LEWIATAN

Warszawa, 6 października 2020 r.
KL/467/334/AM/2020

Pan

Marek Zagórski

Minister Cyfryzacji

Szanowny Panie Ministrze,

W odpowiedzi na zaproszenie Ministerstwa Cyfryzacji do konsultacji w sprawie projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy – Prawo zamówień publicznych (projekt z dnia 7 września 2020 r.), Konfederacja Lewiatan przedstawia w załączeniu stanowisko do przedłożonego projektu.

Z poważaniem,

Maciej Witucki

Prezydent Konfederacji Lewiatan

Załącznik:

Stanowisko Konfederacji Lewiatan wobec projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy – Prawo zamówień publicznych.

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS

LEWIATAN

Stanowisko Konfederacji Lewiatan wobec projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy – Prawo zamówień publicznych

Konfederacja Lewiatan aktywnie i od samego początku uczestniczy w dyskusjach na temat tworzącego się krajowego systemu cyberbezpieczeństwa oraz regulacji dotyczących rynku komunikacji elektronicznej. Naszymi członkami są kluczowi gracze polskiego rynku cyfrowego, a także podmioty zaliczane do krajowego systemu cyberbezpieczeństwa w różnych sektorach. Dzięki tym doświadczeniom dobrze rozumiemy i w pełni popieramy ideę maksymalnego bezpieczeństwa w cyberprzestrzeni. Wszelkie ryzyka w tym obszarze są bowiem bezpośrednio ryzykiem dla nas samych, jak i reprezentowanych przez nas przedsiębiorstw. Ryzykiem o tyle kluczowym, że niewłaściwe zarządzanie nim może oznaczać ogromne skutki finansowe, a w skrajnych przypadkach przesądzać o dalszym losie danej organizacji.

Stąd, co do zasady wspieramy działania rządu mające na celu podniesienie poziomu cyberbezpieczeństwa zarówno w sektorze publicznym, jak i prywatnym. Podobnie za zasadne uznajemy, o ile nie ingeruje to zbytnio w konkurencyjny rynek, wzmacnianie publicznych instytucji w zakresie ich finansowania, organizacji i kompetencji. **Jednak, pod dogłębnej analizie stwierdzamy, że przedstawiony do konsultacji projekt ustawy stanowi bardzo poważne wyzwanie, a po części także zaskoczenie dla podmiotów, które miałyby zostać objęte nowymi regulacjami.** W znakomitej bowiem części kształt proponowanych przepisów został ustalony bez udziału partnerów społecznych i adresatów nowych przepisów. Tymczasem jak zakładamy, to na wzajemnym dialogu, zrozumieniu potrzeb oraz współpracy powinien być budowany spójny i efektywny system cyberbezpieczeństwa. Z tych względów uważamy, że tak daleko idąca interwencja legislacyjna powinna zostać poprzedzona szeroką dyskusją merytoryczną z wszystkimi zainteresowanymi uczestnikami rynku, a kształt projektu winien odzwierciedlać gruntownie przemyślaną i kompromisową koncepcję poprawy cyberbezpieczeństwa. Podobnie jak dzieje się to w ramach dyskusji nad kształtem przyszłych aktów prawnych na poziomie unijnym, czy jak udało się to przeprowadzić w toku dyskusji nad przyjętymi niedawno rozporządzeniami do art. 176a i 175d ustawy – Prawo telekomunikacyjne.

Dlatego już na wstępie przedstawiamy nasze postulaty o charakterze podstawowym, które w dalszej części uszczegóławiamy i dodatkowo uzasadniamy. Liczymy na możliwość ich przedyskutowania, a przede wszystkim uwzględnienia w toku dalszych prac legislacyjnych.

1. W pierwszej kolejności za zasadne uważamy przeprowadzenie oraz przedstawienie w projekcie szerszego odniesienia do oceny skutków regulacji. To w naszej ocenie kluczowy element dla dalszej

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS

rzetelnej dyskusji na temat projektu ustawy. Obszary takiej analizy przedstawiamy w uwagach szczegółowych.

2. Postulujemy, aby przyspieszyć prace na poziomie UE w celu przyjęcia wspólnego podejścia do oceny bezpieczeństwa sprzętu i oprogramowania. Zauważamy bowiem, że kwestie cyberbezpieczeństwa nie są ograniczone granicami państwowymi. Tym bardziej takich ograniczeń nie będą znały bazujące na sieciach 5G rozwiązania, jak chociażby korytarze transportowe umożliwiające autonomiczny ruch pojazdów. Niestety na poziomie UE przyjęto dotychczas dość ogólne wytyczne kierunkowe, które skutkują w praktyce tym, że kraje UE, w tym sąsiedzi Polski przyjmują zupełnie odmienne podejście do kwestii bezpieczeństwa sieci 5G oraz dostawców. Takie wyspowe podejście do cyberbezpieczeństwa nie służy w naszej ocenie tworzeniu równego i jednolitego rynku cyfrowego na poziomie UE.

3. Obok konsultowanych rozwiązań za istotne uważamy zaadresowanie zagrożeń cyberbezpieczeństwa po stronie użytkowników końcowych, w tym związanych z używanymi przez nich aplikacjami, które wielokrotnie stanowią istotne wektory ataków. Ten obszar pozostawiony jest dotychczas bez wyraźnego zaadresowania, podczas gdy z perspektywy większości użytkowników właśnie tutaj istnieje największe zagrożenie dla bezpieczeństwa.

4. Rynek komunikacji elektronicznej powinien nadal pozostać kompleksowo regulowany sektorowo ze względu na jego szczególne cechy, aktualny kształt przepisów unijnych oraz bardzo ograniczony czas na wprowadzenie rewolucyjnych zmian w tym zakresie. Tym samym, na obecnym etapie należałoby zrezygnować w projekcie z przepisów dotyczących objęcia przedsiębiorców komunikacji elektronicznej nowymi obowiązkami w ramach ustawy o krajowym systemie cyberbezpieczeństwa, w tym w zakresie włączenia ich do krajowego systemu cyberbezpieczeństwa oraz wprowadzenia nowego reżimu raportowego w zakresie incydentów. Szczególnie, że istnieje już właściwy dla takich podmiotów kanał raportowania do Prezesa Urzędu Komunikacji Elektronicznej, a następnie do podmiotów krajowego systemu cyberbezpieczeństwa. Właściwy tryb w tym zakresie został już przedstawiony w projekcie PKE, a jego ewentualne rozszerzenie wymaga pogłębionej dyskusji i czasu.

5. Jeśli podmioty krajowego systemu cyberbezpieczeństwa potrzebują dodatkowych lub bardziej bezpośrednich informacji o incydentach w sieciach telekomunikacyjnych jesteśmy otwarci na dyskusję na temat możliwości poprawy aktualnego systemu raportowania, w którym to Prezes UKE powinien przekazywać CSIRT takie informacje. Rozwiązaniem mogłoby być zobowiązanie Prezesa UKE do przekazywania wszystkich informacji o incydentach w sieciach do CSIRT krajowych i pozostawienie im

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS

oceny wpływu na cyberbezpieczeństwa oraz ewentualnego powiadamiania objętych zagrożeniem podmiotów.

6. Przepisy dotyczące nowych uprawnień Pełnomocnika oraz Kolegium wymagają w naszej ocenie rewizji, w szczególności pod kątem skupienia na samych urządzeniach i oprogramowaniu, mocniejszym uwzględnieniu kwestii technicznych, a wreszcie zapewnienia większej elastyczności i czasów na dostosowanie dla użytkowników urządzeń i oprogramowania uznanych za stwarzające wysokie lub umiarkowane ryzyko. W szczególności powinny zostać poszanowane okresy amortyzacji użytkowanych już w sieciach urządzeń, a także możliwość pełnego (w tym okresie) użytkowania posiadanego sprzętu lub oprogramowania, w tym ewentualnych zakupów lub wdrożeń, które są niezbędne dla napraw awarii i utrzymania ciągłości świadczenia usług, w tym telekomunikacyjnych. W zakresie samej oceny proponujemy przede wszystkim wykorzystanie modeli certyfikacji na poziomie unijnego schematu certyfikacji bazującego na Akcie o cyberbezpieczeństwie, tj. wprowadzenie zasad wymagających od producentów dokonania odpowiedniej certyfikacji swoich urządzeń i oprogramowania.

7. Mechanizm oceny ryzyka powinien dotyczyć sprzętu i oprogramowania wchodzącego w skład infrastruktury krytycznej oraz opierać się przede wszystkim o wymagania techniczne, a nie geopolityczną charakterystykę dostawcy. Przepisy w tym zakresie powinny być wyjątkowo precyzyjne, a procedura oparta o obiektywne merytoryczne kryteria z uwzględnieniem skutków dla konkurencyjności rynku, kosztów wdrożenia etc., w celu uniknięcia zarzutu dyskryminacji.

8. Ocenę sprzętu i oprogramowania należy przeprowadzać według obowiązujących przepisów ustawy Kodeksu postępowania administracyjnego oraz ustawy Prawo przedsiębiorców. Koniecznym jest stosowanie przejrzystych zasad, umożliwiających aktywny udział dostawcy w postępowaniu oraz zapewnienie procedury odwoławczej, w tym prawo weryfikacji decyzji przez sądy administracyjne.

9. Przeprowadzenie ewentualnej oceny powinno zostać powierzone wyspecjalizowanemu organowi regulacyjnemu, który dysponuje odpowiednimi kompetencjami i zasobami tj. np. Prezes Urzędu Komunikacji Elektronicznej.

10. Z uwagi na dotychczasowe doświadczenia operatorów usług kluczowych (OUK) przedstawiamy propozycje modyfikacji proponowanych zasad realizacji obowiązków OUK, w szczególności poprzez dopuszczenie innych form organizacyjnych niż wyodrębniony SOC. W naszej ocenie taka elastyczność, w tym w zakresie możliwości realizacji zadań w strukturze rozproszonej, gdzie SOC jest jedynie jej częścią jest kluczowa dla OUK realizujących zadania własnymi siłami. Natomiast OUK, którzy korzystają z usług zewnętrznych powinni mieć możliwość ich realizacji w modelu mieszanym, tj. wykorzystania struktury

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS

wewnętrznej oraz zamawiania na zewnątrz jedynie części usług niezbędnych dla kompleksowej ochrony usługi kluczowej.

Dalsze konsultacje projektu. Uwzględniając zakres podmiotów, na jakie może wpływać projektowana ustawa (wszystkie podmioty KSC) należy przygotować pełną listę interesariuszy i umożliwić ich rzeczywisty udział w konsultacjach, w tym obejmując w szczególności: organizacje samorządów terytorialnych, organizacje przedsiębiorców reprezentujących wszystkie kategorie operatorów usług kluczowych, organizacje konsumentów, instytucje odpowiedzialne za ochronę konkurencji i konsumenta, Radę Dialogu Społecznego. Zwracamy się również z uprzejmą prośbą o zorganizowanie przez Ministerstwo konferencji uzgodnieniowej oraz zaproszenie do udziału wszystkich interesariuszy, którzy wnieśli swoje uwagi.

Nasze uwagi wynikają z faktu, że po wnikliwej analizie projektu zauważamy, że występują w nim pewne braki zarówno w warstwie merytorycznej, celowościowej, jak i techniczno-legislacyjnej skłaniają do jego krytycznej oceny. W pierwszej kolejności należy odnotować następujące kwestie: zakres zmian, ich wyraźne kolizje lub powielanie dotychczasowych regulacji (w tym tych dopiero projektowanych w ramach Prawa Komunikacji Elektronicznej), brak niezbędnej precyzji, lakoniczne uzasadnienie oraz pomijająca kluczowe zagadnienia Ocena Skutków Regulacji; budzące wątpliwości pod kątem proporcjonalności nowe, niemal kierownicze uprawnienia Pełnomocnika Rządu ds. Cyberbezpieczeństwa czy Kolegium, a także brak rozważenia rozwiązań alternatywnych oraz brak oszacowania kosztów finansowych i organizacyjnych, które miałyby zostać poniesione w niezwykle krótkim czasie przez przedsiębiorców.

Należy także odnotować, że wbrew uzasadnieniu projektu przedłożony projekt nie jest niezbędny dla implementacji Europejskiego Kodeksu Łączności Elektronicznej (EKŁE), a może wręcz bardzo skomplikować terminowe wprowadzenie i wdrożenie Prawa Komunikacji Elektronicznej, które w swoim projekcie, co do zasady kompleksowo adresuje wszystkie wymagania dot. bezpieczeństwa, jakie wynikają z EKŁE.

Jako uważni obserwatorzy obszaru polityki publicznej oraz legislacji, w zakresie m.in. bezpieczeństwa mamy oczywiście świadomość, że przedstawiony projekt ustawy jest realizacją unijnego „5G Toolbox", w zakresie mechanizmu oceny bezpieczeństwa rozwiązań dostawców dla sieci 5G. Projekt wydaje się jednak wykraczać poza ten zakres, co w zakresie samego mechanizmu oceny dostawców, oznacza, że nie ma on dotyczyć obszaru określonej kategorii sieci telekomunikacyjnej, ale wszystkich obszarów wchodzących do krajowego systemu cyberbezpieczeństwa. Tym samym, potencjalnie oceny takie mogłyby dotyczyć wszelkich dostawców, w tym z sektorów kluczowych w rozumieniu KSC tj. energii,

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS

transportu, bankowości i infrastruktury rynków finansowych, ochrony zdrowia, zaopatrzenia w wodę, infrastruktury cyfrowej.

Co więcej, skala zaproponowanych do pilnego wdrożenia reform, a szczególnie wzmocnienia uprawnień administracji publicznej i krajowych CSIRT zaskakuje szczególnie, że dotychczas jedną z kluczowych barier w sprawnym wdrażaniu ustawy KSC był faktyczny brak wystarczających kadr mających się zajmować w sektorze publicznym cyberbezpieczeństwem, a sytuacja w tym zakresie nie uległa w ostatnim okresie istotnej poprawie. System przeznaczony do współpracy jednostek w ramach krajowego systemu cyberbezpieczeństwa zgodnie ze Strategią Cyberbezpieczeństwa RP na lata 2019-2024 ma dopiero zostać uruchomiony od 2021 r., a w ramach planowanych projektów UE, MC zakłada finansowanie ze środków publicznych wielu projektów z obszaru cyberbezpieczeństwa, które mają służyć budowie potencjału administracji. Jednocześnie, takich jak przewidziane w projekcie ustawy zmian nie zakłada wprost wspomniana Strategia Cyberbezpieczeństwa RP na lata 2019-2024. Dyrektywa NIS, która była podstawą dla ustawy KSC jest dopiero w toku szczegółowej rewizji. Jednocześnie przygotowanie do planowanych zmian wymagało będzie istotnych nakładów finansowych po stronie administracji już od momentu wejścia nowej ustawy w życie. Tymczasem środki finansowe na pokrycie nowych zadań po stronie administracji publicznej zaplanowano dopiero od 2022 r., a oszacowania kosztów po stronie sektora prywatnego niestety nawet nie próbowano w OSR podjąć. Postulujemy zabezpieczenie środków finansowych na pokrycie zadań administracji publicznej w tym zakresie od 2021 r., a w przypadku braku takiej możliwości opóźnić wejście w życie ustawy do czasu kiedy faktyczna realizacja zadań będzie mogła być wykonywana.

Na obecnym etapie, należałoby zrezygnować w projekcie z przepisów dotyczących objęcia przedsiębiorców komunikacji elektronicznej nowymi obowiązkami w ramach ustawy o krajowym systemie cyberbezpieczeństwa, w tym w zakresie włączenia ich do krajowego systemu cyberbezpieczeństwa oraz wprowadzenia nowego reżimu raportowego w zakresie incydentów, który miałby zostać wprowadzony mimo, że istnieje już właściwy dla takich podmiotów kanał raportowania do Prezesa Urzędu Komunikacji Elektronicznej. Właściwy tryb w tym zakresie został już przedstawiony w projekcie PKE, a jego ewentualne rozszerzenie wymaga pogłębionej dyskusji i czasu.

CZĘŚĆ SZCZEGÓŁOWA

1. Stanowisko w zakresie nowych obowiązków przedsiębiorców komunikacji elektronicznej.

Projektowane przepisy rozdziału 4a, a także związany z nimi nowy art. 1, definicje oraz zamiar powołania CSIRT Telco stanowią propozycję pilnego wprowadzenia zupełnie nowego reżimu prawnego i organizacyjnego funkcjonowania przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa. Koncepcja ta zdaje się przy tym pomijać obiektywny fakt, że sektor ten jest i tak

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS

znacząco obciążony z uwagi na najpierw opóźnione, a ostatnio prowadzone w dużym tempie zmiany całego systemu prawnego w ramach przyjęcia nowego Prawa Komunikacji Elektronicznej, które, mimo, że wciąż jest na etapie prac rządowych, ma obowiązywać już od 21 grudnia br.

Analiza przedłożonego projektu oraz uzasadnienia w tym zakresie wskazuje, że głównym celem i identyfikowanym brakiem jest deficyt odpowiedniej informacji o incydentach dotyczących komunikacji elektronicznej po stronie CSIRT krajowych oraz operatorów usług kluczowych. Takie wnioski są o tyle zastanawiające, że już dzisiaj w reżimie prawnym Prawa telekomunikacyjnego, przedsiębiorca telekomunikacyjny jest zgodnie z art. 175a ust. 1 obowiązany niezwłocznie informować Prezesa UKE o naruszeniu bezpieczeństwa lub integralności sieci lub usług, które miało istotny wpływ na funkcjonowanie sieci lub usług, o podjętych działaniach zapobiegawczych i środkach naprawczych. Jednocześnie, w celu zapewnienia odpowiednich informacji dla podmiotów krajowego systemu cyberbezpieczeństwa, zgodnie z art. 175a ust. 1a dodanym właśnie ustawą o krajowym systemie cyberbezpieczeństwa z 2018 r., obowiązkiem Prezesa UKE, jest przekazywanie informacji o naruszeniach, jeżeli dotyczą one zdarzeń będących incydentami w rozumieniu ustawy z dnia 5 lipca 2018 r. o krajowym systemie CSIRT właściwemu dla zgłaszającego przedsiębiorcy telekomunikacyjnego. Co więcej, Prezes UKE ma możliwość korzystania z systemu informatycznego tworzonego na potrzeby krajowego systemu cyberbezpieczeństwa (art. 46 KSC). Konsultowany już projekt PKE utrzymuje te kluczowe rozwiązania i to one powinny być w pierwszej kolejności rozważane.

Oznacza to, że już istnieje mechanizm raportowania i przekazywania informacji o incydentach w obszarze telekomunikacji, które mają wpływ na cyberbezpieczeństwo. Jeśli ten mechanizm nie funkcjonuje zgodnie z oczekiwaniami, należy rozważyć jego dostosowanie, a nie wprowadzanie drugiego, na poziomie przepisów potencjalnie zbliżonego mechanizmu raportowania przedsiębiorców do CSIRT. Zauważamy jednocześnie, że między definicjami incydentów w obu projektach występują istotne różnice, które nie pozwalają uznać, że mowa jest o identycznym zakresie raportowania. Takie działanie jest w naszej ocenie niezgodne m.in. z art. 67 pkt 1, 2 i 3, a przynajmniej częściowo także z art. 68 ustawy – Prawo przedsiębiorców, które nakazują, aby opracowując projekt aktu normatywnego określającego m.in. wykonywania działalności gospodarczej (a tego przepisy KSC dotyczą) kierować się zasadami proporcjonalności i adekwatności, a w szczególności dążyć do nienakładania nowych obowiązków administracyjnych, a jeżeli nie jest to możliwe, dążyć do ich nakładania jedynie w stopniu koniecznym do osiągnięcia ich celów; dążyć do ograniczenia obowiązków informacyjnych, zwłaszcza, gdy wymagane informacje są przekazywane przez obowiązanych organom władzy publicznej na podstawie obowiązujących przepisów; implementując prawo Unii Europejskiej i prawo międzynarodowe, dążyć do nakładania wyłącznie obowiązków administracyjnych niezbędnych do osiągnięcia celów implementowanych przepisów. Tymczasem uzasadnienie i OSR ograniczają się jedynie do stwierdzeń,

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS

że przedsiębiorcy komunikacji elektronicznej zostaną włączeni do KSC oraz otrzymają wsparcie CSIRT (o które według wiedzy naszej organizacji nie wnioskowali).

Jednocześnie, niezrozumiałe, przynajmniej z uwagi na brak wcześniejszej dyskusji w tym temacie, są zawarte w OSR sformułowania wskazujące, że raportowanie przedsiębiorców telekomunikacyjnych miałoby odbywać się do CSIRT zamiast do UKE. Jakkolwiek utrzymanie jednego, podstawowego kanału komunikacji jest postulowanym rozwiązaniem, tak jednak CSIRT są podmiotami wyspecjalizowanymi w zakresie cyberbezpieczeństwa i nie są w naszej ocenie właściwe do zastąpienia UKE w realizacji zadań odnośnie całego obszaru bezpieczeństwa i integralności usług i infrastruktury telekomunikacyjnej, które dalece przekraczają same kwestie cyberbezpieczeństwa. System współpracy z UKE w tym zakresie jest ugruntowany od lat i jedyną dodatkową kwestią, jaka mogłaby zostać w tym zakresie dopracowana to ew. sposób kwalifikowania przez UKE naruszeń/incydentów jako takich, które są incydentami w rozumieniu ustawy o krajowym systemie cyberbezpieczeństwa oraz sprawność ich przekazywania do CSIRT zgodnie z obowiązującymi już, i utrzymywanymi w projekcie PKE przepisami. Kwestie te, jak się wydaje powinny zostać jednak zorganizowane przez samą administrację i nie powinny wpływać na zakres obowiązków przedsiębiorców telekomunikacyjnych.

Ponadto, zauważamy, że planowany do wprowadzenia do KSC zakres przepisów dot. bezpieczeństwa jest wybiórczy i kopiowane z projektu PKE przepisy nie tworzą spójnego systemu odpowiedzialności przedsiębiorców komunikacji elektronicznej wobec CSiRT (niebędących same w sobie organami administracji), a nie Prezesa UKE. Istotne wątpliwości wiążą się również z praktycznym aspektem raportowania, tj. brakiem aktów wykonawczych dot. określenia progów istotności oraz wzoru formularza raportowego. Jakkolwiek utrzymanie w mocy dotychczasowych rozporządzeń dotyczących raportowania wobec UKE zostało przewidziane w projekcie PKE, tak w przypadku przeniesienia/zdublowania tych obowiązków w KSC i w relacji z CSIRT nie do pominięcia jest fakt, że rozporządzeń tych dla tego kanału zgłoszeń nie będzie już w systemie prawnym. A biorąc pod uwagę zakres planowanych zmian w upoważnieniu do wydania rozporządzenia dot. progów istotności zmiany, jakie musiałoby wprowadzić nowe rozporządzenie, mogą okazać się w praktyce bardzo znaczące pozostawiając podmioty obowiązane w poważnej niepewności co do kształtu przyszłych obowiązków jakie miałyby obowiązywać już od 21 grudnia br.

Wyłączenie dostawców usługi interpersonalnej niewykorzystującej numerów z zakresu rozdziału 4a

Zgodnie z rozdziałem 4a pt. „obowiązki przedsiębiorców komunikacji elektronicznej" przedsiębiorcy komunikacji elektronicznej mają stać się częścią krajowego systemu cyberbezpieczeństwa. Należy zwrócić uwagę, że podmiotem obowiązków wskazanych w tym rozdziale jest „przedsiębiorca komunikacji elektronicznej". Tym samym projektowana ustawa o KSC odwołuje się w zakresie definicyjnym do pojęcia przedsiębiorcy telekomunikacyjnego z projektu ustawy o PKE, wedle którego

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS

(zob. art. 2 pkt 41 projektu PKE) przedsiębiorca komunikacji elektronicznej to przedsiębiorca telekomunikacyjny lub podmiot świadczący usługę komunikacji interpersonalnej niewykorzystującej numerów. Z kolej usługa komunikacji interpersonalnej niewykorzystująca numerów oznacza usługę umożliwiającą bezpośrednią interpersonalną i interaktywną wymianę informacji za pośrednictwem sieci telekomunikacyjnej między skończoną liczbą osób, gdzie osoby inicjujące połączenie lub uczestniczące w nim decydują o jego odbiorcy lub odbiorcach, z wyłączeniem usług, w których interpersonalna i interaktywna komunikacja stanowi wyłącznie funkcję podrzędną względem innej usługi podstawowej, w tym usługę, która nie umożliwia realizacji połączeń z numerami z planu numeracji krajowej lub międzynarodowych planów numeracji (art. 2 pkt 77 projektu PKE). Innymi słowy to ostatnie pojęcie oznacza usługę np. poczty elektronicznej czy czatów internetowych. Świadczy o tym choćby motyw 17 zd. 1 EKŁE, który wyraźnie wskazuje, że usługi łączności interpersonalnej obejmują wszystkie rodzaje poczty elektronicznej: „*Usługi łączności interpersonalnej są to usługi, które umożliwiają interpersonalną i interaktywną wymianę informacji, obejmujące takie usługi, jak tradycyjne połączenia głosowe między dwiema osobami, lecz również wszystkie rodzaje poczty elektronicznej, usług przekazywania wiadomości lub czatów grupowych*”.

Z powyższego wynika, że wykorzystanie w nowelizacji ustawy o KSC terminu „przedsiębiorcy komunikacji elektronicznej” powoduje, iż wskazane, obszerne i uciążliwie obowiązki będą musiały być stosowane także przez np. dostawców poczty elektronicznej. Takie podejście nie znajduje jednak uzasadnienia w charakterystyce usługi poczty elektronicznej, która w zasadniczy sposób różni się od usługi telekomunikacyjnej.

Niewątpliwie przepisy ustawy o KSC uwzględniając regulacje zawarte w EKŁE powinny w odmienny sposób traktować dostawców usług lub sieci telekomunikacyjnych oraz dostawców usług łączności interpersonalnej niewykorzystującej numerów. Takie stanowisko jest zgodne z motywem 95 EKŁE:

> *„Z uwagi na rosnące znaczenie usług łączności interpersonalnej niewykorzystujących numerów należy zapewnić aby podlegały one również odpowiednim wymogom bezpieczeństwa zgodnie z ich specyficznym charakterem i istotną rolą w gospodarce. Dostawcy usług powinni również zapewnić poziom bezpieczeństwa proporcjonalny do istniejącego ryzyka. Ze względu na to, że dostawcy usługi interpersonalnej łączności niewykorzystujące numerów zazwyczaj nie sprawują rzeczywistej kontroli nad transmisją sygnałów w sieciach, stopień ryzyka w przypadku takich usług można uznać za niższy pod pewnymi względami niż w przypadku tradycyjnych usług łączności elektronicznej. Dlatego też, jeżeli tylko jest to uzasadnione aktualną oceną ryzyka dla bezpieczeństwa, środki podejmowane przez dostawców usługi interpersonalnej łączności niewykorzystujące numerów powinny być łagodniejsze.*

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS

Takie samo podejście powinno być stosowane odpowiednio do usług łączności interpersonalnej wykorzystującej numery, jeżeli dostawca nie sprawuje rzeczywistej kontroli nad transmisją sygnału".

Planowane w KSC regulacje nie powinny naruszać zasad wynikających z dyrektywy EKŁE, ponieważ całkowicie nieuzasadnione jest zrównywanie obowiązków w zakresie bezpieczeństwa sieci i usług dla wszystkich przedsiębiorców komunikacji elektronicznej, jeśli ich realny wpływ na wskazane bezpieczeństwo jest całkowicie różne. Co więcej, nałożenie na rodzimych dostawców wskazanych usług (np. poczty elektronicznej) dodatkowych obowiązków może naruszyć zasady konkurowania lokalnych dostawców z globalnymi graczami. Więcej, nałożenie na tych ostatnich szeregu nowych obowiązków będzie wymagało istotnego zwiększenia zatrudnienia, jak i doprowadzi do wzrostu innego rodzaju obciążeń, co w ostatecznym rezultacie może sprawić, że działalność wielu dostawców poczty elektronicznej może po prostu nie sprostać rachunkowi ekonomicznemu takiej działalności.

Na marginesie, projekt KSC nie harmonizuje z projektem PKE. Dla przykładu, art. 20c ustawy o KSC przywołuje pojęcie „przedsiębiorcy komunikacji elektronicznej", o którym mowa w art. 47 ust. 1 projektu PKE. Jednakże wskazany przepis PKE odnosi się wyłącznie do przedsiębiorcy telekomunikacyjnego, który nie wyczerpuje całości kategorii „przedsiębiorców komunikacji elektronicznej".

Z tych względów postulujemy:

1) Usunięcie przepisów dot. włączenia przedsiębiorców komunikacji elektronicznej do KSC.
2) Przywrócenie wyłączenia przedsiębiorców telekomunikacyjnych oraz dostawców usług zaufania z obowiązków dot. bezpieczeństwa oraz zgłaszania incydentów.
3) Usunięcie Rozdziału 4a art. 20a-20f pt. „obowiązki przedsiębiorców komunikacji elektronicznej", a także związanych z tymi obszarami definicji oraz zamiaru wprowadzenia CSIRT Telco.
4) Dyskusję na temat możliwości usprawnienia aktualnego systemu pod kątem potrzeb podmiotów KSC, w sposób, który nie będzie skutkował dodatkowymi obowiązkami przedsiębiorców oraz nie będzie rewolucjonizował w przyspieszony sposób dotychczasowego modelu działania. W naszej ocenie tak doniosłe zmiany nie powinny być wprowadzone bez dogłębnej i rzeczowej dyskusji z ich głównymi adresatami, a na pewno nie w zaproponowanym trybie i terminach.
5) Ponadto podtrzymujemy uwagi przedstawione w toku konsultacji PKE w zakresie przepisów, które zostały powtórzone w projekcie nowelizacji ustawy KSC.

Usunięcie z projektu ustawy zakładanych zmian dotyczących włączenia przedsiębiorców komunikacji elektronicznej do krajowego systemu cyberbezpieczeństwa, usunięcie wyłączenia przedsiębiorców telekomunikacyjnych oraz dostawców usług zaufania z przewidzianych w ksc przepisów dot.

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS

bezpieczeństwa i zgłaszania incydentów, dodania nowego rozdziału 4a. dotyczącego obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa, a także związanych z tymi obszarami definicji oraz zamiaru wprowadzenia CSIRT Telco. W naszej ocenie tak doniosłe zmiany nie powinny być wprowadzone bez dogłębnej i rzeczowej dyskusji z ich głównymi adresatami, a na pewno nie w zaproponowanym trybie i terminach.

Stanowisko w zakresie oceny dostawców

Część ogólna

W zakresie proponowanego modelu oceny bezpieczeństwa dostawców urządzeń lub oprogramowania, zakładamy, że proponowane rozwiązanie ma stanowić wdrożenie rekomendacji wynikających z tzw. „5G Security Toolbox". Jednocześnie jednak należy brać pod uwagę, że skutki wydawanych ocen mogą de facto oznaczać wykluczenie wymiany handlowej między polskimi przedsiębiorstwami, a określonymi w ocenie dostawcami. W tym zakresie oceniamy także, że proponowane rozwiązania wydają się być bardziej restrykcyjne niż te, które rekomendowane są na poziomie UE.

W naszej ocenie, projekt wymaga precyzyjnej oceny i rewizji pod kątem spełnienia podstawowych wzorców konstytucyjnych wywodzonych z kluczowej zasady demokratycznego państwa prawa, przepisów ustawy Prawo przedsiębiorców, a także obowiązku notyfikacji uregulowanego na poziomie prawa krajowego w Rozporządzeniu Rady Ministrów z dnia 23 grudnia 2002 r. (w szczególności w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych). Podobne obawy wiążą się z zachowaniem zasad przepisów unijnych na poziomie TFUE, dyrektywy o konkurencji, zasad swobodnego przepływu towarów czy zasady niedyskryminacji. Istotnym argumentem, który należy podnieść jest kwestia obowiązku notyfikacji uregulowanego na poziomie prawa krajowego w Rozporządzeniu Rady Ministrów z dnia 23 grudnia 2002 r. (w szczególności w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych). Przedmiotowy obowiązek jest także uregulowany w Dyrektywie 2015/1535 Parlamentu Europejskiego i Rady z dnia 9 września 2015 r. ustanawiającej procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego. Wreszcie, wątpliwości budzi zgodność z zasadami przyjętymi na poziomie WTO. Na tym etapie jednak nie przedstawiamy uszczegółowionego stanowiska w tym zakresie, zakładając, że w toku merytorycznego dialogu uda się wypracować rozwiązania, które będą racjonalne i służące faktycznej poprawie poziomu cyberbezpieczeństwa w Polsce. Wskazujemy

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS

jedynie, że z uwagi na istotne ryzyka, tak dla przedsiębiorców jak i budżetu państwa, przepisy w tym zakresie muszą być wyjątkowo precyzyjne, a procedura oparta o obiektywne, merytoryczne kryteria.

Przede wszystkim jednak uważamy, że efektywne podejście do zwiększenia poziomu cyberbezpieczeństwa w obszarze urządzeń i oprogramowania wymaga podejścia spójnego na poziomie przynajmniej Unii Europejskiej, jeśli nie globalnym. Naszym zdaniem tym celom będą prawidłowo służyć opracowywane obecnie schematy certyfikacji europejskiej bazujące na unijnym „Cybersecurity Act". Już dzisiaj zapewnieniu bezpieczeństwa urządzeń służą narzędzia certyfikacyjne w ramach chociażby „Common Criteria", Nesas czy same specyfikacje techniczne urządzeń, np. dla 5G przygotowywane przez 3GPP, które adresują już kwestie bezpieczeństwa. Dopiero po ich opracowaniu, wdrożeniu oraz zebraniu pierwszych doświadczeń, w tym wykryciu realnych zagrożeń, należałoby ewentualnie przejść do dalszych działań skutkujących wykluczaniem określonych podmiotów z rynku. Drugim aspektem jest fakt, że wdrażane obecnie przez poszczególne kraje europejskie rozwiązania nie są spójne, tj. posługują się różnymi narzędziami i kryteriami. Nie sprzyja to tworzeniu wspólnego potencjału w zakresie cyberbezpieczeństwa, a w przyszłości może generować niezbadane jeszcze problemy w warstwie technicznej interoperacyjności oraz konkurencji, szczególnie w przypadkach zastosować transgranicznych w stosujących różne podejście krajach sąsiednich.

Stąd w pierwszej kolejności apelujemy o:

- Zintensyfikowanie prac na poziomie UE, w ramach, których precyzyjnie i klarownie powinno zostać określone wspólne podejście UE do kwestii bezpieczeństwa urządzeń i oprogramowania, które mają krytyczne znaczenie dla bezpieczeństwa.
- Oparcie planowanego do przyjęcia w Polsce mechanizmu oceny, o ocenę samych urządzeń i oprogramowania, a nie wyłącznie samych dostawców, w sposób bazujący na rzetelnych mechanizmach certyfikacji i oceny technicznej, w tym tj.:
    - NESAS: Określany wspólnie przez 3GPP i GSMA. Jest to dobrowolny program stosowany przez sektor telefonii komórkowej, zapewniający podstawowy i kompleksowy audyt bezpieczeństwa dowodzi, że sprzęt sieciowy spełnia wymogi bezpieczeństwa, a sprzedawcy sprzętu sieciowego – standardy bezpieczeństwa w procesie rozwoju produktów i cyklu życia. GSMA posiada radę akredytacyjną, która jest odpowiedzialna za monitorowanie i opracowywanie planów oraz udzielanie akredytacji.
    - ENISA: Unijne ramy certyfikacji bezpieczeństwa cybernetycznego mają na celu przyjęcie wspólnego podejścia i ustanowienie europejskich ram certyfikacji bezpieczeństwa cybernetycznego, które określają główne wymogi dla europejskich systemów bezpieczeństwa cybernetycznego i europejskich certyfikatów zgodności produktów ICT,

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS

usługi ICT lub procesów ICT, które mają być uznane i stosowane we wszystkich państwach członkowskich.

- Przyjęcie rozwiązań, które nie będą budziły wątpliwości w zakresie wymogów dotyczących dobrych praktyk legislacyjnych, jak i obowiązujących unijnych, umów międzynarodowych czy prawa krajowego.

Odniesienie do poszczególnych projektowanych przepisów ustawy:

Przepisy w tym zakresie muszą być wyjątkowo precyzyjne, a procedura oparta o obiektywne merytoryczne kryteria z uwzględnieniem skutków dla konkurencyjności rynku, kosztów wdrożenia etc.

1) Art. 66a ust. 1– doprecyzowanie możliwości wykorzystania nowych uprawnień Kolegium

Kolegium w ramach dokonywanej oceny jako organ o charakterze administracyjno-politycznym powinno obligatoryjnie korzystać z oceny technicznej wydawanej przez odpowiednio certyfikowane laboratorium. Zdaniem KL w skład Kolegium powinni wchodzić wysokiej rangi i posiadający wszechstronną wiedzę w temacie cyberbezpieczeństwa przedstawiciele biznesu. Ponadto uważamy, że ocena powinna dotyczyć przede wszystkich samych urządzeń i oprogramowania, a ewentualnie pomocniczo samego dostawcy. Zgodnie z Toolbox 5G, (str. 12) "*Ocena profilu ryzyka dostawców i zastosowanie ograniczeń do dostawców uznanych za wysokiego ryzyka — ma następować w odniesieniu do kluczowych aktywów*". Projekt ustawy nie bierze natomiast pod uwagę kategorii aktywów z punktu widzenia bezpieczeństwa, wraz z poziomem wrażliwości i listą kluczowych elementów (kategorie elementów i funkcji). Niewłaściwe jest w naszej ocenie nakładanie takich samych zobowiązań na wszystkie aktywa. Ponadto zauważamy niezgodność ze środkiem SM03 Toolbox (strony 12 i 21 Toolbox), również dlatego, że przewiduje się całościowe wyłączenie dostawcy. Toolbox 5G SM03 przewiduje natomiast możliwość wyłączenia, ale z wyłączeniem dostaw określonej infrastruktury (aktywa kluczowe) takie jak sprzęt i oprogramowanie dotyczące sieci rdzeniowej. Innymi słowy, polskie propozycje zawarte w projekcie wykraczają poza wymagania zawarte w Toolbox.

Z tego względu proponujemy, aby art. 66a ust. 1 otrzymał następujące brzmienie:

„1. Kolegium może, na wniosek członka lub członków Kolegium, sporządzić ocenę ryzyka związaną ze sprzętem lub oprogramowaniem o znaczeniu krytycznym, decydującym o sposobie zarządzania: przetwarzaniem informacji i przesyłania danych, mechanizmami kryptograficznymi, mechanizmami

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS

zarządzania wirtualizacją oraz interfejsami zapewniającymi uprawnionym podmiotom dostęp do przekazów nadawanych lub odbieranych w sieci podmiotów krajowego systemu bezpieczeństwa cybernetycznego. Wniosek o sporządzenie oceny może zostać złożony po:

1) *stwierdzonym istotnym incydencie bezpieczeństwa lub integralności u podmiotów krajowego systemu cyberbezpieczeństwa lub dostawców usług komunikacji elektronicznej na poziomie krajowy, które zostało spowodowane przez sprzęt lub oprogramowanie danego dostawcy, w zakresie objętym incydentem, lub*

2) *wykryciu wysokiej podatności sprzętu lub oprogramowania zwiększającej istotnie poziom ryzyka wystąpienia incydentu bezpieczeństwa lub integralności u podmiotów krajowego systemu cyberbezpieczeństwa lub dostawców usług komunikacji elektronicznej w zakresie objętym wykrytą podatnością i kiedy podmiot u którego wystąpiła podatność poinformuje o braku możliwości wdrożenia rozwiązań technicznych lub organizacyjnych ograniczających ryzyko związane z wykrytą podatnością.*

Kryteria dotyczące oceny są nieprecyzyjne i uznaniowe.

Uwaga 1: Tryb odwoławczy w zasadzie nie istnieje, o zmianę oceny MUSI wnosić Członek Kolegium.

Uwaga 2: Zasady powinny mieć charakter obiektywny i techniczny, w szczególności dla sprzętu i oprogramowania typu Commercial-of-the-Shelf (COTS). Należy bowiem przyjąć, że te ostatnie nie są modyfikowane dla potrzeb wybranych klientów, a dostosowane są dla ogólnego charakteru.

Uwaga 3: W przypadku takiego sprzętu i oprogramowania COTS jest możliwa sytuacja, że może nie spełniać kryteriów w konfiguracji podstawowej, ale po odpowiedniej konfiguracji (tzw. hardening) lub przy zastosowaniu dodatkowych środków ze strony producenta lub firm trzecich wypełnia wszystkie wymagania. Aktualny zapis nie przewiduje takiego scenariusza patrząc się na ten rodzaj sprzętu i oprogramowania jako zamkniętą całość pochodzącą od jednego producenta.

> Podsumowując: producenci sprzętu i oprogramowania, w szczególności tzw. COTS, a w zasadzie to użytkownicy takich rozwiązań (tak!) powinni mieć określoną jasną listę kryteriów do spełnienia i jeśli są one wypełnione to produkty i usługi mogą być wykorzystywane. Jednocześnie przy zmianie kryteriów lub ich podwyższeniu dotychczas wykorzystywane produkty/usługi powinny być w określonym czasie zmienione na nowe lub zastąpione.

2) Art. 66a ust. 2 i 3 – doprecyzowanie wniosku

W pierwszej kolejności zauważamy, że zakres możliwych ocen znacząco wykracza poza pierwotnie dyskutowany obszar sieci 5G. W myśl projektowanych przepisów skutkami ocen mogłyby być objęte

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS

wszystkie podmioty krajowego systemu cyberbezpieczeństwa, w tym operatorzy usług kluczowych. Oznacza to, że każdorazowo niezbędne będzie zachowanie bardzo wysokiej precyzji wniosku o dokonanie oceny oraz dokonania jeszcze przed jego złożeniem szczegółowej analizy wpływu i potencjalnych skutków, wraz z identyfikacją podmiotów, jakie mogą zostać objęte skutkami wydanej oceny.

Wniosek o przeprowadzenie oceny wymaga bardzo istotnego doprecyzowania, w taki sposób, aby zawierał już kluczowe elementy planowanego rozstrzygnięcia, w szczególności w zakresie:

- Wskazania zakresu badania bezpieczeństwa określającego, jakie konkretnie kategorie urządzeń lub oprogramowania danego dostawcy, a także zakres ich stosowania mają zostać poddane badaniu.
- Określenie zakresu użytkowania danego typu urządzeń lub oprogramowania, w tym wskazanie podmiotów, które mogą być objęte potencjalnymi skutkami wydawanej oceny.
- Opis rynku dostawców urządzeń lub oprogramowania, które poddawane jest badaniu.
- Oceny skutków planowanej do wydania oceny, w tym w zakresie wpływu na konkurencję i konsumentów oraz koszty jej wdrożenia.
- Określenie poziomu proponowanej do wydania przez Kolegium oceny.

3) Art. 66a ust. 4 – doprecyzowanie kryteriów oceny

a) **art. 66a ust. 4 pkt 1 KSC**

Nawiązując do powyższych postulatów dot. skupienia się na ocenie sprzętu i oprogramowania, w art. 66a ust. 4 pkt 1 postulujemy usunąć słowa *„jakie stanowi dostawca sprzętu i oprogramowania*”.

b) **art. 66 ust. 4 pkt 2 KSC**

Postulujemy usunięcie przepisu.

Ocena musi być przeprowadzana na podstawie jasno określonych, jasnych, jednoznacznych i możliwych do zweryfikowania kryteriów. W przeciwnym razie nie będzie to obiektywna ocena, lecz ocena uznaniowa. W warstwie legislacyjnej jest to w naszej ocenie jest to sprzeczne z przepisami §6 rozporządzenia Prezesa Rady Ministrów z dnia 20 czerwca 2002 r. w sprawie zasad techniki prawodawczej, który wskazuje, że: *Przepisy prawa są tak sformułowane, że intencje prawodawcy są dokładnie wyrażone adresatom zawartych w nich norm*. Przepisy te naruszają przepisy rozporządzenia, ponieważ są one niezrozumiałe i nie jest możliwe określenie ich treści. W szczególności trudno ustalić

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS

faktyczne znaczenie zwrotu "*prawdopodobieństwo wpływu dostawcy sprzętu lub oprogramowania na kraj spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego*".

4) Art. 66a ust. 4 pkt 2-5: Kryteria oceny dostawcy

W naszej ocenie kryteria oceny powinny zostać uzupełnione o:

- Ocenę wpływu na konkurencyjność rynku (w tym ocena tego, czy ograniczona liczba dostawców nie przyczyni się do wzrostu cen czy opóźnień w realizacji dostaw), konsumentów, koszty oraz możliwość zapewnienia ciągłości działania usług przez podmioty będące aktualnie użytkownikami urządzeń lub oprogramowania poddanego badaniu, w szczególności jeśli wydawana byłaby ocena dot. wysokiego lub umiarkowanego ryzyka.
- Kryteria techniczne oceny, w tym dot. odniesienia do zgodności urządzeń lub oprogramowania z dokumentami standaryzacyjnymi, a także w zakresie posiadanych przez badane urządzenia lub oprogramowanie certyfikatów bezpieczeństwa. Należy również odnieść się do budowanego obecnie schematu certyfikacji dla 5G w ramach Cybersecurity Act, który wydaje się, że powinien być kluczowym narzędziem do profesjonalnego badania bezpieczeństwa. W procesie oceny należy uwzględnić opinie certyfikowanych laboratoriów.
- Uzyskanie opinii użytkowników urządzeń lub oprogramowania poddawanych ocenie.

Poniżej przedstawiamy propozycję zmiany w zakresie art. 66a ust. 4 pkt 2 w sposób, który w naszej ocenie będzie charakteryzował się obiektywizmem w zakresie weryfikacji kryteriów oraz bardzo wysokim stopniem profesjonalizacji weryfikacji, co zapewni poprawność wyników stosowanych kryteriów oceny. Kryteria nietechnologicznie są często niezdefiniowane i bardzo trudno jest zweryfikować i ocenić niejasne pojęcia, ale nie powinny odgrywać kluczowej roli, gdyż mogą prowadzić do błędnych wniosków.

„2) analizę sposobu i zakres wdrożenia przez dostawców środków technicznych i organizacyjnych, zwanych dalej „środkami", w celu zapewnienia bezpieczeństwa lub integralności sieci lub usług, a w szczególności:

a) uzyskanie certyfikatu (takich jak ISO27001, Common Criteria, Network Equipment Security Scheme, unijny program certyfikacji cyberbezpieczeństwa) *dla sprzętu lub oprogramowania o znaczeniu krytycznym, które mogą podlegać ocenie Kolegium, o której mowa w art. 66 a ust. 1 KSC,*

b) posiadanie deklaracji wiarygodności zawierającej zobowiązania do: pełnej współpracy w zakresie bezpieczeństwa z użytkownikami sprzętu lub oprogramowania; nieprzekazywania wbrew zawartym

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS

umowom danych i informacji osobom trzecim; wyrażenia zgody i odpowiedniego wsparcia w zakresie kontroli bezpieczeństwa i analiz penetracyjnych jego produktu w wymaganym zakresie; potwierdzenia, że sprzęt lub oprogramowanie nie posiadają celowo wdrożonych i wrażliwych pod względem bezpieczeństwa funkcjonalności i że nie zostaną one wbudowane w późniejszym czasie; niezwłocznego powiadomienia przedsiębiorcy o wszelkich znanych mu lub wykrytych zagrożeniach dla zapewnienia bezpieczeństwa,

c) poziom zapewnianej przez dostawcę integralności sprzętu lub oprogramowania, a w szczególności zapewnienie ich użytkownikom: możliwości weryfikacji integralności nabytych składników krytycznych w każdym czasie; możliwości weryfikacji czy dane składniki krytyczne nie zostały podczas dostawy zmanipulowane, naruszone lub w inny sposób zmienione; prowadzonego przez dostawcę monitoringu bezpieczeństwa w celu zidentyfikowania zagrożeń bezpieczeństwa oraz podejmowania środków zapobiegawczych;"

5) Art. 66a ust. 5 - gradacja ryzyk

Jak już wskazano wyżej, w naszej ocenie proponowana konstrukcja nie jest zgodna ze środkiem SM03 Toolbox (strony 12 i 21 Toolbox) dlatego, że przewiduje całościowe wyłączenie dostawcy bez odniesienia do konkretnych „krytycznych aktywów". Toolbox przewiduje możliwość wyłączenia, ale w zakresie określonej infrastruktury. Innymi słowy, projekt wydaje się wykraczać poza ramy określone w europejskich rekomendacjach.

Wątpliwości budzi także przyjęta w art. 66a ust. 5 Projektu gradacja ryzyk, a ściśle ich definiowanie. Chodzi o różnicę pomiędzy wysokim ryzykiem a ryzykiem umiarkowanym. W przypadku bowiem obu definicji jest to poważne zagrożenie a różnica polega na tym, że w przypadku wysokiego ryzyka zmniejszenie tego ryzyka nie jest możliwe a w przypadku umiarkowanego jest możliwe. Tymczasem poziomy powinny wyraźnie (art. 66a ust. 5 lit a-b Projektu) różnić się gradacją, tak jak się różnią ryzyka opisane w art. 66a ust. 5 lit b-d Projektu, a nie wyłącznie oceną czy można to ryzyko zmniejszyć czy też nie. Jednocześnie należałoby przyjąć, że zawsze można poziom takiego ryzyka zmniejszyć, a przynajmniej powinno się stworzyć możliwość dla dostawcy podjęcia próby jego zmniejszenia. Poważne, więc zastrzeżenia budzi przyjęcie z góry założenia, że w przypadku „wysokiego ryzyka" zmniejszenie poziomu tego ryzyka przez wdrożenie środków technicznych lub organizacyjnych nie jest możliwe.

Tym samym sposób opisu poziomów ryzyka wydaje się zbyt ogólny, a w świetle braku uwypuklenia w kryteriach oceny kwestii technicznych, istotne wątpliwości budzi także w jaki sposób miałoby być weryfikowane czy dla danego przypadku możliwe jest wdrożenie dodatkowych rozwiązań technicznych

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS

lub organizacyjnych uzasadniających nadanie danemu dostawcy oceny ryzyka umiarkowanej, a nie wysokiej.

Tym samym w zakresie ryzyk wysokiego i umiarkowanego:

- Postulujemy wykreślenie odniesienia do oceny dostawcy, na rzecz oceny sprzętu lub oprogramowania.
- W ryzyku wysokim postulujemy wskazanie, że oznacza ono bardzo poważne (a nie tylko poważne) zagrożenie.

6) Przepis art. 66a ust. 5 lit a Projektu powinien otrzymać następujące brzmienie:
a) wysokie ryzyko, jeżeli dostawca sprzętu lub oprogramowaniea stanowi bardzo poważne zagrożenie dla cyberbezpieczeństwa państwa i zmniejszenie poziomu tego ryzyka przez wdrożenie środków technicznych lub organizacyjnych nie jest możliwe".
b) umiarkowane ryzyko, jeżeli dostawca sprzętu lub oprogramowaniae stanowi poważne zagrożenie dla cyberbezpieczeństwa państwa a zmniejszenie poziomu tego ryzyka możliwe jest przez wdrożenie środków technicznych lub organizacyjnych, albo
c) niskie ryzyko, jeżeli dostawca sprzętu lub oprogramowaniae stanowi niewielkie zagrożenie dla cyberbezpieczeństwa państwa, albo
d) brak zidentyfikowanego poziomu ryzyka, jeżeli nie stwierdzono zagrożenia dla cyberbezpieczeństwa państwa lub jego poziom jest znikomy.

7) Art. 66a ust. 7 KSC – plan naprawczy w przypadku uzyskania określonej oceny ryzyka

W naszej ocenie uprawnienie do przedstawienia środków naprawczych powinno przysługiwać także w przypadku określenia wysokiego poziomu ryzyka, a Kolegium będzie miało uprawnienie do oceny takich propozycji. Jednocześnie, konsekwentnie postulujemy rezygnację z oceny samego dostawcy, na rzecz oceny urządzeń lub oprogramowania.

Postulujemy więc nadanie art. 66a ust. 7 Projektu następującego brzmienia:

> *7. W przypadku określenia wysokiego, umiarkowanego lub niskiego ryzyka dostawca sprzętu lub oprogramowania, którego sprzętu lub oprogramowania dotyczy ocena może przedstawić*

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS

Kolegium środki zaradcze i plan naprawczy. W przypadku akceptacji tych środków zaradczych i planu naprawczego, Kolegium zmienia ocenę.

8) Art. 66 a ust. 5 i 8 KSC - forma Komunikatu oraz brak administracyjnej ścieżki odwoławczej od oceny dostawcy

W zakresie planowanej formy ogłoszenia oceny tj. Komunikatu, mamy istotne wątpliwości, co do adekwatności takiego sposobu działania. Komunikat będzie miał bardzo istotne skutki dla potencjalnie szerokiego kręgu adresatów, którzy aktualnie wykorzystują urządzenia lub oprogramowanie ocenianych dostawców. Nie powinno ulegać wątpliwości, że krąg tych adresatów Kolegium powinno określić precyzyjnie w toku prowadzonego postępowania dot. oceny bezpieczeństwa. Skoro to wpływ na bezpieczeństwo, w tym bezpieczeństwo narodowe miałby być badany to również skala i rodzaj działalności podmiotów korzystających lub mogących korzystać z danych rozwiązań musi zostać uwzględniona. Sam Komunikat, będzie jednocześnie rodził dla nich określone obowiązki i ograniczenia, doniosłe także w sferze prawa cywilnego (np. zawarte umowy długoterminowe), a przede wszystkim w zakresie własnej organizacji i sposobu prowadzenia działalności. W tym ujęciu Komunikat posiada cechy indywidualnego aktu o skutkach zbliżonych dla decyzji administracyjnej lub wręcz określenia praw i obowiązków, które co do zasady powinny być nakładane w drodze ustawy.

W tym zakresie uważamy, że forma ogłoszenia powinna zostać zrewidowana, a w szczególności zapewniać możliwość udziału w procesie oceny także podmiotom, których dotkną skutki dokonanej oceny, przynajmniej w formie konsultacji dot. możliwości redukcji poziomu ryzyka oraz identyfikowanego przez nie aktualnego poziomu ryzyka, a także w formie środków odwoławczych od takich rozstrzygnięć.

Od rozstrzygnięcia Kolegium powinna być zapewniona możliwość wniesienia środków odwoławczych przez podmiot niezadowolony z rozstrzygnięcia (dokonanej oceny ryzyka dostawcy) do organów sprawujących wymiar sprawiedliwości, niezależnie, do jakiej kategorii ryzyka, o którym mowa w art. 66a ust. 5 Projektu zaliczony zostanie dostawca sprzętu lub oprogramowania. Nie powinna być bowiem dokonywana gradacja środków odwoławczych w zależności od tego, czy rozstrzygnięcie (ocena) jest bardziej lub mniej dotkliwe.

Obecna konstrukcja art. 66a ust. 8 Projektu w zakresie środków odwoławczych, pomimo że używa się w tym przepisie słowa „odwołanie" jest pozorowana, pozbawiająca podstawowych praw podmiotów zainteresowanych weryfikacją dokonanej oceny przez Kolegium w sposób obiektywny i niezależny przez sąd. Przyjęta konstrukcja pozwala na to, że Kolegium będzie „sędzią we własnej sprawie" tj. będzie sprawdzało własną decyzję. Ogólne przepisy prawne, przewidują oczywiście konstrukcję wniosku

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS

o ponowne rozpoznanie sprawy przez organ, który wydał decyzję, ale zawsze przysługują także środki odwoławcze do sądu od takiego ponownego rozpoznania sprawy.

Potwierdzeniem tezy o pozorowanej konstrukcji odwołania, jest także okoliczność, że zgodnie z obecnym brzmieniem art. 66a ust. 8 Projektu, zdanie ostatnie: Wniesienie odwołania nie wstrzymuje działań określonych w art. 66b. W praktyce oznacza to, więc, że przewidziane w tym przepisie „odwołanie" nie ma praktycznego znaczenia, skoro pomimo jego wniesienia będą podejmowane praktycznie nieodwracalne w swoich skutkach decyzje w zakresie np. wycofania sprzętu z sieci operatora czy utraty kontaktu na sprzedaż infrastruktury telekomunikacyjnej. W tym ujęciu oznacza to, że nawet niezasadna decyzja Kolegium może wywołać taki skutek, jaki wywołałoby jej utrzymanie.

Ponadto przedstawiamy poniższą propozycje zmiany brzmienia przepisów:

a) Przepis art. 66a ust. 8 Projektu otrzymuje brzmienie:

„8. Dostawcy sprzętu lub oprogramowania, którego dotyczy ocena, przysługuje wniosek do Kolegium o ponowne rozpoznanie sprawy w zakresie oceny. Przepisy działu 2 rozdziału 10 ustawy z dnia 14 czerwca 1960 r. - Kodeks postępowania administracyjnego w zakresie odwołań od decyzji stosuje się odpowiednio. Od decyzji Kolegium wydanej po rozpoznaniu wniosku o ponowne rozpoznanie sprawy przysługuje skarga do Wojewódzkiego Sądu Administracyjnego."

b) W Art. 66a Projektu należy dodać nowy ust. 10:

„*Postępowanie przed Kolegium prowadzone jest zgodnie z przepisami ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego*"

Postanowienia k.p.a. regulują tryb postępowania i wydawanie decyzji przez organy państwowe. Obecnie projektowane przepisy odrębnie regulują te kwestie za pomocą zaledwie kilku przepisów, które można uznać za posiadające charakter proceduralny. Przepisy te nie mogą jednak zastąpić odpowiednich regulacji k.p.a. Uwagi te dotyczą także projektowanych wymogów, jakie elementy powinna zawierać ocena Kolegium (art. 66a ust. 5 Projektu), w tym zakresie przedstawienia uzasadnienia oceny.

9) Art. 66a ust. 7 i 9 KSC – ostateczność Komunikatu

Jednocześnie nNiezależnie od uwag dot. formy Komunikatu oraz możliwości odwołania, nasze praktyczne wątpliwości budzi możliwość modyfikacji Komunikatu po jego ogłoszeniu w wyniku odwołania lub przedstawienia środków naprawczych przez dostawcę. Aby ograniczyć ryzyko związane ze zbyt szybkim wejściem w życie publikowanego Komunikatu należy przewidzieć w nim odpowiedni okres przejściowy, w którym możliwe są jeszcze zmiany w wyniku przewidzianych w projekcie środków

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS

odwoławczych. Z perspektywy podmiotów, które mają mieć obowiązek dostosowania się do treści Komunikatu nie jest akceptowalna sytuacja, w której tak ważne rozstrzygnięcie będzie skuteczne, mimo, że jeszcze nie jest ostateczne i może zostać zweryfikowane. Ewentualnie środki odwoławcze/konsultacyjne należy zintegrować z procedurą oceny tak, aby w życie wprowadzana była ostateczna ocena.

art. 66b

1) Art. 66b – ocena ryzyka

Jednocześnie nasze wątpliwości budzi możliwość modyfikacji Komunikatu po jego ogłoszeniu w wyniku odwołania lub przedstawienia środków naprawczych przez dostawcę. Aby ograniczyć ryzyko związane ze zbyt szybkim wejściem w życie publikowanego Komunikatu należy przewidzieć w nim odpowiedni okres przejściowy, w którym możliwe są jeszcze zmiany w wyniku przewidzianych w projekcie środków odwoławczych. Z perspektywy podmiotów, które mają mieć obowiązek dostosowania się do treści Komunikatu nie jest akceptowalna sytuacja, w której tak ważne rozstrzygnięcie będzie skuteczne mimo, że jeszcze nie jest ostateczne i może zostać zweryfikowane. Ewentualnie środki odwoławcze/konsultacyjne należy zintegrować z procedurą oceny tak aby w życie wprowadzana była ostateczna ocena.

2) Art. 66b – ocena ryzyka

a) Jak wskazaliśmy wyżej, skuteczność Komunikatu musi następować od jego wejścia w życie w formie ostatecznej, a nie od wskazanego w projekcie ustawy „sporządzenia" oceny, co jest czynnością faktyczną kończącą pewien etap oceny.

b) Postulujemy wykreślenie odniesienia do oceny dostawcy, na rzecz oceny sprzętu lub oprogramowania.

a) W zakresie określenia ryzyka, jako wysokiego należy doprecyzować skutki poprzez wskazanie, że w okresie na wycofanie urządzeń lub oprogramowania możliwe jest też dokonywanie zakupów lub wdrożeń mających na celu utrzymanie funkcjonowania dotychczasowych funkcjonalności, a w szczególności utrzymanie ciągłości świadczenia usług. Ma to absolutnie kluczowe znaczenie dla możliwości reakcji na awarie i uszkodzenia. Ponadto okres na wycofanie należy wydłużyć do 10 lat co ma na celu poszanowanie praw nabytych użytkowników urządzeń lub infrastruktury i umożliwienie im korzystania z danych rozwiązań przynajmniej w pełnym okresie ich amortyzacji i podstawowej przydatności technicznej. Ewentualnie postulujemy, aby Kolegium dokonywało oceny, jaki okres jest niezbędny na dostosowanie (po zasięgnięciu opinii użytkowników), przy czym nie powinien on być

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS

w żadnym przypadku krótszy niż 7-letni podstawowy okres amortyzacji dla niektórych kategorii urządzeń stosowanych w sieciach telekomunikacyjnych.

b) W Projekcie nie ma różnicy pomiędzy skutkami oceny wysokiego ryzyka (art. 66b ust. 1 pkt 1 Projektu) oraz skutkami oceny umiarkowanego ryzyka (art. 66b ust. 2 pkt 1 Projektu). Skutki te, w przypadku umiarkowanego ryzyka powinny być mniej dotkliwe niż w przypadku wysokiego ryzyka. Propozycja przewiduje dwojakiego rodzaju skutki i obowiązki. Pierwszy realizuje postanowienia 5G Toolbox i polega na dywersyfikacji dostawców, identycznie jak w w § 3 ust. 1 pkt 2 rozporządzenia Ministra Cyfryzacji z dnia 22 czerwca 2020 r. w sprawie minimalnych środków technicznych i organizacyjnych oraz metod, jakie przedsiębiorcy telekomunikacyjni są obowiązani stosować w celu zapewnienia bezpieczeństwa lub integralności sieci lub usług (Dz.U. z 2020 r. poz. 1130). Drugi obowiązek związany jest z realizacją postanowień art. 66a ust. 7, w postaci podjęcia odpowiednich działań naprawczych w celu usunięcia stwierdzonych uchybień, podejmowanych przez obie strony tj. przez podmioty krajowego systemu cyberbezpieczeństwa oraz dostawców, co gwarantuje skuteczność działań w zakresie poprawy bezpieczeństwa.

W przypadku braku wprowadzenia przepisów zapewniających wymaganą elastyczność w zakresie uwzględniania oceny Kolegium, za zasadne uznajemy wprowadzenie mechanizmów finansowej rekompensaty z tytułu poniesionych kosztów i strat związanych z wydaniem oceny.

Projekt przepisu*:* ***Art. 66 b ust. 1 KSC – ocena ryzyka na poziomie wysokim***
„W przypadku sporządzenia oceny ryzyka określającej wysokie ryzyko określonego krytycznego sprzętu lub oprogramowania podmioty krajowego systemu cyberbezpieczeństwa:
1) nie wprowadzają do użytkowania sprzętu, oprogramowania i usług infrastruktury krytycznych określonych w ocenie danego dostawcy sprzętu lub oprogramowania, z wyjątkiem sytuacji kiedy dokonanie zakupów lub wdrożeń jest niezbędne dla funkcjonowania ich sieci, infrastruktury lub usług, a także naprawy awarii lub uszkodzeń;
2) wycofują z użytkowania sprzęt, oprogramowanie i usługi określone w ocenie danego dostawcy sprzętu lub oprogramowania nie później niż 5 10 lat od dnia ogłoszenia komunikatu o ocenie.”

Projekt przepisu: ***Art. 66b ust. 2 KSC– ocena ryzyka na poziomie umiarkowanym***
W przypadku sporządzenia oceny określającej umiarkowane ryzyko określonego krytycznego sprzętu lub oprogramowania, podmiotu krajowego systemu cyberbezpieczeństwa stosują strategię skutkującą brakiem uzależnienia od jednego dostawcy poszczególnych elementów sieci telekomunikacyjnej

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS

a dostawcy sprzętu lub oprogramowania wprowadzają środki zaradcze oraz plan naprawczy, o których mowa w art. 66a ust. 7"

3) Art. 66 b : propozycja rekompensat: należy dodać ust. 3 oraz 4 w art. 66b po ust. 2:

3. dotychczasowi użytkownicy sprzętu lub oprogramowania otrzymują odszkodowanie za koszty związane z wymianą sprzętu lub oprogramowania;
4. rekompensata jest obliczana na podstawie wydatków poniesionych na zakup sprzętu lub oprogramowania, z uwzględnieniem amortyzacji i kosztów usunięcia. Rekompensata jest wypłacana w ciągu 30 dni.

Uzasadnienie:
Wprowadzenie przepisów art. 66b Projektu spowoduje oczywiste dla operatorów telekomunikacyjnych koszty, niezawinione przez nich, spowodowane nowymi regulacjami, które to koszty powinny być operatorom zrekompensowane przez Skarb Państwa reprezentowany przez Prezesa UKE. Zaproponowane regulacje w praktyce oznaczają de facto „wywłaszczenie" operatorów z posiadanego Sprzętu, w tym znaczeniu, że muszą się pozbyć sprzętu wcześniej zakupionego, pomimo, że gdyby nie wprowadzone nowe regulacje mogliby korzystać z tego sprzętu dłużej. W konsekwencji będą musieli ponieść wydatki związane z koniecznością zakupu nowego sprzętu, a ponadto wydatki związane z usuwaniem z sieci istniejącego sprzętu.

Art. 66c punkt 1 „Plan naprawczy"

Okres 3 miesięcy na sporządzenie i przedstawienie planu oraz harmonogramu odstąpienia od sprzętu i oprogramowania usługodawcy jest praktycznie niemożliwy do zrealizowania. Jednocześnie, jak zostało wskazanie powyżej, wszelkie środki związane z oceną powinny być stosowane do oprogramowania lub sprzętu, a nie w stosunku do dostawców.

Propozycja zmiany:

„W szczególnie uzasadnionych przypadkach Pełnomocnik może zobowiązać podmiot krajowego systemu cyberbezpieczeństwa lub przedsiębiorcę komunikacji elektronicznej, do którego zastosowanie ma ocena, do sporządzenia i dostarczenia w ciągu 3 miesięcy roku planu i harmonogramu wycofania

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS

z użytkowania sprzętu, oprogramowania i usług dostawcy sprzętu lub oprogramowania, którego dotyczy ocena określająca wysokie ryzyko."

Art. 67a – ostrzeżenia i polecenia zabezpieczające

a) Instytucja ostrzeżenia powinna zostać zmodyfikowana do formy zgodnej ze swoją nazwą. Należy więc wykreślić z przepisów wszelkie odniesienia wskazujące na skutki ostrzeżenia jako „polecenia", „nakazu", „zakazu". Obecnie bowiem, niezależnie od procesu opiniowania przez Kolegium, już samo ostrzeżenie, mogłoby skutkować wykluczeniem wskazanych w nim dostawców. Takie uprawnienie rodzi bardzo daleko idące obawy potencjalnych adresatów tych ostrzeżeń. Tym samym ostrzeżenie, jeśli miałoby zostać utrzymane musi otrzymać charakter, w którym w przypadku identyfikacji wystąpienia ryzyka incydentu krytycznego odpowiednie podmioty byłyby o tym informowane oraz otrzymywały informacje w sprawie możliwych działań. Aktualna formuła może być stosowana jedynie do podmiotów publicznych, a nie sektora prywatnego, wobec, którego rozwiązanie takie miałoby charakter nadania Pełnomocnikowi uprawnień o charakterze kierowniczym wobec podmiotów prywatnych, w tym spółek giełdowych.
b) 2-letni okres, na jaki mają być wydawane ostrzeżenia lub polecenia zabezpieczające jest zdecydowanie zbyt długi i musi zostać ograniczony do okresu faktycznego zagrożenia, który powinien być liczony w dniach, a nie latach.
c) Zgodnie z art. 67c ust. 1 Projektu: *Polecenie zabezpieczające wydaje się w formie decyzji administracyjnej.* Analogiczny przepis powinien obowiązywać w przypadku wydania ostrzeżenia tj. art. 67c pkt 1 powinien otrzymać brzmienie: *"Pełnomocnik wydaje ostrzeżenia i polecenia zabezpieczające w formie decyzji administracyjnej".*
d) Kluczowy bowiem element zarówno ostrzeżenia, jak polecenia zabezpieczającego, tj. „określone zachowanie", jest taki sam. Przepis art. 67c ust. 4 pkt 1 Projektu dotyczący polecenia zabezpieczającego, odsyła w zakresie „*określonego zachowania*" do art. 67b ust. 3 Projektu, który szczegółowo reguluje elementy określonego zachowania w przypadku wydawania ostrzeżenia.
e) Brak odniesienia do postępowania administracyjnego w stosunku do czynności podejmowanych przez Pełnomocnika. Propozycja: Po ustępie 8 dodać ustęp 9: "*Postępowanie przed*

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS

pełnomocnikiem toczy się w oparciu o przepisy ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego. Ostrzeżenie ma formę decyzji administracyjnej."

f) W przypadku utrzymania tych narzędzi w pierwotnym kształcie, Pełnomocnik powinien zwracać koszty i ewentualne straty wynikające z wdrożenia rozwiązań wynikających z ostrzeżeń i poleceń zabezpieczających.

Art. 67c – polecenie zabezpieczające

Z uwagi na nieodwracalne skutki wykonania polecenia zabezpieczającego z rygorem natychmiastowej wykonalności, ten rygor powinien być usunięty.

art. 2 pkt 31 projektu: Art. 73 ust. 2a

Zaproponowany poziom kar pieniężnych jest zdecydowanie zbyt wysoki, a jednocześnie uderzająca jest dysproporcja możliwych kar nakładanych na sektor prywatny wobec kar, jakie za takie same naruszenia mogą obciążać podmioty publiczne -szczególnie w sytuacji, kiedy to w szczególności podmioty publiczne odpowiedzialne są za zapewnienie bezpieczeństwa w kluczowych obszarach definiowanych w aktualnej ustawie o krajowym systemie cyberbezpieczeństwa. Jednocześnie należy wykreślić odwołanie do obrotu „światowego". W przypadku działających w Polsce podmiotów, podlegających krajowym przepisom wysokość ewentualnych kar powinna odnosić się działalności tego podmiotu, a nie rodzić wątpliwości co do uwzględniania także skali działalności jego właścicieli, udziałowców lub akcjonariuszy realizowanej w ramach odrębnych formalnie podmiotów działających poza Polską.

Zmiany w zakresie operatorów usług kluczowych

1) Art. 14 dot. obowiązku powołania SOC:

a) W pierwszej kolejności zauważamy uwzględnienie zgłaszanego przez stronę społeczną postulatu, aby warunki techniczne i organizacyjne były ustalane na podstawie analizy ryzyka przeprowadzonej indywidualnie dla konkretnego operatora usług kluczowych. Nie sposób jednak nie zauważyć – co może być też refleksją dla planowanych obecnie zmian - że dwukrotnie wprowadzane rozporządzenia dot. warunków technicznych i organizacyjnych spowodowały już konieczność ponoszenia dodatkowych kosztów, które w normalnych uwarunkowaniach nie byłyby konieczne. Aktualna refleksja wskazująca, że rozporządzenie do art. 14 ust. 4 KSC w związku z usunięciem upoważnienia ustawowego byłoby uchylone, powinna być naszym zdaniem ostrzeżeniem przed tak daleko idącym jak planowane regulowaniem

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS

obowiązków przedsiębiorców komunikacji elektronicznej. Jednocześnie popieramy model szacowania ryzyka przez samego OUK

b) Odnośnie zamiaru wprowadzenia obowiązku powołania SOC dla operatora usługi kluczowej w celu realizacji zadań operatora usługi kluczowej, w naszej ocenie rozwiązanie to nie odpowiada praktyce adresowania wymagań ustawy przez operatorów usług kluczowych. SOC to centrum operacyjne bezpieczeństwa. Wyraźne ograniczenie możliwości realizacji zadań tylko do takiej struktury byłoby realizowalne wyłącznie gdyby podmiot świadczący usługę kluczową miał tylko jedną usługę, byłaby nią usługa kluczowa, a jednocześnie byłaby ona związana wyłącznie z obszarem, na którego ciągłość może mieć wpływ zagrożenia cyberbezpieczeństwa (a nie np. katastrofa naturalna czy fizyczne uszkodzenie), a wszystkie zadania wynikające z KSC miałyby charakter operacyjny. Tymczasem działalność podmiotów będących operatorami usług kluczowych często daleko wykracza poza zakres usługi kluczowej. Jednocześnie działalność ta jest wielokrotnie realizowana w skali ogólnopolskiej. Tym samym infrastruktura i usługi są rozproszone. Jednocześnie rozproszone mogą być struktury bezpieczeństwa dla całej tej organizacji. W tym celu powoływane są wyspecjalizowane jednostki działające w obszarach analizy ryzyk, ciągłości działania, ochrony informacji, wykrywania incydentów, reakcji na nie itp.. W tym zakresie mogą być też powoływane SOC, które jednak są jedynie częścią większej struktury organizacyjnej w zakresie bezpieczeństwa. Tym samym to, czym w praktyce są istniejące już SOC nie odpowiada założeniom przedstawionym w nowelizacji. Skutkiem proponowanych zapisów byłoby natomiast wprowadzenie dodatkowego obciążenia w postaci konieczności powołania odrębnego SOC wyłącznie na potrzeby usługi kluczowej, co nie jest uzasadnione, ani z uwagi na troskę o bezpieczeństwo, ani koszty i efektywność.

Tym samym, postulujemy utrzymanie dotychczasowego nazewnictwa tj. obowiązku powołania wewnętrznej struktury bezpieczeństwa lub zamówienia odpowiedniej usługi zewnętrznej w tym zakresie (także dla części zadań), która pozwala na zintegrowanie zabezpieczeń usługi kluczowej z istniejącymi już strukturami i procesami. Jednocześnie nie powinno być używane proponowane nazewnictwo (SOC), bowiem będzie mylące w świetle ugruntowanego już na rynku rozumienia zwrotu SOC. Zakres możliwości zamawiania usług zewnętrznych powinien być również uelastyczniony zgodnie z dalszymi postulatami.
Ewentualnie należy wprowadzić dodatkowe zapisy wskazujące na możliwość realizacji zadań także w dotychczasowym trybie tj. poprzez wewnętrzną strukturę, która lepiej niż wydzielony SOC, odpowiada praktyce podejścia do zabezpieczenia usługi kluczowej, jako części większej działalności.

c) Jeszcze dalej idące obawy wynikają z proponowanej konstrukcji art. 14 ust. 2, która w naszej ocenie będzie szkodliwa dla OUK, zarówno tych dobrze przygotowanych do swojej roli, jak i tych wciąż budujących ten potencjał. Przewidziano, bowiem tylko dwie możliwości tj. realizację zadań w ramach

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS

wewnętrznej struktury lub zamówienia całości usług, jako usług zewnętrznego „SOC". Pomijając już kwestie faktycznego znaczenia terminu SOC w świetle wymagań wskazanych w ustawie KSC, dla bardzo wielu praktycznych przypadków podstawowym i efektywnym modelem działania jest połączenie tych obu modeli tj. realizacja części zadań, w szczególności dotyczących działań typowo związanych z samą materią przedsiębiorstwa będącego OUK, w tym dot. bezpośrednio systemów odpowiedzialnych za usługę kluczową w ramach struktury wewnętrznej (przez istniejące już lub stworzone struktury bezpieczeństwa), a części zadań, jak np. tych związanych z wykrywaniem incydentów, monitorowaniem sieci oraz reakcją na cyberataki poprzez zamówienie usług zewnętrznych od wyspecjalizowanych podmiotów działających już na rynku. Taki model funkcjonuje już obecnie w praktyce. Co prawda, w redakcji przepisu użyto spójnika „lub", który jako alternatywa łączna może dopuszczać model mieszany, jednak faktyczna dopuszczalność takiego modelu, także w świetle dalszych przepisów dot. rejestru „SOC" dających kompleksową obsługę budzi nasze bardzo poważne wątpliwości.

W naszej ocenie aktualny kształt rynku rozwiązań cyberbezpieczeństwa pozwala stwierdzić, że nie istnieją, lub bardzo ograniczona jest dostępność podmiotów, które mogłyby na wysokim poziomie jakości zapewnić OUK kompleksową, zewnętrzną obsługę w zakresie wszystkich jego zadań. W tym zakresie niezbędne byłoby powoływanie wielostronnych konsorcjów złożonych z podmiotów o różnych specjalizacjach, w których dodatkowo niezbędny byłby koordynator całości zadań. Brak odpowiedniego poziomu konkurencji na rynku w tym zakresie skazywałby jednocześnie OUK na korzystanie wyłączenie z bardzo drogich i „szytych na miarę" rozwiązań lub stwarzał ryzyko powstawania podmiotów, które dopiero na bazie nawiązanej z OUK relacji uczyłyby się zarządzania całością tej materii. Jednocześnie poważnie ograniczona, ze szkodą dla samych OUK, byłaby możliwość elastycznego zarządzania zamawianiem na zewnątrz realizacji tylko wybranych zadań.
Z tych względów postulujemy nadanie przepisom kształtu dopuszczającego wyraźnie zamawianie przez OUK wybranych i wynikających z faktycznych potrzeb usług w zakresie realizacji zadań wskazanych w KSC, a nie tylko całości obsługi w ramach zewnętrznego „SOC". Odpowiednich modyfikacji, w przypadku ich utrzymania, wymagałyby też przepisy dot. rejestru, które powinny dopuszczać wpisywanie również podmiotów, które są wyspecjalizowane w określonych obszarach świadczenia usług dla OUK.

d) W art. 14 ust. 5 należy doprecyzować, że zakres dostępu nie może naruszać tajemnic prawnie chronionych, w tym tajemnic przedsiębiorstwa świadczącego usługi na rzecz OUK.

2) życie zwrotu SOC, który nie jest zarezerwowany wyłącznie dla operatorów usług kluczowych czy podmiotów świadczących na ich rzecz usługi, ma swoje konsekwencje także w zakresie dalszych przepisów projektowanej ustawy, które w naszej ocenie wymagają następujących poprawek:

   a) W art. 14 ust. 6 aktualnie sformułowany obowiązek może być rozumiany tak, że każdy prowadzony w Polsce SOC miałby podlegać obowiązkowi ogłoszenia na stronie internetowej,

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS

podczas gdy jak zakładamy intencją było jedynie wprowadzenie obowiązku ogłaszania informacji o możliwości i potencjale podmiotu, który chce i może świadczyć tego typu usługi na rzecz operatorów usług kluczowych. Zapisy w tym zakresie należy więc przeredagować.

b) W art. 14a dotyczącym prowadzenia rejestru SOC, należy odpowiednio zmodyfikować to odwołanie, aby nie mogło dotyczyć wszystkich SOC, ale jedynie podmiotów świadczących określone usługi na rzecz operatorów usług kluczowych. W ust. 3 należy odwołać się do art. 14 ust. 4, a nie do art. 14 ust. 2, bowiem to ust. 4 oznacza obowiązek przekazania informacji o zawarciu umowy z podmiotem zewnętrznym organowi właściwemu.

c) W zakresie art. 14a ust. 7 wątpliwości budzi czy przesłanki wpisania z urzędu (jak rozumiemy na wniosek „SOC") mają być rozumiane łącznie, a dodatkowo w naszej ocenie nie jest uzasadnione tworzenie dodatkowych wymagań wobec podmiotów wpisywanych z urzędu/na wniosek wobec podmiotów, które po prostu zawarły umowę z OUK.

3. Uzupełnienie Oceny Skutków Regulacji

W przedstawionym OSR nie została opisana kompleksowa i szczegółowa ocena skutków regulacji. Jednocześnie, za nieuzasadnione uznajemy tutaj potencjalne przyjęcie założenia, że ustawa sama w sobie nie prowadzi do wykluczenia jakichkolwiek dostawców. Ustawa daje do takich rozwiązań narzędzia, a sama możliwość ich zastosowania powinna zostać oceniona pod kątem możliwego wpływu. Każda, bowiem ocena skutków, musi odnosić się właśnie do potencjalnych skutków zastosowania wprowadzanych przepisów. W innym, bowiem przypadku zupełnie umyka sens jej prowadzenia. W tym

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS

ujęciu w naszej ocenie projekt ustawy będzie miał istotny wpływ na operatorów i dostawców (własność, ciągłość działalności, otoczenie biznesu, wolna konkurencja, gospodarka krajowa).

1) Potencjalny wpływ projektu ustawy na dostawców:

a. Należy przeprowadzić i przedstawić analizę potencjalnego stosowania ustawy w zakresie rynku dostawców.
b. Skrajne oceny mogą w związku z faktycznym wykluczeniem z rynku oznaczać istotną zmianę warunków konkurencji oraz dyskryminację niektórych podmiotów.
c. Zagrożenie to jest bardzo realne, szczególnie w kontekście zaproponowanych kryteriów oceny, które są ogólne i niewystarczająco oparte na normach technicznych i certyfikacji, takich jak NESAS i ENISA.
d. Stąd, postulujemy doprecyzowanie mechanizmów oceny, w tym poprzez skupienie się na badaniu technicznych aspektów sprzętu i oprogramowania.

2) Potencjalny wpływ projektu ustawy na operatorów telekomunikacyjnych, w zakresie dot. oceny dostawców:

a. Istotne zwiększenie poziomu niestabilności otoczenia prawnego i regulacyjnego, wpływające na zakres i tempo realizowanych inwestycji.
b. Konieczność poniesienia kosztów finansowych i organizacyjnych związanych z potencjalnym wydaniem opinii przez Kolegium.
c. Ograniczone tempo i zwiększenie kosztów realizacji inwestycji w sieć 5G, przede wszystkim z uwagi na brak jasnych i przewidywalnych w długim horyzoncie warunków dla realizacji inwestycji.
d. Zwiększenie poziomu niepewności w zakresie procedur alokacji częstotliwości oraz ich warunków, w tym w zakresie kosztów i możliwości wykonania ewentualnych zobowiązań. Ryzyko dalszych opóźnień w obszarze pilnej wciąż potrzeby alokacji pasma C.
e. Istotne ryzyko ograniczenia konkurencji na rynku dostawców urządzeń i oprogramowania wywoła naturalne dla takich sytuacji zwiększenie kosztów oraz ograniczenie możliwości negocjacji w toku procedur zakupowych. W efekcie spodziewany jest wzrost kosztów urządzeń i oprogramowania, wydłużenie okresów dostaw, a także ogólne pogorszenie warunków współpracy z dostawcami, których pozycja w wyniku stosowania ustawy może zostać wzmocniona.
f. Nieodpowiednie, nieostrożne oraz niedostoswane do przedstawionych w niniejszym stanowisku postulatów stosowanie projektowanych przepisów, może w skrajnych przypadkach powodować ryzyko konieczności ograniczenia lub wręcz zaprzestania

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS

świadczenia usług telekomunikacyjnych przez konkretne podmioty na rynku. Skutki takich sytuacji mogą być dramatyczne zarówno w zakresie wpływu na dane przedsiębiorstwo, jak i wpływu na ciągłość świadczenia usług, w tym usług o kluczowym znaczeniu dla bezpieczeństwa państwa i obywateli.

g. Wpływ na zawarte i obowiązujące, także wieloletnie umowy z dostawcami, które w wyniku opinii Kolegium musiałyby zostać rozwiązane lub zmienione.
h. Operatorzy, jako podmioty prawa krajowego, niezależnie od oceny docelowych rozwiązań prawnych będą zmuszeni do poddania się nowym regulacjom, co nie zamyka oczywiście drogi do możliwego kwestionowania wprowadzonych przepisów oraz związanych z tym konsekwencji, również o charakterze finansowym.
i. W efekcie, ostatecznymi „beneficjentami" zastosowania projektowanych przepisów będą niestety użytkownicy usług telekomunikacyjnych, a także krajowa gospodarka, dla których usługi, szczególnie w zakresie sieci 5G będą dostępne później i bardzo prawdopodobne, że po wyższej cenie.
j. Jednocześnie, w związku z projektem ustawy nie jest spodziewany wzrost bezpieczeństwa/cyberbezpieczeństwa na poziomie świadczonych usług telekomunikacyjnych. Głównym wektorem zagrożeń w tym zakresie są przede wszystkim aplikacje, złośliwe oprogramowanie oraz celowe działania przestępcze prowadzone przez jednostki lub podmioty zupełnie odrębne od samych dostawców urządzeń i oprogramowania sieciowego. Projekt ustawy nie adresuje jednak tych zagadnień.

3) Potencjalny wpływ projektu ustawy na konkurencję:

a. Polska ma ograniczoną liczbę dostawców sieci. Jeśli jeden z dostawców zostanie wyłączony, będzie to szkodzić innowacjom w technologii i może odroczyć digitalizację Polski.
b. Realny jest również wpływ na ceny i warunki współpracy z dopuszczonymi dostawcami, tj. wzrost kosztów urządzeń i oprogramowania, wydłużone okresy dostaw, utrudnienia w zakresie bieżącej obsługi.
c. Rozważone powinny zostać również kwestie możliwego wpływu na koszty i jakość usług świadczonych konsumentom i innym odbiorcom. W każdym przypadku ograniczenie rynku wiąże się ze wzrostem cen, które ostatecznie będą obciążać użytkowników końcowych.

4) Potencjalny wpływ projektu ustawy na budżet Polski i gospodarkę krajową:

a. potencjalna strata wskutek opóźnienia implementacji sieci 5G o 3 lata jest liczona w miliardach euro, ,w tym objęłaby ona wartość utraconych korzyści operacyjnych, korzyści

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS

konsumentów oraz innych podmiotów działających w sektorach takich jak przemysł samochodowy, służba zdrowia, transport oraz dostawy mediów.

b. Utrzymujący się brak precyzyjnych ustaleń dot. bezpieczeństwa sieci, może mieć negatywny wpływ na przebieg i spodziewane efekty procedur alokacji częstotliwości radiowych.
c. Potencjalne roszczenia o odszkodowanie wobec rządu polskiego podniesione przez dostawców zostaną ostatecznie wypłacone przez podatników i konsumentów.
d. Negatywny wpływ na życie i pracę podczas pandemii i po pandemii: jeśli Polska opóźni wdrożenie 5G, straci możliwość stworzenia nowych miejsc pracy

5) Potencjalny wpływ projektu ustawy na postęp technologiczny:

Wyłączenie któregokolwiek dostawcy, zwłaszcza w sytuacji ograniczonej podaży, spowoduje opóźnienie postępu w całym ekosystemie rozwoju cyfrowego. W naszej ocenie projekt ustawy będzie miał negatywny wpływ na rozwój Przemysłu 4.0. Opóźniona zostanie budowa niezbędnych kompetencji w obszarze samochodów podłączonych do sieci 5G, produkcji 5G, high-tech, rolnictwa 5G, usług portowych, zdalnej edukacji, sprzętu medycznego 5G, itp.

Konfederacja Lewiatan, KL/467/334/AM/2020

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS