OPINIA

Polskiej Izby Informatyki i Telekomunikacji

w sprawie projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy – Prawo zamówień publicznych

Uwagi ogólne

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.

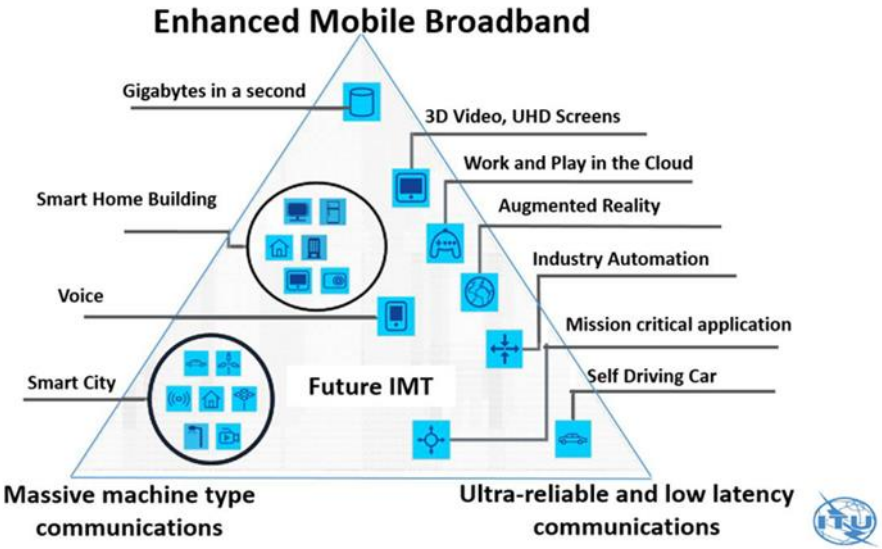
   Część przepisów PKE została przepisana do ustawy KSC bez wyjaśnienia intencji czy demarkacji, czego skutkiem byłoby np. wprowadzenie dwóch identycznych upoważnień do wydania rozporządzenia przez Ministra Cyfryzacji dla rozporządzenia w zakresie środków technicznych i organizacyjnych, jak i rozporządzenia 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.”.*

3. **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.

4. **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.
5. **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.
6. 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.
7. 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.
8. 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.

Uwagi szczegółowe

I. Włączenie przedsiębiorstw komunikacji elektronicznej do krajowego systemu cyberbezpieczeństwa i nowe obowiązki

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;

2. 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:

a) tworzenie, weryfikację i walidację podpisów elektronicznych, pieczęci elektronicznych lub elektronicznych znaczników czasu, usług rejestrowanego doręczenia elektronicznego oraz certyfikatów powiązanych z tymi usługami; lub
b) tworzenie, weryfikację i walidację certyfikatów uwierzytelniania witryn internetowych; lub
c) 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.”

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:

- 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.

4. Art. 1 pkt 12 dot. dodania nowego rozdziału 4a pt. „Obowiązki przedsiębiorców komunikacji elektronicznej"

4.1. 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.

4.2. 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.

PKE	KSC
Obowiązek raportowy – różne podmioty zobowiązane	
Z uwagi na utrzymanie dotychczasowych aktów wykonawczych do PT w zakresie raportowania dotyczyłoby pełnego dotychczasowego zakresu, w tym określania przyczyny incydentu, jako cyberataku. Przedstawiony projekt zmian KSC nie modyfikuje również w żadnym zakresie przepisów art. 42, 45, 46 projektu PKE, co oznacza, że Prezes UKE wciąż byłby podmiotem właściwym do odbierania zgłoszeń incydentów w rozumieniu PKE oraz współpracy z CISRT krajowymi. Jednocześnie obowiązki dotyczyłyby wg PKE wszystkich przedsiębiorców komunikacji elektronicznej.	Miałby dotyczyć w myśl art. 20c wyłącznie przedsiębiorców komunikacji elektronicznej obowiązanych do sporządzenia planu działania na wypadek szczególnych zagrożeń. To istotna różnica wobec projektu PKE, który obowiązek raportowy adresuje do wszystkich przedsiębiorstw komunikacji elektronicznej. Projekt KSC do wszystkich przedsiębiorców komunikacji elektronicznej w art. 20b adresuje wyłącznie obowiązki w zakresie obsługi incydentu i zapewniania informacji o rejestrowanych incydentach dla CSIRT MON, NASK, GOV. Dalsze przepisy projektu KSC, w art. 20c określają procedurę działania w zakresie klasyfikowania incydentu, jako incydentu telekomunikacyjnego. W tym zakresie należałoby uznać, że celem jest stworzenie odrębnej od raportowania do UKE ścieżki bezpośredniego raportowania incydentów telekomunikacyjnych w rozumieniu ustawy KSC
Definicja incydentu – nierozłączny zakres obowiązku oraz niespójna siatka pojęciowa	
incydent bezpieczeństwa – każde zdarzenie, które ma rzeczywisty, niekorzystny skutek dla bezpieczeństwa sieci i usług; Rekonstruując tą definicję z jedynie część wykorzystaniem pozostałych definicji z PKE oznacza on: *incydent bezpieczeństwa – każde zdarzenie, które ma rzeczywisty, niekorzystny skutek dla zdolności* *sieci telekomunikacyjnych (systemów transmisyjnych, a także urządzeń telekomunikacyjnych, oprócz telekomunikacyjnych urządzeń końcowych, oraz innych zasobów, w tym nieaktywnych elementów sieci, które umożliwiają przekazywanie sygnałów za pomocą przewodów, fal radiowych, optycznych lub innych środków wykorzystujących energię elektromagnetyczną, niezależnie od rodzaju przekazywanej informacji)* *lub usług komunikacji elektronicznej (usług świadczonych za*	*incydent telekomunikacyjny – incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi komunikacji elektronicznej;* Rekonstruując tą definicję z wykorzystaniem pozostałych definicji z KSC oznacza on: *incydent telekomunikacyjny - zdarzenie, które ma lub może mieć niekorzystny wpływ na odporność* *systemów informacyjnych (zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu przepisów ustawy z dnia ... 2020 r. – Prawo komunikacji elektronicznej (Dz. U. poz. …)*

pośrednictwem sieci telekomunikacyjnej, zwykle za wynagrodzeniem, z wyłączeniem usług związanych z zapewnianiem albo wykonywaniem kontroli treści przekazywanych przy wykorzystaniu sieci telekomunikacyjnych lub usług komunikacji elektronicznej, obejmująca: a) usługę dostępu do internetu w rozumieniu art. 2 akapit drugi pkt 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2015/2120; b) usługę komunikacji interpersonalnej; c) usługę polegającą całkowicie lub głównie na przekazywaniu sygnałów, w tym usługę transmisyjną stosowaną na potrzeby świadczenia usług komunikacji maszyna – maszyna oraz na potrzeby nadawania)	
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.*	*na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy,* *i które powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi komunikacji elektronicznej*
Wytyczne dla ustalenia kryteriów zgłoszenia – identyczne przy czym odwołujące się do różnych definicji incydentu	
Art. 42 ust. 2 zawiera upoważnienie do wydania rozporządzenia. Obowiązujące rozporządzenia do PT dot. progów jak i formularza zostaną utrzymane na okres maks. 24 miesięcy od wejścia w życie PKE.	Art. 20c ust. 4 zawiera upoważnienie do wydania rozporządzenia. Brak jest rozporządzenia, ani nawet projektu, który określi progi dla incydentów.
Minister właściwy do spraw informatyzacji określi, w drodze rozporządzenia: *1) progi incydentu bezpieczeństwa, których przekroczenie powoduje powstanie obowiązku, o którym mowa w ust. 1, mając na uwadze:* *a) liczbę użytkowników, na których incydent bezpieczeństwa miał wpływ,* *b) czas trwania skutków incydentu bezpieczeństwa,* *c) obszaru, na którym wystąpiły skutki incydentu*	*Minister właściwy do spraw informatyzacji określi, w drodze rozporządzenia* *progi incydentu telekomunikacyjnego, których przekroczenie powoduje powstanie obowiązku zgłoszenia incydentu, uwzględniając:* *1) liczbę użytkowników, na których incydent telekomunikacyjny miał wpływ,* *2) czas trwania skutków incydentu telekomunikacyjnego,* *3) obszar, na którym wystąpiły skutki incydentu*

bezpieczeństwa, *d) zakres wpływu incydentu bezpieczeństwa na funkcjonowanie sieci i usług,* *e) wpływ incydentu bezpieczeństwa na zachowanie tajemnicy komunikacji elektronicznej,* *f) 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,* *g) wpływ incydentu bezpieczeństwa na połączenia do numerów alarmowych,* *h) wpływ incydentu bezpieczeństwa na wykonywanie obowiązków, o których mowa wart. 46-56 ustawy;* *2) wzór formularza do przekazywania informacji o wystąpieniu incydentu bezpieczeństwa* *–kierując się rekomendacjami lub wytycznymi ENISA oraz koniecznością zapewnienia Prezesowi UKE informacji niezbędnych do właściwego realizowania jego obowiązku, o którym mowa w art. 382 ust. 1 pkt 11.*	*telekomunikacyjnego,* *4) zakres wpływu incydentu telekomunikacyjnego na funkcjonowanie sieci i usług,* *5) wpływ incydentu telekomunikacyjnego na zachowanie tajemnicy komunikacji elektronicznej,* *6) wpływ incydentu telekomunikacyjnego na świadczenie usług kluczowych oraz funkcjonowanie infrastruktury krytycznej w rozumieniu ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym,* *7) wpływ incydentu telekomunikacyjnego na połączenia do numerów alarmowych, o których mowa w art. 2 pkt 29 ustawy z dnia … – Prawo komunikacji elektronicznej,* *8) wpływ incydentu telekomunikacyjnego na wykonywanie obowiązków, o których mowa w art. 47-62 ustawy z dnia … – Prawo komunikacji elektronicznej* *– kierując się rekomendacjami lub wytycznymi Agencji Unii Europejskiej do spraw Cyberbezpieczeństwa (ENISA) oraz koniecznością zapewnienia Prezesowi Urzędu Komunikacji Elektronicznej informacji niezbędnych do właściwego realizowania jego obowiązku, o którym mowa w art. 382 ust. 1 pkt 11 ustawy z dnia … – Prawo komunikacji elektronicznej.*
Zakres zgłoszenia – odmienne regulacje	
Formularz jest już określony w rozporządzeniu do PT, a PKE zawiera upoważnienie do określenia nowego formularza.	Art. 20d określa zakres zgłoszenia, ale formularz zgłoszenia nie zostanie określony w rozporządzeniu.
Podmioty właściwe do odbierania zgłoszeń - różne	
Zgodnie z art. 42 ust. 1 podmiotem tym jest Prezes UKE. Prezes UKE zgodnie z art. 45 przekazuje informacje właściwemu CSIRT, jeśli incydent dotyczy incydentu w rozumieniu KSC.	Zgodnie z art. 20c podmiotami tym są właściwe CSIRT MON, NASK, GOV. Zgodnie z art. 20c ust. 3 przedsiębiorca przekazuje zgłoszenie również do CSIRT Telco, przy czym CSIRT Telco ma zostać dopiero powołany po 18 miesiącach od wejścia w życie ustawy, co oznacza, że obowiązek będzie niemożliwy do realizacji. KSC nie przewiduje przekazywania informacji z CSIRT do UKE, przy czym możliwe jest, aby CSIRT współpracowały z UKE (art. 34a – informacja przekazywana na żądanie UKE), a także korzystanie przez UKE z systemu, o którym mowa w art. 46.
Wsparcie CSIRT	

Zgodnie z art. 45 ust. 3 UKE może zwrócić się o wsparcie do właściwego CSIRT. Stanowi to bezpośrednią implementację art. 41 ust. 4 EKŁE.	Zgodnie z art. 26 ust. 2 m.in. przedsiębiorcy komunikacji elektronicznej mogliby wnioskować o wsparcie CSIRT MON, NASK, GOV. Regulacja ta wykracza poza zakres niezbędny do wdrożenia art. 41 ust. 4 EKŁE.

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.

5. Art. 20b pkt 1 i art. 20c ust. 1 pkt 1 w zw. z art. 2 pkt 8a dotyczące klasyfikowania incydentu, jako incydentu telekomunikacyjnego.

5.1. Proponowana w art. 20b norma nakłada na wszystkich przedsiębiorców komunikacji elektronicznej, w tym mikroprzedsiębiorstwa obowiązek obsługi incydentu, a więc czynności umożliwiających wykrywanie, rejestrowanie, analizowanie, klasyfikowanie, priorytetyzację, podejmowanie działań naprawczych i ograniczenie skutków incydentu. Dodatkowo dotyczy to wszystkich incydentów w myśl KSC, a więc szerokiego katalogu zdarzeń, które mają lub mogą mieć niekorzystny wpływ na cyberbezpieczeństwo. W naszej ocenie wdrożenie tego obowiązku nie jest możliwe w przewidzianym w ustawie terminie.

Postulat:

- Art. 20b należy usunąć z projektu i przenieść dyskusję na jego temat na okres po implementacji PKE.
- W przypadku jego utrzymania należy doprecyzować, że obowiązek dotyczy wyłącznie sieci telekomunikacyjnych lub usług komunikacji elektronicznej tego przedsiębiorcy. Niezbędne jest bowiem zapewnienie, aby przepisy nie były rozumiane rozszerzająco i nie pozwalały na obarczanie jednych podmiotów obowiązkami, które de facto należą do innych podmiotów.

5.2. Wg art. 20c ust. 1 pkt 1 obowiązkiem będzie klasyfikowanie incydentów, jako telekomunikacyjnych na podstawie progów uznania incydentu za telekomunikacyjny, a następnie ich zgłaszanie. Po pierwsze, jak już sygnalizowaliśmy powyżej, należy wskazać, że takie progi nie są jeszcze znane, ponieważ brak jest aktu wykonawczego w tym zakresie. Także nawet klasyfikowanie nie będzie możliwe. Po drugie skoro incydent ma być klasyfikowany jako telekomunikacyjny na podstawie progów to niepotrzebne wątpliwości wprowadza definicja incydentu telekomunikacyjnego zawarta w słowniczku. W praktyce bowiem mogłoby bowiem dojść do incydentu, który spełniałby kryteria telekomunikacyjnego według definicji, ale nie spełniałby kryteriów wg progów. Czy wówczas incydent byłby telekomunikacyjnym? Wydaje się, że jednocześnie byłby incydentem telekomunikacyjnym i nim nie był. Biorąc pod uwagę, że w pkt 2 jest już mowa o zgłoszeniu incydentu telekomunikacyjnego, a nie incydentu telekomunikacyjnego określonego wg progów pojawia się wątpliwość, co do aktualizacji obowiązku raportowego nawet dla incydentu nieprzekraczającego progów.

Postulat:

- Art. 20c należy usunąć z projektu i przenieść dyskusję na jego temat na okres po implementacji PKE.

5.3. 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.:

e) wpływ incydentu bezpieczeństwa na zachowanie tajemnicy komunikacji elektronicznej,
f) 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,
g) wpływ incydentu bezpieczeństwa na połączenia do numerów alarmowych,
h) 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.

5.4. 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.

6. 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.

7. 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.

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.

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?

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.

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.

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.

II. Ocena dostawców, nowe narzędzia Kolegium i Pełnomocnika, kary pieniężne.

Na obecnym etapie rozwoju gospodarki i społeczeństwa obszar cyfrowy jest jednym z kluczowych, a zagrożenia w jego zakresie szczególnie istotne i jednocześnie trudne do całkowitego wyeliminowania. Na koncepcji weryfikacji bezpieczeństwa opierają się też wszelkie mechanizmy certyfikacji i dopuszczania produktów do wejścia na rynek. W projekcie zaproponowano jednak wprowadzenie, nie jednego, ale kilku rozwiązań w tym zakresie, tj.:

- **Ocena ryzyka dostawcy sprzętu lub oprogramowania** dokonywana przez Kolegium ds. cyberbezpieczeństwa, która może spowodować konieczność wycofania pewnych rozwiązań, przy zachowaniu jednak pewnego zakresu elastyczności, co do czasu na wycofanie.
- **Ostrzeżenia Pełnomocnika**, wydawane w przypadku informacji o zagrożeniu uprawdopodabniającej możliwość wystąpienia incydentu krytycznego, która może spowodować konieczność wycofania pewnych rozwiązań, przy czym nie przewidziano żadnej elastyczności, co do czasu na wycofanie.
- **Polecenia zabezpieczające**, wydawane przez Pełnomocnika, w przypadku wystąpienia incydentu krytycznego, które może spowodować konieczność wycofania pewnych rozwiązań, przy czym nie przewidziano żadnej elastyczności, co do czasu na wycofanie.
- **Powyższe uzupełniają szeroki katalog już funkcjonujących rozwiązań**, jak możliwość wydania rekomendacji przez Pełnomocnika, rozporządzenie do art. 175d PT, a także wprowadzenie wymagań bezpieczeństwa i integralności do procedury aukcyjnej w zakresie częstotliwości radiowych.

Zakres możliwej ingerencji, również w działalność gospodarczą podmiotów prywatnych, a także na świadczone przez nie usługi jest niezwykle szeroki przy jednoczesnym dość ogólnym i w rzeczy samej, uznaniowym podejściu do określenia kryteriów opisu sytuacji, w jakich po odpowiednie narzędzia można sięgać.

Stąd, w poniższym stanowisku przedstawiamy nasze propozycje modyfikacji przedłożonego projektu, w sposób, który zgodnie z dotychczasowymi deklaracjami resortu cyfryzacji, nie będzie ingerował w działalność gospodarczą bardziej niż to absolutnie niezbędne dla bezpieczeństwa w kraju.

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**.

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**.
    - **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
    - 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);
    - **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);
    - 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.

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:
    - 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.
    - 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.
    - Identyfikacja poziomu wykorzystania sprzętu lub oprogramowania w realizacji przez przedsiębiorców telekomunikacyjnych obowiązków wynikających ze stanów nadzwyczajnych i stanu wojny.
    - Identyfikacja poziomu zobowiązań przedsiębiorców telekomunikacyjnych i użytkowników końcowych wobec dostawcy.
    - Identyfikacja innych podmiotów działających na tym samym rynku co oceniany dostawca, w zakresie urządzeń i oprogramowania, w którego zakresie ma zostać dokonana ocena.

- 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).
- Uzasadnienie wniosku, w tym przedstawienie potencjalnych ryzyk związanych z wykorzystaniem urządzeń lub oprogramowania danego dostawcy.
- 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.*
- Identyfikacja rozwiązań alternatywnych działań w stosunku do sprzętu lub oprogramowania danego dostawcy
- 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
- 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.

1.4. 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.

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.

1.6. 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.

2. 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.

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.

3. 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.

3.1. 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."

3.2. 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.

4. 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.

IV. Modyfikacja obowiązków operatorów usług kluczowych

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.*"

2. Art. 14a ust. 7

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.

3. Art. 44 ust. 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;*
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*

Zakres zadań, jakie przewiduje się do realizacji przez CSIRT sektorowy koliduje z zadaniami, jakie zgodnie z ustawą ma realizować operator usługi kluczowej. Zadania w ustawie powinny być jednoznacznie przypisane do poszczególnych podmiotów, a ich odpowiedzialności w sposób niebudzący wątpliwości zdefiniowane. Nie wiemy też jak należy rozumieć wskazane w ustawie zadanie CSIRT sektorowego, które określono jako „reagowanie na incydenty". Ustawa w dotychczasowym brzmieniu używa pojęć „obsługa incydentu" oraz „zarządzanie incydentem". W żadnym z tych pojęć nie używa się określenia „reagowanie na incydenty".

Zamiana roli CSIRT sektorowego z podmiotu wspierającego operatora usługi kluczowej w podmiot odpowiedzialny za przyjmowanie zgłoszeń i „reagowanie na incydenty" itd. bez dookreślenia warunków, na jakich te zadania miałyby być realizowane (chociażby na poziomie odwołania do porozumienia zawieranego przez te podmioty) może być przyczyną sporów (pozytywnych albo negatywnych) i niepotrzebnych konfliktów w ramach danego sektora.

4. **Art. 44 ust 1a.**

CSIRT sektorowy może, w szczególności:

1) zapewniać dynamiczną analizę ryzyka i incydentów oraz wspomagać w podnoszeniu świadomości zagrożeń cyberbezpieczeństwa

Należy rozważyć zwiększenie roli CSIRT-u sektorowego w zakresie podnoszenia świadomości zagrożeń cyberbezpieczeństwa. W obecnym kształcie rola CSIRT-u sektorowego nie jest jednoznaczna – przewiduje się, że będzie aktywnie obsługiwał incydenty, gromadził wiedzę o podatnościach itd., ale już w zakresie podnoszenia świadomości zagrożeń cyberbezpieczeństwa ma pełnić rolę wspomagającą. To CSIRT sektorowy mając kompleksową wiedzę o sektorze, w jakim działa, występujących incydentach oraz podatnościach powinien pełnić rolę wiodącą.

2 Firmy - Członkowie PIIT powstrzymały się od poparcia powyższej opinii.