KRAJOWA IZBA KOMUNIKACJI ETHERNETOWEJ

ul. Lindleya 16, 02-013 Warszawa
tel. + 48 22 2928700, fax +48 22 2928701
www.kike.pl, e-mail: biuro@kike.pl, grap@kike.pl
KRS 0000316678, REGON 141637224, NIP 9512270210

Warszawa, dnia 5 października 2020

ID KIKE: GRAP-571/20

Sz. P. Marek Zagórski
Minister Cyfryzacji

Ministerstwo Cyfryzacji
ul. Królewska 27
00-060 Warszawa

Dotyczy:

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

Szanowni Państwo,

działając na rzecz Krajowej Izby Komunikacji Ethernetowej (**KIKE**), niniejszym przedstawiam uwagi KIKE do *projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy – Prawo zamówień publicznych* (projekt z dn. 7 września 2020 r.), o których zostaliśmy poinformowani w piśmie z dnia 7 września 2020 r., znak: DP-III.0211.4.2020.

***

Biorąc pod uwagę możliwe ograniczenia w zakresie dostarczania sprzętu telekomunikacyjnego od określonych dostawców, wdrożona ustawa będzie miała niebagatelny wpływ nie tylko na działalność dostawców sprzętu, technologii i oprogramowania wykorzystywanego w sieciach telekomunikacyjnych, ale także na działalność samych operatorów telekomunikacyjnych zrzeszonych w Izbie.

Wymiar faktyczny nowych regulacji wpłynie na ciągłość działania dostawców sieci i usług łączności elektronicznej oraz na konkurencję na rynku telekomunikacyjnym, co może mieć także istotne przełożenie na sytuację i interesy konsumentów, będących ostatecznymi odbiorcami usług telekomunikacyjnych, jak również będzie wpływać na dalszy rozwój społeczeństwa cyfrowego, co jest jednym z priorytetów Unii Europejskiej. Skutki te niestety nie zostały w dostatecznym stopniu przeanalizowane ani w uzasadnieniu, ani w Ocenie Skutków Regulacji.

Przechodząc szczegółowo do uwag, zdaniem KIKE **ustawa o krajowym systemie cyberbezpieczeństwa** (dalej **KSC**) **w ogóle nie powinna mieć zastosowania do operatorów telekomunikacyjnych, szczególnie z segmentu małych i średnich przedsiębiorców**.

Należy przypomnieć, iż KSC stanowi implementację dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. (dalej **Dyrektywa**). Również nowelizacja jest motywowana jej implementacją. Zgodnie z motywem (7) Dyrektywy, ***Obowiązki*** *nakładane na operatorów usług kluczowych i dostawców usług cyfrowych* ***nie powinny jednak mieć zastosowania do przedsiębiorstw udostępniających publiczne sieci łączności lub świadczących publicznie dostępne usługi łączności elektronicznej w rozumieniu dyrektywy 2002/21/WE Parlamentu Europejskiego i Rady****, które podlegają szczegółowym wymogom w zakresie bezpieczeństwa i integralności ustanowionym w tej dyrektywie, ani nie powinny mieć zastosowania do dostawców usług zaufania w rozumieniu rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014, którzy podlegają wymogom w zakresie bezpieczeństwa określonym w tym rozporządzeniu.*

Dyrektywa wprost wyłącza spod jej stosowania określonych przedsiębiorców, podlegających w zakresie cyberbezpieczeństwa innym regulacjom. Z tego względu podczas uchwalania KSC w 2018 roku, spod zakresu podmiotowego wyłączono przedsiębiorców telekomunikacyjnych, o których mowa w ustawie z dnia 16 lipca 2004 r. *Prawo telekomunikacyjne*, w zakresie wymogów dotyczących bezpieczeństwa i zgłaszania incydentów. Powyższe zostało podkreślone w uzasadnieniu do KSC, *Wzorem podejścia przyjętego w dyrektywie 2016/1148 ustawa nie ma zastosowania wobec przedsiębiorców telekomunikacyjnych i dostawców usług zaufania, którzy zostali już objęci europejskimi i krajowymi wymaganiami sektorowymi z zakresu cyberbezpieczeństwa.*

Dyrektywa w zakresie podmiotów wyłączonych spod jej stosowania nie uległa zmianie. Nie ma więc powodu ani podstawy, aby ponad 2 lata po uchwaleniu ustawy implementującej Dyrektywę zmienić zakres podmiotowy i objąć stosowaniem KSC przedsiębiorców, którzy dotychczas nie byli objęci regulacją. Zmiana terminologii – *przedsiębiorcy telekomunikacyjnego* na *przedsiębiorcę komunikacji elektronicznej* nie spowoduje, że podmioty te z dnia na dzień zmienią zakres swojej działalności, będą bardziej podatni na cyberzagrożenia i będą w stanie sprostać wymogom stawianym przez KSC.

Co więcej, obowiązki przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci i usług oraz zadań i obowiązków na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego są określone w dziale 1 rozdziale 5 projektowanej ustawy prawo komunikacji elektronicznej (projekt ustawy z dnia 29 lipca 2020 r. – dalej jako **PKE**). To przepisy PKE będą regulować, jakie obowiązki ciążą na przedsiębiorcach komunikacji elektronicznej.

Zgodnie z przepisami PKE (art. 39 i nast. PKE) przedsiębiorcy komunikacji elektronicznej będą zobowiązani m.in. do zgłaszania Prezesowi UKE informacji o wystąpieniu incydentu, kwalifikując go zgodnie z rozporządzeniem wykonawczym. Ponadto przedsiębiorca komunikacji elektronicznej zobowiązany będzie do systematycznego przeprowadzania oceny wystąpienia sytuacji szczególnego zagrożenia czy podejmowania środków technicznych i organizacyjnych

zapewniających poziom bezpieczeństwa adekwatny do poziomu zidentyfikowanego ryzyka. Nie ma zatem powodu, aby obowiązki w zakresie bezpieczeństwa sieci i usług rozdrabniać na dwie regulacje – KSC i PKE. Dodatkowo wskazać należy, że PKE zawiera własną definicję *incydentu bezpieczeństwa.* Nie ma potrzeb, aby obok tego pojęcia wprowadzać pojęcie *incydentu telekomunikacyjnego*.

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. *ustanawiająca Europejski kodeks łączności elektronicznej* (dalej **EKŁE**), którą implementuje PKE, również nie przewiduje innych, szczególnych obowiązków w zakresie bezpieczeństwa sieci i usług niż te już zaprojektowane w PKE. W szczególności EKŁE nie nakazuje stosowania Dyrektywy do przedsiębiorców komunikacji elektronicznej czy też nie nakazuje jej stosowania w zakresie nieuregulowanym w EKŁE. Wszelkie odesłania do Dyrektywy zawarte w EKŁE dotyczą współpracy organów państwowych, a nie obowiązków poszczególnych przedsiębiorców komunikacji elektronicznej (patrz: motyw 98 EKŁE oraz art. 41 ust. 4 i 5 EKŁE).

Część nowych regulacji przewidzianych w KSC stanowi powielenie regulacji projektowanych w PKE. Projektowany art. 20a KSC jest duplikatem projektowanego art. 39 PKE – **treść tych przepisów jest niemalże identyczna.** Oznaczać to będzie, że na przedsiębiorców telekomunikacyjnych zostaną nałożone praktycznie takie same obowiązki, z dwóch różnych podstaw prawnych, a dodatkowo przepisy KSC rozszerzą obowiązki ponad te, przewidziane w EKŁE. Co więcej, zarówno projektowane przepisy KSC jak i PKE zawierają upoważnienie do wydania przepisów wykonawczych o identycznym zakresie.

W zakresie nowych obowiązków niewynikających z PKE wskazać należy, że CSIRT MON, CSIRT NASK i CSIRT GOV w sektorze telekomunikacyjnym uzyskają nowe kompetencje kosztem uprawnień Prezesa UKE oraz CSIRT Telco. Incydenty telekomunikacyjne będą badane przez ww. CSIRT, co należy uznać za błędną regulację - w zakresie bezpieczeństwa usług komunikacji elektronicznej i sieci telekomunikacyjnych główną rolę powinny odgrywać wyspecjalizowane organy telekomunikacyjne. Art. 42 PKE będzie zobowiązywać przedsiębiorcę komunikacji elektronicznej do zgłaszania incydentu bezpieczeństwa Prezesowi UKE, wobec czego nie ma potrzeb, aby przedsiębiorca ten musiał dodatkowo zgłaszać wystąpienie incydentu telekomunikacyjnego do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV i obok tego do CSIRT Telco oraz współdziałać z nimi przy obsłudze incydentu (projektowany art. 20c ust. 1 i 3 KSC). Ocena Skutków Regulacji błędnie zakłada, że wobec przedsiębiorców telekomunikacyjnych nowelizacja będzie oddziaływać w ten sposób, iż będą oni *zobowiązani do zgłaszania incydentów do zespołów CSIRT, <u>zamiast</u> do UKE.* Obowiązek zgłoszenia incydentu do UKE wynikający z PKE będzie niezależny od obowiązku przewidzianego w KSC. Dodatkowo projektowany art. 26 KSC wyraźnie wskazuje na działania CSIRT MON, CSIRT NASK i CSIRT GOV przy badaniu m.in. incydentów telekomunikacyjnych oraz przygotowywaniu materiałów dla Pełnomocnika, gdzie wyklucza się zarówno Prezesa UKE jak i CSIRT Telco. Przedsiębiorcy telekomunikacyjni będą zatem zobowiązani zgłaszać ten sam incydent dwa razy – do Prezesa UKE (na podstawie PKE), oraz do zespołów CSIRT (na podstawie KSC).

Na uwagę zasługuje również szczegółowe wyliczenie elementów zgłoszenia incydentu telekomunikacyjnego, zaproponowane w projektowanym art. 20d KSC. Takie określenie

elementów zgłoszenia nie występuje *ex lege* w PKE i jest ono zbyt szczegółowe, a wręcz nadmierne (np. wpływ na usługi kluczowe innych podmiotów, czego przedsiębiorca komunikacji elektronicznej może nie wiedzieć). Taka szczegółowość utrudni przedsiębiorcom telekomunikacyjnym zgłaszanie incydentów i będzie wprowadzać ich w błąd – przedsiębiorcy do zgłaszania incydentów telekomunikacyjnych będą zobowiązani do stosowania art. 20d KSC, a do zgłaszania incydentów bezpieczeństwa na podstawie PKE zobowiązani będą do stosowania formularza określonego w rozporządzeniu wydanym na podstawie art. 42 ust. 2 pkt. 2) PKE.

Zdaje się, że przepisy z zakresu cyberbezpieczeństwa powinny być spójne, a uchwalenie takich samych obowiązków w dwóch odrębnych aktach prawnych i dołożenie kolejnych z tego samego zakresu, nie będzie sprzyjać spójności przepisów.

Nowelizacja KSC rozszerza również kompetencje Kolegium. Zgodnie z art. 64 KSC Kolegium ma stanowić organ opiniodawczo-doradczy w sprawach cyberbezpieczeństwa. Zgodnie z projektowanymi przepisami art. 66a-66c KSC, Kolegium na wniosek jego członka może sporządzić ocenę ryzyka dostawcy sprzętu lub oprogramowania istotnego dla cyberbezpieczeństwa podmiotów krajowego systemu cyberbezpieczeństwa (czyli również sprzętu telekomunikacyjnego, zarówno wprowadzenia do użytkowania nowego jak i użytkowania starego), przekazywaną następnie Pełnomocnikowi, który ogłasza ją w postaci komunikatu w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski". **Dostawca sprzętu podlegający ocenie nie ma realnej możliwości odwołania się od decyzji**. Po pierwsze, termin na ewentualne odwołanie od oceny określającej ryzyko jako wysokie, wynosi 14 dni od publikacji komunikatu. Oznacza to, że *de facto* dostawcy sprzętu będą musieli codziennie śledzić Dziennik Urzędowy w poszukiwaniu informacji, czy czasem nie zostali objęci oceną ryzyka, o której mowa w art. 66a KSC. Po drugie, ewentualne odwołanie wnoszone jest do tego samego organu, który wydał zaskarżaną ocenę. Mało prawdopodobne, aby Kolegium chciało dokonać samokontroli swojej oceny na korzyść odwołującego. Po trzecie, dostawca sprzętu w ogóle nie ma możliwości odwołania się od oceny Kolegium w przypadku, gdy ryzyko zostało ocenione jako umiarkowane lub niskie – w takiej sytuacji możliwe jest jedynie zgłoszenie środków zaradczych i planu naprawczego poniekąd przyjmując, że w takiej sytuacji ocena Kolegium nie podlega kontroli.

Z uwagi na szerokie wątpliwości co do konstytucyjności projektowanej nowelizacji, Izba zleciła wykonanie opinii prawnej w tym przedmiocie. Opinia – stanowiąca załącznik do niniejszego stanowiska – jednoznacznie potwierdza, że zaprojektowana w nowelizacji procedura jest niekonstytucyjna.

Dalej, w przypadku oceny ryzyka określonego jako umiarkowane, podmioty krajowego systemu cyberbezpieczeństwa *mogą kontynuować użytkowanie dotychczas posiadanych egzemplarzy sprzętu, oprogramowania oraz rodzaju i liczby usług* ***wykorzystywanych przed opublikowaniem komunikatu*** *o ocenie danego dostawcy sprzętu lub oprogramowania* (projektowany art. 66b ust. 2 pkt 2) KSC). Oznacza to, że podmioty korzystające ze sprzętu/oprogramowania danego dostawcy (w tym zrzeszeni w KIKE przedsiębiorcy), nie będą mogły dokonywać ani upgrade'u, ani update'u wykorzystywanych urządzeń/oprogramowania, **co ma bezpośredni, negatywny wpływ na cyberbezpieczeństwo i jest wprost sprzeczne z celami KSC.** Wszelkie luki

zwiększające podatność sprzętu/oprogramowania na cyberataki usuwane są najczęściej poprzez aktualizację sprzętu/oprogramowania. Wyłączenie takiej możliwości spowoduje zmniejszenie poziomu cyberbezpieczeństwa, co stoi w sprzeczności z ogólnym celem KSC.

Cała powyższa koncepcja przeczy charakterowi Kolegium, które – pomimo, że ma być organem opiniodawczo-doradczym – będzie na podstawie art. 66a KSC wydawać opinie wywołujące wprost określone w art. 66b KSC skutki prawne w sferze praw i obowiązków stron. Może to być m.in. zakaz wprowadzenia do użytkowania sprzętu określonego dostawcy czy obowiązek wycofania jego sprzętu/oprogramowania z rynku. Kolegium będzie mogło arbitralnie wywierać wpływ na danego dostawcę decydując o tym, czy jego sprzęt lub oprogramowanie będzie mogło być użytkowane w Polsce czy nie. Jest to uprawnienie leżące poza kompetencjami opiniodawczo-doradczymi. **Nie ma przy tym <u>obiektywnych</u> przesłanek, jakimi ja kierować się Kolegium przy dokonywaniu oceny.**

Projektowany art. 66a ust. 4 KSC przewiduje, że przy wydawaniu oceny Kolegium ma się kierować m.in. tym, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, uwzględniając jednocześnie:

- stopień i rodzaj powiązań pomiędzy dostawcą sprzętu lub oprogramowania i tym państwem,
- prawodawstwo tego państwa w zakresie ochrony praw obywatelskich i praw człowieka,
- prawodawstwo w zakresie ochrony danych osobowych, zwłaszcza tam gdzie nie ma porozumień w zakresie ochrony danych między UE i danym państwem,
- strukturę własnościową dostawcy sprzętu lub oprogramowania,
- zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania.

Są to nieobiektywne przesłanki niemożliwe do zweryfikowania bez podejmowania nadzwyczajnych środków kontrolnych. Kolegium nie ma instrumentów prawnych ani faktycznych aby badać strukturę własnościową zagranicznego dostawcy sprzętu/oprogramowania czy zdolność ingerencji państwa w swobodę działalności gospodarczej tego dostawcy. Powyższe wymagałoby również wnikliwej analizy prawodawstwa tego państwa w zakresie ochrony praw człowieka i ochrony danych osobowych. W konsekwencji Kolegium będzie mogło arbitralnie decydować o wykluczeniu z rynku określonego dostawcy sprzętu lub oprogramowania, pod pretekstem konieczności zapewnienia cyberbezpieczeństwa, co w praktyce będzie nieweryfikowalne.

Nie jest zrozumiałe, dlaczego pod uwagę mają być brane indywidualne cechy dostawcy, a pomijane będą najistotniejsze z punktu widzenia cyberbezpieczeństwa aspekty informatyczno-technologiczne. W infrastrukturze wykorzystywane są również urządzenia pasywne, co do których z punktu widzenia cyberbezpieczeństwa bez znaczenia jest, od jakiego są dostawcy.

Konkludując, na podstawie opinii organu opiniodawczo-doradczego nie można zakazać korzystania z określonych urządzeń telekomunikacyjnych czy oprogramowania bez możliwości realnej obrony przed taką opinią przez zainteresowane podmioty, w tym przedsiębiorców

telekomunikacyjnych, którzy będą zmuszeni ewentualnie ponieść koszt wymiany urządzeń dostawcy objętego oceną.

Co ważne, **przepisy projektowanych art. 66a-66c KSC nie mają oparcia w Dyrektywie.** Procedura sprawdzająca dostawcę nie jest w niej przewidziana, a 5G toolbox[1] przywołany w uzasadnieniu zawiera wytyczne wyłącznie w zakresie zapewnienia bezpieczeństwa przy wdrażaniu sieci 5G, a nie przy infrastrukturze jako takiej.

Zgodnie z motywem (50) Dyrektywy, *Mimo iż producenci sprzętu i twórcy oprogramowania nie są operatorami usług kluczowych ani dostawcami usług cyfrowych, ich produkty zwiększają bezpieczeństwo sieci i systemów informatycznych. Odgrywają oni zatem ważną rolę w umożliwianiu operatorom usług kluczowych i dostawcom usług cyfrowych zabezpieczenia ich sieci i systemów informatycznych.* ***Taki sprzęt i oprogramowanie są już objęte obowiązującymi przepisami dotyczącymi odpowiedzialności za produkt****.* Dyrektywa (którą, jak podkreślamy, ma implementować KSC) nie przewiduje dodatkowej odpowiedzialności dostawców sprzętu czy oprogramowania. W polskim porządku prawnym dostawcy sprzętu i programowania odpowiadają za dostarczany produkt na podstawie art. 449[1] *kodeksu cywilnego* (odpowiedzialność za produkt niebezpieczny).

5G toolbox przewiduje, iż państwa członkowskie powinny mieć możliwość zastosowania *odpowiednich ograniczeń dla dostawców uznanych za stwarzających wysokie ryzyko, w tym niezbędnych wyłączeń w odniesieniu do kluczowych zasobów.* Z powyższego wynika, że:

- wobec dostawców uznanych za stwarzających wysokie ryzyko mogą być stosowane odpowiednie ograniczenia,
- niezbędne wyłączenia mogą być zastosowane w odniesieniu do kluczowych zasobów,
- 5G toolbox nie rozróżnia, czy chodzi o dostawcę pochodzącego z Europejskiego Obszaru Gospodarczego czy z państwa trzeciego,

wobec czego (1) przesłanki i ograniczenia przewidziane w art. 66a-66b KSC są niewspółmierne, (2) nie ma wskazanych kluczowych zasobów, wobec których mogą być zastosowane wyłączenia o najdonioślejszych skutkach, (3) każdy dostawca powinien móc podlegać ocenie, również krajowy. W żadnym wypadku dokonując oceny Kolegium nie powinno kierować się przesłankami zaproponowanymi w projektowanym art. 66a ust. 4 KSC. Należy jeszcze podkreślić, że 5G toolbox stanowi tzw. *soft law* i nie jest instrumentem o takiej samej mocy prawnej jak inne akty prawne. Zgodnie z art. 288 Traktatu o Funkcjonowaniu Unii Europejskiej, źródłami prawa europejskiego są rozporządzenia, dyrektywy i decyzje oraz niemające wiążącej mocy zalecenia i opinie. Ustanawianie tak rygorystycznych, niewspółmiernych do celu i nieobiektywnych przesłanek nie może nastąpić w oparciu o *soft law*.

Powielenie odpowiedzialności dostawców sprzętu w przepisach KSC powinno być zatem niedopuszczalne, szczególnie, że przepisy KSC wprowadzają odpowiedzialność za hipotetyczne, a nie stwierdzone niebezpieczeństwo i to nawet nie tyle samego wykorzystywanego sprzętu/oprogramowania, co osoby dostawcy w oparciu o nieobiektywne przesłanki. Nie ma w

[1] https://ec.europa.eu/digital-single-market/en/news/eu-toolbox-5g-security

polskim porządku prawnym przepisu, który zezwalałaby na represjonowanie przedsiębiorcy z uwagi na kapitał, który za danym przedsiębiorcą stoi w oderwaniu od jakości produkowanego sprzętu.

Jeśli przepisy KSC koniecznie mają regulować bezpieczeństwo sprzętu/oprogramowania, to powinny skupiać się na sprzęcie/oprogramowaniu jako takim (model sprzętu, wersja oprogramowania, itp.), w oderwaniu od podmiotu, który go dostarcza. Zaproponowane przesłanki mogą w konsekwencji doprowadzić do wykluczenia wszelkich dostawców sprzętu o kapitale spoza Unii Europejskiej.

Z uwagi na dalekoidące skutki regulacji, KIKE wykonało badania, obejmujące szczegółową analizę dot. wykorzystania sprzętu dostawców spoza UE. Wyniki załączonego do niniejszego stanowiska *Badania o skali wykorzystania w sektorze telekomunikacyjnym sprzętu dostawców pochodzących spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego* (dalej jako „**Badanie**"), potwierdziło, że czołowi producenci sprzętu elektronicznego, najczęściej wykorzystywanego do budowy sieci w Polsce, mają swoją siedzibę właśnie poza Unią Europejską lub Organizacją Traktatu Północnoatlantyckiego (NATO), co stwarza możliwość objęcia ich oceną ryzyka. Są to przede wszystkim:

i. **Dasan** (siedziba Seongnam, Korea Południowa),
ii. **D-Link** (Siedziba: Tajpej, Tajwan),
iii. **Huawei** (siedziba: Shenzhen, Chiny),
iv. **TP-Link** (siedziba: Shenzhen, Chiny),
v. **ZTE** (siedziba: Shenzhen, Chiny),
vi. **ZyXEL** (siedziba: Xinzhu, Tajwan).

Sprzęt producentów azjatyckich średnio stanowi ponad 80% ogólnie wykorzystywanego przez ISP sprzętu. Co ważne, ponad połowa ankietowanych ISP posiada sieć zbudowaną na asortymencie jednym dostawcy! Są to w największej mierze Huawei (45%), Dasan (21%) oraz ZTE (21%). Wykluczenie z rynku któregokolwiek z producentów azjatyckich może „pogrążyć" małego lub średniego operatora, który *de facto* zmuszony będzie wymienić wszystkie urządzenia na urządzenia innego producenta. **Szacowane koszty takiej wymiany liczone są w milionach złotych.** Na koszt taki składałyby się nie tylko wygenerowana liczba elektrośmieci (tj. liczba wycofanych urządzeń, w tym wydane abonentom routery czy dekodery, co dodatkowo porusza kwestię wpływu regulacji na ochronę środowiska), ale zakup nowych, często kilkukrotnie droższych urządzeń, wynagrodzenie dla osób mających wdrożyć zmiany – zapewnienie kompatybilności urządzeń, wymiana urządzeń w terenie, dostosowanie systemów informatycznych, itp.

Już tylko sami ankietowani mali i średni operatorzy telekomunikacyjni[2] oszacowali koszt ewentualnej wymiany na ponad 160 mln zł, a część z nich wprost wskazywała, że konieczność wymiany urządzeń skutkowałaby bankructwem firmy. Średni koszt wymiany sprzętu

[2] W ankiecie udział wzięło 57 przedsiębiorców z sektora małych i średnich ISP;

przypadający na jednego ankietowanego wyniósłby 2,99 mln zł. Gdyby założyć, że tego rodzaju skutki i w takiej skali dotkną każdego, aktywnie działającego na rynku przedsiębiorcę telekomunikacyjnego (a trzeba dodać, że skala finansowego zaangażowania operatorów dużych będzie zapewne na znacznie wyższym poziomie), to przyjmując liczbę aktywnych w Polsce przedsiębiorców telekomunikacyjnych (tj. takich, którzy składają raporty o swojej infrastrukturze) , których wedle raportów UKE na koniec 2019 było 3000[3], finansowy wpływ na rynek będzie ogromny, sięgając kwoty niemal 9 mld (8.970.000.000 zł).

Dalszym skutkiem uchwalenia nowelizacji KSC będzie zaburzenie konkurencji. Po pierwsze, konsekwencją zmuszenia operatora do wycofania sprzętu dostawcy azjatyckiego i zastąpienia go sprzętem innego dostawcy, będzie konieczność przekalkulowania swojej oferty. To użytkownicy końcowi poniosą finansowe konsekwencje nowelizacji. Oferty operatorów staną się droższe i przez to będą mniej atrakcyjne dla użytkowników końcowych, a w konsekwencji przestaną być konkurencyjne. Po drugie, operator taki nie będzie ryzykować wymiany sprzętu na sprzęt dostawcy „zwiększonego ryzyka" (tj. spoza UE/NATO), co do którego w najbliższym czasie również może zapaść decyzja o wykluczeniu z rynku. Dostawcy spoza UE/NATO staną się tym samym stygmatyzowani i to w oderwaniu od jakichkolwiek aspektów technicznych. Nie będzie istotne, czy sprzęt danego dostawcy rzeczywiście jest bezpieczny czy nie, tylko czy jest to dostawca spoza, czy z obszaru UE/NATO.

Sami ankietowani wskazali, że 95% z nich wydało swoim abonentom w ramach umowy o świadczenie usług, urządzenie producenta spoza UE/NATO. Ankietowani zadeklarowali, że dotyczy to łącznie ok. 222.903 abonentów. **Ewentualna konieczność wymiany tego sprzętu finansowo dotnie przede wszystkich tych ostatnich, poniosą oni bezpośrednie koszty wymiany urządzenia końcowego, oraz pośrednie koszty wymiany kompatybilnych z tymi urządzeniami urządzeń sieciowych operatora.**

Nadmienić należy, że projektowana regulacja stawia pod znakiem zapytania celowość wszystkich projektów POPC (w tym podłączenie do sieci szerokopasmowych placówek oświatowych), w których sprzęt jakiegokolwiek z ww. dostawców został wykorzystany. Zgodnie z podsumowaniem I, II i III naboru[4], w ramach projektów POPC zasięgiem zostało objętych łącznie 1 891 254 gospodarstw domowych oraz 13 246 placówek oświatowych. Wedle informacji przekazywanych przez członków Izby, w znacznej mierze w takich projektach wykorzystywany był sprzęt ww. dostawców, co potwierdziło Badanie. Spośród operatorów realizujących POPC i OSE:

- przy realizacji POPC (lub podobnego programu), 82% operatorów zadeklarowało wykorzystanie sprzętu producenta spoza UE/NATO, gdzie szacowana łączna cena zakupu takich urządzeń wyniosła ok. 49,34 mln zł,

[3] Zob. str. 56 *Raportu UKE o stanie rynku telekomunikacyjnego na koniec 2019 roku*. Źródło: https://www.uke.gov.pl/akt/raport-o-stanie-rynku-telekomunikacyjnego-w-2019-r-,345.html. W tym samym Raporcie przeczytamy, że łączna liczba przedsiębiorców telekomunikacyjnych wynosi 5 313. Zob. str. 45.

[4] https://cppc.gov.pl/po-polska-cyfrowa/po-pc-i-os/dzialania-1-1-wyeliminowanie-terytorialnych-roznic-w-mozliwosci-dostepu-do-szerokopasmowego-internetu-o-wysokich-przepustowosciach

- przy realizacji OSE, 90% operatorów zadeklarowało wykorzystanie sprzętu producenta spoza UE/NATO, gdzie szacowana łączna cena zakupu takich urządzeń wyniosła prawie 1,5 mln zł.

Na zakup takich urządzeń wydane zostały środki publiczne w kwocie ponad 50 mln zł. Wykluczenie z rynku któregokolwiek z ww. dostawców spowoduje m.in. to, że placówki oświatowe (a więc podmioty z sektora finansów publicznych) korzystające ze sprzętu któregokolwiek z ww. dostawców, będą zmuszone do ich wymiany. Projektowana regulacja przyczyni się do stworzenia sytuacji konfliktogennych, gdyż pierwszymi podmiotami, do których będą kierowane roszczenia związane z koniecznością zmiany sprzętu, będą beneficjenci POPC – a więc w tym i zrzeszeni w KIKE przedsiębiorcy telekomunikacyjni. Co więcej, dalsze procedowanie zmian w przyjętym projekcie może doprowadzić do chaosu organizacyjnego i niewykonania projektu *Ogólnopolskiej Sieci Edukacyjnej (OSE)* a to z uwagi na to, że szerokie grono wykonawców korzysta właśnie ze sprzętu i oprogramowania dostawców spoza UE. Z punktu widzenia gospodarności – art. 44 ust. 3 pkt 1) ustawy *o finansach publicznych*, wydanie ponad 50 mln zł na zakup sprzętu, który następnie decyzją ustawodawcy najpewniej będzie musiał zostać wycofany z rynku, nie jest wydatkowaniem środków publicznych *w sposób celowy i oszczędny.* Urządzenia takie zostały zakupione właśnie z uwagi na ich konkurencyjną cenę i wówczas nie było powodów aby przypuszczać, że w najbliższym czasie będą zagrożone koniecznością wycofania z rynku.

Ocena Skutków Regulacji nie bierze pod uwagę jeszcze innych, istotnych kwestii – ewentualnych kosztów i roszczeń związanych z koniecznością wymiany użytkowanych urządzeń, jeśli zgodnie z KSC przedsiębiorcy komunikacji elektronicznej będą zmuszeni je wymienić, a także skutków („czarny PR") opublikowania w Dzienniku Urzędowym informacji Pełnomocnika zawierającej ocenę ryzyka dostawcy sprzętu lub oprogramowania istotnego dla cyberbezpieczeństwa podmiotów krajowego systemu cyberbezpieczeństwa.

Są to koszty i roszczenia na chwilę obecną trudne do przewidzenia i oszacowania z uwagi na to, iż przesłanki, którymi ma się kierować Kolegium są nieobiektywne i nie pozwalają na przewidzenie, jaki dostawca może zostać wykluczony z rynku. Ryzyko to jest jeszcze wyższe, jeśli weźmie się pod uwagę fakt, że zgodnie z treścią obecnie obowiązującej ustawy Kolegium jest organem de facto politycznym, a nie specjalistycznym. **Wykluczenie może zatem objąć teoretycznie każdego dostawcę spoza EOG**. Stawia to przedsiębiorców komunikacji elektronicznej w stanie niepewności. Co więcej, nie wiadomo jakie przedsiębiorcom komunikacji elektronicznej będą przysługiwać roszczenia i przeciwko komu, skoro zgodnie z *kodeksem cywilnym*, przy ocenianiu bezpieczeństwa produktu nie bierze się pod uwagę cech dostawcy (w szczególności tego czy jest to dostawca spoza EOG czy też nie) lecz wyłącznie cechy samego produktu (tj. *niebezpieczny jest produkt niezapewniający bezpieczeństwa, jakiego można oczekiwać, uwzględniając normalne użycie produktu*).

Z kolei opublikowanie w Dzienniku Urzędowym informacji o konkretnym dostawcy sprzętu/oprogramowania może doprowadzić do nieuczciwej walki konkurencyjnej pomiędzy przedsiębiorcami działającymi na tym samym rynku, z których część korzysta ze sprzętu znajdującego się w opublikowanej informacji. Nie trudno wyobrazić sobie sytuację, w której

dojdzie do masowego rezygnowania z usług konkretnego przedsiębiorcy telekomunikacyjnego przez abonentów tylko dlatego, że dojdzie do swoistej stygmatyzacji takiego przedsiębiorcy.

***

Mając na uwadze powyższe, **KIKE rekomenduje:**

1) pozostawienie wyłączenia wskazanego w art. 1 ust. 2 KSC tak, aby objąć wyłączeniem spod nowelizacji przedsiębiorców komunikacji elektronicznej, o których mowa w PKE. W konsekwencji część projektowanych przepisów (w szczególności art. 20a i nast. KSC) powinny zostać całkowicie usunięte. Uregulowanie tej samej materii w dwóch różnych aktach prawnych jest sprzeczne z zasadami legislacji i spowoduje wprowadzenie w błąd adresatów obowiązków. PKE będzie kompleksowo regulować obowiązki przedsiębiorców komunikacji elektronicznej w zakresie zgłaszania incydentów cyberbezpieczeństwa. Nie ma powodu, dla którego obowiązki te powinny być powielone i rozszerzone w osobnym akcie prawnym;

2) zapewnienie przejrzystego postępowania w zakresie art. 66A-66C KSC w oparciu o obiektywne, konkretne i niebudzące wątpliwości kryteria, w szczególności kryteria informatyczno-technologiczne, które powinny być nadrzędne przy podejmowaniu decyzji o wyłączeniu z rynku danego sprzętu;

3) zapewnienie dostawcy sprzętu, którego dotyczy postępowanie, możliwości czynnego udziału w każdym stadium postępowania.

   KIKE proponuje, aby wzorem postępowania przewidzianego w *prawie przedsiębiorców*, postępowanie mogło być przeprowadzone dopiero *po uprzednim dokonaniu analizy prawdopodobieństwa naruszenia prawa w ramach wykonywania działalności gospodarczej* (art. 47 ust. 1 *prawa przedsiębiorców*) oraz aby o zamiarze przeprowadzenia kontroli zawiadomić zainteresowany podmiot (art. 48 ust. 1 *prawa przedsiębiorców*). Umożliwi to podmiotowi zainteresowanemu możliwość wypowiadania się na bieżąco do uwag i spostrzeżeń Kolegium na każdym etapie postępowania i co ważne – zainteresowany podmiot będzie wiedzieć, że poddany zostaje kontroli;

4) zobowiązanie Kolegium do wydania decyzji administracyjnej w przedmiocie uznania danego dostawcy za stwarzającego ryzyko dla cyberbezpieczeństwa – niezależnie od tego, czy ryzyko zostanie ocenione jako wysokie, umiarkowane, czy niskie.

   W każdym przypadku zainteresowany podmiot musi mieć możliwość obrony przed decyzją wywołującą tak dalekoidące skutki, co sprowadza się do rekomendacji opisanej w pkt. 5) poniżej;

5) zapewnienie dwuinstancyjności postępowania, oraz możliwość zaskarżenia decyzji organu dwuinstancyjnego do Sądu Administracyjnego.

   Kolegium nie może być jedynym, nieomylnym organem, którego decyzje nie podlegają kontroli. Regulacja w obecnym kształcie jest sprzeczna z konstytucyjną zasadą dwuinstancyjności postępowania administracyjnego.

6) wprowadzenie procedury, że publikacja ogłoszenia w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski” można następować wyłącznie na podstawie ostatecznej decyzji, a ewentualne zaskarżenie decyzji do sądu administracyjnego wstrzymałoby publikację automatycznie.

Mając na względzie daleko idące skutki rozszerzenia kompetencji Kolegium i Pełnomocnika, KIKE rekomenduje, aby zmienić treść projektowanych przepisów zgodnie z powyższymi rekomendacjami, jako że w obecnej treści są one wysoce szkodliwe, sprzeczne z Dyrektywą i nierealizujące 5G toolbox.

Z poważaniem,

Karol Skupień

Prezes KIKE

Grupa Robocza ds.
Administracji Publicznej KIKE

Łukasz Bazański

Radca prawny

Grupa Robocza ds.
Administracji Publicznej KIKE /
Kancelaria itB Legal

Ewelina Grabiec

Radca prawny

Grupa Robocza ds.
Administracji Publicznej KIKE /
Kancelaria itB Legal

W załączeniu:

- *opracowanie badań ankietowych,*

- *opinia prawna w przedmiocie oceny konstytucyjności projektu ustawy o zmianie ustawy – o krajowym systemie cyberbezpieczeństwa oraz ustawy – prawo zamówień publicznych.*