 lat na wymianę sprzętu jest zbyt krótki. Wymiana sprzętu i oprogramowania uznanego za wysoce ryzykowny będzie wiązała się z koniecznością nabycia nowych komponentów i przystosowania ich do obecnej infrastruktury. Należy mieć na uwadze zarówno koszty wymiany sprzętu, jak i przeszkolenia użytkowników.  **Propozycja**  Czas wycofania sprzętu z eksploatacji: 10 lat od daty opublikowania ogłoszenia o uznaniu produktu za wysoce ryzykowny. | **Uwaga częściowo uwzględniona**  Zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | Liquid Systems | Art. 66b ust. 1 pkt 2 | Artykuł 66b doprowadzi do powstania istotnych kosztów dla operatorów telekomunikacyjnych, których nie powinni ponosić, a które powinny być pokryte przez Skarb Państwa.  **Sugestia**:  Operatorzy telekomunikacyjny powinni dostać odszkodowanie za koszty poniesione w związku z wymianą sprzętu lub oprogramowania.  Odszkodowanie to powinno być naliczone na podstawie kosztów poniesionych na zakup infrastruktury i oprogramowania, przy uwzględnieniu amortyzacji oraz kosztu usunięcia. | **Uwaga nieuwzględniona**  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. |
|  | Liquid Systems | Art. 66b ust. 1 pkt 2 | Okres karencji powinien wynosić 10 lat zamiast 5 lat.  Wymiana związana z krytycznym sprzętem i oprogramowaniem będzie wymagała zmiany całego projektu sieci i ogromnej części sieci. Zajmie to dużo czasu, a jakikolwiek pospiech w tym zakresie wpłynie negatywnie na stabilność sieci. Również wysokie koszty przemawiają za rozłożeniem procesu wycofania w dłuższym przedziale czasu.  Sugestie:  Czas wycofania sprzętu: 10 lat od daty opublikowania ogłoszenia o ocenie. | **Uwaga częściowo uwzględniona**  Zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | Polska Izba Handlu | Art. 66b ust. 1 pkt 2 | **Projekt przepisu*:*** *„W przypadku sporządzenia oceny ryzyka określającej wysokie ryzyko określonego krytycznego sprzętu lub oprogramowania podmioty krajowego systemu cyberbezpieczeństwa:*  *1) nie wprowadzają do użytkowania sprzętu, oprogramowania i usług infrastruktury krytycznych określonych w ocenie danego sprzętu lub oprogramowania;*  *2) wycofują z użytkowania sprzęt, oprogramowanie i usługi określone w ocenie danego sprzętu lub oprogramowania nie później niż ~~5~~ 10 lat od dnia ogłoszenia komunikatu o ocenie.”*  **Uzasadnienie**  Pięcioletni okres na wycofanie jest zdecydowanie za krótki i powinien zostać przedłużony do 10 lat, a wymiana powinna odnosić się do określonego sprzętu i oprogramowaniu zamiast do dostawcy. Konstrukcja wycofywania sprzętu z użytkowania wywołuje poważne wątpliwości z uwagi na obowiązywanie jednej z kardynalnych zasad prawa, tj. zasady „niedziałania prawa wstecz”. Przepis nakazujący wycofywanie sprzętu zakupionego wiele lat wcześniej stanowi objęcie regulacją zdarzeń wcześniejszych, sprzed kilku lat, które dotyczyły zawierania umów o zakup sprzętu w oparciu o obowiązujące wówczas przepisy. Tym bardziej więc powinien być uwzględniony postulat wycofywania sprzętu z użytkowania | **Uwaga częściowo uwzględniona**  Zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | Polska Izba Handlu | Art. 66b sekcja 1 pkt 2 | **Propozycja: należy dodać ust. 3 oraz 4 w art. 66b po ust. 2:**  *3. operatorzy telekomunikacyjni otrzymują odszkodowanie za koszty związane z wymianą sprzętu lub oprogramowania;*  *4. rekompensata jest obliczana na podstawie wydatków poniesionych na zakup infrastruktury lub oprogramowania, z uwzględnieniem amortyzacji i kosztów usunięcia. Rekompensata jest wypłacana w ciągu 30 dni przez Prezesa UKE na podstawie dokumentów uzupełniających*  **Uzasadnienie:**  Wprowadzenie przepisów art. 66b Projektu spowoduje oczywiste dla operatorów telekomunikacyjnych koszty, niezawinione przez nich, spowodowane nowymi regulacjami, które to koszty powinny być operatorom zrekompensowane przez Skarb Państwa reprezentowany przez Prezesa UKE. Zaproponowane regulacje w praktyce oznaczają de facto „wywłaszczenie” operatorów z posiadanego Sprzętu, w tym znaczeniu, że muszą się pozbyć sprzętu wcześniej zakupionego, pomimo, że gdyby nie wprowadzone nowe regulacje mogliby korzystać z tego sprzętu dłużej. W konsekwencji będą musieli ponieść wydatki związane z koniecznością zakupu nowego sprzętu, a ponadto wydatki związane z usuwaniem z sieci istniejącego sprzętu. | **Uwaga nieuwzględniona**  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. |
|  | S4IT Michał Podgórski | Art. 66b ust. 1 i ust. 2 | **Postulowane wprowadzenie rekompensat.**  Artykuł 66b doprowadzi do powstania istotnych kosztów dla operatorów telekomunikacyjnych, których nie powinni ponosić, spowodowanych nowymi regulacjami, które powinny być pokryte przez Skarb Państwa reprezentowany przez Prezesa UKE.  **Propozycja:**  Przedsiębiorcy telekomunikacyjni powinni otrzymać odszkodowanie z tytułu poniesionych kosztów wymiany sprzętu lub oprogramowania. | **Uwaga nieuwzględniona**  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. |
|  | Polsko-Chińska Główna Izba Gospodarcza SinoCham | Art. 66b ust. 1 pkt 2 | **Przepisy projektu:** brak przepisów dotyczących mechanizmu rekompensat  **Propozycja zmiany:** należy dodać ust. 3 oraz 4 w art. 66b po ust. 2.:  „3. Operatorzy telekomunikacyjni otrzymują odszkodowanie za koszty związane z wymianą sprzętu lub oprogramowania;   1. Rekompensata jest obliczana na podstawie wydatków poniesionych na zakup infrastruktury lub oprogramowania, z uwzględnieniem amortyzacji i kosztów usunięcia. Rekompensata jest wypłacana w ciągu 30 dni przez Prezesa UKE na podstawie dokumentów uzupełniających.”   **Uzasadnienie:** Wprowadzenie przepisów art. 66b Projektu spowoduje oczywiste dla operatorów telekomunikacyjnych koszty, niezawinione przez nich, spowodowane nowymi regulacjami, które to koszty powinny być operatorom zrekompensowane przez Skarb Państwa reprezentowany przez Prezesa UKE. Zaproponowane regulacje w praktyce oznaczają de facto „wywłaszczenie” operatorów z posiadanego sprzętu, w tym znaczeniu, że muszą się pozbyć sprzętu wcześniej zakupionego, pomimo, że gdyby niewprowadzone nowe regulacje mogliby korzystać z tego sprzętu dłużej. W konsekwencji będą musieli ponieść wydatki związane z koniecznością zakupu  nowego sprzętu, a ponadto wydatki związane z usuwaniem z sieci istniejącego sprzętu. | **Uwaga nieuwzględniona**  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. |
|  | Signum Edward Kuś Marcin Kuś | Art. 66b ust. 1 pkt 2 | **Przedmiot**  Metody Kontroli Cyberbezpieczeństwa  **Ustawa**  Okres karencji powinien wynosić 10 lat zamiast 5 lat  **Uzasadnienie**  Wymiana związana z krytycznym sprzętem i oprogramowaniem będzie wymagała zmiany całego projektu sieci i ogromnej części sieci. Zajmie to dużo czasu, a wszelki pośpiech negatywnie wpłynie to na stabilność sieci. Również koszty zmiany będą bardzo wysokie. Dlatego powinny zostać rozłożone w dłuższym okresie czasu.  **Przepisy**  Art. 66 b ust. 1 pkt 2  **Sugestie**  Czas wycofania sprzętu z eksploatacji: 10 lat od daty opublikowania ogłoszenia o ocenie. | **Uwaga częściowo uwzględniona**  Zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | Excogitate | art. 66b ust. 1 pkt 2: „Konsekwencje oceny” | **Przepisy projektu**: brak zapisów dotyczących mechanizmu rekompensat  Propozycja zmiany: należy dodać ust. 3 oraz 4 w art. 66b po ust. 2.:  „3. Operatorzy telekomunikacyjni otrzymują odszkodowanie za koszty związane z wymianą sprzętu lub oprogramowania;  4. Rekompensata jest obliczana na podstawie wydatków poniesionych na zakup infrastruktury lub oprogramowania, z uwzględnieniem amortyzacji i kosztów usunięcia. Rekompensata jest wypłacana w ciągu 30 dni przez Prezesa UKE na podstawie dokumentów uzupełniających.”  **Uzasadnienie:** Wprowadzenie przepisów art. 66b Projektu spowoduje oczywiste dla operatorów telekomunikacyjnych koszty, niezawinione przez nich, spowodowane nowymi regulacjami, które to koszty powinny być operatorom zrekompensowane przez Skarb Państwa reprezentowany przez Prezesa UKE. Zaproponowane regulacje w praktyce oznaczają de facto „wywłaszczenie” operatorów z posiadanego sprzętu, w tym znaczeniu, że muszą się pozbyć sprzętu wcześniej zakupionego, pomimo, że gdyby niewprowadzone nowe regulacje mogliby korzystać z tego sprzętu dłużej. W konsekwencji będą musieli ponieść wydatki związane z koniecznością zakupu nowego sprzętu, a ponadto wydatki związane z usuwaniem z sieci istniejącego sprzętu. | **Uwaga nieuwzględniona**  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 |
|  | KIGEIT | Art. 66b ust. 1 pkt 1 i ust. 2 pkt 1 | **Propozycja zmiany:** wykreślenie  *„Art. 66b. 1. W przypadku sporządzenia oceny ryzyka określającej wysokie ryzyko ~~dostawcy~~ określonego krytycznego sprzętu lub oprogramowania podmioty krajowego systemu cyberbezpieczeństwa:*  *~~1) nie wprowadzają do użytkowania sprzętu, oprogramowania i usług określonych w ocenie danego dostawcy sprzętu lub oprogramowania;~~*  *(…)*  *2. W przypadku sporządzenia oceny określającej umiarkowane ryzyko dostawcy sprzętu lub oprogramowania podmioty krajowego systemu cyberbezpieczeństwa:*  *~~1) nie wprowadzają do użytkowania sprzętu, oprogramowania i usług określonych w ocenie danego dostawcy sprzętu lub oprogramowania;~~*  **Uzasadnienie:**  Niezmiernie istotne jest uwzględnienie faktu, iż w przypadku kilkuletniego procesu wycofywania sprzętu, oprogramowania i usług określonego dostawcy (wskazanego w pkt 2)) niezbędne będzie realizowanie procesów utrzymaniowych istniejącego sprzętu w tym okresie. Procesy utrzymaniowe mogą m.in. obejmować niezbędną wymianę sprzętu na stacjach bazowych (uszkodzonego w wyniku awarii, wandalizmu, zjawisk atmosferycznych itp.) lub instalację nowego oprogramowania niezbędnego dla funkcjonowania sieci (np. adresującego zidentyfikowane luki w zakresie bezpieczeństwa lub możliwość korzystania z nowych urządzeń sieciowych w bezpieczny sposób), czy też zwiększenie pojemności danego sprzętu.  Jednocześnie podmioty, na których będzie ciążył obowiązek wycofania sprzętu, oprogramowania i usług danego dostawcy w ciągu 5 (lub 10 – jak postulujemy) lat nie będą miały ekonomicznego interesu w zwiększaniu współpracy z danym dostawcom powyżej niezbędnego minimum.  W konsekwencji postulujemy wykreślenie niniejszego punktu w całości.  Gdyby uwaga Izby nie została rozpatrzona pozytywnie, alternatywnym – jednakże dużo mniej elastycznym i nie w pełni przystającym do wieloletniego okresu wycofywania sprzętu, oprogramowania i usług – rozwiązaniem byłoby poniższe doprecyzowanie niniejszego punktu:  *„1) nie wprowadzają do użytkowania sprzętu, oprogramowania i usług określonych w ocenie danego dostawcy sprzętu lub oprogramowania, z wyjątkiem sytuacji niezbędnych dla realizacji funkcji utrzymania oraz niezbędnego rozwoju istniejącego sprzętu, oprogramowania i usług, w odpowiedzi na zgłaszane zapotrzebowanie;”* | **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. |
|  | KIGEIT | Art. 66b ust. 1 pkt 2 | Projekt przepisu*: „Art. 66b. 1. W przypadku sporządzenia oceny ryzyka określającej wysokie ryzyko ~~dostawcy~~ określonego krytycznego sprzętu lub oprogramowania podmioty krajowego systemu cyberbezpieczeństwa:*  *2) wycofują z użytkowania sprzęt, oprogramowanie i usługi określone w ocenie danego ~~dostawcy~~ sprzętu lub oprogramowania na obszarze gmin określonych jako najbardziej istotne dla funkcjonowania krajowego systemu cyberbezpieczeństwa nie później niż ~~5~~ 10 lat od dnia ogłoszenia komunikatu o ocenie.”*  **Uzasadnienie**  Ze względu na to, iż obowiązek wycofania sprzętu z użytkowania stanowi poważną ingerencję w swobodę prowadzenia działalności gospodarczej powinien być on ograniczony jedynie do obszarów gmin, które mogą mieć strategiczne znaczenie dla funkcjonowania krajowego systemu cyberbezpieczeństwa, np. obszarów poligonów wojskowych, kluczowych węzłów komunikacyjnych np. lotnisk, terenów związanych z wytwarzaniem i magazynowaniem energii elektrycznej, miejsc składowania rezerw żywności itp.  Należy podkreślić, że obowiązek wycofania sprzętu z użytkowania nie powinien mieć zastosowania do obszarów gmin, gdzie w zdecydowanej przewadze prowadzona jest działalność cywilna, w tym gospodarcza. Obszary te nie mają istotnego znaczenia dla funkcjonowania krajowego systemu cyberbezpieczeństwa.  W konsekwencji pożądanym jest stworzenie listy gmin najbardziej istotnych dla funkcjonowania krajowego systemu cyberbezpieczeństwa, do której będą odnosić się obowiązki wycofania z użytkowania sprzętu, oprogramowania i usług dostawców wysokiego ryzyka. Lista ta może podlegać okresowym przeglądom weryfikującym jej aktualność.  Pięcioletni okres na wycofanie jest zdecydowanie za krótki i powinien zostać przedłużony do 10 lat, a wymiana powinna odnosić się do określonego sprzętu i oprogramowania zamiast do dostawcy.  Typowy okres eksploatacyjny aktywnej infrastruktury telekomunikacyjnej wynosi co najmniej 7 lat kalendarzowych. Okres 7-letni jest również przyjmowany na potrzeby księgowe jako czas życia aktywów radiowych na potrzeby wyznaczenia odpisów amortyzacyjnych (mimo, iż w praktyce często są one wykorzystywane również po upływie tego okresu). Jednakże amortyzacji będzie podlegał również dodatkowy sprzęt, który został zakupiony w okresie do 7 roku, którego czas amortyzacji będzie wykraczał poza okres 7 letni. Dlatego wskazane jest przyjęcie okresu 10 lat.  Okres 7-letni na wycofanie z użytkowania sprzętu i oprogramowania danego dostawcy jest również wskazywany w rozwiązaniach regulacyjnych stosowanych na rynkach międzynarodowych, w szczególności w Wielkiej Brytanii.  Konstrukcja wycofywania sprzętu z użytkowania wywołuje poważne wątpliwości z uwagi na obowiązywanie jednej z kardynalnych zasad prawa, tj. zasady „niedziałania prawa wstecz”. Przepis nakazujący wycofywanie sprzętu stanowi objęcie regulacją zdarzeń wcześniejszych, sprzed kilku lat, które dotyczyły zawierania umów o zakup sprzętu w oparciu o obowiązujące wówczas przepisy. Tym bardziej więc powinien być uwzględniony postulat przedłużenia okresu wycofywania sprzętu z użytkowania | **Uwaga nieuwzględniona**  Podmioty krajowego systemu cyberbezpieczeństwa, będą musiały wycofać sprzęt lub oprogramowanie od dostawcy wysokiego ryzyka w terminie do 7 lat**.** |
|  | Excogitate | Art. 66c section 1 | Metody Kontroli Cyberbezpieczeństwa  Okres na dostarczenie planu wycofania wynosi 1 rok zamiast 3 miesięcy. Okres 3 miesięcy dla przygotowania i przedstawienia planu i harmonogramu dla wycofania z infrastruktury dostawcy usług sprzętu i oprogramowania w jest praktycznie niemożliwy do wdrożenia.  Okres przygotowania i przedstawienia planu oraz harmonogramu powinien został wydłużony do jednego roku. | **Wyjaśnienie**  Zrezygnowano z planów wycofania sprzętu lub oprogramowania. |
|  | T-Mobile Polska | Art. 66c ust. 1 | **Proponujemy zmianę art. 66c ust. 1**  *Art. 66c 1. W szczególnie uzasadnionych przypadkach Pełnomocnik może zobowiązać podmiot krajowego systemu cyberbezpieczeństwa, do którego zastosowanie ma ocena, do sporządzenia i dostarczenia w ciągu 6~~3~~ miesięcy planu i harmonogramu wycofania z użytkowania sprzętu, oprogramowania i usług dostawcy sprzętu lub oprogramowania, którego dotyczy ocena określająca wysokie ryzyko.*  *2. Plan i harmonogram podlega zatwierdzeniu przez Pełnomocnika po uzgodnieniu z organem właściwym dla danego sektora, a w przypadku przedsiębiorcy komunikacji elektronicznej z Prezesem UKE.*  *3. Zmiana planu i harmonogramu wymaga zatwierdzeniu przez Pełnomocnika po uzgodnieniu z organem właściwym dla danego sektora, a w przypadku przedsiębiorcy komunikacji elektronicznej z Prezesem UKE*  **Uzasadnienie:**  Okres 3 miesięcy jest zbyt krótkim okresem, aby opracować plan i harmonogram planofwanych zmian, w szczególności, gdy plan/harmonogram będzie w przyszłości podstawą weryfikacji działań prowadzonych przez przedsiębiorców telekomunikacyjnych, którzy uzależnienie są od podmiotów zewnętrznych „starego” i „nowego” dostawcy. | **Wyjaśnienie**  Zrezygnowano z planów wycofania sprzętu lub oprogramowania. |
|  | Excogitate | art. 66c pkt. 1 “Plan naprawczy” | **Przepis projektu:** W szczególnie uzasadnionych przypadkach Pełnomocnik może zażądać od podmiotu krajowego systemu cyberbezpieczeństwa, którego dotyczy ocena, sporządzenia i dostarczenia w terminie 3 miesięcy planu i harmonogramu odstąpienia od dostawcy usługi, sprzętu lub oprogramowania, którego dotyczy ocena określająca wysokie ryzyko.  Propozycja zmiany: cyfrę i słowo „3 miesięcy” zastępuje się cyfrą i słowem „1 roku”, skreślić „dostawca” tak, aby plan dotyczył konkretnego sprzętu i oprogramowania zamiast dostawcy. „W szczególnie uzasadnionych przypadkach Pełnomocnik może zażądać od podmiotu krajowego systemu cyberbezpieczeństwa, którego dotyczy ocena, do sporządzenia i dostarczenia w terminie 1 roku planu i harmonogramu odstąpienia od usługi, sprzętu lub oprogramowania, którego dotyczy ocena określająca wysokie ryzyko.”  **Uzasadnienie:** Okres 3 miesięcy na sporządzenie i przedstawienie planu oraz harmonogramu odstąpienia od sprzętu i oprogramowania usługodawcy jest praktycznie niemożliwy do zrealizowania. Jednocześnie, jak zostało wskazanie powyżej, wszelkie środki związane z oceną powinny być stosowane do oprogramowania i do sprzętu, a nie w stosunku do dostawcy. | **Wyjaśnienie**  Zrezygnowano z planów wycofania sprzętu lub oprogramowania. |
|  | Polsko-Chińska Główna Izba Gospodarcza SinoCham | Art. 66c pkt 1 | **Przepis projektu:** W szczególnie uzasadnionych przypadkach Pełnomocnik może zażądać od podmiotu krajowego systemu cyberbezpieczeństwa, którego dotyczy ocena, sporządzenia i dostarczenia w terminie 3 miesięcy planu i harmonogramu odstąpienia od dostawcy usługi, sprzętu lub oprogramowania, którego dotyczy ocena określająca wysokie ryzyko.  **Propozycja zmiany:** cyfrę i słowo „3 miesięcy” zastępuje się cyfrą i słowem „1 roku", skreślić „dostawca" tak, aby plan dotyczył konkretnego sprzętu i oprogramowania zamiast dostawcy. „W szczególnie uzasadnionych przypadkach Pełnomocnik może zażądać od podmiotu krajowego systemu cyberbezpieczeństwa, którego dotyczy ocena, do sporządzenia i dostarczenia w terminie 1 roku planu i harmonogramu odstąpienia od usługi, sprzętu lub oprogramowania, którego dotyczy ocena określająca wysokie ryzyko.”  **Uzasadnienie:** Okres 3 miesięcy na sporządzenie i przedstawienie planu oraz harmonogramu odstąpienia od sprzętu i oprogramowania usługodawcy jest praktycznie niemożliwy do zrealizowania. Jednocześnie, jak zostało wskazanie powyżej, wszelkie środki związane z oceną powinny być stosowane do oprogramowania i do sprzętu, a nie w stosunku do dostawcy. | **Wyjaśnienie**  Zrezygnowano z planów wycofania sprzętu lub oprogramowania. |
|  | Liquid Systems | Art. 66c ust. 1 | Okres na dostarczenie planu wycofania wynosi rok zamiast 3 miesięcy**.**  Okres 3 miesięcy dla przygotowania i przedstawienia planu i harmonogramu dla wycofania z infrastruktury dostawcy usług, sprzętu i oprogramowania jest praktycznie niemożliwy do odtrzymania.  **Sugestie:**  **Okres przygotowania i przedstawienia planu oraz harmonogramu powinien zostać wydłużony do jednego roku.** | **Wyjaśnienie**  Zrezygnowano z planów wycofania sprzętu lub oprogramowania. |
|  | Polska Izba Handlu | Art. 66c pkt 1 | **3 miesiące na dostarczenie harmonogramu**  **Propozycja zmiany:**  „W szczególnie uzasadnionych przypadkach Pełnomocnik może zobowiązać podmiot krajowego systemu cyberbezpieczeństwa, do którego zastosowanie ma ocena, do sporządzenia i dostarczenia w ciągu roku planu i harmonogramu wycofania z użytkowania sprzętu, oprogramowania i usług sprzętu lub oprogramowania, którego dotyczy ocena określająca wysokie ryzyko.”  **Uzasadnienie:**  Okres 3 miesięcy na sporządzenie i przedstawienie planu oraz harmonogramu odstąpienia od sprzętu i oprogramowania usługodawcy jest praktycznie niemożliwy do zrealizowania. Jednocześnie, jak zostało wskazanie powyżej, wszelkie środki związane z oceną powinny być stosowane do oprogramowania i do sprzętu, a nie w stosunku do przymiotów | **Wyjaśnienie**  Zrezygnowano z planów wycofania sprzętu lub oprogramowania. |
|  | KIGEIT | Art. 66c ust. 1 | **3 miesiące na dostarczenie harmonogramu**  **Propozycja zmiany:**  „*W szczególnie uzasadnionych przypadkach Pełnomocnik może zobowiązać podmiot krajowego systemu cyberbezpieczeństwa, do którego zastosowanie ma ocena, do sporządzenia i dostarczenia w ciągu ~~3 miesięcy~~ roku planu i harmonogramu wycofania z użytkowania sprzętu, oprogramowania i usług ~~dostawcy~~ sprzętu lub oprogramowania, którego dotyczy ocena określająca wysokie ryzyko*.”  **Uzasadnienie:**  Okres 3 miesięcy na sporządzenie i przedstawienie planu oraz harmonogramu odstąpienia od sprzętu i oprogramowania usługodawcy jest praktycznie niemożliwy do zrealizowania. Jednocześnie, jak zostało wskazanie powyżej, wszelkie środki związane z oceną powinny być stosowane do oprogramowania i do sprzętu, a nie w stosunku do podmiotów. | **Wyjaśnienie**  Zrezygnowano z planów wycofania sprzętu lub oprogramowania. |
|  | Signum Edward Kuś Marcin Kuś | art. 66c ust.1 | **Przedmiot**  Metody Kontroli Cyberbezpieczeństwa  **Ustawa**  Okres na dostarczenie planu wycofania wynosi rok zamiast 3 miesięcy  **Uzasadnienie**  Okres 3 miesięcy dla przygotowania i przedstawienia planu i harmonogramu dla wycofania z infrastruktury dostawcy usług sprzętu i oprogramowania jest praktycznie niemożliwy do dochowania.  **Przepisy**  Art.. 66c ust. 1  **Sugestie** Okres przygotowania i przedstawienia planu oraz harmonogramu powinien zostać wydłużony do jednego roku. | **Wyjaśnienie**  Zrezygnowano z planów wycofania sprzętu lub oprogramowania. |
|  | Związek Pracodawców Mediów Elektronicznych i Telekomunikacji MEDIAKOM  Reprezentowany przez adw. Annę Gąsecką | Art. 66a, 66b, 66c | Odnosząc się do planowanej zmiany polegającej na dodaniu przepisów art. 66a, 66b i 66c Mediakom wskazuje, że nie popiera proponowanych zmian w zakresie w jakim uprawniają one do wydawania wiążących rozstrzygnięć skutkujących powstaniem zakazu wprowadzania do użytkowania sprzętu, oprogramowania i usług danego dostawcy oraz obowiązku wycofania ich z obrotu. Mediakom rozumie potrzebę kontroli bezpieczeństwa i jakości sprzętu, oprogramowania i usług dostawców, jednak w jego ocenie proponowana procedura może prowadzić de facto do wykluczenia z rynku dowolnych dostawców i będzie wiązać się z poważnymi kosztami dla przedsiębiorców komunikacji elektronicznej, którzy będą zmuszeni do wymiany być może znacznej części wykorzystywanych urządzeń. Jednocześnie okres wymiany tych urządzeń (5 lat od ogłoszenia komunikatu o ocenie) nie pokrywa się z okresem amortyzacji urządzeń, co dodatkowo wpływa na zwiększenie kosztów nowych urządzeń. Jeśli więc możliwość wydawania wiążących ocen miałaby pozostać, to należy postulować wydłużenie okresu czasu na wymianę urządzeń do 7-8 lat. | **Uwaga częściowo uwzględniona**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3.  Zrezygnowano z planów wycofania sprzętu lub oprogramowania. |
|  | 1Innosystem | Art. 66a-66c | Przepisy ustawy w art. 66a - 66c łączą zagrożenia gospodarcze, kontrwywiadowcze i terrorystyczne z dostawcą sprzętu i oprogramowania, co jest w dużej mierze nieprawdziwe w realnym odniesieniu. Dużo ważniejsze w tej kwestii jest to, kto sprzęt produkuje oraz jakie elementy hardware np.: „chipsety” zainstalował na pokładzie, a co za tym idzie, co się może dziać po upgrade’dzie software, jakie dane przez łącza Internetu, a potem routery brzegowe są wysyłane za granicę, a co za tym idzie, dane te mogą nadrzędnie być monitorowane i wychwycone.  Znacząca rola tu jest po stronie Instytucji Teletechnicznych i badań, zanim zostanie dany sprzęt wprowadzony na rynek Polski. Pokazuje to przykład otrzymanych telefonów Huawei, gdzie ta kontrola powinna być znacząco większa. | **Uwaga nieuwzględniona**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3.  Zrezygnowano z planów wycofania sprzętu lub oprogramowania. |
|  | 1Innosystem | Art. 66a, 66b, 66c | Ponadto analiza art. 66a, 66b i 66c pokazuje, że w systemie cyberbezpieczeństwa wprowadza się jednostronną, uznaniową i subiektywną procedurę oceny działalności dostawców  sprzętu, oprogramowania i usług. Taka ocena podaje w wątpliwość, że kontrola zostanie wszczęta z zachowaniem zasady równości i niedyskryminacji dostawców usług czy sprzętu. Dobrze byłoby do tego zaprząc jednostki naukowe, inne firmy IT oraz niezależnych ekspertów (programiści), a  także stworzyć bardzo dokładne ramy sposobu badania i elementów analizy kodu, które będą  traktowane jako zagrożenie.  Sam sposób możliwości reakcji budzi wiele wątpliwości, zanim przedsiębiorca dowie się o ocenie, nie ma możliwości wytłumaczyć „wątpliwości”, bo nie dostanie szansy odwołania czy  wybronienia swojej racji, jedynie już z MONITORA POLSKIEGO dowiaduje się o orzeczonej winie.  Będzie to z wielką szkodą jaką wyrządzą w majątku przedsiębiorców po publikacji komunikatu.  Zauważmy też, iż w legislacji nie przewidziano odpowiedzialności i prawa do odszkodowania za naruszenie przepisów przez organ oceniający w przypadku pomyłek, a zapewne się zdarzą. | **Uwaga nieuwzględniona**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3.  Zrezygnowano z planów wycofania sprzętu lub oprogramowania. |
|  | Excogitate | Art. 66a -66c | **Metody Kontroli Cyberbezpieczeństwa**  Przedmiotem oceny ryzyka jest sprzęt lub oprogramowanie, a nie dostawca,   * + - 1. Łączenie zagrożeń gospodarczych, kontrwywiadowczych i terrorystycznych z dostawcą sprzętu i oprogramowania jest nieracjonalne i nielogiczne.       2. Istotą regulacji powinno być, jak nie korzystać z tego sprzętu tak, aby stanowił on takie zagrożenie, a nie kto go sprzedaje.   Zestaw narzędzi UE (Toolbox) przewiduje możliwość podjęcia środków ograniczających w odniesieniu do kluczowych aktywów. Polskie propozycje w projekcie wykraczają poza wymagania zestawu narzędzi UE.’  Zmienić słowo "dostawca sprzętu i oprogramowania" na "krytyczny **sprzęt lub oprogramowanie**" w artykule. 66a -66c. | **Uwaga nieuwzględniona**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3.  Zrezygnowano z planów wycofania sprzętu lub oprogramowania. |
|  | Signum Edward Kuś Marcin Kuś | Art. 66 a-c | **Przedmiot**  Metody Kontroli Cyberbezpieczeństwa  **Ustawa**  Przedmiotem oceny ryzyka powinien być sprzęt lub oprogramowanie, a nie dostawca.  **Uzasadnienie**  Łączenie zagrożeń gospodarczych, kontrwywiadowczych i terrorystycznych z dostawcą sprzęt i oprogramowania jest nieracjonalne i nielogiczne.  Ważniejszym pytaniem, od tego, kto jest sprzedawcą, powinno być pytanie, jak korzystać z sprzętu tak, aby nie stanowił onzagrożenia.  Zestaw narzędzi UE (Toolbox) przewiduje możliwość podjęcia środków ograniczających w odniesieniu do kluczowych aktywów. Polskie propozycje w projekcie wykraczają poza wymagania Zestawu Narzędzi UE  **Przepisy**  Art. 66a -66c  **Sugestie**  Zmienić słowo "dostawca sprzętu i oprogramowania" na "krytyczny sprzęt lub oprogramowanie" w artykule. 66a -66c. | **Uwaga nieuwzględniona**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3.  Zrezygnowano z planów wycofania sprzętu lub oprogramowania. |
|  | Polsko-Chińska Główna Izba Gospodarcza  SinoCham | Art. 66 a-c | Uzasadnienie:  1) Łączenie zagrożeń gospodarczych, kontrwywiadowczych i terrorystycznych z dostawcą sprzętu i oprogramowania jest nieracjonalne i nielogiczne.  2) Ważniejszym pytaniem powinno być, jak nie korzystać z tego sprzętu tak, aby stanowił on takie zagrożenie, a nie kto go sprzedaje.  3) Zestaw narzędzi UE (Toolbox) przewiduje możliwość podjęcia środków ograniczających w odniesieniu do kluczowych aktywów. Polskie propozycje w projekcie wykraczają poza wymagania zestawu narzędzi UE..  **Propozycja zmiany:**  Zmienić słowo "dostawca sprzętu i oprogramowania" na "krytyczny sprzęt lub oprogramowanie" w artykule. 66a - 66c. | **Uwaga nieuwzględniona**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3.  Zrezygnowano z planów wycofania sprzętu lub oprogramowania. |
|  | Izba Gospodarcza Gazownictwa/Polska Spółka Gazownictwa Sp. z.o.o. | Art. 66 a-c | **Rola, zadania, obowiązki Kolegium**  W zapisach brak informacji czy w ramach pracy Kolegium zostanie wypracowana metodyka oceny ryzyka dostawców systemów i usług, w zakresie cyberbezpieczeństwa – np. w formie aktu wykonawczego - rozporządzenia ?  Metodyka oceny ryzyka pozwoliłaby na możliwość wstępnego szacowania ryzyka przez podmioty OUK, DUC, na etapie wyboru technologii i dostawców, nie czekając na ocenę Kolegium i konieczność wycofania wybranej technologii. | **Wyjaśnienie**  Postępowanie administracyjne będzie prowadził minister właściwy do spraw informatyzacji. |
|  | ETOB-RES | Art. 66 a-c | W omawianym projekcie przedmiotem oceny ryzyka jest sprzęt lub oprogramowanie, a nie dostawca. Sugeruję zmienić słowo "dostawca sprzętu i oprogramowania" na "krytyczny sprzęt lub oprogramowanie" w artykule. 66a -66c. | **Uwaga nieuwzględniona**  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 planów wycofania sprzętu lub oprogramowania. |
|  | Digital Poland | Art. 66a-66c | Pragniemy zauważyć że w większości Państw unijnych sektor telekomunikacyjny nie stanowi elementu KSC. Nie ma go również w tzw. NIS - dyrektywnie unijnej. Wnosimy stąd o usunięcie zatem zapisów dotyczących tego sektora telekomunikacyjnego by zapewnić spójność prawa krajowego z unijnym.  W artykule 66a przedstawiono szereg nie merytorycznych kryteriów oceny dostawców. Pozwala to stwierdzić, że w wyniku zmian KSC **wcale nie ulegnie polepszeniu system cyberbezpieczeństwa w Polsce**. To tak jakby z Polskiego rynku wyeliminować samochody produkowane w Meksyku czy Chinach. Wyeliminowanie tych samochodów na bazie czysto politycznych decyzji, nie zwiększy bezpieczeństwa poruszania się po krajowych drogach. Kluczem jest bowiem homologacja czy ocena **testów zderzeniowych Euro NCAP**. Innymi słowy brak jakichkolwiek merytorycznych analiz, brak centra certyfikującego sprzęt, powoduje, że de facto w wyniku proponowanych decyzji osłabimy KSC w Polsce. Zwracamy uwagę, że takie kraje jak Wielka Brytania (uznany sojusznik Stanów Zjednoczonych), ma swoje centrum certyfikacji oraz dokonuje merytorycznej oceny dostawców. Wnosimy się zatem prośbę o podobne zapisy i zmianę, obecnie głównie politycznych, zapisów w zakresie oceny dostawców. **Uważamy, że najwyższym celem jest zwiększenie realnego bezpieczeństwa Polski, a nie** „**papierowe**”.  Wnosimy o zmianę **okresu usunięcia dostawców wysokiego ryzyka z sieci** (obecnie 5 lat) – tak złych zapisów nie znajdujemy w Stanach Zjednoczonych, Wielkiej Brytanii czy każdym innym kraju sojuszniczym, a nie w Unii Europejskiej. Co więcej kraje takie jak Stany Zjednoczone zaoferowały fundusz refundacyjny dla operatorów regionalnych, którego nie sposób znaleźć w ustawie. Zwracamy na okres 2028 wskazany w Wielkiej Brytanii i mając na uwadze okres amortyzacji sprzętu telekomunikacyjnego w Polsce, **wnosimy o zmianę na 2030** tzn. 10 lat. | **Uwaga częsciowo uwzględniona**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3.  Zrezygnowano z planów wycofania sprzętu lub oprogramowania. |
|  | Home.pl | Art. 66a-c | Nowelizacja przyzna Kolegium do spraw cyberbezpieczeństwa (organ opiniodawczo-doradczy przy Radzie Ministrów) nową kompetencję, jaką będzie możliwość oceny ryzyka dostawcy sprzętu lub oprogramowania istotnego dla cyberbezpieczeństwa podmiotów krajowego systemu cyberbezpieczeństwa. Przy sporządzeniu oceny przeprowadza się analizę zagrożeń bezpieczeństwa narodowego o charakterze ekonomicznym, kontrwywiadowczym i terrorystycznym, oraz prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego. Wniosek o sporządzenie oceny składa członek Kolegium. Sporządzona przez Kolegium ocena ryzyka dostawcy sprzętu lub oprogramowania przekazywana jest Pełnomocnikowi, który ogłasza ją w postaci komunikatu w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski”. Skutkiem oceny określającej wysokie ryzyko korzystania ze sprzętu lub oprogramowania będzie zakaz wprowadzenia do użytkowania takiego sprzętu lub oprogramowania. Z kolei dotychczas używany sprzęt i oprogramowanie ocenione jako wysoce ryzykowne - będą musiały zostać wycofane z użycia przez podmioty z nich korzystające w ciągu 5 lat od ogłoszenia komunikatu o ocenie. W przypadku operatorów usług kluczowych nie stosujących się do powyższych obowiązków kara wynosi do 3% całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego.  **Uwagi w ramach konsultacji:**  - do art. 66a ust. 1: nowelizacja nie zawiera definicji „sprzętu lub oprogramowania”, co powoduje brak pewności co do grona adresatów przepisu, należy zasugerować sprecyzowanie tego pojęcia w nowelizacji;   - do art. 66a: nowelizacja nie zakłada udziału dostawcy w toku postępowania poprzedzającego wydanie oceny, nie wskazuje również czy w postępowaniu znajdują zastosowanie przepisy kodeksu postępowania administracyjnego; należy zasugerować uzupełnienie nowelizacji w tym zakresie;   - do art. 66a ust. 8: dostawca sprzętu lub oprogramowania którego dotyczy ocena może odwołać się od oceny do Kolegium - w terminie 14 dni od publikacji komunikatu o sporządzonej ocenie. Kolegium rozpatruje odwołanie w ciągu 2 miesięcy od otrzymania. Wniesienie odwołania nie wstrzymuje działań związanych z ograniczeniami prowadzenia działalności dostawcy w zakresie dot. sprzętu lub oprogramowanie podlegającego ocenie; nie ma również możliwości dalszego zaskarżenia decyzji do sądu administracyjnego; należy zasugerować odstąpienie od natychmiastowej wykonalności oceny ewent. wprowadzenie rekompensat dla dostawców z powodu ograniczenia w obrocie sprzętem/oprogramowaniem, jeśli na skutek odwołania od oceny, Kolegium przywróci możliwość ich swobodnej sprzedaży; należy zasugerować wprowadzenie trybu odwoławczego od orzeczenia Kolegium dot. oceny; | **Uwaga nieuwzględniona**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3. |
|  | IAB Polska | Art. 66a  66b  66c | Projektowane artykuły 66a, 66b i 66c ustawy o KSC (art. 1 ust. 29 i n. Projektu) przewidują, że Kolegium do spraw cyberbezpieczeństwa nabędzie nową kompetencję dotyczącą oceny ryzyka dostawcy sprzętu lub oprogramowania istotnego dla cyberbezpieczeństwa podmiotów krajowego systemu cyberbezpieczeństwa. Wynik powyższego postępowania będzie ogłaszany w Monitorze Polskim. Tylko dostawcy z oceną wysokiego ryzyka będą mieli legitymację do złożenia odwołania, które będzie rozpatrywane ponownie przez Kolegium (projektowany art. 66a ust 8 ustawy o KSC).  W przypadku uzyskania oceny ryzyka określającej wysokie lub umiarkowane ryzyko dostawca sprzętu lub oprogramowania, będzie podlegał sankcjom przewidzianym w projektowanym art. 66b ustawy o KSC. Należy również podkreślić, że sankcja za uzyskanie wysokiej oceny ryzyka jest równoznaczna z zakazem wprowadzania do użytkowania sprzętu, oprogramowania i usług określonych w ocenie danego dostawcy sprzętu lub oprogramowania oraz koniecznością ich wycofania z rynku w ciągu 5 lat. Powyższa sankcja w ocenie konstytucjonalistów wydaje się być sprzeczna z zasadą niedziałania prawa wstecz.  Dodatkowo, zgodnie z art. 66c projektu ustawy o KSC, 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 sprzętu lub oprogramowania, którego dotyczy ocena określająca wysokie ryzyko. Z projektowanych art. 66b i 66c wynika, że de facto przedsiębiorcy (w tym dostawy i operatorzy) w wyniku oceny Kolegium będą na przykład musieli wycofać się z już prowadzonych inwestycji, które planowane są często w trybie długofalowym. W praktyce może to po prostu oznaczać zakaz prowadzenia działalności gospodarczej dla konkretnego przedsiębiorcy, co w sposób oczywisty zaburza cały system konkurencyjności na rynku podobnych usług czy towarów. W tym miejscu należy również wskazać, że decyzje Kolegium dotyczące dostawców sprzętu i oprogramowania dotykają wszystkie podmioty krajowego systemu cyberbezpieczeństwa. Decyzje dla konkretnych dostawców są wydawane dla poszczególnych obszarów, a co za tym idzie - takie decyzje mogą być wydane nie tylko dla usług telekomunikacyjnych, ale również dla usług komunikacji elektronicznej – co wynika z przyjęcia przez ustawodawcę w nowelizacji wspólnego pojęcia stanowiącego, że usługi o różnym charakterze i przeznaczeniu są traktowane jak usługi „jednego rodzaju”, Niesie to za sobą zagrożenie, że dostawcy usług komunikacji elektronicznej świadczący usługi w zakresie np. czatów albo poczty elektronicznej będą tak samo traktowani jak dostawcy usług telekomunikacyjnych. W konsekwencji może to oznaczać, że serwery danego producenta używane również do świadczenia usługi komunikacji interpersonalnej muszą zostać na mocy decyzji Kolegium wymienione w ciągu 5 lat, co pociągnie za sobą istotne nakłady pieniężne dla każdego podmiotu zaangażowanego lub pośredniczącego w dostawie takiej usługi, a w konsekwencji wpłynie również na konsumenta. Wzrost ceny takiej usługi wobec użytkownika końcowego może oznaczać, że korzystanie z niej przestanie być dla niego opłacalne i doprowadzi tym samym do wyeliminowania usługi z rynku. Dla średnich i małych przedsiębiorców może to oznaczać koniec prowadzonej działalności, a dla społeczeństwa obniżenie dostępności nowoczesnych usług czy nawet wzrost wykluczenia cyfrowego. Kolejną konsekwencją przyjęcia regulacji pozwalającej na wydawanie dyskrecjonalnych decyzji przez Kolegium może być również wycofanie się lub ograniczenie zaangażowania inwestorów zagranicznych z ryku krajowego przez wzgląd na brak pewności co do otoczenia inwestycyjnego Polski.  Ponadto konsekwencje przewidziane przez projekt nie kończą się jednak tylko na powyższym zakresie, ponieważ projekt przewiduje również zmiany w ramach Prawa zamówień publicznych.  Jak **wskazują konstytucjonaliści powyższe regulacje budzą uzasadnione wątpliwości z perspektywy podstawowych zasad konstytucyjnych**, takich jak niedziałanie prawa wstecz (art. 2 Konstytucji), zasady wolności działalności gospodarczej (art. 20 i 22 Konstytucji) oraz zasady równości wobec prawa i zakazu dyskryminacji (art. 32 Konstytucji).  Szczególne zastrzeżenia budzą poniższe kwestie:   * Opisana procedura dokonywania oceny przez Kolegium cechuje się jednostronnością, uznaniowością i subiektywnością; * Kryteria oceny w zakresie omawianego postępowania są nieprecyzyjne, co rodzi niebezpodstawne obawy o zachowanie w ramach postępowania zasady niedyskryminacji; * Kolegium prowadzi postępowanie bez udziału stron, a o jego rezultacie podmiot dowiaduje się z Monitora Polskiego; * Zasadność odwołania budzi również organ je rozpatrujący tj. to samo Kolegium, które dokonało oceny; * Ponadto uprawnienie do odwołania się od oceny dokonanej przez Kolegium przysługuje tylko i wyłącznie przedsiębiorcy, który uzyskał wysoką ocenę, co stanowi istotne pokrzywdzenie interesów pozostałych podmiotów z ocenami niższymi.   Na marginesie warto również zwrócić uwagę, że w przypadku wystąpienia nowych okoliczności, mogących mieć wpływ na ocenę ryzyka dostawcy sprzętu lub oprogramowania, tylko członek Kolegium może złożyć wniosek o zmianę oceny przez Kolegium. Zatem, również na tym etapie zostały wykluczone jakiekolwiek działania ze strony dostawcy sprzętu lub oprogramowania, będącego przedmiotem uprzedniej oceny ze strony Kolegium.  W ocenie IAB Polska konieczne jest dokonanie następujących zmian w ramach przedmiotowej procedury. W pierwszej kolejności, kryteria które są brane pod uwagę w czasie postępowania powinny zostać zrewidowane i skonkretyzowane. Obecne ich brzmienie pozostawia zbyt wiele miejsca na subiektywne podejście Kolegium. W dalszym zakresie niezbędne jest zapewnienie dostawcom sprzętu lub oprogramowania czynnego udziału w zakresie całego postępowania oraz na etapie po jego zakończeniu (wspomniana powyżej zmiana okoliczności). Kolejnym postulatem jest zmiana charakteru wydawanej decyzji, która powinna podlegać kontroli instancyjnej i weryfikacji sądowej. IAB Polska postuluje również modyfikację zasad publikacji oceny w Monitorze Polskim, która powinna być uzależniona od uprawomocnienia się decyzji Kolegium. Na zakończenie tej części, należy również podkreślić, że jedynie ostateczna decyzja administracyjna w zakresie oceny Kolegium, powinna być kwalifikowana jako przesłanka wykluczenia z postępowania toczącego się w trybie Prawa zamówień publicznych | **Uwaga częsciowo uwzględniona**  Przepisy art. 66a-66c zostały zmienione.  Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa jest oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek 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 prowadzone 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. Zostały określone zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostały określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.  W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne 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. Zrezygnowano z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.  Ponadto zmieniony został 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 został dołączony do ustawy jako załącznik nr 3.  Zrezygnowano z planów wycofania sprzętu lub oprogramowania. |
|  | PIIT | 67 ust 4 pkt 5 | 1. **Art. 2 pkt 30 – art. 67a ust. 4 pkt 5**   W obecnym brzmieniu projektu ustawy ostrzeżenia i polecenia zabezpieczające mogą dotyczyć kwalifikowanych dostawców usług zaufania, o którym mowa w art. 3 pkt 20 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.), zwanego dalej „eIDAS”.  W pierwszej kolejności należy wyjść od definicja pojęcia „usługa zaufania”, za którą zgodnie z art. 3 pkt 16 eIDAS uważa się:  „usługa zaufania” oznacza usługę elektroniczną zazwyczaj świadczoną za wynagrodzeniem i obejmującą:   1. tworzenie, weryfikację i walidację podpisów elektronicznych, pieczęci elektronicznych lub elektronicznych znaczników czasu, usług rejestrowanego doręczenia elektronicznego oraz certyfikatów powiązanych z tymi usługami; lub 2. tworzenie, weryfikację i walidację certyfikatów uwierzytelniania witryn internetowych; lub 3. konserwację elektronicznych podpisów, pieczęci lub certyfikatów powiązanych z tymi usługami.   Z kolei za kwalifikowanego dostawcę usług zaufania zgodnie z art. 3 pkt 20 eIDAS należy uznać dostawcę usług zaufania, który świadczy przynajmniej jedną kwalifikowaną usługę zaufania i któremu status kwalifikowany nadał organ nadzoru. Natomiast dostawca usług zaufania (art. 3 pkt 19 eIDAS) to osobę fizyczną lub prawną, która świadczy przynajmniej jedną usługę zaufania, jako kwalifikowany lub niekwalifikowany dostawca usług zaufania. W praktyce obrotu gospodarczego różnica pomiędzy dostawcą usług zaufania, a kwalifikowanym dostawcą usług zaufania sprowadza się w do wpisu na listę kwalifikowanych dostawców usług zaufania, bowiem po względem skutków prawnych przykładowo w kontekście podpisu elektronicznego, który może być już wydawany przez każdego dostawcę usług zaufania, zgodnie z art. 25 ust. 1 eIDAS nie można odmówić podpisowi elektronicznemu skutku prawnego ani dopuszczalności jako dowodu w postępowaniu sądowym wyłącznie z tego powodu, że podpis ten ma postać elektroniczną lub że nie spełnia wymogów dla kwalifikowanych podpisów elektronicznych. Tym samym, to już na poziomie Unii Europejskiej wprowadzono przepisy, które w praktyce pod względem skutków prawnych zrównują podpis elektroniczny lub zaawansowany podpis elektroniczny na równi z kwalifikowanym podpisem elektronicznym. Od strony technicznej należy zwrócić uwagę na to, że zarówno podpis elektroniczny, zawansowany podpis elektroniczny i kwalifikowany podpis elektroniczny zapewniają integralność danych i umożliwiają identyfikację osoby, która złożyła dane oświadczenie woli.  W naszej ocenie do ujętego w projekcie ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy – Prawo zamówień publicznych nowego art. 67a ust. 4 pkt 5, który miałby pojawić się w ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, do katalogu podmiotów, które miałyby się stosować do ostrzeżeń i poleceń zabezpieczających, należy włączyć wszelkie osoby lub podmioty wydające środki identyfikacji elektronicznej. Zgodnie art. 3 pkt 2 eIDAS środek identyfikacji elektronicznej oznacza materialną lub niematerialną jednostkę zawierającą dane identyfikujące osobę i używaną do celów uwierzytelniania dla usługi online. Usługi identyfikacji elektronicznej umożliwiają identyfikację danej osoby fizycznej, oraz co do zasady umożliwia udostępnienie danych osobowych danej osoby fizycznej odbiorcy (tzw. klientowi) tych danych, na których przekazanie osoba fizyczna wyraziła zgodę. Jak wynika z przepisów Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) dane osobowe są na poziomie unijnym objęte szczególną ochroną prawną, a podmioty, które są administratorami danych osobowych lub przetwarzają takiej dane na polecenie administratora, z mocy powszechnie obowiązującego prawa muszą stosować środki techniczne na określonymi przepisami poziomie, które w głównej mierze mają zabezpieczyć dane osobowe przed ich ujawnieniem osobom lub podmiotom do tego nieuprawnionym, jak również administrator lub podmiot przetwarzający musi rejestrować wszystkie osoby dopuszczone do przetwarzania danych w jego imieniu. Z tej przyczyny widzimy konieczność objęcia podmiotów świadczących usługi wydawania środków identyfikacji elektronicznej obowiązkiem stosowania się do ostrzeżeń i poleceń zabezpieczających.  **Propozycja zmiany przepisu**  Art. 2 pkt 30 – art. 67a ust. 4 pkt 5:  „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 osoby lub podmioty wydające środki identyfikacji elektronicznej w rozumieniu art. 3 pkt 2 wymienionego rozporządzenia.” | **Uwaga częściowo uwzględniona**  Do katalogu podmiotów, wobec których może być skierowane ostrzeżenie lub polecenie zabezpieczające zostaną dodani niekwalifikowani dostawcy usług zaufania. |
|  | KIGEIT | art. 67a | *„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 ~~zatwierdzeniu~~ wyrażeniu opinii przez Kolegium.*  *~~2. 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.~~*  *8. W przypadku ~~odmowy zatwierdzenia przez~~ negatywnej opinii Kolegium Pełnomocnik ~~odwołuje ostrzeżenie lub polecenie zabezpieczające w części lub w całości albo stosuje~~ wydaje inne ostrzeżenie lub polecenie zabezpieczające.*  **Uzasadnienie:**  Zgodnie z art. 67a ust. 1 Projektu Pełnomocnik może wydać ostrzeżenia i polecenia zabezpieczające we współdziałaniu z Kolegium. Zastosowanie znajdzie więc przepis art. 106 k.p.a., który reguluje współdziałanie organów | **Wyjaśnienie**  Przepisy art. 67a -67c zostały 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. Zatem także minister właściwy ds. informatyzacji będzie podejmował decyzje o ewentualnych karach także w formie decyzji administracyjnej. Przepis art. 73 został uzupełniony o wysokość kary za nie zastosowanie się do polecenia zabezpieczającego.  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 Zepole 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. |
|  | Polska Izba Handlu | Art. 67a | **Ostrzeżenia i polecenia zabezpieczające -** brak odniesienia do postępowania administracyjnego w stosunku do czynności podejmowanych przez Pełnomocnika  **Propozycja:**Po ustępie 8 dodać ustęp 9*:*  *"Postępowanie przed pełnomocnikiem toczy się w oparciu o przepisy ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego. Ostrzeżenie ma formę decyzji administracyjnej."*  **Uzasadnienie**  Zgodnie z art. 67a ust. 1 Projektu Pełnomocnik może wydać ostrzeżenia i polecenia zabezpieczające. Powinno być wskazane w oparciu o jakie przepisy toczy się postępowanie przed Pełnomocnikiem. W szczególności, że zgodnie z art. 67a ust. 2 Projektu „*ostrzeżenia lub polecenia zabezpieczające wymagają zatwierdzenia przez Kolegium na najbliższym posiedzeniu*”. Konsekwencją stosowania przepisów k.p.a. będzie zastosowanie art. 106 k.p.a., który reguluje współdziałanie organów.  Zgodnie z art. 67c ust. 1 Projektu: *Polecenie zabezpieczające wydaje się w formie decyzji administracyjnej.* Analogiczny przepis powinien obowiązywać w przypadku wydania ostrzeżenia tj. *Ostrzeżenie wydaje się w formie decyzji administracyjnej.* Kluczowy bowiem element zarówno ostrzeżenia, jak polecenia zabezpieczającego, tj. „określone zachowanie”, jest taki sam. Przepis art. 67c ust. 4 pkt 1 Projektu dotyczący polecenia zabezpieczającego, odsyła w zakresie „określonego zachowania” do art. 67b ust. 3 Projektu, który szczegółowo reguluje elementy określonego zachowania w przypadku wydawania ostrzeżenia. | **Wyjasnienie**  Przepisy art. 67a -67c zostały 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. Zatem także minister właściwy ds. informatyzacji będzie podejmował decyzje o ewentualnych karach także w formie decyzji administracyjnej. Przepis art. 73 został uzupełniony o wysokość kary za nie zastosowanie się do polecenia zabezpieczającego.  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 Zepole 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. |
|  | PIIT | Art. 67a-67c | 1. **Art. 67a – ostrzeżenie i polecenie zabezpieczające**   Drugą, jeszcze bardziej interwencyjną metodą działania mogącą skutkować wykluczeniem określonych dostawców są przewidziane w projekcie ustawy ostrzeżenia oraz polecenia zabezpieczające.  Takie instrumenty Pełnomocnik może wydawać po analizie i współpracując z Zespołem (*CSIRT MON, CSIRT NASK, Szefa Agencji Bezpieczeństwa Wewnętrznego realizującego zadania w ramach CSIRT GOV oraz Rządowego Centrum Bezpieczeństwa.*). Konsultacje z podmiotami, których ostrzeżenie lub polecenie może dotyczyć, są fakultatywne. Środki te podlegają zatwierdzeniu Kolegium. Stosowanie rozwiązań wynikających z ostrzeżeń i poleceń zabezpieczających może wiązać się ze skutkami na poziomie umów cywilnoprawnych oraz potencjalnej odpowiedzialności odszkodowawczej. W związku z tym należy wprowadzić wyraźne przepisy zwalniające podmioty zobowiązane z jakiejkolwiek odpowiedzialności cywilnoprawnej wobec stron trzecich, które mogą wysuwać roszczenia związane ze skutkami zastosowania ostrzeżeń lub poleceń zabezpieczejących.   * 1. **Art. 67b ust. 1 pkt 3 oraz ust. 3 - ostrzeżenie**   Instytucja wydawania ostrzeżeń, jako taka może być uznana za zasadną. Może ona stanowić istotną wytyczną dla podmiotów związanych z cyberprzestrzenią do podejmowania określonych działań. W zakresie podmiotów publicznych rozwiązanie takie może być nawet obligatoryjne.  W przypadku jednak podmiotów prywatnych zaproponowany zakres oczekiwanych zachowań, jakie takie podmioty miałyby podejmować jest dalece nieproporcjonalne i stanowi de facto mechanizm zewnętrznego sterowania działalnością przedsiębiorstw przez Pełnomocnika. Potencjalnie zbyt lekkie, ostrożnościowe jedynie korzystanie z tego środka może prowadzić do bardzo wysokich obciążeń przedsiębiorców oraz konieczności podejmowania ogromnego wysiłku organizacyjnego i finansowego. W skrajnych przypadkach może prowadzić do faktycznego zamknięcia działalności, np. w przypadku zakazu stosowania określonego sprzętu (podczas gdy tego mają co do zasady przecież dotyczyć oceny Kolegium) bez jakichkolwiek okresów przejściowych. Wydaje się również, że Pełnomocnik nie będzie też posiadał odpowiedniej wiedzy, aby nakazywać (a nie podpowiadać lub rekomendować) jakie poprawki czy konfigurację sprzętu należy zastosować w danym przypadku. Ponadto rozwiązania takie jak szacowanie ryzyka, czy przegląd planów są działaniami bardzo czasochłonnymi i kosztownymi, które w przypadku nawet realnego i bliskiego ryzyka nie stanowią bezpośredniej odpowiedzi i reakcji na zagrożenie.  Dodatkowo zwracamy uwagę, iż nakaz wprowadzenia reguły ruchu sieciowego zakazującego połączeń z określonymi adresami IP lub nazwami URL jest technicznie niemożliwy do realizacji przez przedsiębiorców telekomunikacyjnych. Działanie takie jest możliwe do realizacji przez administratorów sieci niepublicznych/prywatnych, zarządzających dostępem użytkowników tych sieci do sieci Internet.  Przepisy dot. ostrzeżeń oraz poleceń zabezpieczających należy również zmodyfikować w sposób wskazujący, że mogą one dotyczyć wyłączenie sprzętu, oprogramowania lub usług podmiotów, których może dotyczyć lub których dotyczy incydent krytyczny.  **Postulaty:**   * Art. 67b ust. 1 pkt 3 należy usunąć lub zmodyfikować tak, aby w zakresie, w jakim ma dotyczyć przedsiębiorców był traktowany, jako faktyczne ostrzeżenie i wskazanie możliwości wyboru ścieżek działania, a nie „polecenie”, „nakaz”, „zakaz”. * W przypadku utrzymania formy nakazowej, w której rozstrzygnięcie stanowi o prawach i obowiązkach konkretnego podmiotu ostrzeżenie powinno być wydawane w drodze decyzji administracyjnej, która jest zaskarżalna w normalnym trybie administracyjnym i sądowym. Wydanie go w formie „Komunikatu” zamyka jego adresatom możliwość ścieżki odwoławczej. Rolą wydającego tak ważne rozstrzygnięcia musi być ustalenie adresatów i ocena skutków. * Okres, na jaki może być wydane ostrzeżenie musi być ściśle skorelowany z zagrożeniem. Proponowany termin 2 lat jest zupełnie abstrakcyjny i wskazuje na zamiar stosowania ostrzeżeń, w sposób oderwany od faktycznych zagrożeń. Okres, jaki ostrzeżenie powinno obowiązywać to maksymalnie 10 dni, z możliwością przedłużenia o ile zagrożenie nie minęło. * Ostrzeżenia nie mogą być również stosowane do rozwiązywania kwestii oceny dostawców, które powinny być procedowane ścieżką oceny ryzyka właściwą dla Kolegium. * Konsultacje z podmiotem objętym decyzją powinny być obligatoryjne. * Z uwagi na postulowaną zmianę charakteru „ostrzeżeń” należy rozważyć przeniesienie tego obowiązku na właściwe CSiRT, które zresztą już dzisiaj powinny podobne działania realizować. * W przypadku utrzymania charakteru ostrzeżeń należy je wprowadzać w drodze decyzji administracyjnej. * W przypadku utrzymania tego narzędzia, Pełnomocnik powinien być każdorazowo zobowiązany do zwrotu kosztów i ewentualnych strat związanych z wydaniem ostrzeżenia. * W art. 67a ust. 3 należy dodać pkt. 6 o następującej treści „6) ocenę możliwości technicznych wdrożenia ostrzeżenia oraz polecenia zabezpieczającego;” * W art. 67b ust. 3 po punktach 1 – 7 dodać „- o ile jest to techniczne możliwe.”   1. **Art. 67c – polecenie zabezpieczające**   Polecenie zabezpieczające może być stosowane w przypadku wystąpienia incydentu krytycznego i przewiduje jeszcze dalej idące środki niż w przypadku ostrzeżenia.  **Postulaty:**   * Art. 67c ust. 4 należy usunąć lub zmodyfikować tak, aby w zakresie, w jakim ma dotyczyć przedsiębiorców był traktowany, jako określenie możliwych ścieżek działania, a nie „polecenie”, „nakaz”, „zakaz”. * W przypadku utrzymania tego narzędzia, Pełnomocnik powinien być każdorazowo zobowiązany do zwrotu kosztów i ewentualnych strat związanych z wydaniem ostrzeżenia. * Okres, na jaki może być wydane polecenie musi być ściśle skorelowany z zagrożeniem. Proponowany termin 2 lat jest zdecydowanie zbyt długi. Polecenie może być wydawane wyłącznie na okres obsługi incydentu krytycznego. * Ostrzeżenia nie mogą być również stosowane do rozwiązywania kwestii oceny dostawców, które powinny być procedowane ścieżką oceny ryzyka właściwą dla Kolegium. * Konsultacje z podmiotem objętym decyzją powinny być obligatoryjne. | **Uwaga częściowo przyjęta**  Przepisy art. 67a -67c zostały 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. Zatem także minister właściwy ds. informatyzacji będzie podejmował decyzje o ewentualnych karach także w formie decyzji administracyjnej. Przepis art. 73 został uzupełniony o wysokość kary za nie zastosowanie się do polecenia zabezpieczającego.  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 Zepole 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. |
|  | SmartWeb Media | Art. 67a ust.1 | Z punktu widzenia poprawności legislacyjnej, należałoby również doprecyzować, że uprawnienia Pełnomocnika, o których mowa w projektowanym art. 67a ust. 1 ustawy o krajowym systemie cyberbezpieczeństwa, tj. wydawanie ostrzeżeń i poleceń zabezpieczających, winny być wydawane w formie decyzji administracyjnej, oraz podlegać pod reżim odwoławczy wyznaczony przepisami k.p.a. | **Wyjaśnienie**  Przepisy art. 67a -67c zostały 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. Zatem także minister właściwy ds. informatyzacji będzie podejmował decyzje o ewentualnych karach także w formie decyzji administracyjnej. Przepis art. 73 został uzupełniony o wysokość kary za nie zastosowanie się do polecenia zabezpieczającego.  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 Zepole 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. |
|  | Narodowy Bank Polski | art. 67a ust. 4 pkt 1 | Zmianę brzmienia projektowanego art. 67a ust. 4 pkt 1 na następujące:  „1) podmiotów, o których mowa w art. 4 pkt 1-8 oraz pkt 10-16;”. | **Uwaga nieuwzględniona**  Obowiązek dostosowania się do polecenia zabezpieczającego nie wpływa na konstytucyjną niezależność Narodowego Banku Polskiego. Nie dotyczy jego zadań konstytucyjnych i ustawowych. |
|  | Narodowy Bank Polski | art. 67a ust. 4 pkt 6 | Narodowego Banku Polskiego jedynie w zakresie w jakim nie wywiera wpływu na realizację zadań NBP. Po ogłoszeniu komunikatu, o którym mowa w ust. 6, NBP przekazuje Pełnomocnikowi informację o ewentualnym ograniczeniu stosowania wydanych ostrzeżeń i poleceń zabezpieczających.”. | **Uwaga nieuwzględniona**  Obowiązek dostosowania się do polecenia zabezpieczającego nie wpływa na konstytucyjną niezależność Narodowego Banku Polskiego. Nie dotyczy jego zadań konstytucyjnych i ustawowych. |
|  | Fundacja Bezpieczna Cyberprzestrzeń | art. 67a ust. 8 | po ust. 8 należy dodać ust. 9 lub inny przepis, w którym podmiot, któremu zostało wydane polecenie zabezpieczające może wystąpić o zwrot poniesionych kosztów, w przypadku odmowy zatwierdzenia tego polecenia przez Kolegium i odwołania polecenia zabezpieczającego w części lub w całości, o czym mowa w art. 67a ust. 8. | **Wyjaśnienie**  Uwaga jest bezprzedmiotowa, ponieważ według nowej wersji projektu Kolegium nie będzie zatwierdzać polecenia zabezpieczającego. |
|  | SayF | Art. 67 a i b | Nowo wprowadzone artykuły nie określają na podstawie jakich kryteriów pełnomocnik wydaje ostrzeżenia i polecenia zabezpieczające. | **Wyjaśnienie**  Przepisy art. 67a -67c zostały 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. Zatem także minister właściwy ds. informatyzacji będzie podejmował decyzje o ewentualnych karach także w formie decyzji administracyjnej. Przepis art. 73 został uzupełniony o wysokość kary za nie zastosowanie się do polecenia zabezpieczającego.  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 Zepole 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. |
|  | Nanocoder | Art. 67 a i c | Art. 67a i 67c również powinny zostać objęte poprawkami, z uwagi na fakt, że zarówno ostrzeżenie jak i polecenie zabezpieczenia powinny mieć formę decyzji administracyjnej, a polecenie zabezpieczające nie powinno być wydane z rygorem natychmiastowej wykonalności. Wynika to z faktu, iż działania Pełnomocnika powinny podlegać Kodeksowi Postępowania Administracyjnego, tym samym ostrzeżenie i polecenie zabezpieczenia powinno być przyjęte w formie decyzji administracyjnej. W niniejszym projekcie występuje kilka wyjątków, tj. sytuacji, w których polecenie zabezpieczające wdrożone ma zostać natychmiast. Będzie to miało nieodwracalne skutki, tego rodzaju zabezpieczenia powinny być pozbawione rygoru natychmiastowej wykonalności. | **Wyjaśnienie**  Przepisy art. 67a -67c zostały 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. Zatem także minister właściwy ds. informatyzacji będzie podejmował decyzje o ewentualnych karach także w formie decyzji administracyjnej. Przepis art. 73 został uzupełniony o wysokość kary za nie zastosowanie się do polecenia zabezpieczającego.  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 Zepole 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. |
|  | Home.pl | Art. 67 a-c | W celu zapobiegania i zwiększenia skuteczności reagowania na incydenty krytyczne nowelizacja zakłada przyznanie Pełnomocnikowi Rządu do Spraw Cyberbezpieczeństwa nowej kompetencji:  - możliwość wydawania ostrzeżeń i poleceń zabezpieczających (m. in. wobec operatora usług kluczowych). Ostrzeżenie stosuje się w przypadku uzyskania informacji o zagrożeniu cyberbezpieczeństwa, które może skutkować wystąpieniem incydentu krytycznego i nie jest decyzją administracyjną. W jego ramach wskazuje się rodzaje podmiotów, których dotyczy, określone zachowanie, które zmniejszy ryzyko, datę wejścia w życie i okres obowiązywania, a także uzasadnienie. Wydaje się je na okres nie dłuższy niż 2 lata, choć Pełnomocnik będzie mógł jednokrotnie przedłużyć jego okres obowiązywania nie dłużej niż o kolejne dwa lata. Jeżeli przemawia za tym interes publiczny, informacja o zastosowanym ostrzeżeniu może być udostępniona za pomocą środków masowego przekazu. W ramach ostrzeżenia można podmiotowi ~~nakazać zakaz~~ zakazać korzystania z określonego sprzętu lub oprogramowania oraz nakazać wprowadzenie reguły ruchu sieciowego zakazującego połączeń z określonymi adresami IP lub nazwami URL.    Polecenie zabezpieczające jest decyzją administracyjną, która ma rygor natychmiastowej wykonalności. Stosuje je Pełnomocnik w razie wystąpienia incydentu krytycznego. Zawiera wskazanie podmiotów, których dotyczy, wskazanie określonego zachowania, które zmniejszy skutki incydentu lub zapobiegnie jego rozprzestrzenianiu, datę wejścia w życie i uzasadnienie. W razie nie zastosowania się do polecenia zabezpieczającego operator usługi kluczowej podlega administracyjnej karze pieniężnej. Pełnomocnik ogłasza w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski” komunikaty o wydanych i odwołanych ostrzeżeniach i poleceniach zabezpieczających.  **Uwagi w ramach konsultacji:**  **-**do art. 67a ust. 1 pkt 1  (Ostrzeżenie):  Procedura wydania ostrzeżenia jest odformalizowana i nie zapewnia dostawcom udziału w postępowaniu dot. wydania ostrzeżenia (nowelizacja nie zakłada obligatoryjnego udziału dostawcy w ramach postępowania przed wydaniem ostrzeżenia – a jedynie fakultatywny decyduje o tym organ prowadzący postępowanie Pełnomocnik – nowy art. 67a ust.  w przypadku ostrzeżenia nowelizacja nie przewiduje trybu odwoławczego; jednocześnie przy orzekaniu o wydaniu ostrzeżenia organ posiada duży zakres uznaniowości; w konsekwencji – może dojść do istotnych ograniczeń działalności dostawcy na znaczny okres czasu bez możliwości kontrolowania prawidłowości działań organu lub sprzeciwienia się tym działaniom; należy w związku z tym zasugerować: dodanie do nowelizacji zapisów precyzujących przesłanki wydana ostrzeżenia, aby ograniczyć uznaniowość organu, gwarantujących dostawcom udział w postępowaniu o wydanie ostrzeżenia, zapewnienie możliwości odwołania od ostrzeżenia, zapewnienie rekompensat za szkody spowodowane wydaniem ostrzeżenia.   - do art. 67a ust. 1 pkt 2  (Polecenia):  ograniczenia związane poleceniem mogą zostać wprowadzone niezwłocznie, a ich skutki mogą znacznie ingerować w prowadzenie działalności gospodarczej dostawcy; rozstrzygniecie organu – choć wydawane w formie decyzji adm. i podlegające zaskarżeniu, cechuje się znaczną uznaniowością; decyzja w przedmiocie wydania polecenia jest natychmiast wykonalna; należy w związku z tym zasugerować: dodanie do nowelizacji zapisów precyzujących przesłanki wydana polecenia, aby ograniczyć uznaniowość organu, zapewnienie rekompensat za szkody spowodowane wydaniem polecenia. | **Uwaga częściowo uwzględniona**  Przepisy art. 67a -67c zostały 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. Zatem także minister właściwy ds. informatyzacji będzie podejmował decyzje o ewentualnych karach także w formie decyzji administracyjnej. Przepis art. 73 został uzupełniony o wysokość kary za nie zastosowanie się do polecenia zabezpieczającego.  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 Zepole 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. |
|  | Mobile Logic | Art. 67c | Ponadto nakładany w art. 67c rygor natychmiastowej wykonalności dla zabezpieczenia powinien zostać usunięty. Tego typu działanie będzie miało nieodwracalne skutki i w związku z tym jest nie do przyjęcia. | **Uwaga nieuwzględniona**  Należy podkreślić, że szybkość reakcji w przypadku wystąpienia incydentu krytycznego jest kluczowa w procesie ograniczenia skutków tego incydentu. Polecenie zabezpieczające ma na celu ograniczyć skutki incydentu krytycznego, który może zagrażać obywatelom, państwu, gospodarce. Dlatego rygor natychmiastowej wykonalności polecenia zabezpieczającego jest niezbędny. |
|  | Polska Izba Handlu | Art. 67c | **Projekt przepisu:** brak odniesienia do postępowania administracyjnego w odniesieniu do „ostrzeżenia”  **Propozycja:** słowo „ostrzeżenie” dodane do Art. 67c punkt 1.  *"Pełnomocnik wydaje ostrzeżenie i polecenia zabezpieczające w formie decyzji administracyjnej".*  **Uzasadnienie**  Zgodnie z art. 67c ust. 1 Projektu: *Polecenie zabezpieczające wydaje się w formie decyzji administracyjnej.* Analogiczny przepis powinien obowiązywać w przypadku wydania ostrzeżenia tj. *Ostrzeżenie wydaje się w formie decyzji administracyjnej.* Kluczowy bowiem element zarówno ostrzeżenia, jak polecenia zabezpieczającego, tj. „określone zachowanie”, jest taki sam. Przepis art. 67c ust. 4 pkt 1 Projektu dotyczący polecenia zabezpieczającego, odsyła w zakresie „określonego zachowania” do art. 67b ust. 3 Projektu, który szczegółowo reguluje elementy określonego zachowania w przypadku wydawania ostrzeżenia | **Wyjaśnienie**  Przepisy art. 67a -67c zostały 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. Zatem także minister właściwy ds. informatyzacji będzie podejmował decyzje o ewentualnych karach także w formie decyzji administracyjnej. Przepis art. 73 został uzupełniony o wysokość kary za nie zastosowanie się do polecenia zabezpieczającego.  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 Zepole 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. |
|  | Polska Izba Handlu | Art. 67c ust. 1 | **Propozycja**: wykreślić rygor natychmiastowej wykonalności decyzji  **Uzasadnienie**  Z uwagi na nieodwracalne skutki wykonania polecenie zabezpieczającego z rygorem natychmiastowej wykonalności, powinien być ten rygor usunięty. Przykładowo w Prawie telekomunikacyjnym, zgodnie z art. 206 ust. 2aa, decyzje regulacyjne podlegają natychmiastowemu wykonaniu, ale z wyjątkiem decyzji w sprawie nałożenia kar, właśnie z uwagi na ich nieodwracalne skutki | **Uwaga nieuwzględniona**  Należy podkreślić, że szybkość reakcji w przypadku wystąpienia incydentu krytycznego jest kluczowa w procesie ograniczenia skutków tego incydentu. Polecenie zabezpieczające ma na celu ograniczyć skutki incydentu krytycznego, który może zagrażać obywatelom, państwu, gospodarce. Dlatego rygor natychmiastowej wykonalności polecenia zabezpieczającego jest niezbędny. |
|  | KIGEIT | Art. 67c ust. 1 | **Proponowana zmiana:**  *"Art. 67c. 1. Pełnomocnik wydaje ostrzeżenie i polecenie zabezpieczające w ~~drodze~~ formie decyzji administracyjnej, od której przysługuje odwołanie albo wniosek o ponowne rozpatrzenie sprawy do ministra właściwego do spraw informatyzacji. ~~Decyzja podlega natychmiastowemu wykonaniu.~~ "*  **Uzasadnienie**  Zgodnie z art. 67c ust. 1 Projektu: *Polecenie zabezpieczające wydaje się w formie decyzji administracyjnej.* Wprowadza to niejasność w odniesieniu do charakteru ostrzeżenia, które również stanowi decyzję administracyjną.Kluczowy element zarówno ostrzeżenia, jak polecenia zabezpieczającego, tj. „określone zachowanie”, jest taki sam. Przepis art. 67c ust. 4 pkt 1 Projektu dotyczący polecenia zabezpieczającego, odsyła w zakresie „określonego zachowania” do art. 67b ust. 3 Projektu, który szczegółowo reguluje elementy określonego zachowania w przypadku wydawania ostrzeżenia.  Mając na uwadze, że Pełnomocnikiem może zostać sekretarz stanu lub podsekretarz stanu z każdego ministerstwa, zasadne jest zmodyfikowanie zasady ogólnej odwołania do organu wyższego stopnia. W każdym przypadku organem rozpoznającym sprawę w drugiej instancji winien być minister właściwy do spraw informatyzacji, nawet jeśli Pełnomocnika powołano w innym ministerstwie.  Z uwagi na nieodwracalne skutki wykonania polecenia zabezpieczającego z rygorem natychmiastowej wykonalności, powinien być ten rygor usunięty | **Wyjaśnienie**  Ostrzeżenie będzie miękkim środkiem, zalecającym działania. Za niedostosowanie się do ostrzeżenia nie będą grozić kary. |
|  | Fundacja Bezpieczna Cyberprzestrzeń | art. 67c ust. 2 | należy doprecyzować, kiedy kończy się czas koordynacji obsługi incydentu krytycznego, gdyż w przepisach ustawy zmieniającej i zmienianej nie ma obowiązku ogłaszania tego faktu. Należy połączyć ten przepis z przepisem wskazującym w obowiązkach CSIRT poziomu krajowego informowania o zakończeniu koordynacji obsługi incydentu krytycznego | **Uwaga nieuwzględniona**  Nie jest możliwe określenie czasu koordynacji incydentu krytycznego. Polecenie zabezpieczające będzie obowiązywać maksymalnie dwa lata. |
|  | T-Mobile Polska | Art. 73 pkt 14 | ***14) ust. 2a wynosi:***  *a) w przypadku podmiotów określonych w art. 4 pkt 1-2a nie stosujących się do art. 66b ust. 1 w wysokości do 3% jego całkowitego rocznego ~~światowego~~ obrotu z poprzedniego roku obrotowego, osiągniętego na obszarze Rzeczypospolitej Polskiej,*  *b) w przypadku podmiotów określonych w art. 4 pkt 1-2a nie stosujących się do art. 66b ust. 2 w wysokości do 1% jego całkowitego rocznego ~~światowego~~ obrotu z poprzedniego roku obrotowego, osiągniętego na obszarze Rzeczypospolitej Polskiej,*  **Uzasadnienie:**  Dla uniknięcia ewentualnych wątpliwości interpretacyjnych, proponujemy zmianę mającą na celu doprecyzowanie, iż w przypadku międzynarodowych grup telekomunikacyjnych, ewentualna sankcja dotyczy wyłącznie przedsiębiorcę telekomunikacyjnego (operatora) funkcjonującego na obszarze RP, a nie całej międzynarodowej grupy kapitałowej, do której należy przedsiębiorca prowadzący działalność w Polsce. | **Uwaga nieuwzględniona**  Kary, których wymiar odnosi się do światowego obrotu, są niezbędne w celu zapewnienia skuteczności przepisów, które mają na celu ochronę bezpieczeństwa narodowego. |
|  | PIIT | Art. 73 ust. 2a | 1. **Art. 73 ust. 2a – kary pieniężne**   **Postulat:**   * Zwracamy uwagę na bardzo wysokie potencjalne kary pieniężne związane z naruszeniem określonych przepisów. W naszej ocenie powinny one zostać określone na poziomie zbliżonym do pozostałych kar określonych w ustawie KSC, a w wypadku pozostawienia wartości procentowej nie powinny odnosić się do obrotu na poziomie globalnym, co rodzi zbędne wątpliwości dot. określania podstawy kary dla podmiotów działających i zarejestrowanych w Polsce, ale posiadających międzynarodową strukturę właścicielską. | **Uwaga nieuwzględniona**  Kary, których wymiar odnosi się do światowego obrotu, są niezbędne w celu zapewnienia skuteczności przepisów, które mają na celu ochronę bezpieczeństwa narodowego. |
|  | Narodowy Bank Polski | Art. 73 ust. 2a | Z punktu widzenia NBP wątpliwości budzi projektowany art. 73 ust. 2a, który przewiduje nałożenie administracyjnej kary pieniężnej na podmiot krajowego systemu cyberbezpieczeństwa, który nie dostosował się do obowiązków określonych w art. 66b ustawy o KSC. Do kręgu podmiotów objętych sankcjami, zalicza się także Narodowy Bank Polski, na który – w myśl aktualnie projektowanego art. 74 ust. 1a pkt 1 – może zostać nałożona kara pieniężna przez organ nadzorujący. Ze względu na konstytucyjny status Narodowego Banku Polskiego, a także obowiązujące rozwiązania w ustawie  o KSC, brak jest organu sprawującego nadzór nad NBP, co oznacza, że przytoczone powyżej przepisy odnoszące się do możliwości nakładania administracyjnej kary pieniężnej na NBP nie będą miały zastosowania. Zasadnym jest zatem wyłączenie NBP  z zakresu podmiotowego omawianych przepisów, tj. projektowanego art. 73 ust. 2a oraz art. 74 ust. 1a pkt 1. | **Uwaga nieuwzględniona**  Obowiązek dostosowania się do polecenia zabezpieczającego nie wpływa na konstytucyjną niezależność Narodowego Banku Polskiego. Nie dotyczy jego zadań konstytucyjnych i ustawowych. |
|  | Związek Banków Polskich | Art. 73 pkt 14 | 4) ust. 2a wynosi:  a)w przypadku podmiotów określonych w art. 4 pkt 1-2a nie stosujących się do art. 66b ust. 1 w wysokości do 300 000 zł,  b)w przypadku podmiotów określonych w art. 4 pkt 1-2a nie stosujących się do art. 66b ust. 2 w wysokości do 100 000 zł,  c)w przypadku podmiotów publicznych do 300 000zł”.  Wysokość kar w tym zakresie jest niewspółmiernie wyższa niż w przypadku innych uchybień.  Proponujemy zmianę z % odnoszących się do obrotu firm z sektora prywatnego na konkretne kwoty. Kara wprowadza dotkliwość jednak nie ma aż tak dużej niewspółmierności kary sektora prywatnego w porównaniu z sektorem publicznym. | **Uwaga nieuwzględniona**  Kary, których wymiar odnosi się do światowego obrotu, są niezbędne w celu zapewnienia skuteczności przepisów, które mają na celu ochronę bezpieczeństwa narodowego. |
|  | Narodowy Bank Polski | Art. 74 ust. 1a pkt 1 | Zmianę brzmienia projektowanego art. 74 ust. 1a pkt 1 na następujące:  „1) w przypadku podmiotów określonych w art. 4 pkt 7-8 oraz pkt 10-15 – organ nadzorujący” | **Wyjaśnienie**  Przepis został zmieniony |
|  | SayF | Rozdział 14 | Brak wskazania kar dla przedsiębiorców komunikacji elektronicznej. | **Uwaga 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 ksc poprzez ustawę wprowadzającą PKE. |
|  | Związek Przedsiębiorców i Pracodawców | Rozdział 4a | Przedstawiony projekt zakłada wprowadzenie do ustawy o krajowym systemie cyberbezpieczeństwa zupełnie nowego rozdziału 4a dotyczącego obowiązków przedsiębiorców komunikacji elektronicznej. Pragniemy podkreślić, że analogiczne regulacje znajdują się już w projekcie prawa komunikacji elektronicznej. Istnieje zatem potrzeba przyjęcia jednolitego podejścia i uregulowania obowiązków przedsiębiorców komunikacji elektronicznej w jednym akcie. Część z opisywanych obowiązków podmiotów ma charakter dosyć ogólny (jak choćby „podejmowanie środków technicznych i organizacyjnych zapewniających poziom bezpieczeństwa adekwatny do poziomu zidentyfikowanego ryzyka”). Faktyczna „głębokość” tychże obowiązków zależeć będzie w dużej mierze od wydanych na podstawie nowych przepisów aktów wykonawczych. Szczegółowe parametry tychże obowiązków, takie jak minimalny zakres ww. środków technicznych i organizacyjnych, czy sposób dokumentowania ich, mają być zgodnie z analizowanym projektem opisane w rozporządzeniu ministra właściwego ds. informatyzacji. Minister ten będzie również określał próg incydentu telekomunikacyjnego, którego przekroczenie spowoduje obowiązek zgłoszenia incydentu przez przedsiębiorcę. Należy w tym miejscu podkreślić, że proponowane regulacje wykraczają nieco ponad minimalny poziom obowiązków przewidziany w EKŁE, choćby w zakresie dostawców interpersonalnej komunikacji elektronicznej niewykorzystujących numerów. | **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 przez ustawę wprowadzającą PKE.  Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowym.  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. |
|  | KIGEIT | Rozdział 4a | **Propozycja zmiany:** Przeniesienie Rozdziału 4a art. 20a-20f „obowiązki przedsiębiorców komunikacji elektronicznej” do Rozdziału 5 PKE i dokonanie ich ujednolicenia  **Uzasadnienie:**  Zakres rozdziału 4 a pokrywa się z treścią rozdziału 5 PKE. Istnieje ryzyko powstania wątpliwości interpretacyjnych i trudności w stosowaniu przepisów w praktyce. Obowiązki związane z kwestiami cyberbezpieczeństwa podlegają wymogom Art. 13a i 13b dyrektywy 2002/21/WE. | **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 przez 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. |
|  | SayF | Rozdział 4a | Pełny obraz obowiązków przedsiębiorcy komunikacji elektronicznej będzie znany po analizie przepisów z zakresu bezpieczeństwa zawartych w KSC oraz w PKE.  Proponuje się przeredagować Rozdział 4 w taki sposób, aby obowiązki tam określone związane były wyłącznie z cyberbezpieczeństwem w komunikacji elektronicznej.  Regulując sprawy związane z „sytuacjami szczególnego zagrożenie” rozszerza się zakres regulacji o przedmioty nie mające wiele (albo nic) wspólnego z cyberbezpieczeństwem.  Na przykład: co wspólnego z cyberbezpieczeństwem ma działanie przedsiębiorcy telekomunikacyjnego po wprowadzeniu stanu nadzwyczajnego? | **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 przez ustawę wprowadzającą PKE.  Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowyvm.  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. |
|  | Polska Izba Handlu | Art. 2 pkt 12 projektu  Rozdział 4a | **Propozycja zmiany:** Przeniesienie Rozdziału 4a art. 20a-20f „obowiązki przedsiębiorców komunikacji elektronicznej” do Rozdziału 5 PKE i dokonanie ich ujednolicenia.  **Uzasadnienie:**  Zakres rozdziału 4 a pokrywa się z treścią rozdziału 5 PKE. W przeciwnym wypadku istnieje ryzyko powstania wątpliwości interpretacyjnych i trudności w ich stosowaniu w praktyce. Obowiązki związane z kwestiami cyberbezpieczeństwa podlegają wymogom Art. 13a i 13b dyrektywy 2002/21/WE. | **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 przez ustawę wprowadzającą PKE.  Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowym.  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. |
|  | Fundacja Bezpieczna Cyberprzestrzeń | [ustawa zmieniana] art. 8 pkt 2 lit c | proponuje się usunąć ten przepis. Rozciąga on w sposób nieuzasadniony zakres systemu zarządzania bezpieczeństwem w systemie informacyjnym wykorzystywanym do świadczenia usługi kluczowej na usługi, które mogą nie być świadczone w sposób elektroniczny oraz które są świadczone przez podmioty zewnętrze, tym samym to w zakresie ich odpowiedzialności powinno być utrzymanie ciągłości ich działania | **Uwaga nieuwzględniona**  Uwaga nie dotyczy projektowanej ustawy. |
|  | Fundacja Bezpieczna Cyberprzestrzeń | [ustawa zmieniana] art. 8 pkt 5 lit. c | Proponuje się usunąć ten przepis. Przedmiotowy przepis zawiera się w przepisie w lit. a . | **Uwaga nieuwzględniona**  Uwaga nie dotyczy projektowanej ustawy. |
|  | Fundacja Bezpieczna Cyberprzestrzeń | [ustawa zmieniana] art. 11 ust. pkt 1 | Proponuje się usunąć ten przepis. Obsługa incydentu zawiera się w szerszym znaczeniowo zarządzaniu incydentem, który jest obowiązkiem z art. 8 pkt 4. Wydaje się, że nie można zarządzać incydentem, nie podejmując jego obsługi lub co najmniej są to pojęcia tożsame (np. FIRST CSIRT Services Framework nie wymienia oddzielnej usługi ani funkcji związanej z obsługą w obszarze zarządzania incydentami wskazując szereg usług, które mogą być utożsamiane z obsługą incydentu np. triage, analizy czy reagowanie). | **Uwaga nieuwzględniona**  Uwaga nie dotyczy projektowanej ustawy. |
|  | KIGEIT | Art. 1 pkt 30 Projektu | **Propozycja dodania art. 67d:**  *„****Art. 67d.*** *1. Postępowanie przed Pełnomocnikiem lub Kolegium toczy się na podstawie przepisów ustawy z dnia 14 czerwca 1960 r. - Kodeks postępowania administracyjnego ze zmianami wynikającymi z niniejszej ustawy.”*  **Uzasadnienie:**  W projektowanych przepisach zostały przewidziane modyfikacje wobec regulacji przewidzianych w KPA, wobec czego zasadne jest potwierdzenie zakresu stosowania przepisów KPA w odniesieniu do postępowań toczących się przed Pełnomocnikiem lub Kolegium | **Wyjaśnienie**  Stosowny przepis został dodany w nowelizacji |
|  | PKN Orlen | Art. 1 ust. 3 Projektu | Propozycja nadania art.  1 punkt 3) Projektu następującego brzmienia:  „ użyte w art. 4 w pkt 6, w art. 7 w ust. 7 oraz w art. 9 w ust. 2, w różnej liczbie i różnym przypadku, wyrazy „sektorowy zespół cyberbezpieczeństwa ”, zastępuje się użytymi w odpowiedniej liczbie i odpowiednim przypadku wyrazami „ CSIRT sektorowy ”. ”  „użyte w art. 12 w ust. 3 i 4, w art. 13 w ust. 3, w art. 15 w ust. 2 w pkt   1. w art. 26 w ust. 3 w pkt 10, w art. 42 w ust. 1 w pkt 5, w art. 44, w art. 48 w pkt 1, w art. 49 w ust. 3, w art. 64, w art. 65 w ust. 1 w pkt 2 i 2. w art. 66 w ust. 7   oraz w art. 93 w ust. 11 w pkt 4 w różnej liczbie i różnym przypadku, wyrazy „ sektorowy  zespół cyberbezpieczeństwa ”, zastępuje się użytymi w odpowiedniej liczbie i odpowiednim  przypadku wyrazami „ CSIRT sektorowy ” **oraz „CSIRT grupy kapitałowej”. ”**   1. Wprowadzenie pojęcia „CSIRT grupy kapitałowej” ma **zapewnić możliwość ustanowienia CSIRT grupy kapitałowej w ramach krajowego systemu cyberbezpieczeńs twa.** 2. Podział na dwie grupy przepisów wynika z tego, iż zdaniem PKN Orlen obowiązki i prawa wymienione w art. art. 4 w pkt 6, w art. 7 w ust. 7, w art. 9 w ust. 2 oraz w art. 11 w ust. 3 aktualnej Ustawy o KSC **nie powinny dotyczyć** CSIRT grupy kapitałowej. 3. Jednocześnie   uprzejmie zauważamy, że art. 11 ust. 3 Ustawy o KSC już jest zmieniany w treści Projektu w wyniku czego  zawarcie odwołania w  punkcie Projektu wprowadzającym omawianą zmianę nie ma  uzasadnienia. | **Uwaga nieuwzględniona.**  Nie jest konieczne tworzenie nowego rodzaju CSIRT. Zadania doskonale wypełni podmiot w ramach grupy kapitałowej świadczący usługę SOC dla operatorów usługi kluczowej w ramach grupy kapitałowej. |
|  | PKN Orlen | Art. 4 pkt 16 Projektu | Propozycja zmiany aktualnego art. 4 punkt 16) Ustawy o KSC jak poniżej:  „Podmiot prowadzący SOC. ”  W przypadku przyjęcia zawartego w Projekcie art. 4 punkt 16) Projektu doszłoby do sytuacji, w ramach której SOC stanowiłyby odrębne podmioty krajowego systemu cyberbezpieczeństwa. | **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.  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. |
|  | Transition Software | Art. 4 ust. 5 PZP | *Art. 4. Ustawy nie stosuje się do:(…)*  *5) zamówień lub konkursów:*  *a) którym nadano klauzulę zgodnie z przepisami o ochronie informacji niejawnych, lub*  *b) jeżeli wymaga tego istotny interes bezpieczeństwa państwa, lub*  *c) jeżeli wymaga tego ochrona bezpieczeństwa publicznego, lub*  *d) którym muszą towarzyszyć, na podstawie odrębnych przepisów, szczególne środki bezpieczeństwa*  *– w zakresie, w jakim ochrona istotnych interesów dotyczących*  *-bezpieczeństwa państwa określonych w lit. a–d nie może zostać*  *zagwarantowana w inny sposób niż udzielenie zamówienia bez zastosowania ustawy;* | **Wyjaśnienie**  W ramach projektu zrezygnowano ze zmian w Prawie Zamówień Publicznych. |
|  | Transition Software | Art., 131a PZP | 1. *(…);*   *1a. Przepisy niniejszego rozdziału stosuje się do zamówień dotyczących infrastruktury krytycznej, o której mowa w ustawie z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym.*  *2. Przepisy niniejszego rozdziału stosuje się również do zamówień obejmujących równocześnie zamówienia w dziedzinach obronności i bezpieczeństwa oraz inne zamówienia, do których zastosowanie mają przepisy ustawy, jeżeli udzielenie jednego zamówienia jest uzasadnione z przyczyn obiektywnych.*  *3. Ustawy nie stosuje się do zamówień obejmujących równocześnie zamówienia w dziedzinach obronności i bezpieczeństwa oraz zamówienia, co do których wyłączono stosowanie ustawy, jeżeli udzielenie jednego zamówienia jest uzasadnione z przyczyn obiektywnych* | **Wyjaśnienie**  W ramach projektu zrezygnowano ze zmian w Prawie Zamówień Publicznych. |
|  | PKN Orlen | Art. 2 pkt 4a KSC | Propozycja dodania do Ustawy o KSC art. 2 punkt 4a), w myśl którego:  „grupa kapitałowa - rozumie się przez to wszystkich przedsiębiorców, którzy są kontrolowani w sposób bezpośredni lub pośredni przez jednego przedsiębiorcę (w tym również tego przedsiębiorcę), do  którego należy więcej niż jeden operator usługi kluczowej z określonego sektora. ”  Wprowadzenie definicji pojęcia ,grupy kapitałowej” ma zapewnić możliwość wprowadzenia do Ustawy o KSC pojęcia „CSIRT grupy kapitałowej”' | **Uwaga nieuwzględniona.**  Nie jest konieczne tworzenie nowego rodzaju CSIRT (i dodawania definicji grupy kapitałowej). Zadania doskonale wypełni podmiot w ramach grupy kapitałowej świadczący usługę SOC dla operatorów usługi kluczowej w ramach grupy kapitałowej. |
|  | PKN Orlen | Art. 3 pkt 6a KSC | Propozycja dodania do Ustawy o KSC art. 3 punkt 6a), w myśl którego  „ CSIRT grupy kapitałowej - Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający w **ramach oraz na poziomie grupy kapitałowej** ustanowiony przez organ właściwy do spraw cyberbezpieczeństwa. ”  Wprowadzenie definicji pojęcia „CSIRT grupy kapitałowej” ma zapewnić możliwość ustanowienia „CSIRT grupy kapitałowej” w ramach krajowego systemu cyberbezpieczeństwa. | **Uwaga nieuwzględniona.**  Nie jest konieczne tworzenie nowego rodzaju CSIRT. Zadania doskonale wypełni podmiot w ramach grupy kapitałowej świadczący usługę SOC dla operatorów usługi kluczowej w ramach grupy kapitałowej. |
|  | PKN Orlen | Art. 4 pkt 6a KSC | Propozycja dodania do Ustawy o KSC art. 4 punkt 6a) jak poniżej:„ CSIRT grupy kapitałowej”  W przypadku zawarcia w krajowym systemie cyberbezpieczeństwa „CSIRT grupy kapitałowej” niezbędne jest uwzględnienie w/w podmiotu w kolejnych przepisach Ustawy o KSC. | **Uwaga nieuwzględniona.**  Nie jest konieczne tworzenie nowego rodzaju CSIRT. Zadania doskonale wypełni podmiot w ramach grupy kapitałowej świadczący usługę SOC dla operatorów usługi kluczowej w ramach grupy kapitałowej. |
|  | PKN Orlen | Obecne przepisy Ustawy o KSC czyli: art. 26 ust. 4., art. 32 ust. 4., art. 34 ust. 1, art. 39 ust. 1 - ust. 3 oraz ust 5 - ust. 9 art. 40 oraz art. 46, **które zawierają pojęcie: „sektorowy zespół cyberbezpieczeństwa”.** | Przepisy projektu zastępują w treści przepisów wymienionych obok pojęcie „ sektorowy zespół cyberbezpieczeństwa ” użytymi w odpowiedniej liczbie odpowiednim przypadku pojęciami: „ CSIRT sektorowy i CSIRT Telco. ”.   1. Propozycja zastąpienia pojęcia „ sektorowy zespół cyberbezpieczeństwa ” użytymi w odpowiedniej liczbie i odpowiednim przypadku pojęciami: „ CSIRT sektorowy, CSIRT Telco oraz **CSIRT grupy** **kapitałowej.”** 2. Ponadto w projektowanych przepisach Projektu (np. art. 46 ust. 2a)) pojęcia „CSIRT sektorowy oraz CSIRT Telco” należy zastąpić użytymi w odpowiedniej liczbie i odpowiednim przypadku: „ CSIRT sektorowy, CSIRT TELCO oraz CSIRT grupy kapitałowej ”.   W przypadku zawarcia w krajowym systemie cyberbezpieczeństwa „ CSIRT grupy kapitałowej ” **niezbędne jest uwzględnienie w/w podmiotu w kolejnych przepisach Ustawy o KSC.** | **Uwaga nieuwzględniona.**  Nie jest konieczne tworzenie nowego rodzaju CSIRT. Zadania doskonale wypełni podmiot w ramach grupy kapitałowej świadczący usługę SOC dla operatorów usługi kluczowej w ramach grupy kapitałowej. |
|  | Izba Gospodarcza Gazownictwa/Polska Spółka Gazownictwa Sp. z.o.o. | OSR - Katalog Opisu usług | **Szacowane terminy dla poszczególnych usług**  Prosimy o rozważenie podziału szacowanych terminów realizacji poszczególnych usług z Katalogu Usług cyberbezpieczeństwa wg np. kryterium wielkości firmy/ilości zatrudnionych pracowników.  Z naszych doświadczeń wynika, że usługa np. analizy podatności - może być znacznie dłuższa niż proponowane 4-8 dni czy też usługa podnoszenia świadomości o zagrożeniach, przy ponad 10 tys. Pracownikach, nie jest w stanie być zrealizowana w zaproponowanym terminie 8-15 roboczodni, chyba że założenia terminowe dotyczyłyby tylko konkretnych działań w ramach tych usług. | **Uwaga nieuwzględniona**  Terminy podane w OSR są prawidłowe. |
|  | KIGEIT | OSR | **Brak przeprowadzenia oceny skutków regulacji**  Zmiany zawarte w projekcie nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa mogą wiązać się z daleko idącymi negatywnymi skutkami społecznymi (likwidacja miejsc pracy, obniżenie dostępności nowoczesnych usług, wzrost wykluczenia cyfrowego), gospodarczymi (obniżenie konkurencyjności polskiej gospodarki, spadek zaufania inwestorów oraz wzmocnienie oligopoli) i politycznymi (uderza w harmonizację europejską oraz relacje międzynarodowe z krajami dotkniętymi sankcjami). Wynika to z konieczności wymiany sprzętu oraz aplikacji, które są obecnie w użyciu, na alternatywne, pochodzące od innych dostawców. Tymczasem w uzasadnieniu Projektu na s. 33 poświęconym skutkom gospodarczym i finansowym w ogóle nie ma o tym mowy. Wspomina się tylko o kosztach związanych z powoływaniem nowych struktur administracyjnych z zakresu cyberbezpieczeństwa (s. 49-52 uzasadnienia Projektu). Jest to istotne naruszenie procesu legislacyjnego (§ 28 Regulamin Pracy Rady Ministrów,t.j. M.P. z 2016 r. poz. 1006) świadczące o wadliwym charakterze Projektu. | **Uwaga częściowo uwzględniona**  OSR został uzupełniony. |
|  | KIGEIT | OSR | **Brak ocen skutków dotyczących projektu ustawy i powiązanych rodzajów ryzyka**   1. Projektodawca nie przeprowadził kompleksowej, wystarczającej i szczegółowej oceny skutków przed konsultacjami publicznymi w sprawie projektu prawa. 2. Projekt ustawy będzie miał istotny wpływ na operatorów i dostawców (własność, ciągłość działalności, otoczenie biznesu, wolna konkurencja, gospodarka krajowa). 3. Operatorzy, dostawcy, stowarzyszenia branżowe ICT oraz odpowiednie zainteresowane strony nie są w stanie ocenić wpływu projektu ustawy w wyznaczonym terminie. 4. Termin wyznaczony na konsultacje publiczne nie jest zgodny z rygorem przejrzystości procesu decyzyjnego w administracji publicznej ze względu na znaczące skutki projektu ustawy, a także bez wstępnych konsultacji z zainteresowanymi stronami.   **Potencjalny wpływ projektu ustawy na dostawców**   1. Kryteria oceny są niejasne, nieprzejrzyste, a zakres oceny jest zbyt szeroki. 2. Kryteria oceny są zbyt polityczne i nie obejmują mechanizmu norm technicznych i certyfikacji, takich jak NESAS i ENISA. 3. Spowoduje to dyskryminację między producentami i naruszenie konstytucyjnego prawa do dostaw towarów w Polsce i zakłócenie konkurencji.   **Potencjalny wpływ projektu ustawy na operatorów telekomunikacyjnych**   1. Obecnie nie ma zbyt wielu dostawców technologii 5G, więc wymagane ogromne zmiany w ramach sieci komórkowych, mogą opóźnić się o 3-5 lat. 2. Prawo operatorów do wyboru producenta będzie ograniczone. Ministerstwo Obrony Narodowej i Kolegium powinni ustanowić jasne kryteria techniczne i wymogi, do których operatorzy powinni się stosować. W przeciwnym razie naruszy to prawo konkurencji na szczeblu krajowym. Ostateczny wybór dostawcy przez operatorów powinien opierać się na normach techniki i technologii, innowacji, kosztów oraz bezpieczeństwa cybernetycznego. 3. Może dojść do określonych strat aktywów i dodatkowych nieprzewidzianych przez operatorów kosztów (migracji, integracji systemów), które mogą wpłynąć na koszt usług co znajdzie przełożenie w cenach taryf i innych usług. 4. Dla operatorów w Polsce projekt ustawy będzie miał poważne negatywne implikacje i będzie wyrządzał wielką szkodę ich poprzednim inwestycjom i prawom własności. Projekt tego prawa nie daje pewności prawa i zwiększa koszty operacyjne, co jest sprzeczne z warunkami określonymi w decyzjach administracyjnych dotyczących prowadzenia działalności.   **Potencjalny wpływ projektu ustawy na konkurencję**   1. W Polsce nie ma aż tak wielu dostawców sprzętu do sieci. Jeśli jeden z dostawców zostanie wyłączony, będzie to bardzo szkodzić innowacjom w technologii i odroczy digitalizację Polski. Może to też oznaczać wzrost kosztów operatorów. 2. Przesłanki bezpieczeństwa narodowego nie powinno się nadużywać, a wyjątek dotyczący bezpieczeństwa narodowego powinien być stosowany z zachowaniem zasad proporcjonalności, obiektywności, przejrzystości i minimalnej ingerencji.   **Potencjalny wpływ projektu ustawy na budżet Polski i gospodarkę krajową**   1. Mogą wystąpić straty w sektorze ICT (potencjalny wzrost cen z powodu braku konkurencji). Straty mogą powstać także w całej gospodarce (lokalne zatrudnienie, zamówienia publiczne, negatywny wpływ na PKB). 2. Projekt ustawy może mieć negatywny wpływ na gotowość podmiotów do składania ofert na spektrum 5G. 3. Ograniczenie operatorów do wyboru dostawcy może odroczyć również uruchomienie sieci 5G, a tym samy opóźni to rozwój Przemysłu 4.0. Może to przełożyć się na brak wykorzystania nowego „skoku technologicznego” (jakim jest Przemysł 4.0) do zbudowania kompetencji w tym obszarze. Szansę taką (jako Polska) już raz udało się wykorzystać budując kompetencje przemysłu elektronicznego w zakresie montażu elektronicznego (przejście z technologii telewizorów CRT na LCD).   **Potencjalny wpływ projektu ustawy na postęp technologiczny**   1. Wyłączenie jakiegokolwiek producenta, spowoduje opóźnienie postępu w całym ekosystemie. Polska utraci możliwość skorzystania z dojrzałego ekosystemu 5G innych krajów. 2. Negatywny wpływ na życie i pracę podczas pandemii i po pandemii: jeśli Polska opóźni wdrożenie 5G, może to ograniczyć wzrost miejsc pracy, który wiązany jest z nową technologią. 3. Projekt ustawy będzie miał negatywny wpływ na rozwój Przemysłu 4.0 i może opóźnić szansę na stworzenie kompetencji w obszarze „usieciowienia gospodarki” w tym m.in.: urządzeń sieciowych nowej generacji, jak np.: samochodów podłączonych do sieci 5G, maszyn produkcyjnych 5G, różnych urządzeń high-tech w automatyce i sterowaniu, maszyn rolniczych i systemów dla produkcji rolniczej, usług portowych, zdalnej edukacji, sprzętu medycznego, itp. 4. Projekt ustawy nie generuje zachęty dla odbudowy i rozwoju krajowego potencjału technologicznego w obszarze wytwarzania podzespołów elektronicznych (rewitalizacja przemysłu mikroelektronicznego). | **Uwaga częściowo uwzględniona**  OSR został uzupełniony. |
|  | Polska Izba Handlu | OSR | **Brak ocen skutków dotyczących projektu ustawy i powiązanych rodzajów ryzyka；**   1. Projektodawca nie przeprowadził kompleksowej, wystarczającej i szczegółowej oceny skutków przed konsultacjami publicznymi w sprawie projektu prawa; 2. projekt ustawy będzie miał istotny wpływ na operatorów i dostawców (własność, ciągłość działalności, otoczenie biznesu, wolna konkurencja, gospodarka krajowa); 3. Operatorzy, dostawcy, stowarzyszenia branżowe ICT oraz odpowiednie zainteresowane strony nie są w stanie ocenić wpływu projektu ustawy w ciągu zaledwie 10 dni roboczych; 4. Termin wyznaczony na konsultacje publiczne 22.09.2020 nie jest zgodny z rygorem przejrzystości procesu decyzyjnego w administracji publicznej ze względu na znaczące skutki projektu ustawy, a także bez wstępnych konsultacji z zainteresowanymi stronami.   **Potencjalny wpływ projektu ustawy na dostawców；**   1. kryteria oceny są niejasne, nieprzejrzyste, a zakres oceny jest zbyt szeroki 2. Kryteria oceny są zbyt polityczne i nie obejmują mechanizmu norm technicznych i certyfikacji, 3. Spowoduje to dyskryminację między producentami i naruszenie konstytucyjnego prawa do dostaw towarów w Polsce i zakłócenie konkurencji; projekt jest sprzeczny z zasadą niedyskryminacji i równego traktowania UE.   **Potencjalny wpływ projektu ustawy na operatorów telekomunikacyjnych；**   1. Ze względu na brak wiodących dostawców technologii 5G, jak również wymagane ogromne zmiany w ramach sieci komórkowych, Polska 5G i Agenda Cyfrowa mogą opóźnić 3-5 lat; 2. Operatorzy mogą stracić zaufanie do otoczenia inwestycyjnego naszego kraju Mogą oni również stracić siłę napędową w celu przyspieszenia uruchomienia 5G z powodu ograniczenia inwestycji i opóźnień technicznych. 3. Prawo operatorów do wyboru producenta będzie ograniczone. Ustawodawca i rząd powinni ustanowić jasne kryteria techniczne i wymogi, do których operatorzy powinni się stosować. W przeciwnym razie naruszy to prawo konkurencji zarówno na szczeblu krajowym, jak i unijnym. Ostateczny wybór dostawcy przez operatorów powinien opierać się na normach technologii, innowacji, kosztów i bezpieczeństwa cybernetycznego; 4. Dla operatorów w Polsce, projekt ustawy będzie miał poważne negatywne implikacje i będzie wyrządzał wielką szkodę ich poprzednim inwestycjom i prawom własności. Projekt tego prawa nie daje pewności prawa i zwiększa koszty operacyjne, co jest sprzeczne z warunkami określonymi w decyzjach administracyjnych dotyczących prowadzenia działalności.   **Potencjalny wpływ projektu ustawy na konkurencję；**   1. Polska ma ograniczoną liczbę dostawców sieci. Jeśli jeden z dostawców zostanie wyłączony, będzie to bardzo szkodzić innowacjom w technologii i odroczy digitalizację Polski. Koszty operatorów wzrosną , a ceny usług dla konsumentów wzrosną ; 2. Artykuł 3 pkt 1 ustawy o zwalczaniu nieuczciwej konkurencji i nie pozwala na utrudnienie dostępu do rynku 3. Przyczyny bezpieczeństwa narodowego nie powinno się nadużywać, a wyjątek dotyczący bezpieczeństwa narodowego powinien być stosowany z zachowaniem zasada proporcjonalności , obiektywności, przejrzystości i minimalnej ingerencji.   **Potencjalny wpływ projektu ustawy na budżet Polski i gospodarkę krajową；**   1. Ponad 8 mld euro straty w sektorze telekomunikacyjnym (wzrost cen z powodu braku konkurencji) ponad 10 mld euro straty w całej gospodarce (lokalne zatrudnienie, zamówienia publiczne, negatywny wpyw na PKB) 2. Projekt ustawy będzie miał negatywny wpływ na gotowość podmiotów do składania ofert na infrastrukturę i usługi 5G; 3. Ograniczenie operatorów do wyboru dostawcy odroczy również uruchomienie sieci 5G, Rozwój Przemysłu 4.0 zostanie zablokowany. Polska ucierpi na brakach związanych z niskimi kompetencjami w dziedzinie kompetencji międzynarodowych 4. Roszczenia o odszkodowanie wobec rządu polskiego podniesione przez operatorów i dostawców zostaną ostatecznie wypłacone przez podatników i konsumentów. Budżet będzie zasilał operatorów i producentów zamiast ułatwić życie obywatelom, , szczególnie po pandemii   **Potencjalny wpływ projektu ustawy na postęp technologiczny；**   1. Wyłączenie producenta, zwłaszcza wiodącego w branży ICT, spowoduje opóźnienie postępu w całym ekosystemie. Polska utraci możliwość skorzystania z rozwiniętej infrastruktury 5G innych krajów. 2. Operatorzy mogą stracić zaufanie do otoczenia inwestycyjnego w Polsce,. Mogą oni również stracić siłę napędową przyspieszenia uruchomienia 5G z powodu ograniczenia inwestycji i opóźnień technicznych. 3. Negatywny wpływ na życie i pracę podczas pandemii i po pandemii: jeśli Polska opóźni wdrożenie 5G, straci możliwość stworzenia nowych miejsc pracy dla ponad 250 000 osób 4. Projekt ustawy będzie miał negatywny wpływ na rozwój Przemysłu 4.0, Polska straci kompetencje w obszarze samochodów podłączonych do sieci 5G, produkcji 5G, high-tech, rolnictwo 5G, usługi portowe, zdalna edukacja, sprzęt medyczny 5G. itp | **Uwaga częściowo uwzględniona**  OSR zostanie uzupełniony. |
|  | Stowarzyszenie Inżynierów Telekomunikacji | OSR  Art. 66b | W uzasadnieniu zmian, oceniając skutki regulacji wskazano wyłącznie, że nowoprojektowane przepisy będą mieć wpływ na przedsiębiorców telekomunikacyjnych i to tylko w takim zakresie, że zamiast do Prezesa UKE będą oni zobligowani zgłaszać incydenty do zespołów CSIRT, uznając jednocześnie brak skutków dla tego sektora w ujęciu pieniężnym.  Należy jednak podkreślić, że w opisie celu i skutkach wprowadzenia art. 66b do ustawy o cyberbezpieczeństwie pominięte zostały koszty wymiany sprzętu lub oprogramowania, który był dostępny na rynku i z którego branża telekomunikacyjna korzystała przy budowie sieci i  świadczeniu usług. Nie można uznać, że takie działanie jest bez kosztowe. Wymiana sprzętu lub oprogramowania (często niezamortyzowanego księgowo) na nowy, wygeneruje dodatkowe  koszty dla przedsiębiorcy telekomunikacyjnego, koszty, których poniesienia nie mógł przewidzieć, decydując się na zakup sprzętu lub oprogramowania, które następnie musi wycofać.  Biorąc powyższe pod uwagę, wnosimy o uwzględnienie przedstawionych argumentów i wprowadzenie odpowiednich zmian w art. 66b ustawy o cyberbezpieczeństwie. | **Uwaga częściowo uwzględniona**  OSR zostanie uzupełniony. |
|  | EXATEL | OSR | Niezależnie od wyżej wymienionych zagrożeń wskazać należy, że w kosztach OSR budowy i funkcjonowanie CSIRT nie uwzględniono części kosztów, które niewątpliwie powstaną przy budowie CSIRT:   1. **Kosztów dotyczących etatyzacji:**  * kosztów utrzymania kadry zarządczej dla CSIRT (poza administratorem ktoś musi zarządzać całą strukturą), * kosztów rekrutacji z rynku potrzebnych pracowników (koszt zewnętrznej rekrutacji na jeden etat to minimum 20 000 zł miesięcznie brutto), * kosztów szkolenia pozyskanych pracowników (koszty od 10 000 zł rocznie na pracownika),  1. **Kosztów pośrednich dotyczących budowy CSIRT**  * kosztów technicznego przystosowania pomieszczeń do budowy CSIRT; * kosztów przygotowania koncepcji dla samego sposobu funkcjonowania CSIRT, wyboru platformy sprzętowej; * kosztów narzędzi niezbędnych do obsługi incydentów (np. serwery, systemy trackingowe do obsługi zgłoszeń etc.)   Biorąc powyższe pod uwagę, istnieją zagrożenia, które mogą uniemożliwić budowę CSIRT przez organy właściwe. Z tego względu wskazujemy, że konieczne jest umożliwienie organom właściwym zlecanie funkcji CSIRT sektorowego jednostkom spoza art. 4 ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych (Dz. U. poz. 2019), w szczególności spółkom kontrolowanym w 100% przez Skarb Państwa. Niezbędne i zasadne wydaje się być wykorzystanie  w tym procesie podmiotów będących własnością Skarbu Państwa i dysponujących niezbędnym doświadczeniem w zakresie budowy i funkcjonowania SOC.  Zlecanie części zadań na zewnątrz da dostęp do zasobów ludzkich i narzędzi, a poprzez to umożliwi szybkie osiągnięcie zdolności operacyjnej do świadczenia usług CSIRT w planowanym okresie 18 miesięcy od dnia wejścia w życie niniejszej ustawy. Dostęp do wiedzy bazującej na zdobytych już doświadczeniach z rynku przez podmioty świadczące podobne usługi zapewni transfer wiedzy niezbędny do wypracowania wewnętrznych procedur. Ponadto wykorzystanie istniejących już zasobów po stronie Skarbu Państwa przyczyni się do obniżenia kosztów funkcjonowania samego systemu CSIRT sektorowych. W przypadku powierzenie realizacji CSIRT działającemu już podmiotowi dojdzie do efektu synergii, a poprzez to obniżenia kosztów jednostkowych. Biorąc powyższe pod uwagę zasadnym i koniecznym jest dopisanie do katalogu podmiotów, którym może zostać powierzona realizacja zadań CSIRT sektorowego spółkom akcyjnym pozostającym pod całkowitą kontrolą Skarbu Państwa. | **Uwaga nieuwzględniona.**  CSIRT sektorowe mają być wyznaczone w pierwszej kolejności spośród jednostek podległych lub nadzorowanych przez organ właściwy do spraw cyberbezpieczeństwa, który już funkcjonuje. |
|  | Związek Banków Polskich | Art. 2 pkt. 5 | **Propozycja zmiany**  Incydent - każde zdarzenie, które ma rzeczywiście niekorzystny wpływ na bezpieczeństwo sieci i systemów informatycznych;  **Uzasadnienie:**  Konieczność dostosowania definicji do definicji w Dyrektywie Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii. | **Uwaga nieuwzględniona**  Dyrektywy unijne mają być wdrożone do porządku prawnego państwa członkowskiego w sposób zgodny z celem dyrektywy, niekoniecznie musi to oznaczać dosłowne skopiowanie treści dyrektywy.  Obecna definicja incydentu dobrze spełnia swoją funkcję obejmując wszystkie zdarzenia zagrażające sieciom i systemom informatycznym. |
|  | Związek Banków Polskich | Art. 2 pkt. 12 | **Propozycja zmiany**  12) Ryzyko - każdą dającą się racjonalnie określić okoliczność lub zdarzenie, które ma potencjalny niekorzystny wpływ na bezpieczeństwo sieci i systemów informatycznych;  **Uzasadnienie:**  Konieczność dostosowania definicji do definicji w Dyrektywie Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii. | **Uwaga nieuwzględniona**  Dyrektywy unijne mają być wdrożone do porządku prawnego państwa członkowskiego w sposób zgodny z celem dyrektywy, niekoniecznie musi to oznaczać dosłowne skopiowanie treści dyrektywy. |
|  | Związek Banków Polskich | Art. 5 –  Załącznik nr 1 Bankowość i infrastruktura rynków finansowych | **Propozycja zmiany:**  **Proponuje się dodanie do załącznika nr 1 - Bankowość i infrastruktura rynków finansowych następujące podmioty: - dostawców usług płatniczych, o których mowa w art. 4 ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych; - krajowa instytucja płatnicza, o której mowa w art. 2 pkt 16 ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych; - izba rozliczeniowa, o której mowa w art. 67 ustawy z dnia 29 sierpnia 1997 r. - Prawo bankowe.**  **Uzasadnienie:**  Brak ww. podmiotów powoduje stworzenie luki w systemie płatniczym kraju, co oznacza faktyczną niemożliwość wykrywania, przeciwdziałania i zwalczania cybericydnetów w obszarze realizacji i rozliczeń transakcji płatniczych. | **Uwaga nieuwzględniona**  Uwaga nie dotyczy projektu nowelizacji. Na dzień dzisiejszy nie planuje się zmiany treści załącznika nr 1. |
|  | Związek Banków Polskich | Art. 8 pkt 7) (nowy) | **Propozycja zmiany:**  Proponuje się dodanie w art. 8 pkt 7 w brzmieniu: **7) zasoby ludzkie adekwatne do zakresu świadczonych usług kluczowych oraz ryzyka związanego ze świadczeniem tych usług.**  **Uzasadnienie:**  Posiadanie odpowiednich i proporcjonalnych do ryzyka środków technicznych i organizacyjnych, bez zapewnienia odpowiedniego i kompetentnego zespołu pracowników, będzie niekompletnym systemem cyberbezpieczeństwa, gdyż system ten winieni opierać się na trzech równoważnych komponentach: sprzęcie, procesach i ludziach. | **Uwaga nieuwzględniona** |
|  | Związek Banków Polskich | Art. 9 ust. 1 pkt. 1 | **Propozycja zmiany:**  Proponuje się aby w art. 9 ust. pkt 1 otrzymał brzmienie: Operator usługi kluczowej:  1) wyznacza osobę, **osoby** **lub komórkę organizacyjną** odpowiedzialne za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa.  **Uzasadnienie:**  Nie możemy wyznaczyć fizycznie jednej osoby musi to być cała lista kontaktowa osób lub tzw. punktu kontaktowego | **Uwaga nieuzwględniona**  Istotą jest, żeby była możliwość kontaktu z konkretną osobą podczas obsługi incydentu. |
|  | Związek Banków Polskich | Art. 12. Ust. 3 | **Propozycja zmiany:**  Proponuje się aby w art. 12 ust. 3 otrzymał brzmienie: 3. Operator usługi kluczowej przekazuje w niezbędnym zakresie w zgłoszeniu, o którym mowa w ust. 1, **dane osobowe** i informacje stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa, gdy jest to konieczne dla realizacji zadań, właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV.  **Uzasadnienie:**  Ustawa wyraźnie rozgranicza dane osobowe od tajemnic prawnie chronionych. W związku z potrzebą sprawnej obsługi incydentu, jego koordynacji i zarządzania często zdarza się konieczność przekazania nie tylko tajemnic prawnie chronionych ale także danych osobowych np. osób pokrzywdzonych w celu ich ochrony | **Uwaga nieuwzględniona**  Już jest to uregulowane w art. 11 ust 1 pkt 5 in fine. |
|  | Związek Banków Polskich | Art. 15 ust. 2 pkt 2 | **Propozycja zmiany:**  2. Audyt może być przeprowadzony przez:  2) **zespół składający się z** co najmniej dwóch audytorów posiadających:  a)certyfikaty określone w przepisach wydanych na podstawie ust. 8 lub  b)co najmniej trzyletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych, lub  c)co najmniej dwuletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych i legitymujących się dyplomem ukończenia studiów podyplomowych w zakresie audytu bezpieczeństwa systemów informacyjnych, wydanym przez jednostkę organizacyjną, która w dniu wydania dyplomu była uprawniona, zgodnie z odrębnymi przepisami, do nadawania stopnia naukowego doktora nauk ekonomicznych, technicznych lub prawnych;  **Uzasadnienie:**  Proponujemy, aby ustawa wskazywała na możliwość przeprowadzania audytu przez **zespół** co najmniej dwóch audytorów. | **Uwaga nieuwzględniona**  Uwaga nie niesie ze sobą dodatkowej wartości normatywnej. |
|  | Związek Banków Polskich | Art. 26 ust. 3 pkt 12 | **Propozycja zmiany:**  Proponuje się aby w art. 26 ust. 3 pkt. 12 otrzymał brzmienie: 3. Do zadań CSIRT MON, CSIRT NASK i CSIRT GOV, zgodnie z właściwością wskazaną w ust. 5–7, należy: 12) przekazywanie, w terminie do dnia 30 maja każdego roku, do Pojedynczego Punktu Kontaktowego zestawienia zgłoszonych w poprzednim roku kalendarzowym przez operatorów usług kluczowych incydentów poważnych **mających lub mogących spowodować obniżenie jakości lub** mających wpływ na ciągłość świadczenia przez nich usług kluczowych w Rzeczypospolitej Polskiej oraz ciągłość świadczenia przez nich usług kluczowych w państwach członkowskich Unii Europejskiej, a także zestawienia zgłoszonych w poprzednim roku kalendarzowym przez dostawców usług cyfrowych incydentów istotnych, w tym dotyczących dwóch lub większej liczby państw członkowskich Unii Europejskiej;  **Uzasadnienie:**  Definicja incydentu poważnego określa dwa czynniki a mianowicie:  1. powodujący lub mogący spowodować poważne obniżenie jakości lub  2. przerwanie ciągłości świadczenia usługi kluczowej. Natomiast w art. 26 ust. 3 pkt 12 powołano się chyba błędnie jedynie na kwestie związane z ciągłością świadczenia usługi kluczowej? | **Uwaga nieuwzględniona**  Dyrektywa NIS w art. 14 i 16 mówi wyłącznie o incydentach poważnych lub istotnych. |
|  | Związek Banków Polskich | Art. 26 ust. 3 pkt 14 ppkt a), i c) | **Propozycja zmiany:**  Proponuje się aby art. 26 ust. 3 pkt. 14 ppkt a) i c) otrzymały brzmienie: 3. Do zadań CSIRT MON, CSIRT NASK i CSIRT GOV, zgodnie z właściwością wskazaną w ust. 5–7, należy: 14) zapewnienie zaplecza analitycznego oraz badawczo-rozwojowego, które w szczególności: a) prowadzi zaawansowane analizy złośliwego oprogramowania oraz analizy podatności **i zagrożeń cyberbezpieczeństwa**, ... c) rozwija narzędzia i metody do wykrywania podatności i zagrożeń cyberbezpieczeństwa **oraz skutecznej obsługi incydentów**,  **Uzasadnienie:**  W zakresie analiz oprócz podatności analizowane są także zagrożenia cyberbezpieczeństwa. Dodatkowo nie wolno pominąć przy rozwijaniu narzędzi i metod niezbędnych do zwalczania incydentów. | **Uwaga nieuwzględniona**  Art. 32 już umożliwia analizę zagrożeń cyberbezpieczeństwa. |
|  | Związek Banków Polskich | Art. 26 ust. 5 pkt 3 (nowy) | **Propozycja zmiany:**  Do zadań CSIRT MON należy koordynacja obsługi incydentów zgłaszanych przez:  podmioty, o których mowa w ust. 6, jeżeli incydent wymaga współpracy w zakresie zadań Służby Kontrwywiadu Wojskowego, o których mowa w art. 5 ust. 1 i ust. 2 ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego.  **Uzasadnienie:**  Doświadczenia sektora bankowego wskazują, że podział podmiotowy pomiędzy poszczególnymi CSIRTami jest niewystarczający. W uzasadnionych przypadkach konieczne jest również wprowadzenie podziału przedmiotowego. | **Uwaga nieuwzględniona.**  CSIRT MON koordynuje obsługę incydentu o charakterze terrorystycznym, o którym mowa w art. 5 ust. 1 pkt 2a ustawy o SKW co konsumuję niniejszą uwagę. |
|  | Związek Banków Polskich | Art. 26 ust. 7 pkt 7 (nowy) | **Propozycja zmiany:**  Do zadań CSIRT GOV należy koordynacja obsługi incydentów zgłaszanych przez:  podmioty, o których mowa w ust. 6, jeżeli incydent wymaga współpracy w zakresie zadań Agencji Bezpieczeństwa Wewnętrznego, o których mowa w art. 5 ust. 1 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu.  **Uzasadnienie:**  Doświadczenia sektora bankowego wskazują, że podział podmiotowy pomiędzy poszczególnymi CSIRTami jest niewystarczający. W uzasadnionych przypadkach konieczne jest również wprowadzenie podziału przedmiotowego. | **Uwaga nieuwzględniona.**  CSIRT GOV koordynuje obsługę incydentu o charakterze terrorystycznym co konsumuję niniejszą uwagę. |
|  | Związek Banków Polskich | Art. 30 ust. 3 | **Propozycja zmiany:**  Proponuje się usunięcie art. 30 ust. 3, a dotychczasowy ust. 4 oznaczony zostaje jako ust. 3  **Uzasadnienie:**  Proponuje się usunięcie tego przepisu, gdyż CSIRT NASK miałby możliwość samodzielnie decydować o zarządzaniu danym incydentem. Z doświadczeń sektora bankowego wynika, że bardzo często pierwsze informacje o incydentach pochodzą od klientów i ich zbagatelizowanie mogłoby wpłynąć negatywnie na reputację banku. | **Uwaga nieuwzględniona**  Obsługa incydentów które dotknęły osoby fizyczne i podmioty spoza krajowego systemu cyberbezpieczeństwa nie jest głównym zadaniem CSIRT NASK. Dlatego te zgłoszenia muszą być w miarę dysponowania zasobami przez CSIRT NASK. |
|  | Związek Banków Polskich | Art. 32 ust. 1 | **Propozycja zmiany:**  Proponuje się aby w art. 32 ust. 1 otrzymał brzmienie: 1. CSIRT MON, CSIRT NASK i CSIRT GOV **oraz właściwy CSIRT sektorowy oraz właściwy ISAC dla danego sektora, sektorów lub podsektorów** mogą wykonywać niezbędne działania techniczne związane z analizą **podatności i** zagrożeń cyberbezpieczeństwa, zarządzaniem obsługi incydentu, koordynacją obsługi incydentu poważnego, incydentu istotnego i incydentu krytycznego.  **Uzasadnienie:**  CSIRT sektorowe oraz ISAC mogąc przeprowadzać techniczne analizy zagrożeń mogą w istotny sposób wesprzeć CSIRT MON, CSIRT NASK i CSIRT GOV w zakresie zarządzania incydentami poważnymi, istotnymi i krytycznymi. | **Uwaga nieuwzględniona**  ISAC nie są jednostką operacyjną. Zatem nie może dokonywać analizy podatności, lecz może przekazywać informacje uzyskane od zespołów CSIRT o wykrytych podatnościach. |
|  | Związek Banków Polskich | Art. 34 ust. 3 **- nowy** | **Propozycja zmiany:**  Proponuje się dodanie w art. 34 ust. 3 w brzmieniu: 3. Do CSIRT sektorowych oraz ISAC koordynujących obsługę incydentu, który doprowadził do naruszenia danych osobowych przepis ust. 2 stosuje się odpowiednio.  **Uzasadnienie:**  CISIRT sektorowe i ISAC koordynując obsługę incydentu powinny współpracować z organem właściwym do spraw ochrony danych osobowych. Brak tej możliwości współpracy znacząco ogranicza skuteczność obsługi incydentu przez OUK. | **Uwaga nieuwzględniona.**  ISAC nie są jednostką operacyjną, a więc nie zajmują się na reagowaniem na incydenty. |
|  | Związek Banków Polskich | Art. 37 ust. 2 i 3 | Proponuje się aby było jedno miejsce, w którym będą publikowane informacje o incydentach poważnych i istotnych. Użytkownicy mogą być zdezorientowani gdzie szukać informacji. Dlatego proponuje się ustalenie jednego centralnego miejsca publikacji na poziomie zarządzania ww. incydentami. Dodatkowo, takie publikacje na poziomie koordynacji mogą dokonywać CISRT sektorowe oraz na poziomie obsługi incydentu - operatorzy usług kluczowych oraz dostawcy usług internetowych. | **Uwaga nieuwzględniona.**  Podłączenie się podmiotów krajowego systemu cyberbezpieczeństwa do systemu z art. 46 pozwoli na otrzymywanie tych informacji z tego systemu w ramach określonych w porozumieniu z ministrem do spraw informatyzacji. |
|  | Związek Banków Polskich | Art. 39 ust. 1 | **Propozycja zmiany:**  Proponuje się aby w art. 39 ust. 1 otrzymał brzmienie: Art. 39. 1. W celu realizacji zadań, o których mowa w art. 26 ust. 3 pkt 1–11 oraz 14 i 15 i ust. 5–8 oraz art. 44 ust. 1–3, CSIRT MON, CSIRT NASK, CSIRT GOV **i CSIRT sektorowe oraz ISAC** przetwarzają **informacje stanowiące tajemnice prawnie chronione** oraz **informacje** **związane** z incydentami i zagrożeniami cyberbezpieczeństwa, w tym dane osobowe, obejmujące także dane określone w art. 9 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 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. U. UE L 119 z 04.05.2016, str. 1), zwanego dalej „rozporządzeniem 2016/679”, w zakresie i w celu niezbędnym do realizacji tych zadań.  **Uzasadnienie:**  W celu skutecznego działania CSIRT MON, CSIRT NASK, CSIRT GOV niezbędne jest wprowadzenie podstawy prawnej do przetwarzania informacji stanowiących tajemnice prawnie chronionych oraz dane osobowe.  Konieczne jest również wprowadzenie do tego przepisu CSIRT sektorowych i ISAC. | **Uwaga nieuwzględniona.**  Taki przepis naruszałby zasady przetwarzania informacji niejawnych oraz inne tajemnice prawnie chronione. |
|  | Związek Banków Polskich | Art. 39 ust. 3 | **Propozycja zmiany:**  Proponuje się aby w art. 39 ust. 3 otrzymał brzmienie: 3. CSIRT MON, CSIRT NASK, CSIRT GOV, **CSIRT sektorowe i ISAC** przetwarzają **tajemnice prawnie chronione oraz informacje, w tym dane osobowe** związane z incydentami i zagrożeniami cyberbezpieczeństwa: 1) dotyczące użytkowników systemów informacyjnych oraz użytkowników telekomunikacyjnych urządzeń końcowych; 2) dotyczące telekomunikacyjnych urządzeń końcowych w rozumieniu ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne; 3) gromadzone przez operatorów usług kluczowych i dostawców usług cyfrowych w związku ze świadczeniem usług; 4) gromadzone przez podmioty publiczne w związku z realizacją zadań publicznych dotyczące podmiotów zgłaszających incydent zgodnie z art. 30 ust. 1.  **Uzasadnienie:**  Obok danych osobowy należy dodać również tajemnice prawnie chronione, gdyż wówczas podmioty uprawnione mogą pozyskać kompletną - pełną informację.  Zasadne jest również dodanie do wskazanego przepisu ISAC. | **Uwaga nieuwzględniona**.  Taki przepis naruszałby zasady przetwarzania informacji niejawnych oraz inne tajemnice prawnie chronione. |
|  | Związek Banków Polskich | Art. 39 ust. 7 | **Propozycja zmiany:**  Proponuje się aby w art. 39 ust. 7 otrzymał brzmienie: 7. W celu realizacji zadań określonych w ustawie CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT sektorowy, CISRT telco i **ISAC** mogą przekazywać sobie wzajemnie **informacje**, o których mowa w ust. 3, w zakresie niezbędnym do realizacji tych zadań i współpracować z organem właściwym do spraw ochrony danych osobowych.  **Uzasadnienie:**  W ust. 3 jest mowa nie tylko o danych osobowych, więc wskazane jest aby użyć innego określenia np. informacje.  Ponadto w celu skutecznej realizacji zdań ISAC, zasadne jest wskazanie go również w tym przepisie. | **Uwaga nieuwzględniona**  ISAC nie jest jednostką operacyjną. |
|  | Związek Banków Polskich | Art. 39 ust. 10 - nowy | **Propozycja zmiany:**  Proponuje się dodanie w art. 39 ust. 10 w brzmieniu: 10**. Operatorzy usług kluczowych, dostawcy usług cyfrowych, przedsiębiorcy komunikacji elektronicznej, dostawcy usług internetowych oraz ISAC są uprawnieni do przetwarzania, w tym udostępniania sobie nawzajem informacji stanowiących tajemnice prawnie chronione, w szczególności danych osobowych obejmujących także dane określone w art. 9 ust. 1 rozporządzenia 2016/679, w przypadkach przestępstw lub uzasadnionych podejrzeń popełnienia przestępstw dokonywanych na szkodę operatorów usług kluczowych, dostawców usług cyfrowych, przedsiębiorców telekomunikacyjnych oraz dostawców usług internetowych oraz ich klientów w celu ich wykrywania, analizowania, zapobiegania i zwalczania.**  **Uzasadnienie:**  Brak przepisów umożlwiających przetwarzanie informacji stanowiących tajemnice prawnie chronione, w tym dane osobowe pomiędzy OUK, DUC, telekomami, ISP oraz ISAC uniemożliwia sprawą wymianę informacji o incydentach w celu skutecznej ich obsługi i koordynacji oraz przeprowadzania analiz. | **Uwaga nieuwzględniona**.  Taki przepis naruszałby zasady przetwarzania informacji niejawnych oraz inne tajemnice prawnie chronione. |
|  | Związek Banków Polskich | Art. 39 ust. 11 - nowy | **Propozycja zmiany:**  **Proponuje się dodanie w art. 39 ust. 11 w brzmieniu: 11. W przypadkach, o których mowa w ust. 10 w zakresie przetwarzania danych osobowych przepisów art. 5 oraz art. 12-22 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych nie stosuje się.**  **Uzasadnienie:**  Jest to niezmiernie ważny przepis z punktu widzenia skutecznego wykrywania i ścigania przestępców popełniających przestępstwa na szkodę operatorów usług kluczowych oraz dostawców usług cyfrowych i ich klientów - absurdem byłby obowiązek informacyjne względem tych osób, że podmioty uprawnione przetwarzają ich dane osobowe i dodatkowo wystąpienie o ich zgodę na przetwarzanie ich danych. Na powyższe zezwala art. 23 ust. 1 lit. d) RODO - d)zapobieganiu przestępczości, prowadzeniu postępowań przygotowawczych, wykrywaniu lub ściganiu czynów zabronionych lub wykonywaniu kar, w tym ochronie przed zagrożeniami dla bezpieczeństwa publicznego i zapobieganiu takim zagrożeniom; | **Uwaga nieuwzględniona**  Uwaga nie dotyczy projektowanej ustawy. |
|  | Związek Banków Polskich | Art. 39 ust. 12 - nowy | **Propozycja zmiany:**  Proponuje się dodanie w art. 39 ust. 12 w brzmieniu: **12. Operator usług kluczowych, dostawca usług cyfrowych lub ISAC nie ponoszą odpowiedzialności cywilnej za szkodę, która może wynikać z wykonywania przez nich ustawowych obowiązków w zakresie przeciwdziałaniu przestępstwom, gdy działając z należytą starannością i w dobrej wierze zgłosili właściwym organom zawiadomienie o podejrzeniu popełniania przestępstwa, a te po weryfikacji uznały podejrzenie za nieuzasadnione. W takich przypadkach odpowiedzialność za szkodę wynikłą z podjętych działań przez operatora usług kluczowych lub dostawcy usług cyfrowych ponosi Skarb Państwa.**  **Uzasadnienie:**  Potrzeba prowadzenia prawnej ochrony OUK, DUC i ISAC w sytuacjach wypełniania przez nich obowiązków wynikających z niniejszej ustawy w dobrej wierze. | **Uwaga nieuwzględniona**  Zasady odpowiedzialności Skarbu Państwa regulują przepisy Kodeksu cywilnego. Skarb Państwa nie może ponosić odpowiedzialności deliktowej za niepaństwowe osoby prawne. |
|  | Związek Banków Polskich | Art. 46 ust. 4 - nowy | **Propozycja zmiany:**  **Proponuje się dodanie w art. 46 ust. 4 w brzmieniu: 4. O ile istnieją sektorowe lub podsektorowe systemy informacyjne, zapewniające, w szczególności, obsługę incydentów lub koordynację obsługi incydentów, Minister właściwych do spraw informatyzacji włącza te systemy do systemu, o którym mowa w ust. 1. Zasady korzystania z tych systemów określa porozumienie zawarte pomiędzy Ministrem a właścicielami tych systemów.**  **Uzasadnienie:**  Sektor bankowy własnym kosztem wytworzył wiele systemów wspierających bezpieczeństwo banków oraz ich klientów. Istotne jest aby wykorzystywać je w ramach krajowego systemu cyberbezpieczeństwa. Poza tym obowiązki informacyjne o incydentach np. względem CSIRT MON, CSIRT NASK i CSIRT GOV mogłyby być realizowane z ich użyciem. Pozwoli to uniknąć dublowania czynności związanych z notyfikacją incydentów do wielu instytucji państwowych np. KNF, PUODO, prokuratury, policji itp**.** | **Uwaga nieuwzględniona**  Uwaga nie dotyczy projektu nowelizacji. |
|  | Związek Banków Polskich | Art. 51 - nowy | **Propozycja zmiany:**  Proponuje się dodanie nowego art. 51 w brzmieniu (zmianie ulegnie numeracja kolejnych artykułów):  Art. 51. Minister właściwy do spraw informatyzacji, na wniosek i w uzgodnieniu z organami właściwymi do spraw cyberbezpieczeństwa, CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT sektorowymi lub ISAC może wydać w drodze rozporządzenia techniczne i proceduralne mechanizmy zwiększające bezpieczeństwa operatorów usług kluczowych i dostawców usług cyfrowych oraz ich klientów.  **Uzasadnienie:**  Proponuje się dodanie przepisu umożliwiającego ministrowi właściwemu do spraw informatyzacji, na wniosek w uzgodnieniu z wymienionymi podmiotami wydawanie w drodze rozporządzenia określającego techniczne i proceduralne mechanizmy zwiększające bezpieczeństwa operatorów usług kluczowych i dostawców usług cyfrowych oraz ich klientów. Przykładowym rozwiązaniem mogłoby być wprowadzenie przepisu o możliwości blokowania ruchu na serwery wykorzystywane przez przestępców do gromadzenia tajemnic prawnie chronionych i danych osobowych. | **Uwaga nieuwzględniona**  Uwaga nie dotyczy projektu nowelizacji. |
|  | Związek Banków Polskich | Art. 54 ust. 1 | **Propozycja zmiany:**  Proponuje się aby w art. 54 ust. 1 otrzymał brzmienie: 1. **O ile odrębne przepisy nie stanowią inaczej** do kontroli, której zakres określony jest w art. 53 ust. 1 pkt 1, stosuje się przepisy rozdziału 5 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców.  **Uzasadnienie:**  Zakres sprawowania kontroli i nadzoru w sektorze finansowych określony jest m. in. W ustawie - prawo bankowe oraz ustawie o KNF. Zawarte w tych ustawach uregulowania powinny być lex specialis względem przepisów dotyczących kontroli w ustawie o krajowym systemie cyberbezpieczeństwa. | **Uwaga nieuwzględniona**  Uwaga nie dotyczy projektu nowelizacji. |

1. Patrz str. 7 Memorandum. [↑](#footnote-ref-2)
2. Patrz str. 10 Memorandum. [↑](#footnote-ref-3)
3. Patrz str. 7 Memorandum. [↑](#footnote-ref-4)
4. Rozporządzenie implementuje dyrektywę 2015/1535 Parlamentu Europejskiego i Rady z dnia 9 września 2015 r. ustanawiającej procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego. [↑](#footnote-ref-5)
5. Patrz str. 11 Memorandum. [↑](#footnote-ref-6)
6. Artykuł 1 Protokołu nr 1 do Konwencji o ochronie praw człowieka i podstawowych wolności. [↑](#footnote-ref-7)
7. Wyrok TSUE z dnia 1 marca 2011 r. w sprawie C-236/09, Association belge des Consommateurs Test-Achats ASBL i inni p. Conseil des ministres, ECLI:EU:C:2011:100, pkt 28. [↑](#footnote-ref-8)
8. Patrz str. 8 Memorandum. [↑](#footnote-ref-9)
9. Sformułowany w Projekcie mechanizm oceny ryzyka dostawcy może potencjalnie naruszać także art. 18 TFUE, który zakazuje wszelkich form dyskryminacji ze względu na narodowość. Patrz też pkt II.2.3 niniejszego dokumentu. [↑](#footnote-ref-10)
10. Umowa z 7 czerwca 1988 r. między Rządem Polskiej Rzeczypospolitej Ludowej a Rządem Chińskiej Republiki Ludowej w sprawie wzajemnego popierania i ochrony inwestycji; Umowa z 8 czerwca 2004 r. między Rządem Rzeczypospolitej Polskiej a Rządem Chińskiej Republiki Ludowej o współpracy gospodarczej. [↑](#footnote-ref-11)
11. Patrz s. 9 Memorandum. [↑](#footnote-ref-12)
12. Kwotę 13 mld euro podaje raport Oxford Economics <https://www.oxfordeconomics.com/recent-releases/The-Economic-impact-of-restricting-competition-in-5g-network-equipment>, s. 65. Kwotę 10 mld potencjalnych korzyści wskazuje raport Assembly Research https://www.assemblyresearch.co.uk/press-comments/poland-5g-delay [↑](#footnote-ref-13)
13. Patrz raport Oxford Economics, s. 65. [↑](#footnote-ref-14)
14. <https://www.gsma.com/security/network-equipment-security-assurance-scheme/> [↑](#footnote-ref-15)
15. [↑](#footnote-ref-16)
16. (wyrok TK z 13.04.1999 r., K 36/98, OTK 1999, Nr 3, poz. 40) [↑](#footnote-ref-17)