04.03.2020

**Zestawienie zgłoszonych uwag do projektu rozporządzenia Ministra Cyfryzacji w sprawie minimalnych środków technicznych i organizacyjnych oraz metod, jakie przedsiębiorcy telekomunikacyjni są obowiązani stosować w celu zapewnienia bezpieczeństwa lub integralności sieci lub usług – opiniowanie**

Uwagi zgłoszone przez:

* Urząd Komunikacji Elektronicznej
* Urząd Ochrony Danych Osobowych – nie było przedstawiciela na konferencji uzgodnieniowej
* Urząd Ochrony Konkurencji i Konsumentów – nie było przedstawiciela na konferencji uzgodnieniowej

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Nr uwagi** | **Jednostka redakcyjna projektu** | **Zgłaszający** | **Treść uwagi** | **Stanowisko MC** |
|  | Ogólna | Urząd Komunikacji Elektronicznej | Wbrew deklaracjom zawartym w uzasadnieniu, projektowane rozporządzenie nie precyzuje w wystarczającym stopniu obowiązków ciążących na przedsiębiorcach telekomunikacyjnych. Treść normatywna poszczególnych obowiązków jest trudna do odczytania, w związku z ogólnym i szerokim zakresem znaczeniowym użytych do ich określenia sformułowań (patrz uwagi szczegółowe). Tekst jest w wielu miejscach nieprecyzyjny, a tym samym przenosi kwestię skonkretyzowania obowiązków w sferę interpretacji zarówno podmiotu obowiązanego, jak i regulatora, powodując ryzyko rozbieżności.  W rezultacie rozporządzenie nie dostarcza Prezesowi Urzędu Komunikacji Elektronicznej adekwatnych wzorców kontroli koniecznych dla merytorycznej weryfikacji sposobu realizacji przez przedsiębiorców telekomunikacyjnych nałożonych na nich obowiązków. Kontrole przeprowadzane w oparciu o tak sformułowane przepisy będą miały iluzoryczny charakter. | Do ustalenia na konferencji uzgodnieniowej.  Rozporządzenie powinno uwzględniać różnice w profilach działalności i wykorzystywanych technologiach przez poszczególnych operatorów. Kontrola prowadzona przez UKE także powinna brać pod uwagę ww. różnice.  Na konferencji:  Przedstawiono wyjaśnienie MC.  Po konferencji dokonano zmian w projekcie aby usunąć wątpliwości dotyczące słownictwa użytego do opisu środków. |
|  | Ogólna | Urząd Komunikacji Elektronicznej | Równolegle procedowany jest projekt nowego rozporządzenia z upoważnienia zawartego w art. 176a ust. 5 Prawa telekomunikacyjnego, zwanego dalej „Pt”. Rozporządzenie to, jak i opiniowane rozporządzenie z upoważnienia zawartego w art. 175d Pt, mają wiele wspólnych obszarów, a mimo to regulowane są przez projektodawcę w odmienny sposób i przy użyciu innej siatki pojęciowej. Ten stan rzeczy należy ocenić negatywnie. Konieczne jest zapewnienie spójności przepisów obu projektowanych rozporządzeń. | Wyjaśnienie.  Projekty są procedowane równolegle. Oba rozporządzenia mają różne cele i podstawę prawną. Rozporządzenie 175d korzysta z europejskiej siatki pojęciowej, podczas gdy 176a już nie, bo jest powiązane z przepisami obronnymi. W ocenie MC są to dwie różne materie, jednak w zakresach, gdzie są zbieżne, zostanie uzyskana niezbędna spójność. Prośba do UKE o wskazanie na konferencji uzgodnieniowej potencjalnych obszarów zbieżnych.  Na konferencji:  UKE przyjęło wyjaśnienia. |
|  | Ogólna | Urząd Ochrony Danych Osobowych | Projektowane przepisy określają minimalne środki techniczne i organizacyjne, a także metody jakie obowiązani są stosować przedsiębiorcy telekomunikacyjni dla zapewnienia bezpieczeństwa lub integralności sieci lub usług, a ich stosowanie powinno właściwie korespondować w tej działalności ze stosowaniem przepisów wynikających z rozporządzenia 2016/679.  W szczególności na przedsiębiorcach telekomunikacyjnych spoczywa obowiązek wdrożenia odpowiednich środków technicznych i organizacyjnych, w tym odpowiednich polityk ochrony danych osobowych (art. 24 rozporządzenia 2016/679).  Przedsiębiorcy telekomunikacyjni uwzględniać powinni również ochronę danych w fazie projektowania wszelkich procesów związanych  z przetwarzaniem (art. 25 ust. 1 rozporządzenia 2016/679). A zatem wdrażać powinni odpowiednie środki techniczne i organizacyjne - przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania - zaprojektowane w celu skutecznej realizacji zasad ochrony danych oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń. Wdrażanie takich środków powinno następować z uwzględnieniem stanu wiedzy technicznej, kosztu wdrażania oraz charakteru, zakresu, kontekstu i celów przetwarzania. Działania te powinny być podejmowane również z uwzględnieniem ryzyka naruszenia praw lub wolności osób fizycznych, jego różnego prawdopodobieństwa wystąpienia, jak i różnej wagi zagrożeń wynikających z przetwarzania. Przyjmowanie takich rozwiązań służyć ma spełnianiu wymogów rozporządzenia 2016/679 oraz ochronie praw osób, których dane przetwarzane przez przedsiębiorców telekomunikacyjnych dotyczą Obowiązek uwzględniania ochrony danych powinien być realizowany na każdym etapie funkcjonowania systemów, z których korzystają przedsiębiorcy telekomunikacyjni, tj. w fazie ich projektowania (privacy by design), a także w trakcie ich rozwoju, utrzymania i wygaszania. | Wyjaśnienie.  Przedsiębiorcy telekomunikacyjni są zobowiązani przestrzegać rozporządzenia 2016/679. Jest to niezależne od obowiązków wynikających z ustawy – Prawo telekomunikacyjne.  Na konferencji:  Przedstawiono wyjaśnienie MC. |
|  | Ogólna | Urząd Ochrony Danych Osobowych | Ponadto, przedsiębiorcy telekomunikacyjni świadczący usługi telekomunikacyjne uwzględniać powinni zarówno wymogi norm PN-EN ISO/IEC 27001, PN-EN ISO 22301, określających zasady bezpieczeństwa informacji w organizacji, jak i normy PN-ISO/IEC 29151:2019-01, która określa wytyczne dotyczące wdrożenia zabezpieczeń w celu spełnienia wymagań zidentyfikowanych w trakcie szacowania ryzyka i oceny skutków związanych z ochroną informacji o identyfikowalnych osobach. Ponadto przedsiębiorcy telekomunikacyjni powinni w ocenie organu nadzorczego spełniać wymogi normy ISO/IEC 27002, wyznaczającej wytyczne związane z ustanowieniem, wdrożeniem, eksploatacją, monitorowaniem, przeglądaniem, utrzymaniem i doskonaleniem Systemu Zarządzania Bezpieczeństwem Informacji. Norma ta przeznaczona jest do stosowania przez organizacje, które zamierzają wdrażać zabezpieczenia zgodnie z ISO/IEC 27001. | Wyjaśnienie.  Zgodnie z polskim prawem, stosowanie norm jest dopuszczalne. Uczynienie ich obowiązkowymi jest możliwe jedynie w drodze ustawy.  Możliwe jest za to rozszerzenie uzasadnienia o wskazane elementy jako preferowaną drogę realizacji obowiązków.  Na konferencji:  Przedstawiono wyjaśnienie MC. |
|  | Ogólna | Urząd Ochrony Konkurencji  i Konsumentów | Projekt przewiduje, że przedsiębiorca telekomunikacyjny dostarczający sieć piątej generacji (5G), zobowiązany jest do zapewnienia i stosowana środków minimalizujących skutki wystąpienia zagrożeń, w zakresie bezpieczeństwa i integralności sieci i usług, uwzględniając m.in. podwyższanie odporności na zakłócenia sieci i usług telekomunikacyjnych. Projektodawca jednocześnie nie wskazuje środków osiągnięcia tego celu, mając na uwadze fakt, iż można gdyż można go zrealizować na różne sposoby (np. poprzez redundancję sprzętu czy zapewnienie roamingu krajowego).  Jednocześnie w uzasadnieniu do Projektu, odwołując się do art. 8 ust. 1 ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. z 2019 r. poz. 369, ze zm.)(dalej: u.o.k.k.), wskazano, że wprowadzenie redundantnej konfiguracji sieci „nie naruszy reguł konkurencji”. Projektodawca stwierdza, że zawarcie przez przedsiębiorców porozumienia dotyczącego wprowadzenia redundantnej konfiguracji sieci na podstawie art. 8 ust. 1 u.o.k.k., będzie legalne, o ile spełnione zostaną przesłanki określone w art. 8 u.o.k.k. Jednocześnie w dalszej części uzasadnienia podjęto próbę wykazania, że porozumienie, które ma na celu zapewnienie większego poziomu bezpieczeństwa i zachowania integralności sieci, będzie spełniało określone w ww. przepisie przesłanki.  W istocie, zgodnie z art. 8 ust. 1 u.o.k.k. niektóre porozumienia mogą zostać indywidualnie wyłączone spod zakazu porozumień ograniczających konkurencję. Dotyczy to sytuacji, w których uczestnik naruszenia wykaże, że dane porozumienie jednocześnie:  1. przyczynia się do polepszenia produkcji, dystrybucji lub postępu technicznego, lub gospodarczego,  2. zapewnia nabywcy lub użytkownikowi odpowiednią część wynikających z porozumienia korzyści,  3. nie nakłada na zainteresowanych przedsiębiorców ograniczeń, które nie są niezbędne do osiągnięcia tych celów,  4. nie stwarza tym przedsiębiorcom możliwości wyeliminowania konkurencji na rynku właściwym w zakresie znacznej części określonych towarów.  Wyłączenie indywidualne opiera się na założeniu, że porozumienie, pomimo że z formalnego punktu widzenia jest antykonkurencyjne i powinno być zakazane, może wywoływać prokonkurencyjne skutki (jest korzystne dla rynku). Negatywne skutki takiego porozumienia muszą być równoważone przez korzyści płynące z jego zawarcia.  Zwolnienie w takim wypadku, rzeczywiście następuje z mocy prawa,  a orzeczenie sądowe lub administracyjne, w którym dokonane zostanie stwierdzenie zastosowania art. 8 ust. 1 do danego porozumienia, ma charakter deklaratoryjny . Pragniemy jednak wyjaśnić, że ocena spełnienia przesłanek, dokonywana jest indywidualnie w wypadku danego porozumienia. Ponadto podkreślamy, że w wypadku dokonywania weryfikacji spełnienia warunków zwolnienia w ramach postępowania wyjaśniającego lub antymonopolowego prowadzonego przez Prezesa UOKiK wykazanie prokonkurencyjnych skutków porozumienia spoczywa na przedsiębiorcy (art. 8 ust. 2 u.o.k.k).  Mając na uwadze powyższe wyjaśnienia, zwracamy uwagę, że zawarte  w uzasadnieniu do przedmiotowego Projektu stwierdzenie, iż należy przyjąć, że wskazany rodzaj porozumień nie będzie naruszał reguł konkurencji, może wprowadzać uczestników wskazanych rynków w błąd co do ich sytuacji prawnej. Jak słusznie wskazuje projektodawca, w wypadku spełnienia określonych przesłanek, porozumienie będzie legalne. Jednak weryfikacja tej okoliczności jest przeprowadzana indywidualnie dla danego, potencjalnie antykonkurencyjnego porozumienia.  W tym miejscu zwracamy uwagę, że zgodnie z art. 8 ust. 3 u.o.k.k. Rada Ministrów jest upoważniona, by biorąc pod uwagę korzyści, jakie mogą przynieść określone rodzaje porozumień, dokonać wyłączenia spod zakazu określonego w art. 6 u.o.k.k. takich rodzajów porozumień, które w ocenie ustawodawcy, spełniają przesłanki, o których mowa w art. 8 ust. 1 u.o.k.k. Takie wyłączenie, nazywane „grupowym”, dokonywane jest w drodze rozporządzenia. Tego rodzaju zwolnienie wprowadza domniemanie legalności i ważności porozumień objętych zakresem zastosowania danego rozporządzenia. W takim wypadku jeżeli porozumienie spełnia przesłanki określone w akcie wykonawczym, nie ma konieczności każdorazowego badania, czy istnieją przesłanki do wyłączenia indywidualnego.  Ponadto wskazujemy, że art. 8 ust. 1 u.o.k.k. znajduje zastosowanie jedynie do porozumień ograniczających konkurencję w rozumieniu w art. 6 ust. 1 u.o.k.k. Zgodnie z tym przepisem dotyczy to podejmowania przez niezależnych przedsiębiorców jakichkolwiek uzgodnień, których celem lub skutkiem jest eliminowanie, ograniczenie lub zniekształcenie konkurencji, polegające w szczególności na:  1. ustalaniu, bezpośrednio lub pośrednio, cen i innych warunków zakupu lub sprzedaży towarów;  2. ograniczaniu lub kontrolowaniu produkcji lub zbytu oraz postępu technicznego lub inwestycji;  3. podziale rynków zbytu lub zakupu;  4. stosowaniu w podobnych umowach z osobami trzecimi uciążliwych lub niejednolitych warunków umów, stwarzających tym osobom zróżnicowane warunki konkurencji;  5. uzależnianiu zawarcia umowy od przyjęcia lub spełnienia przez drugą stronę innego świadczenia, niemającego rzeczowego ani zwyczajowego związku z przedmiotem umowy;  6. ograniczaniu dostępu do rynku lub eliminowaniu z rynku przedsiębiorców nieobjętych porozumieniem;  7. uzgadnianiu przez przedsiębiorców przystępujących do przetargu lub przez tych przedsiębiorców i przedsiębiorcę będącego organizatorem przetargu warunków składanych ofert, w szczególności zakresu prac lub ceny.  Należy zatem rozważyć czy uzgodnienia dotyczące redundantnej konfiguracji sieci faktycznie będą zawierały elementy pozwalające uznać je za porozumienia ograniczające konkurencję w rozumieniu u.o.k.k. | Wyjaśnienie.  Nie jest planowane zastosowanie wyłączenia grupowego – każdy przypadek będzie musiał być analizowany indywidualnie przez przedsiębiorcę w zależności od posiadanej infrastruktury, zasięgu działania, rodzaju świadczonych usług i sytuacji na rynku.  Na konferencji:  Uzgodniono, że uzasadnienie w tym zakresie zostanie uzupełnione. |
|  | § 2 pkt 2 | Urząd Komunikacji Elektronicznej | § 2 pkt 2 – pojęcie „wykaz infrastruktury” wymaga doprecyzowania. Proponuję ograniczyć ten wykaz do urządzeń mających istotny wpływ na funkcjonowanie sieci i usług telekomunikacyjnych. Ponadto nie wiadomo, czego dotyczy określenie „rodzaj i konfigurację” | Uwaga nieuwzględniona.  Nie istnieje definicja urządzeń mających istotny wpływ na funkcjonowanie sieci i usług telekomunikacyjnych. Wykazy mogą wtedy w istotny sposób się między sobą różnić.  Po konferencji:  Przygotowano nowe brzmienie przepisu, odnoszące się do wykazu, który będzie zawierał kluczową infrastrukturę. |
|  | § 2 pkt 3 | Urząd Komunikacji Elektronicznej | § 2 pkt 3 – w przepisie odwołano się wyłącznie do dokumentu na poziomie europejskim publikowanego przez ENISA, z pominięciem publikacji i raportów przygotowywanych przez podmioty spełniające kluczowe role w krajowym systemie cyberbezpieczeństwa. Ponadto należy doprecyzować, o jakie „zagrożenia” chodzi w przepisie. | Wyjaśnienie.  W ocenie MC dokument jest wyczerpujący i nie ma potrzeby powoływać się na inne publikacje. Należy dodatkowo wskazać, że zgodnie z wytyczą, zawartą w upoważnieniu ustawowym należy opierać się przede wszystkim na publikacjach ENISA.  Na konferencji:  Na wniosek Lewiatana i PIIT usunięto odniesienie do dokumentów ENISA. Zostanie rozszerzone uzasadnienie w tym zakresie. |
|  | § 2 pkt 5 | Urząd Komunikacji Elektronicznej | § 2 pkt 5 – redakcja tego punktu sprowadzająca się do określenia, że „minimalnym środkiem technicznym lub organizacyjnym” (o którym mowa w §1) stosowanym przez przedsiębiorcę jest „zapewnienie środków minimalizujących” jest nielogiczna i nie zawiera żadnej treści normatywnej | Uwaga uwzględniona.  Propozycja nowego zapisu: „minimalizuje skutki wystąpienia oddziaływań zagrożeń, o których mowa w pkt 3”.  Na konferencji:  Postanowiono o połączeniu pkt 5 i 6 („przygotowuje i stosuje”). |
|  | § 2 pkt 6 | Urząd Komunikacji Elektronicznej | § 2 pkt 6 – przepis zawiera wymóg stosowania środków minimalizujących skutki zagrożeń, co jest już przedmiotem regulacji przepisu ustawowego (art. 175c ust. 1 Pt) | Wyjaśnienie.  Zagrożeń określonych w art. 175c PT nie należy utożsamiać z zagrożeniami, które zostały zidentyfikowane przez przedsiębiorcę zgodnie z § 2 pkt 3.  Przepis § 2 pkt 3 odnosi się do typowych zagrożeń dla działalności telekomunikacyjnej, podczas gdy w art. 175c PT bardzo konkretnie chodzi o przekazy komunikatów oraz świadczenia usługi telekomunikacyjnej na zakończeniu sieci, z którego następuje wysyłanie komunikatów zagrażających bezpieczeństwu sieci lub usług.  Na konferencji:  Postanowiono o połączeniu pkt 5 i 6 („przygotowuje i stosuje”). |
|  | § 2 pkt 7 | Urząd Komunikacji Elektronicznej | § 2 pkt 7 – należy doprecyzować, kogo mają dotyczyć zasady i procedury dostępu, o których mowa w przepisie. Niejasne jest pojęcie „kluczowe zasoby systemowe”. Nie wiadomo również, do czego odnoszą się użyte w przepisie wyrazy „obejmujących” oraz „mających” | Uwaga częściowo uwzględniona.  Wskazanie kluczowych zasobów systemowych należy do decyzji przedsiębiorcy.  Zgodnie z wyjaśnieniami przedsiębiorców przekazywanymi podczas warsztatów w ramach prekonsultacji, kluczowe zasoby systemowe mogą się znacząco różnić w zależności od modelu sieci. Będą zatem wskazywane przez przedsiębiorców indywidualnie.  Wyrazy „obejmujących” oraz „mających” odnoszą się do zasad i procedur, a ich forma zostanie poprawiona.  Na konferencji:  Przedstawiono wyjaśnienie MC. |
|  | § 2 pkt 7-8 | Urząd Komunikacji Elektronicznej | § 2 pkt 7-8 – zastosowane pojęcie „kluczowe zasoby infrastruktury” jest niejasne, zwłaszcza w zestawieniu z zastosowanym w pkt 7 pojęciem „kluczowych zasobów systemowych” – czy chodzi tu o te same zasoby? Dodatkowo w pkt 8 brakuje wskazania, o czyim dostępie jest mowa w przepisie | Uwaga częściowo uwzględniona.  Przepisy zostaną doprecyzowane – termin zostanie ujednolicony przez wskazanie „kluczowych zasobów infrastruktury”.  Po konferencji:  Nadano nowe brzmienie § 2 pkt 2, w którym zastosowano skrót „kluczowa infrastruktura” oraz ujednolicono terminologię w całym projekcie. |
|  | § 2 pkt 9 | Urząd Komunikacji Elektronicznej | § 2 pkt 9 – niejasne jest, jakie dane miałyby być objęte przepisem (wszystkie, osobowe, transmisyjne, objęte tajemnicą telekomunikacyjną?) | Wyjaśnienie.  Wszystkie. Poziom bezpieczeństwa zależy od rodzaju danych – tajemnicę przedsiębiorstwa chroni się inaczej niż dane osobowe.  Tu istotny jest element przetwarzania zdalnego – należy minimalizować ilość przechowywanych lokalnie danych etc.  Na konferencji:  Przyjęto nowe brzmienie przepisu („…zasady bezpiecznego przetwarzania…”). |
|  | § 2 pkt 10 | Urząd Komunikacji Elektronicznej | § 2 pkt 10 – podobnie jak w przypadku pkt 9 niejasne jest, o jakie dane chodzi w przepisie. Ponadto sformułowanie „znacząco redukujący” jest w wysokim stopniu ocenne, a tym samym niemożliwe do jednoznacznej weryfikacji w toku kontroli, | Uwaga uwzględniona.  Przeformułowano nadając brzmienie:  „10) stosuje, wynikające z oceny prawdopodobieństwa wystąpienia oddziaływania zagrożeń, środki zabezpieczające dla poszczególnych kategorii danych”. |
|  | § 2 pkt 12 | Urząd Komunikacji Elektronicznej | § 2 pkt 12 – zapis niezrozumiały ze względu na niewłaściwą formę wyrazu „mających” | Uwaga uwzględniona. |
|  | § 2 pkt 13 | Urząd Komunikacji Elektronicznej | § 2 pkt 13 – sformułowanie „procedury umożliwiające zgłaszanie naruszeń” jest niespójne z ustawą, bowiem przepis art. 175a ust. 1 Pt stanowi o obowiązku, a nie uprawnieniu do zgłaszania takich naruszeń. W projektowanym przepisie powinna być mowa o procedurach wewnętrznych przedsiębiorcy telekomunikacyjnego mających na celu niezwłoczne i wiarygodne przekazywanie informacji Prezesowi Urzędu Komunikacji Elektronicznej. Przedsiębiorca powinien również ustalić procedurę zgłaszania naruszeń przez abonentów lub odbiorców – jako jeden z minimalnych środków lub metod zapobiegania zagrożeniom | Uwaga uwzględniona.  Przepis zostanie zmieniony tak, aby było jasne, że zgłaszanie incydentów jest obligatoryjne.  Na konferencji:  przyjęto propozycję brzmienia przepisu: „ustala wewnętrzne procedury zgłaszania naruszeń bezpieczeństwa”. |
|  | § 3 | Urząd Komunikacji Elektronicznej | W projektowanym § 3 zawarto określenie obowiązków dla przedsiębiorców telekomunikacyjnych dostarczających sieć piątej generacji. Taka norma prawna pozostaje w niejasnej relacji do obowiązków określonych w § 2. Nie wiadomo bowiem, czy obowiązki z § 3 mają być stosowane zamiast obowiązków z § 2, czy łącznie z nimi, tym bardziej że zawarte we wprowadzeniu do § 3 ust. 1 sformułowanie „identyfikuje zagrożenia, ocenia prawdopodobieństwo ich wystąpienia, zapewnia i stosuje środki minimalizujące skutki wystąpienia zagrożeń” stanowi właściwie częściowe powtórzenie przepisów odpowiednio  § 2 pkt 3 – 6 | Wyjaśnienie.  Obowiązki z § 2 i § 3 mają być stosowane łącznie. Różnica jest w wykorzystywanej technologii.  Częściowe powtórzenie przepisów zastosowano, aby obowiązki były jasne.  Przepis § 3 zostanie doprecyzowany w ten sposób, aby jasno wynikało, że przedsiębiorcy dostarczający sieć 5G mają obowiązek stosować zarówno § 2 jak i § 3.  Na konferencji:  Przedstawiono wyjaśnienie MC.  MC przygotowało nowe brzmienie przepisu, który będzie przedmiotem posiedzenia komisji prawniczej. |
|  | § 3 ust. 1 | Urząd Komunikacji Elektronicznej | Zawarte w § 3 ust. 1, w ramach określenia sieci piątej generacji, odesłanie do dokumentu technicznego - Raportu ETSI TR 121 915 V.15.0.0. (2019-10) jest niezgodne z § 4 ust. 3 w związku z § 132 Zasad Techniki Prawodawczej.  Co więcej, odwołanie do określenia zawartego w ww. Raporcie jest zbyt ogólne (zakres Raportu jest zwykle szerszy niż norma ETSI opracowywana na jego podstawie) i jako takie może powodować problemy ze stosowaniem tego przepisu w praktyce. Dodatkowo w razie ewentualnego wprowadzenia kolejnej wersji raportu w przedmiotowym zakresie nie będzie jasne, która wersja raportu powinna być stosowana | Wyjaśnienie.  Odesłanie do dokumentu technicznego jest zabiegiem dopuszczalnym w praktyce polskiej legislacji.  Został zastosowany m.in. w rozporządzeniu Rady Ministrów z dnia 28 grudnia 2015 r. w sprawie organizacji i funkcjonowania systemu gromadzącego i udostępniającego informacje i dane od przedsiębiorcy telekomunikacyjnego (Dz. U. poz. 2333), rozporządzeniu Ministra Cyfryzacji z dnia 5 października 2016 r. w sprawie krajowej infrastruktury zaufania (Dz. U. poz. 1632) czy też rozporządzeniu Ministra Cyfryzacji z dnia 5 października 2016 r. w sprawie szczegółowych warunków organizacyjnych i technicznych, które powinien spełniać system teleinformatyczny służący do uwierzytelniania użytkowników (Dz. U. poz. 1627).  Na konferencji:  Przyjęto propozycję PKN: „Raporcie ETSI TR 121 915 V.15.0.0. (2019-10) lub dokumencie go zastępującym” |
|  | § 3 ust. 1 pkt 1 | Urząd Komunikacji Elektronicznej | Odesłanie w § 3 ust. 1 pkt 1 do rekomendacji, o której mowa w art. 33 ust. 4 ustawy z dnia 5 lipca 2018 r. krajowym systemie cyberbezpieczeństwa, zwanej dalej „UKSC”, jest nieuprawnione. Łączy ono dwa reżimy prawne, które ustawodawca celowo uczynił odrębnymi, tj. reżimu wymogów dotyczących bezpieczeństwa oraz integralności sieci i usług, wynikającego dla przedsiębiorców telekomunikacyjnych z Pt (art. 175 – art. 175e Pt; implementacja dyrektywy ramowej) oraz reżimu odnoszącego się do systemu bezpieczeństwa oraz zgłaszania incydentów, zawartego w UKSC (implementacja tzw. dyrektywy NIS), z której to ustawy (w nawiązaniu do dyrektywy NIS) wprost wynika wyłączenie przedsiębiorców telekomunikacyjnych spod jej stosowania (art. 1 ust. 2 pkt 1 UKSC). Odesłanie przedsiębiorców telekomunikacyjnych do ww. rekomendacji, wydawanych na podstawie UKSC, celem ich stosowania w procesie zarządzania ryzykiem prowadzonym w reżimie Pt jest zatem niewłaściwe | Wyjaśnienie.  Wyłączenie przedsiębiorców telekomunikacyjnych spod ustawy o KSC nie jest zupełne – odnosi się tylko do wymogów bezpieczeństwa i zgłaszania incydentów określonych w tej ustawie. Jest możliwe odniesienie się do rekomendacji jako jednego z elementów, który ma być brany pod uwagę w trakcie szacowania ryzyka u danego przedsiębiorcy.  Na konferencji:  Przedstawiono wyjaśnienie MC.  MC przygotowało nowe brzmienie przepisu, który będzie przedmiotem posiedzenia komisji prawniczej. |
|  | § 3 ust. 1 pkt 2 | Urząd Komunikacji Elektronicznej | Zawarty w § 3 ust. 1 pkt 2 zapis „unikanie uzależnienia od jednego producenta poszczególnych elementów sieci telekomunikacyjnej przy jednoczesnym zapewnieniu interoperacyjności usług oraz wykorzystaniu najnowocześniejszych osiągnięć technicznych” nie zawiera jednoznacznej treści normatywnej - czy chodzi tu de facto o nałożenie obowiązków zapewniania interoperacyjności usług oraz wykorzystania najnowocześniejszych osiągnięć technicznych? Jaka jest relacja tych wymogów do zakresu delegacji ustawowej? | Uwaga częściowo uwzględniona.  Usunięto wyrazy „z uwzględnieniem najnowocześniejszych osiągnięć technicznych”.  Odnosząc się do drugiej części uwagi - nie jest to nałożenie nowego obowiązku, tylko doprecyzowanie istniejącego.  Na konferencji:  Przedstawiono wyjaśnienie MC. |
|  | § 3 ust. 1 pkt 3 | Urząd Komunikacji Elektronicznej | Użyte w § 3 ust. 1 pkt 3 pojęcie „podwyższanie odporności na zakłócenia” jest praktycznie tożsame z zastosowaniem wszystkich pozostałych środków w celu zapewnienia bezpieczeństwa. Należy wykreślić tak sformułowany zapis jako niewnoszący żadnej dodatkowej treści normatywnej | Uwaga nieuwzględniona.  Zapis wskazuje element, którym ma się kierować przedsiębiorca telekomunikacyjny podczas szacowania ryzyka.  Na konferencji:  Przedstawiono wyjaśnienie MC. |
|  | § 3 ust. 1 | Urząd Komunikacji Elektronicznej | Zawarty w § 3 ust. 1 wymóg jedynie „uwzględniania”, przy realizacji obowiązków zawartych w tym przepisie, odpowiednich rekomendacji, unikania uzależniania i podwyższania odporności pozostawia przedsiębiorcom znaczny margines swobody w zakresie stopnia uwzględnienia wskazanych w pkt 1 – 3 wytycznych, trudny do weryfikacji w procesie kontroli. Nie kwestionując potrzeby miękkiego sformułowania obowiązków na obecnym etapie rozwoju sieci 5G, należałoby przynajmniej wspomniane wytyczne sformułować w bardziej jednoznaczny sposób, a także wymagać od przedsiębiorców zawarcia w dokumentacji, o której mowa w § 3 ust. 2, uzasadnienia dla sposobu czy stopnia, w jakim te wytyczne zostały uwzględnione. Dotyczy to zwłaszcza zawartego w § 3 ust. 1 pkt 2 wymogu „unikania uzależnienia od jednego producenta poszczególnych elementów sieci telekomunikacyjnej”, który powinien być określony jednoznacznie z jednoczesnym wskazaniem, w jakich przypadkach możliwe jest odstąpienie od jego stosowania, np. tylko wówczas, gdy zastosowanie urządzeń różnych dostawców jest wykluczone z uwagi na brak ich kompatybilności, brak możliwości współpracy lub też wyklucza współpracę pomiędzy przedsiębiorcami telekomunikacyjnymi przy dostarczaniu sieci/świadczeniu usług. | Uwaga uwzględniona.  Propozycja zapisu uwzględniająca niniejszą uwagę zostanie wypracowana podczas konferencji uzgodnieniowej.  Na konferencji.  Wskazanie jako obowiązkowego jedynie „uwzględniania” m.in. odpowiednich rekomendacji jest celowym zabiegiem – nie jest planowane nałożenie nowego obowiązku, jedynie wskazanie koniecznych środków. |