Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji

Warszawa, dnia 6 października 2020 r.
KIGEiT/2423/10/2020

Szanowny Pan
Marek Zagórski
Kancelaria Prezesa Rady Ministrów

Szanowny Panie Ministrze,

działając w imieniu Krajowej Izby Gospodarczej Elektroniki i Telekomunikacji (dalej „***Izba***" lub „***KIGEiT***") odnosząc się do pisma z dn. 7 września 2020 r., znak: DP-III.0211.4.2020, przy którym w ramach konsultacji przesłano projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy – Prawo zamówień publicznych (UD68), oraz mając na względzie pismo z dnia 17 września 2020 r., znak: DP-III.0211.4.2020, informujące o przedłużeniu terminu na zgłaszanie stanowisk, Izba przedstawia następujące uwagi.

Część I: Uwagi ogólne.

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[1], 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.

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

[1] Dz. Urz. UE. L Nr 108, str. 33,

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.

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.

Naruszenie przepisów WTO

a) 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.

b) 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).

c) 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.

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.

Część II: Uwagi dotyczące oceny skutków projektu ustawy

1. 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.

2. 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.

3. 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.

4. 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.

5. 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).

6. 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).

CZĘŚĆ III. Uwagi techniczne dotyczące ryzyka i rozwiązań bezpieczeństwa

1. Kryteria powinny być neutralne technologicznie, a nie uwzględniać względy polityczne:

1) 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.
2) Kryteria powinny mieć charakter techniczny, być obiektywne, rozsądne i proporcjonalne oraz zawierać odniesienie do oceny ryzyka zawartej w Toolbox 5G i specyfikacjach technicznych.
3) 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.

2. Normy techniczne i normy certyfikacji

1) Projekt ustawy powinien raczej koncentrować się na normach technicznych i normach certyfikacji, które powinny zostać wprowadzone, takich jak NESAS, system certyfikacji ENISA.
2) **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.
3) **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.

3. 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.

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***”.
   a. Nie jest w żaden sposób określony merytoryczny zakres wspomnianej wyżej **procedury sprawdzającej**.
   b. 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.
   c. 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.
2. 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** to wciąż 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.

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.
8. Prawne usankcjonowanie:
   a. 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.
   b. 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).

Część IV. Komentarze do poszczególnych przepisów projektu

1) **Art. 1 punkt 1) litera a) Projektu: Art. 1 ust. 1 pkt 4 KSC:** Zadania i obowiązki przedsiębiorców dotyczące bezpieczeństwa i incydentów.

   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.

2) **Art. 1 pkt 1) litera b) Projektu: Art 1 ust. 2 pkt 1) KSC** (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

3) **Art. 1 pkt 2) litera a) Projektu: Art. 2 pkt 3b KSC:** (Użyte w ustawie określenie CSIRT Telco)

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.

4) **Art. 1 pkt 2) litera a) Projektu: Art. 2 pkt 8a KSC:** (definicja incydentu telekomunikacyjnego)

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).

5) **Art. 1 pkt 2 lit. b) Projektu: art. 2 pkt 8f KSC**

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.

6) **Art. 1 pkt 2 lit. b) Projektu: art. 2 pkt 8g KSC**

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.

7) **Art. 1 pkt 4) litera a) Projektu: Art. 4 pkt 2a i 5a KSC:** (objęcie Krajowym systemem cyberbezpieczeństwa przedsiębiorców komunikacji elektronicznej)

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.

8) **Art. 1 pkt 10 Projektu: art. 14 ust. 3 KSC**

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

9) **Art. 1 pkt 12) Projektu: Obowiązki przedsiębiorców komunikacji elektronicznej**

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.

10) **Art. 1 pkt 12) Projektu: art. 20a, art. 20e, art. 20f KSC**

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.

11) Art. 1 pkt 12) Projektu: art. 20c ust. 1, 3 i 4 KSC

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.

12) **Art. 1 pkt 29) Projektu: art. 66a ust. 1 KSC**: **Przeprowadzenie oceny przez Kolegium**

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 oprogramowania~~e~~m ~~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.

13) **Art. 1 pkt 29) Projektu: art. 66a ust. 2-3 KSC** (analiza zagrożeń bezpieczeństwa narodowego o charakterze ekonomicznym, kontrwywiadowczym i terrorystycznym dotycząca dostawcy).

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.

14) **Art. 1 pkt 29) Projektu: art. 66a ust. 4 pkt 1 KSC** (analiza zagrożeń bezpieczeństwa narodowego o charakterze ekonomicznym, kontrwywiadowczym i terrorystycznym dotycząca dostawcy).

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.

15) **Art. 1 pkt 29) Projektu**: **Przepis art. 66a ust. 4 pkt 2 KSC** (ocena prawdopodobieństwa, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego

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?

16) **Art. 1 pkt 29) Projektu: art. 66a ust. 4 pkt 2-5:** Kryteria oceny dostawcy

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. 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.

17) Art. 1 pkt 29 Projektu: art. 66a ust. 5 KSC – gradacja ryzyk

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).

18) **Art. 1 pkt 29 Projektu: art. 66a ust. 7 KSC –** plan naprawczy w przypadku uzyskania określonej oceny ryzyka

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.

19) Art. 1 pkt 29 Projektu: Art. 66 a ust. 8 KSC: brak administracyjnej ścieżki odwoławczej od oceny dostawcy

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.

20) Artykuł 1 pkt 29: Art. 66b ust. 1 pkt 1 i ust. 2 pkt 1 KSC

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;”

21) Artykuł 1 pkt 29: Art. 66 b ust. 1 pkt 2 KSC

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.

22) **Artykuł 1 pkt 29: Art. 66 b: Konsekwencje oceny** - brak przepisów związanych z mechanizmem rekompensat

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.

23) art. 1 pkt 29: Art. 66c ust. 1 „Plan naprawczy"

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.

24) Art. 1 pkt 30 Projektu: art. 67a KSC

Proponowana zmiana:

„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.

25) 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.

26) **Art. 1 pkt 30 Projektu: Art. 67c ust. 1 KSC Ostrzeżenia i polecenia zabezpieczające**

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.

Część V: 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.

2. 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.

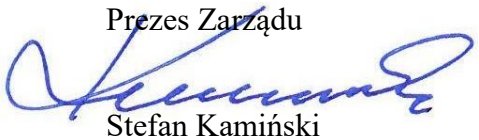
3. PROPONOWANY KIERUNEK ZMIAN

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.

Z poważaniem

Prezes Zarządu



Stefan Kamiński