**15.05.2020**

**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**

**III TURA KONSULTACJI – konferencja uzgodnieniowa**

Uwagi zgłoszone przez:

1. Business Centre Club (BCC) – nie było przedstawiciela na konferencji uzgodnieniowej
2. Fundacja Digital Poland
3. Izba Rzeczoznawców Polskiego Towarzystwa Informatycznego (PTI)
4. Konfederacja Lewiatan (KL)
5. Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji (KIGEIT)
6. Krajowa Izba Komunikacji Ethernetowej (KIKE) – nie było przedstawiciela na konferencji uzgodnieniowej
7. Nokia Solutions and Networks Sp. Z.o.o (Nokia)
8. Polska Izba Komunikacji Elektronicznej (PIKE)
9. Polska Izba Informatyki i Telekomunikacji (PIIT)
10. Związek Cyfrowa Polska
11. Związek Przedsiębiorców i Pracodawców (ZPP) – nie było przedstawiciela na konferencji uzgodnieniowej

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **L.p.** | **Jednostka redakcyjna projektu** | **Podmiot zgłaszający uwagę** | **Treść uwagi** | **Stanowisko MC** |
|  | Ogólne | BCC | Przede wszystkim sygnalizujemy, że z uwagą obserwujemy dyskusję dotyczącą wdrażania sieci 5G w Polsce. Jej **szybkie i sprawne uruchomienie postrzegamy za istotny impuls, który może w znaczącym stopniu wspierać rozwój nowych modeli biznesowych, a tym samym całego sektora przedsiębiorstw**. Szczególnie teraz, gdy gospodarka jest w stanie kryzysu, związanego z Covid-19 dostrzegamy znaczenie dostępności szybkiej i niezawodnej łączności. Jednocześnie, tempo rozwoju sieci 5G może okazać się jednym z istotnych czynników wspierających odbudowę potencjału gospodarczego Polski, również w ujęciu konkurencji z krajami naszego regionu i UE. Dlatego w naszej ocenie **priorytetowe powinny być działania polskiej administracji, które stworzą odpowiednie warunki dla szybkiego wdrożenia i rozwoju sieci 5G**.  W tym kontekście naszą uwagę zwraca procedowane obecnie rozporządzenie, w którego kolejnych wersjach modyfikowane i zaostrzane są warunki, jakie mieliby spełniać przedsiębiorcy uruchamiający w Polsce sieci mobilne kolejnej generacji. W naszej ocenie **skutkują one zwiększeniem niepewności inwestycyjnej, a tym samym mogą skutkować opóźnieniem realizacji inwestycji lub ograniczeniem ich skali**.  Biorąc powyższe pod uwagę, **zwracamy się z prośbą o możliwość przeprowadzenia dogłębnej debaty, której celem byłoby ustalenie i przyjęcie rozwiązań docelowych dot. bezpieczeństwa sieci 5G**, które zapewnią ich szybkie wdrożenie, szczególnie poprzez stabilne otoczenie prawne dla inwestycji oraz pełne uwzględnienie łańcucha interesariuszy bezpieczeństwa sieci, w tym także podmiotów będących dostawcami urządzeń i usług dla sieci 5G. | Wyjaśnienie.  Niniejszy projekt jest procedowany od ponad pół roku. Obecnie trwa trzecia tura konsultacji. W ramach prekonsultacji odbyły się warsztaty na temat wybranych zapisów z operatorami telekomunikacyjnymi i UKE.  Rozwiązania w tym zakresie i propozycje przepisów są analizowane i modyfikowane w wyniku prowadzonych uzgodnień, opiniowania i konsultacji publicznych przedmiotowego projektu.  Na konferencji:  Przedstawiono wyjaśnienie MC. |
|  | Ogólne | Fundacja Digital Poland | **Żadne państwo nie powinno zmuszać operatorów do stosowania konkretnego rozwiązania, gdyż to łamie fundamentalną zasadę wolności gospodarczej, a w konsekwencji podwyższa cena zakupu urządzeń co przekłada się na wyższe ceny usług telekomunikacyjnych oferowanych konsumentom i firmom przez operatorów**. To operatorzy powinni określać urządzenia jakie kupują w drodze postępowań zakupowych dbając przy tym o m.in. bezpieczeństwo sieci. Pragnę przy tym podkreślić, że **sieć 5G jest najbezpieczniejszym standardem sieci komórkowej jaki do tej pory powstał**. Sieć 5G jest wręcz **zbyt bezpieczna**, gdyż chociażby Europol szuka sposobów na jej złamanie. Więcej informacji: <https://www.gov.pl/web/5g/przeczytaj-siec-5g-jest-zbyt-bezpieczna-europol-szuka-sposobow-na-jej-zlamanie>.  Operatorzy są doskonale świadomi sytuacji, w której większość elementów RAN dostarczana jest przez kilku wiodących dostawców takich jak Ericsson, Huawei, Nokia czy ZTE. Właśnie dlatego połączono zachodnie (xRan) i azjatyckie (cRan) inicjatywy tworząc kilka lat temu operatorską inicjatywę O-RAN. Inicjatywę powołało do życia pięciu operatorów: amerykański AT&T, francuski Orange, niemiecki DT, japoński NTT Docomo i chiński China Mobile. Obecnie O-Ran tworzy ponad 110 podmiotów w tym 21 operatorów z całego świata. **Open Ran znajduje się jednak ciągle w pierwszej niedoskonałej fazie rozwoju** w zakresie sieci 5G. Pierwsze wdrożenia trwają w Japonii (np. japoński operator Rakuten, czy ostatnio amerykański Dish), a kolejne grupy telekomów potwierdzają gotowość pilotaży (np. Vodafone, Telefonia, O2, Etisalat). W pierwszych wdrożeniach Open Ran pierwsze skrzypce mają obecnie firmy z Izraela i Stanów Zjednoczonych. **Grupa Deutsche Telekom w 2020 stwierdziła, że każdy kolejny przetarg na sieci 5G będzie uwzględniał otwarte interfejsy radiowe co ma pobudzić innowacje w sektorze**. Kolejne podmioty tworzą centra testów Open RAN (np. DT w Berlinie, czy Cisco w US), **jednakże ciągle rozwiązania te nie są gotowe do masowe wdrożenia**.  Analitycy z amerykańskiego Wall Street, prezesi firm telekomunikacyjnych (np. Orange), najwięksi dostawcy (np. Nokia) jasno komunikują: **Open Ran nie jest gotowy do masowego wdrożenia 5G**. Na pewno jest to jednak obiecujący kierunek, który będzie rozwijany przez cały ekosystem innowatorów. Jest to bowiem w interesie operatorów telekomunikacyjnych, a obecnie w Senacie i Izbie Reprezentantów USA procesowane są projekty mające na celu udzielenia grantów wspierających rozwój Open Ran. | Wyjaśnienie.  Bezpieczeństwo informacji składa się z trzech aspektów (integralności, poufności i dostępności).  “Bezpieczeństwo” o którym mowa w tej uwadze to wyłącznie ochrona poufności. Fakt, że komunikacja jest poufna (trudna do odczytania, trudna do rozszyfrowania) nie oznacza, że jest dostępna (co ma krytyczne znaczenie dla niektórych usług).  Należy wskazać, że **sieć 5G nie jest jeszcze ustandaryzowana.** Dopiero trwają nad tym prace. Stąd powoływanie się, że jest to bezpieczny standard, nie jest precyzyjną tezą.  Ministerstwo Cyfryzacji nie zmusza przedsiębiorców do stosowania jakiegokolwiek rozwiązania ani ograniczania swobody działalności gospodarczej.  Na konferencji:  Przedstawiciel Fundacji przyjął wyjaśnienia MC. |
|  | Ogólna | ZPP | Zgodnie z rekomendacjami zawartymi w opublikowanym ostatnio raporcie pt. „Wdrożenie 5G w Polsce – szanse i perspektywy”, Związek Przedsiębiorców i Pracodawców opowiada się za możliwie jak najszybszym wdrożeniem standardu 5G, przy jednoczesnym zachowaniu warunków konkurencji oraz ścisłych standardów bezpieczeństwa. Przedstawiony projekt rozporządzenia odnosi się do tej ostatniej kwestii – w uzasadnieniu wprost podkreśla się, że „rozwój w telekomunikacji nowych technologii wrażliwych na naruszenia bezpieczeństwa (incydenty) wskazuje na potrzebę określenia minimalnych środków technicznych i organizacyjnych w celu zapewnienia bezpieczeństwa sieci, świadczonych usług oraz przetwarzania danych”. Podzielając tezę o konieczności zapewnienia bezpieczeństwa sieci 5G, pragniemy jednocześnie zwrócić uwagę na kilka aspektów przedstawionego projektu, generujących potencjalną niepewność po stronie operatorów i dostawców infrastruktury. | Wyjaśnienie.  Ministerstwo Cyfryzacji aktywnie działa na rzecz opracowania i wdrożenia standardów 5G.  Zauważyć należy, że w ramach Grupy Roboczej NIS w Zespole ds. 5G trwają obecnie prace nad przyjęciem wspólnego europejskiego podejścia dotyczącego standaryzacji i certyfikacji sieci 5G.  Na konferencji:  Przedstawiono wyjaśnienie MC. |
|  | Ogólna | ZPP | Tytułem wstępu należy zaznaczyć, że rozpoczęła się już aukcja częstotliwości niezbędnych do świadczenia usług w technologii 5G. Tym samym, przedmiotowy projekt rozporządzenia, w istotnym stopniu wpływający na zasady projektowania i budowy sieci, pojawił się w trakcie trwania aukcji, po tym jak oferty wstępne mogli złożyć pierwsi oferenci. Wydaje się, że z punktu widzenia zasady pewności prawa kolejność winna być odwrotna, tj. uczestnicy aukcji powinni brać w niej udział z pełną świadomością wymogów i standardów, których spełnienie będzie konieczne przy projektowaniu i budowie sieci 5. Generacji. | Wyjaśnienie.  Niniejsze rozporządzenie jest odrębne od kwestii aukcji. Zauważyć należy, że obowiązek zabezpieczania sieci wynika z normy ustawowej, którą niniejsze rozporządzenie tylko wykonuje.  Projekt nie nakłada dalej idących środków niż te, które opisano w dokumentach technicznych i uznanych międzynarodowo za dobre praktyki.  Na konferencji:  Przedstawiono wyjaśnienie MC. |
|  | Ogólne | KIKE | Przede wszystkim KIKE podtrzymuje swoje stanowisko z marca 2020 r. w zakresie konieczności ograniczenia wymaganych środków bezpieczeństwa do niezbędnego minimum, z uwzględnieniem faktu, że jego zapisy będą dotyczyć wszystkich przedsiębiorców telekomunikacyjnych, w tym mikro, małych i średnich. Tymczasem fakt, ten niestety jest pomijany w pracach legislacyjnych nad tym rozporządzeniem. Już w marcowym stanowisku KIKE wskazała, że tylko część tych środków można określić jako minimalny wymów, a stosowanie pozostałych wskazanych w projekcie środków powinna być stosowana przez operatorów dobrowolnie, na zasadzie decyzji biznesowej, lub powinna zostać określona jako minimalne środki dla nie MŚP.  Wprowadzenie w rozporządzenia rozróżnienia obowiązujących minimalnych środków bezpieczeństwa w zależności od wielkości przedsiębiorcy telekomunikacyjnego jest wręcz konieczne z uwagi na przepisy ustawy Prawo przedsiębiorców. Nałożenie na MŚP pełnego zestawy środków bezpieczeństwa (a nie minimalnego) jest w istocie działaniem nieproporcjonalnym i nieuzasadnionym z punktu widzenia bezpieczeństwa. Ponownie zwracamy uwagę na art. 66 i 67 ustawy Prawo przedsiębiorców, zgodnie z którymi należy zmniejszać obciążenia obowiązkami nakładanymi na mikroprzedsiębiorców oraz małych przedsiębiorców, zwłaszcza w sferze obowiązków informacyjnych takich jak w projekcie rozporządzenia.  Tymczasem zgodnie ze stanowiskiem Rządu do Komisji Europejskiej z 31 marca 2020 r. w sprawie bezpiecznego wprowadzania sieci 5G w UE - wdrażanie unijnego zestawu narzędzi, projektowane rozporządzenie ma tak dużą ilość wymaganych środków bezpieczeństwa właśnie z powodu sieci 5G. KIKE protestuje przeciwko ujednoliceniu wymaganych (wcale nie minimalnych) środków bezpieczeństwa dla wszystkich przedsiębiorców telekomunikacyjnych tylko ze względu na przyszły rozwój sieci 5G dużych operatorów sieci mobilnych. | Uwaga nieuwzględniona.  Jak wspomniano w poprzednich turach konsultacji, nie jest możliwe rozróżnienie w obecnym stanie prawnym różnych wymogów bezpieczeństwa. Uniemożliwia to upoważnienie do wydania rozporządzenia.  Środki określone w rozporządzeniu dotykają różnych technologii i usług w różnych rodzajach podmiotów (od MŚP do międzynarodowych koncernów).  Punktem wyjścia będzie przeprowadzone szacowanie ryzyka. To od zidentyfikowanych zagrożeń będzie wynikać konieczny poziom wprowadzonych zabezpieczeń.  Na konferencji:  Przedstawiono wyjaśnienie MC. |
|  | Ogólne | Nokia | W nawiązaniu do naszego workshopu oraz do prowadzonych obecnie konsultacji chciałbym podzielić się uwagami, które pojawiły się podczas przygotowywania odpowiedzi w ramach konsultacji w Izbach Przemysłowych. Dotyczy to przede wszystkim kwestii dywersyfikacji dostawców. Tu Wielka Brytania przedstawiana jest jako wzór do naśladowania. Stanowisko to należy jednak właściwie zrozumieć w kontekście oceny i ograniczenia udziału dostawców wysokiego ryzyka.  Rząd w Wielkiej Brytanii przeprowadził ocenę dostawców pod kątem ryzyka. Określono tam jednocześnie odgórnie ograniczenie udziału w rynku podmiotu wysokiego ryzyka a nie dostawców ogólnie jak niektórzy błędnie to interpretują. Rząd wprowadził następujące ograniczenia: dopuszczony jest tylko jeden dostawca wysokiego ryzyka (dlatego „inny” dostawca wysokiego ryzyka został automatycznie wykluczony). Dostawca wysokiego ryzyka nie może dostarczać sieci core’owej a w dostępie nie może dostarczać sprzętu, gdy w pobliżu jest infrastruktura krytyczna i tylko do maksymalnego udziału w rynku w wysokości 35%, przy czym planowane są dalsze ograniczenia. Odzwierciedlają one zdolność brytyjskiego NCSC (a właściwie ocenę zdolności) do zarządzania ryzykiem i odnoszą się do istniejących sieci. Wprowadzenie analogicznej oceny możliwości ograniczenia ryzyka i dostosowania do zdolności kraju określałyby pułap udziału w rynku dostawcy wysokiego ryzyka w Polsce.  Z tego co się orientuję w Wielkiej Brytanii wiele osób skłania także się do sugestii, że w przyszłych sieciach udział dostawcy wysokiego ryzyka musi być ograniczony do zera szczególnie, że wyraźne podziały między core a dostępem zaczynają się zacierać (Mobile Edge Computing, Cloud RAN).  Więcej informacji na ten temat podejścia w UK w Q&A brytyjskiego NCSC: https://www.ncsc.gov.uk/information/hrv-faq oraz załączonych dokumentach.  Na marginesie jeszcze komentarz dotyczący Strategic Measures: SM05, i jej stosowania w kontekście SM03. Zgodnie z celem i uzasadnieniem toolboxa, różnorodność dostawców i strategie dotyczące wielu dostawców mają być stosowane tam, gdzie zwiększają ogólny poziom bezpieczeństwa. Dotyczy to w szczególności ograniczenia lub zmniejszenia udziału dostawców wysokiego ryzyka. Może być również stosowany w przypadkach, w których potencjalne korzyści bezpieczeństwa wynikające z posiadania sieci zbudowanej ze sprzętu więcej niż jednego wiarygodnego dostawcy (np. w celu ograniczenia ryzyka związanego przykładowo z potencjalnym łańcuchem dostaw) przewyższają ryzyko wynikające bezpośrednio z obowiązkowych wymogów dotyczących różnorodności (np. więcej potencjalnych problemów z konfiguracją czy aktualizacją oprogramowania itp.). Biorąc pod uwagę SM05 w kontekście SM03, nie należy go narzucać dodając dostawcę „wysokiego ryzyka”, po to by zwiększyc różnorodność dostawców.  Załączniki:   1. Comprehensive technology Final 2. Advice-on-use-equipment-from-high-risk-vendors-in-UK-telecoms | Wyjaśnienie.  Brane są pod uwagę różne możliwe rozwiązania. Ministerstwo Cyfryzacji bada rozwiązania stosowane w innych krajach (w Unii i poza nią). Propozycje w uwadze wykraczają jednak poza upoważnienie ustawowe do wydania niniejszego rozporządzenia.  Na konferencji:  Przedstawiciel Nokii przyjął wyjaśnienia MC. |
|  | Ogólne | Związek Cyfrowa Polska | Ponadto rozważyłbym pójście drogą obraną przez regulatora brytyjskiego, który  w odpowiednich swoich regulacjach określił maksymalny udział jednego dostawcy w sieci na poziomie 35% ( <https://www.reuters.com/article/us-health-coronavirus-britain-huawei/uk-made-a-firm-decision-on-huawei-in-5g-foreign-ministrys-top-official-idUSKCN22327E>). Może warto w Polsce zaproponować ten maksymalny udział jednego dostawcy na poziomie np. 50%? | Wyjaśnienie.  Brane są pod uwagę różne możliwe rozwiązania. Ministerstwo Cyfryzacji bada rozwiązania stosowane w innych krajach (w Unii i poza nią). Propozycje w uwadze wykraczają jednak poza upoważnienie ustawowe do wydania niniejszego rozporządzenia.  Na konferencji:  Przedstawiciel Związku Cyfrowa Polska przyjął wyjaśnienia MC. |
|  | Ogólne | Związek Cyfrowa Polska | Warto przy projektowaniu stosownych regulacji kształtujących rynek w tym zakresie uwzględniać zapisy stwarzające szanse dla polskich firm, aktywnego udziału w tym projekcie. Zachęcam do zastanowienia się czy nie warto uwzględnić kwestii zapewnienia udziału polskich firm w projektach realizowanych w oparciu o 5 G. Warto rozważyć konieczność zapewnienia otwartych i powszechnie dostępnych standardów. Inaczej polskie firmy będą tylko asystować przy podziale rynku pomiędzy 3 głównych dostawców i nie pokonamy "vendor lock". Uważam, że powinniśmy nadążać za najnowszymi trendami w branży telekomunikacyjnej, a w szczególności w ramach ORAN (<https://www.o-ran.org/>), TIP (<https://telecominfraproject.com/>) czy ONF (<https://www.opennetworking.org/>). Model, w którym cały sprzęt, oprogramowanie i integracja do danego elementu infrastruktury sieciowej dostarczane są od jednego dostawcy, jest sukcesywnie wypierany przez zakupy od niezależnych od siebie dostawców, z zachowaniem interoperacyjności opartej na standardach telekomunikacyjnych. Wirtualizacja wielu funkcji sieciowych, w tym rozwiązania typu Open RAN dają możliwość znacznie skuteczniejszego zapewnienia niezależności od dostawców i potencjał do korzystania z rozwiązań znacząco efektywniejszych kosztowo. Z perspektywy polskiej gospodarki, wskazanie na rozdzielenie źródła pochodzenia sprzętu i oprogramowania jako istotnego elementu dywersyfikacji elementów 5G jest ważne, bo tworzy szanse dla polskich firm i podmiotów R&D zwłaszcza w segmencie tworzenia i dostaw oprogramowania.  jest też znacznie bardziej bezpieczne niż tylko niwelowanie uzależnienia od dostawców. | Wyjaśnienie.  Niniejsze rozporządzenie nie dotyczy realizowania projektów sieci 5G, tylko, w ograniczonym zakresie, kwestii bezpieczeństwa sieci. Projekt jest neutralny technologicznie i nie promuje żadnego rozwiązania krajowego - MC promuje stosowanie otwartych standardów.  Na konferencji:  Przedstawiciel Związku Cyfrowa Polska przyjął wyjaśnienia MC. |
|  | § 2 | KIKE | Ze zmian w projekcie rozporządzenia, które dotyczą również członków KIKE, dodano w § 2 pkt 12 nowy obowiązek umożliwienia użytkownikom końcowym dokonywania zgłoszeń wszelkich naruszeń bezpieczeństwa sieci i usług telekomunikacyjnych. Izba wskazuje, że obowiązek ten w przypadku małych i średnich operatorów jest zbędnym obciążeniem, i nie może być traktowany jako wymóg minimalnych środków bezpieczeństwa. Z tego względu Izba postuluje jego usunięcie z projektu. | Uwaga nieuwzględniona.  Dokonywanie zgłoszeń przez użytkowników można np. umożliwić w ramach istniejącej pomocy technicznej bądź zgłoszenia mailowego.  Na konferencji:  Przedstawiono wyjaśnienie MC. |
|  | § 2 | PIKE | Izba w dalszym ciągu wskazuje na brak uwzględnienia w całości w projekcie rozporządzenia najistotniejszego postulatu dotyczącego zmiany w § 2 pkt 11, przez co pomimo pozytywnego rozpatrzenia wcześniejszych uwag PIKE, projekt rozporządzenia pozostaje niespójny. Mianowicie, w paragrafie tym wprowadza się obowiązek zapewnienia monitorowania i dokumentowania funkcjonowania sieci i usług telekomunikacyjnych mający na celu wykrycie naruszenia bezpieczeństwa oraz ustalenie przyczyn naruszenia. Pozytywnym aspektem jest ograniczenie tego obowiązku wyłącznie do naruszeń bezpieczeństwa i integralności mających istotny wpływ na funkcjonowanie sieci lub usług, tj. do naruszeń wskazanych w art. 175a Pt. Opisany obowiązek pozostaje jednak w dalszym ciągu nieproporcjonalnie określony do celu jakim jest zwalczanie zagrożeń. Nakazuje on bowiem ciągłe monitorowanie stanu sieci i jego dokumentowanie. Taka jego konstrukcja może być rozumiana jako konieczność ciągłego monitorowania wszelkich elementów jego sieci i sporządzania z tego niepotrzebnej dokumentacji. W opinii Izby obowiązek ten powinien zostać ograniczony wyłącznie do monitorowania kluczowych elementów sieci – infrastruktury krytycznej, tak jak ma to miejsce w pozostałych elementach projektu rozporządzenia, np. w § 2 pkt 7. Ponadto, co się tyczy ustalania przyczyn naruszenia bezpieczeństwa, według Izby operator powinien jedynie określać rodzaj naruszenia. Wszelkie bardziej szczegółowe dane powinien on przekazywać jedynie w wypadku posiadania ich przy okazji świadczenia usług. Przepis ten nie może bowiem zmuszać przedsiębiorców telekomunikacyjnych do prowadzenia samodzielnego dochodzenia w celu wykrycia szczegółowych źródeł naruszenia bezpieczeństwa sieci, zwłaszcza tych pochodzących spoza jego sieci. | Uwaga nieuwzględniona.  Monitorowanie i dokumentowanie funkcjonowania sieci i usług służy wykrywaniu naruszeń w rozumieniu art. 175a PT i ustalania przyczyn. Nie jest to więc ograniczone wyłącznie do kluczowej infrastruktury.  Na konferencji:  Przedstawiciel PIKE przyjął wyjaśnienia MC. |
|  | § 2 | PIKE | W dalszej kolejności, Izba pragnie odnieść się także rozszerzenia regulacji zawartej w § 2 pkt 12 projektu rozporządzenia. Ponownie, jako pozytywne działanie legislacyjne należy uznać dookreślenie, iż obowiązek ten dotyczy wyłącznie naruszeń bezpieczeństwa i integralności mających istotny wpływ na funkcjonowanie sieci lub usług poprzez odwołanie się do art. 175a Pt. Jednakże dodanie kolejnego obowiązku spoczywającego na operatorach, obejmującego umożliwienie użytkownikom końcowym dokonywania zgłoszeń wszelkich naruszeń bezpieczeństwa lub integralności sieci lub usług w opinii Izby jest nieuzasadnione i postuluje ona o jego usunięcie. Przypomnienia wymaga, iż celem rozporządzenia jest wskazanie katalogu minimalnych środków technicznych i organizacyjnych, a nie zaproponowanie kompletnej regulacji w tym zakresie. Nałożenie dodatkowego obowiązku na operatorów telekomunikacyjnych na pewno nie wpisuje się w kryterium minimalizmu. Ponadto, obowiązek ten nie wydaje się stanowić rozwiązania spójnego dla całości regulacji ujętych w projekcie rozporządzenia, przede wszystkim dlatego, że miałby umożliwić użytkownikom końcowym zgłaszanie wszelkich naruszeń, bez względu na to jakich elementów sieci one dotyczą oraz jakie znaczenie mają one na funkcjonowanie sieci lub usług. Izba tymczasem od samego początku postuluje o ograniczenie monitoringu oraz prowadzenia dokumentacji jedynie w zakresie infrastruktury kluczowej oraz wyłącznie względem naruszeń o charakterze istotnym. Zbieranie informacji od użytkowników w sprawie jakiegokolwiek rodzaju naruszenia jest nieproporcjonalne do celu projektu niniejszego rozporządzenia. | Uwaga nieuwzględniona.  Dokonywanie zgłoszeń przez użytkowników można np. umożliwić w ramach istniejącej pomocy technicznej bądź zgłoszenia mailowego.  Na konferencji:  Przedstawiciel PIKE przyjął wyjaśnienia MC. |
|  | § 3 | Fundacja Digital Poland | ***Wykreślić fragment*** *„stosuje rekomendacje, o których mowa w art. 33 ust. 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560, z 2019 r. poz. 2020 i 2248 oraz z 2020 r. poz. 695) w Par 3.1.1* | Uwaga częściowo uwzględniona.  Zmieniono brzmienie § 3 ust. 1 pkt 1.  Na konferencji:  Przedstawiciel Fundacji Digital Poland przyjął wyjaśnienia MC. |
|  | § 3 | Fundacja Digital Poland | ***2.Wykreślić fragment „gwarantuje brak“ wstawiając w jego miejsce fragment „uwzględnia unikanie“ w Par 3.1.2*** | Uwaga częściowo uwzględniona.  Zmieniono brzmienie § 3 ust. 1 pkt 2.  Na konferencji:  Przedstawiciel Fundacji Digital Poland przyjął wyjaśnienia MC. |
|  | § 3 | Fundacja Digital Poland | ***Wykreślić fragment****: „poszczególnych elementów” i* ***wstawić w jego miejsce fragment*** *„budowy” w Par 3.1.2* | Uwaga nieuwzględniona.  Nie chodzi tylko o budowę sieci, ale też o jej funkcjonowanie.  Na konferencji:  Przedstawiciel Fundacji Digital Poland przyjął wyjaśnienia MC. |
|  | § 3 | Fundacja Digital Poland | ***4. Wykreślić fragment: „przy jednoczesnym zapewnieniu interoperacyjności usług” w Par 3.1.2*** | Uwaga nieuwzględniona.  Zachowanie interoperacyjności usług ma kluczowe znaczenie.  Na konferencji:  Przedstawiciel Fundacji Digital Poland przyjął wyjaśnienia MC. |
|  | § 3 | Fundacja Digital Poland | ***5. Wykreślić fragment „zapewnia“ wstawiając w jego miejsce fragment „uwzględnia”*** | Uwaga nieuwzględniona.  Zmiana tego punktu nie pozwala na osiągnięcie celu, jaki był zamierzony.  Na konferencji:  Przedstawiciel Fundacji Digital Poland przyjął wyjaśnienia MC. |
|  | § 3 | KL | Przedstawiona do konsultacji kolejna wersja publicznego 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 (z dnia 22 kwietnia 2020 roku („Projekt”)), zawiera zmiany sprzeczne z przepisami prawa krajowego oraz naruszające zasady prawa unijnego, w szczególności dyrektywy 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii („Dyrektywa NIS”). Konsekwencje prawne związane z potencjalnymi uchybieniami, wiążą się z ryzykiem wniesienia przeciwko Polsce skargi do Trybunału Sprawiedliwości Unii Europejskiej oraz dochodzenia naprawienia szkody materialnej powstałej wskutek nieprawidłowej implementacji.  (…)  Zmieniona treść §3 ust. 1 pkt 1 Projektu nakłada na przedsiębiorcę telekomunikacyjnego dostarczającego sieć 5G, obowiązek stosowania rekomendacji, o której mowa w art. 33 ust. 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa („UKSC”). Rozciągnięcie mechanizmu rekomendacji o których mowa w art. 33 UKSC na przedsiębiorców telekomunikacyjnych budujących sieć 5G jest sprzeczne z zasadą prymatu ustawy, pewności prawa oraz prawa do skutecznego środka odwoławczego.  Na chwilę obecną przedsiębiorcy telekomunikacyjni nie wchodzą w skład krajowego systemu cyberbezpieczeństwa (por. art. 4 UKCS), a wręcz przeciwnie, są oni z zakresu podmiotowego stosowania wyłączeni (art. 1 ust. 2 pkt 1 UKSC). Przedsiębiorcy Ci nie są i nie mogą być zatem adresatami rekomendacji wydawanych na podstawie UKSC.  Rekomendacje są szczególnego rodzaju aktem administracyjnym, sformułowanym arbitralnie przez pełnomocnika rządu ds. cyberbezpieczeństwa w nieprzejrzystej procedurze. Procedura przewidziana w art. 33 UKSC ogranicza sądową i administracyjną kontrolę nad poprawnością rekomendacji. Ustalanie rozwiązań technicznych, regulujących istotne aspekty działalności gospodarczych, tego typu aktami może być sprzeczne z zasadą prymatu ustawy oraz z art. 24 Konstytucji RP, zgodnie z którym ograniczenie wolności działalności gospodarczej jest dopuszczalne tylko w drodze ustawy i jedynie ze względu na ważny interes publiczny.  Co więcej, w obecnym stanie prawnym rekomendacje są aktami skierowanymi jedynie do podmiotów krajowego systemu cyberbezpieczeństwa i tylko te podmioty są uprawnione by poznać ich treść. Ponadto, tylko te podmioty mogą kwestionować rekomendacje i wnosić do pełnomocnika rządu ds. cyberbezpieczeństwa zastrzeżenia do tych rekomendacji z uwagi na ich negatywny wpływ na świadczoną usługę lub realizowane zadanie publiczne. Projekt nakłada na operatorów obowiązek stosowania się do postanowień dokumentów, w których tworzeniu nie brali udziału i których nie mogą kwestionować przed sądem lub innym organem, a których treść może w sposób istotny wpływać na ich prawa i obowiązki. Mogą one także istotnie wpływać na koszty i warunki prowadzenia działalności. Zgodnie z art. 87 Konstytucji RP „źródłami powszechnie obowiązującego prawa Rzeczypospolitej Polskiej są: Konstytucja, ustawy, ratyfikowane umowy międzynarodowe oraz rozporządzenia.” W tym przypadku źródłem prawa dla operatorów telekomunikacyjnych ma być dokument tworzony przez grono podmiotów, którego operator nie jest członkiem. Tego rodzaju rozwiązanie może naruszać art. 87 Konstytucji.  W zaistniałej sytuacji domagamy się wykreślenia całego pkt 1) z §3 ust. 1 Projektu. | Uwaga uwzględniona.  Zmieniono przepis w ten sposób, że należy „uwzględniać” rekomendacje Pełnomocnika w ramach swojego procesu szacowania ryzyka. Nie będą obowiązani stosować rekomendacji na równi z podmiotami krajowego systemu cyberbezpieczeństwa.  Na konferencji:  Przedstawiciel Konfederacji Lewiatan przyjął wyjaśnienia MC. |
|  | § 3 | KL | Wątpliwości budzi treść § 3 ust. 1 pkt 2 Projektu. Zastrzeżenia budzi treść § 3 ust. 1 pkt 2 Projektu pod względem językowym, gdyż nie jest stosowana potocznie konstrukcja językowa w postaci: „gwarantowania braku”. Powoduje to niejasności interpretacyjne i trudność w jej zastosowaniu.  Pod względem legislacyjnym § 3 ust. 1 pkt 2 Projektu jest sprzeczny z § 6 w zw. z § 132 Rozporządzenia Prezesa Rady Ministrów z dnia 20 czerwca 2002 r. w sprawie „Zasad techniki prawodawczej” (Dz.U. Nr 100, poz. 908 ze zm.) („Zasady”). Zgodnie z przepisami tych Zasad przepisy rozporządzenia redaguje się tak, aby dokładnie i w sposób zrozumiały dla adresatów zawartych w nich norm wyrażały intencje prawodawcy. Postanowienie § 3 ust. 1 pkt 2 Projektu naruszają ten przepis, gdyż są niezrozumiałe i nie jest możliwe na podstawie Postanowień Projektu i jego uzasadnienia ustalenie jego treści przy zastosowaniu każdej z możliwych, dostępnych wykładni. Stosując więc w pierwszym rzędzie, zgodnie z zasadami wykładni, wykładnię literalną, gwarantować oznacza, zgodnie ze słownikiem języka polskiego i wyrazów obcych: „dawać gwarancję; dawać rękojmię; ręczyć, zabezpieczać, zapewniać”. Każde z wymienionych słów wyjaśniających słowo gwarancja posiada inne znaczenie, co ważniejsze, nie tylko w języku potocznym, ale także prawniczym, czy nawet prawnym. Funkcjonują bowiem w obrocie prawnym konstrukcje prawne: gwarancji, rękojmi, poręczenia, zabezpieczenia. W których z tych znaczeń jest używane pojęcie w Projekcie „gwarantowania”? Przepis ten w praktyce z tych powodów będzie niezwykle trudny czy wręcz niemożliwy do zastosowania w praktyce.  Budzi zastrzeżenia sformułowanie postanowienia § 3 ust. 1 pkt 2 Projektu także pod względem ściśle merytorycznym. Ani projektowany tekst rozporządzenia ani uzasadnienie Projektu nie zawierają jakichkolwiek wskazówek co do stanu faktycznego i prawnego jaki spełniałby wymóg „braku uzależnienia od jednego producenta”. Wprost przeciwnie, na stronie 13 (uzasadnienie Projektu) wskazuje się, że „Konieczne jest rozważenie dywersyfikacji elementów sieci telekomunikacyjnej. Oczywistym jest, że w niektórych przypadkach będzie to niemożliwe bądź bardzo utrudnione – stąd nie wskazuje się w procentowy sposób, ile urządzeń powinno być od różnych producentów.”. Sam zatem ustawodawca zakłada, że osiągnięcie dywersyfikacji będzie w wielu miejscach niemożliwe lub znacznie utrudnione, niemniej jednak nakłada na operatora telekomunikacyjnej bezwzględny obowiązek gwarantowania zapewnienia takiego stanu rzeczy. Samo bowiem uzasadnienie (s. 14 i 15 Projektu) wskazuje na konieczność osiągnięcia rezultatu, a nie dążenie do niego. Innymi słowy, nałożony obowiązek może okazać się niewykonalny – co sam ustawodawca przyznaje – a mimo to ten sam ustawodawca wymaga jego realizacji. Powiązanie tego wymogu z obowiązkami szacowania ryzyka (§ 2 pkt 3-5 Projektu) nie usuwa tej wewnętrznej sprzeczności. Formułowanie obowiązków nakładanych na adresatów aktu prawnego z jednoczesnym przyznaniem, że nie będą mogli im sprostać, jest nielogiczne oraz narusza zasadę pewności prawa i zaufania do organów państwa. Należy także zwrócić uwagę na wadliwość uzasadnienia Projektu. Uzasadnienie, zamiast wyjaśniać ewentualne wątpliwości związane z zakresem nakładanych na operatorów telekomunikacyjnych obowiązków i sposobem ich prawidłowego wykonania, wprowadza kolejny element niepewności. Wadliwym elementem uzasadnienia jest, między innymi, odwołanie się do koncepcji dostawców o zwiększonym poziomie ryzyka (s. 14, akapit).  Wreszcie, należy stwierdzić, że regulacja § 3 ust. 1 pkt 2 Projektu wkracza w obszar prawa konkurencji, stanowiąc o braku uzależnienia od jednego producenta, który jest regulowany już innymi aktami prawnymi. Przede wszystkim omawiana problematyka pozostaje w zakresie przedmiotowym ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. Nr 50, poz. 331 ze zm.). Zgodnie z art. 1 tej ustawy, w szczególności określa ona warunki rozwoju i ochrony konkurencji. To ta ustawa reguluje zasady i tryb przeciwdziałania praktykom ograniczającym konkurencję. Nie wspominając, że akt prawny w postaci rozporządzenia wkracza w problematykę zastrzeżoną dla ustawy.  Biorąc pod uwagę treść zaproponowanych zmian proponujemy rozważenie nowej treści § 3 ust. 1 Projektu o następującym brzmieniu:  *§ 3. 1. Przedsiębiorca telekomunikacyjny dostarczający sieć piątej generacji (5G), określoną w dokumencie technicznym – Raporcie ETSI TR 121 915 V.15.0.0. (2019-10) lub dokumencie go zastępującym, w ramach realizacji środków, o których mowa w § 2 pkt 3-5, w ramach tej sieci:*  *~~3.stosuje rekomendacje, o których mowa w art. 33 ust. 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560, z 2019 r. poz. 2020 i 2248 oraz z 2020 r. poz. 695);~~*  *4.****uwzględnia unikanie*** *~~gwarantuje brak~~ uzależnienia ~~się~~ od jednego producenta poszczególnych elementów sieci telekomunikacyjnej przy jednoczesnym zapewnieniu interoperacyjności usług;* 5.~~zapewnia~~  ***uwzględnia*** *podwyższanie odporności na zakłócenia sieci i usług telekomunikacyjnych.*  *2. Przedsiębiorca telekomunikacyjny prowadzi dokumentację działań, o których mowa w ust. 1.* | Uwaga częściowo uwzględniona.  Zmieniono brzmienie przepisu, nie będzie się odnosić do „gwarantowania braku uzależnienia”.  Na konferencji:  Przedstawiciel Konfederacji Lewiatan przyjął wyjaśnienia MC. |
|  | § 3 | ZPP | Innym interesującym przepisem zawartym w projekcie jest §3 ust. 1 pkt 2, który stanowi że przedsiębiorca telekomunikacyjny dostarczający sieć 5G ma „gwarantować brak uzależnienia się od jednego producenta poszczególnych elementów sieci telekomunikacyjnej przy jednoczesnym zapewnieniu interoperacyjności usług”. Zabezpieczenie sieci przed uzależnieniem od jednego dostawcy stanowiło jedną z rekomendacji zawartych we wspomnianym wcześniej raporcie ZPP. Tym samym, cel przepisu uznajemy za słuszny, mamy jednak wątpliwości co do jego konstrukcji. Poza pewną językową niezręcznością (potocznie raczej mówi się o „gwarancji czegoś”, a nie „gwarancji braku czegoś”), trzeba stwierdzić że sam projektodawca w przedstawionym uzasadnieniu stwierdził, że w niektórych przypadkach dywersyfikacja elementów sieci telekomunikacyjnej może być niemożliwa bądź bardzo utrudniona. Jednocześnie, jak również podkreślono w uzasadnieniu, przepis nakłada obowiązek osiągnięcia określonego rezultatu. Ta rozbieżność powoduje, że wydaje się, iż cel projektodawcy jest nie do końca spójny z tym, co faktycznie uwzględnił on w propozycji przepisu. Tym samym rekomendowalibyśmy przeformułowanie regulacji w taki sposób, by dyrektywa unikania uzależnienia od jednego producenta poszczególnych elementów sieci była opisana w sposób umożliwiający adresatom tekstu prawnego realizację obowiązku z niego wynikającego i gwarantujący im podstawową pewność prawną w tym zakresie. | Uwaga częściowo uwzględniona.  Zmieniono przepis w ten sposób, że należy „uwzględniać” rekomendacje Pełnomocnika w ramach swojego procesu szacowania ryzyka. Nie będą obowiązani stosować rekomendacji na równi z podmiotami krajowego systemu cyberbezpieczeństwa.  Na konferencji:  Przedstawiono wyjaśnienie MC. |
|  | § 3 | PTI | W § 3 ust. 1 pkt 1 odwołano się do art. 33 ust. 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560 oraz z 2019 r. poz. 2020 i 2248). Odwołanie to budzi poważną wątpliwość, gdyż przedsiębiorstwa telekomunikacyjne są wyłączone z jej stosowania na podstawie art. 1 ust. 2 pkt 1 (*Ustawy nie stosuje się do przedsiębiorców telekomunikacyjnych, o których mowa w ustawie z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2017 r. poz. 1907 i 2201 oraz z 2018 r. poz. 106, 138, 650 i 1118), w zakresie wymogów dotyczących bezpieczeństwa i zgłaszania incydentów*). Poza tym, odwołanie to nie wyczerpuje zaleceń GC 01/2020 w zakresie certyfikacji.  Zapis § 3 ust. 1 pkt 3 jest ogólny, nie ma żadnej miary i nic nie wnosi, zatem może zostać wykreślony. | Uwaga częściowo uwzględniona.  Zmieniono przepis w ten sposób, że należy „uwzględniać” rekomendacje Pełnomocnika w ramach swojego procesu szacowania ryzyka. Nie będą obowiązani stosować rekomendacji na równi z podmiotami krajowego systemu cyberbezpieczeństwa.  Na konferencji:  MC przedstawiło swoje wyjaśnienia, PTI podtrzymało swoje uwagi i zgłosiło zastrzeżenia co do nieokreśloności obowiązków, jakie w opinii PTI tworzy projekt aktu prawnego. |
|  | § 3 | ZPP | W zakresie szczegółowych uwag, pragniemy zwrócić uwagę na przepis §3 ust. 1 pkt 1 projektu, zgodnie z którym przedsiębiorca telekomunikacyjny dostarczający sieć 5G jest obowiązany do stosowania rekomendacji pełnomocnika ds. cyberbezpieczeństwa, o których mowa w art. 33 ust. 4 ustawy o krajowym systemie cyberbezpieczeństwa. Jest to propozycja o tyle kontrowersyjna, że krąg podmiotów uprawnionych do wnoszenia zastrzeżeń do rekomendacji wydanych przez pełnomocnika, jest w ramach ustawy o krajowym systemie cyberbezpieczeństwa ograniczony wyłącznie do podmiotów krajowego systemu cyberbezpieczeństwa. Ustawa wspomniana tymczasem wprost wyłącza przedsiębiorców telekomunikacyjnych ze swojego zakresu – nie są oni częścią krajowego systemu cyberbezpieczeństwa. Tym samym, przedstawiony projekt rozporządzenia zawiera regulację zobowiązującą przedsiębiorców telekomunikacyjnych do stosowania rekomendacji, w tworzeniu których nie brali udziału i do konsultowania których nie są uprawnieni. Tymczasem treść tych rekomendacji może głęboko ingerować w ich prawa i obowiązki, wpływając na koszty i warunki prowadzenia przez nich działalności gospodarczej. Jest to oczywiście sytuacja niepożądana i może ona naruszać słuszne interesy podmiotów objętych konstrukcją przewidzianą w projekcie rozporządzenia. | Uwaga częściowo uwzględniona.  Zmieniono przepis w ten sposób, że należy „uwzględniać” rekomendacje Pełnomocnika w ramach swojego procesu szacowania ryzyka. Nie będą obowiązani stosować rekomendacji na równi z podmiotami krajowego systemu cyberbezpieczeństwa.  Na konferencji:  Przedstawiono wyjaśnienie MC. |
|  | § 3 | PTI | Natomiast § 3 ust. 1 pkt 2 nie zawiera sformułowań wystarczająco jednoznacznych i tym samym wymaga przeredagowania zgodnie z poniższą uwagą szczegółową.  **Było:**  *2) unikanie uzależnienia od jednego producenta poszczególnych elementów sieci telekomunikacyjnej przy jednoczesnym zapewnieniu interoperacyjności usług;*  **Jest:**  *2) gwarantuje brak uzależnienia się od jednego producenta poszczególnych elementów sieci telekomunikacyjnej przy jednoczesnym zapewnieniu interoperacyjności usług;*  **Proponujemy:**  *2) obowiązek dywersyfikacji dostawców poszczególnych elementów sieci 5G, realizowany poprzez:*   1. *unikanie ryzyka zależności od jednego dostawcy lub zależności od grupy dostawców o zwiększonym poziomie ryzyka,* 2. *zapewnienie odpowiedniej równowagi w udziale dostawców na poziomie narodowym w celu zagwarantowania elastyczności i ciągłości dostaw,* 3. *zapewnienie konkurencyjności i otwartości rynku na dostawców poszczególnych elementów sieci,* 4. *stosowanie innowacyjnego i bezpiecznego oprogramowania funkcji sieciowych, niezależnego od dostawców sprzętu, przy jednoczesnym zapewnieniu interoperacyjności usług.*   **Uzasadnienie**  Przedłożony projekt dotyczy „minimalnych środków technicznych i organizacyjnych oraz metod, jakie przedsiębiorcy telekomunikacyjni są obowiązani stosować”. To znaczy, że zawarte w nim zapisy powinny uszczegóławiać i doprecyzowywać. Powinny być jednoznaczne, a ich możliwość interpretacji powinna być ograniczona do minimum.  Jednocześnie należy zauważyć, że przepisy te nakładają na przedsiębiorców telekomunikacyjnych oraz pośrednio na ich dostawców obowiązki, których wypełnienie związane jest z ponoszeniem dodatkowych kosztów bezpośrednich oraz pośrednich. Budzi to naturalne odruchy obronne z ich strony służące ograniczeniu tych kosztów poprzez kontestowanie presji regulatora. Z tego powodu będą pojawiały się interpretacje, takie jak:   * Grupa Współpracy jest jedynie ciałem doradczym, a jej opracowania nie mają charakteru wiążącego; * Grupa Współpracy została powołana na podstawie Dyrektywy NIS, która nie dotyczy usług komunikacji elektronicznej świadczonych operatorów telekomunikacyjnych stąd nie jest dla nich wiążąca; * Istniejące przepisy opierają się na najlepszych praktykach opartych o analizę ryzyka, a istniejąca swoboda działalności gospodarczej zapewnia właściwy dobór zabezpieczeń przez operatora, adekwatny do zidentyfikowanego ryzyka. | Uwaga częściowo uwzględniona.  Zmieniono brzmienie przepisu, nie będzie się odnosić do „gwarantowania braku uzależnienia”.  Zbyt szczegółowe doprecyzowanie obowiązku dywersyfikacji jest o tyle utrudnione, że zawiera wiele niedookreślonych zapisów (“odpowiednia równowaga”) jak i reguluje kwestie, które nie powinny być rozstrzygane przez indywidualnych przedsiębiorców (czym jest dostawca o zwiększonym poziomie ryzyka, zapewnianie otwartości rynku). Odstąpiono zatem od tego brzmienia.  Na konferencji:  MC przedstawiło swoje wyjaśnienia, PTI podtrzymało swoje uwagi i zgłosiło zastrzeżenia co do nieokreśloności obowiązków, jakie w opinii PTI tworzy projekt aktu prawnego. |
|  | § 3 | PTI | **Certyfikacja (§ 3 ust. 1 pkt 1)**  Jednocześnie należy zauważyć światowe trendy w obszarze certyfikacji urządzeń w zakresie bezpieczeństwa. Istniejące od wielu dziesięcioleci schematy certyfikacyjne oparte o normę ISO 15408 (tzw. *Common Criteria*) mają swoje ograniczenia, a w szczególności:   * brak modeli certyfikacji w nowych obszarach oceny; * długotrwałość procedury oceny; * wysokie koszty.   Trwają więc prace nad nowymi światowymi i europejskimi modelami. Polska w nich aktywnie uczestniczy.  W szczególności w prace w ramach projektu KSO3C[[1]](#footnote-2) prowadzone są przez Instytut Łączności Państwowy Instytut Badawczy, EMAG Instytut Badawczy oraz NASK Państwowy Instytut Badawczy, który utrzymuje również krajowy CSIRT (CERT), o którym mowa w ustawie o krajowym systemie cyberbezpieczeństwa.  Certyfikacja jest jednym z, chociaż nie jedynym, elementem zapewnienia cyberbezpieczeństwa. Stąd wymogi z nią związane winny być uwzględnione w ramach minimalnych wymagań w stopniu znacznie szerszym niż proponowany zapis w § 3 ust. 1. Obszar ten winien być uzgodniony w szczególności ze wskazanymi jednostkami badawczymi. | Uwaga nieuwzględniona.  W ramach powstającego Krajowego Systemu Certyfikacji Cyberbezpieczeństwa zostaną zbudowane fundamenty systemu certyfikacji produktów, usług i procesów ICT pod kątem cyberbezpieczeństwa.  Obecnie ten system dopiero powstaje i nie wydaje się zasadne odnosić do certyfikacji na tym etapie.  Na konferencji:  MC przedstawiło swoje wyjaśnienia, PTI podtrzymało swoje uwagi i zgłosiło zastrzeżenia co do nieokreśloności obowiązków, jakie w opinii PTI tworzy projekt aktu prawnego. |
|  | § 3 | PTI | **Ryzyko w Łańcuchu Dostaw (§3 ust. 1 pkt 2)**  Słowo „uzależnienie” nie jest terminem technicznym. Słownik Języka Polskiego PWN definiuje, że uzależniony to „*osoba, która popadła w nałóg*”, natomiast uzależniać to „*uczynić zależnym od kogoś lub czegoś*”. Uzależnienie jest powszechnie wiązane z nałogiem.  „Uzależnienie” nie posiada prostej miary, to znaczy istnieje istotna trudność z ustaleniem kiedy możemy mówić o uzależnieniu lub jego braku, np. osoba uzależniona od alkoholu często kwestionuje to uzależnienie. Dlatego należy unikać takich stwierdzeń, gdyż można je dowolnie interpretować.  Stawiane wymagania są celami do osiągnięcia, a tym samym powinny spełniać kryteria SMART.  **S**  Skonkretyzowany (ang. *Specific*) – jego zrozumienie nie powinno stanowić kłopotu, sformułowanie powinno być jednoznaczne i niepozostawiające miejsca na luźną interpretację, aby ustanowić konkretny cel należy odpowiedzieć sobie na 6 pytań (w wersji angielskiej określanych jako ‘6W’):   1. (*Who*) Kto jest związany z celem? 2. (*What*) Co chcę osiągnąć? 3. (*Where*) Określ miejsce. 4. (*When*) Określ przedział czasu, w którym cel ma zostać osiągnięty. 5. (*Which*) Określ wymagania i ograniczenia związane z realizacją celu. 6. (*Why*) Określ przyczyny realizacji danego celu i korzyści płynące z osiągnięcia go.   **M**  Mierzalny (ang. *Measurable*) – a więc tak sformułowany, by można było liczbowo wyrazić stopień realizacji celu, lub przynajmniej umożliwić jednoznaczną „sprawdzalność” jego realizacji.  **A**  Osiągalny (ang. *Achievable*) – cel zbyt ambitny podkopuje wiarę w jego osiągnięcie i tym samym motywację do jego realizacji.  **R**  Istotny (ang. *Relevant*) – cel powinien być ważnym krokiem naprzód, jednocześnie musi stanowić określoną wartość dla tego, kto będzie go realizował.  **T**  Określony w czasie (ang. *Time-bound*) – cel powinien mieć dokładnie określony horyzont czasowy  w jakim zamierzamy go osiągnąć; alternatywnie. Namacalny (ang. *Tangible*) – możliwy do doświadczenia za pomocą 5 zmysłów, ponieważ taki cel często jest również bardziej konkretny i mierzalny a tym samym bardziej osiągalny.  Określenie „uzależnienie” nie spełnia powyższych kryteriów.  Zmiana opisu postępowania z „*unikania uzależnienia*” na „*gwarantowanie*” w stopniu niewystarczającym doprecyzowuje obowiązek podmiotu. Zgodnie z przywoływanym Słownikiem PWN, gwarancja to:   1. *poręczenie, że coś nastąpi albo że jest prawdziwe;* 2. *zobowiązanie producenta do bezpłatnej naprawy lub wymiany wyrobu na inny, w razie, gdyby w określonym czasie ujawniły się w nim jakieś wady;* 3. *odpowiedzialność osoby trzeciej za zobowiązania dłużnika wobec wierzyciela.*   Adekwatne w tej sytuacji byłoby „*poręczenie, że coś nastąpi albo że jest prawdziwe*”, zatem zamiast oczekiwania„*gwarancji*” powinniśmy zatem żądać wprost albo oświadczenia, albo certyfikatu wydanego przez uprawniony podmiot. Obydwie czynności, aby były skuteczne, powinny być obwarowane rygorem odpowiedzialności (karnej, finansowej lub innej, np. zakazem prowadzenia działalności).  Zupełnie inaczej wygląda kwestia sfomułowania „dywersyfikacja”. Jej definicja wprost wskazuje na powiązanie z ryzykiem, a zatem jest adekwatna i spójna z całym obszarem regulacji. W ślad za wskazanym słownikiem przeczytamy:   * dywersyfikacja - różnicowanie asortymentu produkcji lub usług w celu zmniejszenia ryzyka  w prowadzeniu działalności gospodarczej; * dywersyfikacja portfela papierów wartościowych - zakup i posiadanie różnorodnych papierów wartościowych w celu obniżenia ryzyka inwestora.   Zaproponowane doprecyzowanie kryterium dywersyfikacji (lit. a-d) zapewnia jej precyzję wymaganą od regulacji na poziomie wymagań minimalnych.  Jednocześnie należy uciąć pojawiające się prasowe spekulacje dotyczące „dywersyfikacji dostawców”.   1. Dywersyfikacja dostawców nie jest równoznaczna z zakazem korzystania z dostawcy X. Operator może korzystać z dostawcy X, jednakże nie może ten dostawca mieć zazwyczaj większościowego udziału. Regulator może określić ten próg celem doprecyzowania. 2. Dywersyfikacja nie narusza żadnych przepisów dotyczących konkurencyjności i otwartości rynku. Poziom zamówień do dostawcy X jest uzależniony jedynie od potrzeb nabywcy (operatora). Jedyna różnica dotyczy wolumenu zamówienia – nie może on przekroczyć określonego udziału w poziomie potrzeb całkowitych nabywcy. 3. Dywersyfikacja nie utrudnia działalności i jest korzystna w perspektywie długoterminowej dla klienta, gdyż wspiera kontrolę nad praktykami monopolistycznymi i zapewnia konkurencję (co najmniej dwa konkurujące podmioty). Natomiast w perspektywie krótkoterminowej obowiązek dywersyfikacji może być postrzegany jako niekorzystny poprzez perspektywę możliwości uzyskania krótkoterminowych korzyści wynikającej z dokonania transakcji na postawie ofert z cenami dumpingowymi (innymi słowy „udało się kupić tanio”).   Reasumując, zaproponowana treść regulacji może być kontestowana, gdyż utrudnia osiąganie krótkoterminowych korzyści przez operatorów oraz prowadzenie działań nieuczciwej konkurencji (w kierunku monopolu) przez dostawców. | Uwaga częściowo uwzględniona.  Zmieniono brzmienie przepisu, nie będzie się odnosić do „gwarantowania braku uzależnienia”.  Na konferencji:  MC przedstawiło swoje wyjaśnienia, PTI podtrzymało swoje uwagi i zgłosiło zastrzeżenia co do nieokreśloności obowiązków, jakie w opinii PTI tworzy projekt aktu prawnego. |
|  | § 3 | PTI | **Podwyższanie odporności (§3 ust. 1 pkt 3)**  „Podwyższanie odporności” jest zapisane w innych przepisach i nie wymaga powtarzania. Określając wymagania minimalne należałoby co najwyżej wskazać jakie działania i jakie cele w tym obszarze należałoby osiągnąć. | Uwaga nieuwzględniona.  Jest to środek, który należy brać pod uwagę przy postępowaniu z ryzykiem.  Na konferencji:  MC przedstawiło swoje wyjaśnienia, PTI podtrzymało swoje uwagi i zgłosiło zastrzeżenia co do nieokreśloności obowiązków, jakie w opinii PTI tworzy projekt aktu prawnego. |
|  | § 3 | KIGEIT | ***„§ 3.*** *1. Przedsiębiorca telekomunikacyjny dostarczający sieć piątej generacji (5G), określoną w dokumencie technicznym – Raporcie ETSI TR 121 915 V.15.0.0. (2019-10) lub dokumencie go zastępującym, w ramach realizacji środków, o których mowa w § 2 pkt 3-5, w ramach tej sieci w odniesieniu do kluczowej infrastruktury tej sieci i stosując zasadę, o której mowa w art. 175 ust. 1 zdanie drugie ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne:*  *~~1) stosuje rekomendacje, o których mowa w art. 33 ust. 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560, z 2019 r. poz. 2020 i 2248 oraz z 2020 r. poz. 695);~~*  *~~2)~~1) ~~gwarantuje brak~~ uwzględnia unikanie**uzależnienia ~~się~~ od jednego producenta poszczególnych elementów sieci telekomunikacyjnej przy jednoczesnym zapewnieniu interoperacyjności usług;*  *~~3)~~2) ~~zapewnia~~ stale prowadzi działania w celu**podwyższania odporności na zakłócenia sieci i usług telekomunikacyjnych.”* | Uwaga nieuwzględniona.  W przepisach nie powtarza się brzmienia innych przepisów - zwłaszcza że niniejsze rozporządzenie wykonuje przepisy PT.  Działania powinny być podejmowane wobec całej infrastruktury, a nie tylko kluczowej.  Na konferencji:  Przedstawiciel KIGEIT przyjął wyjaśnienia MC. Uwagę uznano za uzgodnioną. |
|  | § 3 | PIIT | Kluczowe zmiany projektu rozporządzenia dotyczą projektowanego §3, który określa wymagania dot. sieci 5G.  W pierwszej kolejności za pozytywną zmianę przyjmujemy przywrócenie wyraźnego wskazania, że formułowane wymagania dotyczą sieci 5G, poprzez uzupełnienie brzmienia ust. 1 o zwrot „w ramach tej sieci”. Wskazanie to powinno zostać bezwzględnie utrzymane w toku dalszych prac legislacyjnych.  Dodatkowo, dla precyzyjnego określenia zakresu rozporządzenia proponujemy umieszczenie po tych słowach w treści ust. 1 następującego uzupełnienia: „*w odniesieniu do kluczowej infrastruktury tej sieci i stosując zasadę, o której mowa w art. 175 ust. 1 zdanie drugie ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne”* | Uwaga nieuwzględniona.  W przepisach nie powtarza się brzmienia innych przepisów - zwłaszcza że niniejsze rozporządzenie wykonuje zapisy PT.  Działania powinny być podejmowane wobec całej infrastruktury, a nie tylko kluczowej.  Na konferencji:  Przedstawiciel PIIT przyjął wyjaśnienia MC. Uwagę uznano za uzgodnioną. |
|  | § 3 | PIIT | **Rekomendacje Pełnomocnika Rządu ds. Cyberbezpieczeństwa**  W dotychczasowym §3 ust. 1 pkt 1 zawarte było zalecenie “*uwzględniania rekomendacji Pełnomocnika Rządu ds. Cyberbezpieczeństwa*”.  Przepis ten budził nasze istotne wątpliwości, z uwagi na fakt, że wprowadzał do stosowania w ramach reżimu prawnego Prawa telekomunikacyjnego, wymagania, które były projektowane i mają w naszej ocenie wyłączne zastosowanie do porządku prawnego w ramach ustawy o krajowym systemie cyberbezpieczeństwa oraz podmiotów zobowiązanych do jej stosowania. Rekomendacje Pełnomocnika są bowiem narzędziem odrębnym i nieobejmującym przedsiębiorców telekomunikacyjnych, którzy w zakresie wymagań bezpieczeństwa i zgłaszania incydentów powinni kierować się wymaganiami ustawy Prawo telekomunikacyjne. Przedsiębiorcy Ci nie są uczestnikami krajowego systemu cyberbezpieczeństwa i tym samym nie są potencjalnym uczestnikiem procedury wydawania Rekomendacji, a więc tym bardziej nie powinni być ich adresatem. Szczególnie, że w omawianym przypadku nie ma żadnych wątpliwości, że rekomendacje mają dotyczyć kwestii bezpieczeństwa, a tym samym stosowanie wyłączenia przedsiębiorców telekomunikacyjnych spod reżimu ustawy o krajowym systemie cyberbezpieczeństwa powinno być bezsporne.  **Proponowane brzmienie wprowadza jednak jeszcze dalej idące postanowienia, wskazując, że przedmiotowe rekomendacje nie tyle należy „uwzględniać” co wręcz „stosować” co jest w naszej ocenie rozwiązaniem niedopuszczalnym z perspektywy polskiego porządku prawnego i nieakceptowalnym z perspektywy możliwości praktycznej realizacji takiego wymogu.**  Takie określenie powoduje szereg wątpliwości i uwag, wśród których wymienić można  w szczególności:   * W pierwszej kolejności należy zwrócić uwagę, że przewidziany w § 3 ust. 1 pkt 1) projektu rozporządzenia obowiązek stosowania przez przedsiębiorców telekomunikacyjnych rekomendacji, o których mowa w art. 33 ust. 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, jest wprost niezgodny z ustawą o krajowym systemie cyberbezpieczeństwa, która przewiduje mechanizm wydawania rekomendacji. Zgodnie z art. 1 ust. 2 pkt 1) ustawy o krajowym systemie cyberbezpieczeństwa przepisów tej ustawy nie stosuje się do przedsiębiorców telekomunikacyjnych w zakresie wymogów dotyczących bezpieczeństwa i zgłaszania incydentów. Ustawa o krajowym systemie cyberbezpieczeństwa, na podstawie, której Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa może wydawać rekomendacje, zasadnie nie ma zastosowania do przedsiębiorców telekomunikacyjnych, co jest również bezpośrednią konsekwencją przepisów Unii Europejskiej, która w dyrektywie NIS zastrzegła: *W celu uwzględnienia wszystkich istotnych incydentów i ryzyk niniejsza dyrektywa powinna mieć zastosowanie zarówno do operatorów usług kluczowych, jak i dostawców usług cyfrowych.* ***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 (3), które podlegają szczegółowym wymogom w zakresie bezpieczeństwa i integralności ustanowionym w tej dyrektywie,* […].   Innymi słowy zarówno unijny (dyrektywa NIS) jak i polski (ustawa o krajowym systemie cyberbezpieczeństwa) Prawodawca wprost i jednoznacznie uznał, że wymagania wynikające  z tej dyrektywy i tej ustawy, w tym wymagania dotyczące stosowania rekomendacji wydawanych przez Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa, nie będą miały zastosowania wobec przedsiębiorców telekomunikacyjnych. Zatem § 3 ust. 1 pkt 1) projektu rozporządzenia, w zakresie w jakim nakłada na przedsiębiorców telekomunikacyjnych obowiązek stosowania rekomendacji wydawanych przez Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa, stoi w oczywistej sprzeczności z art. 1 ust. 2 pkt 1) ustawy o krajowym systemie cyberbezpieczeństwa (który wprost wyłącza stosowanie przepisów tej ustawy wobec przedsiębiorców telekomunikacyjnych), a jednocześnie stanowi naruszenie przepisów prawa Unii Europejskiej, gdyż ustawa o krajowym systemie cyberbezpieczeństwa stanowi implementację do krajowego porządku prawnego dyrektywy NIS. Biorąc pod uwagę oczywistą i jednoznaczną sprzeczność pomiędzy projektowanym rozporządzeniem a ustawą  o krajowym systemie cyberbezpieczeństwa, aktualnego brzmienia § 3 ust. 1 pkt 1) projektu rozporządzenia nie można uznać za nic innego jak próbę dokonania zmiany w ustawie  o krajowym systemie cyberbezpieczeństwa przepisem rangi rozporządzenia wykonawczego, co jest próbą, która stoi w oczywistej sprzeczności z konstytucyjną hierarchią źródeł prawa powszechnie obowiązującego, w której rozporządzenie stanowi akt prawa niższego rzędu niż ustawa (art. 87 Konstytucji RP) i w której jedynym celem rozporządzenia może być wykonanie ustawy i to tylko w granicach ściśle zakreślonych przez delegację ustawową (art. 92 Konstytucji RP). W żadnym wypadku Konstytucja RP nie dopuszcza przypadków, w których rozporządzenie mogłoby być niezgodne z ustawą lub zmieniałoby ustawę.   * Po drugie, **nie jest dopuszczalne nakładanie na przedsiębiorców obowiązków w sposób blankietowy oraz w drodze odwołania do tekstu zewnętrznego wobec rozporządzenia oraz ustawy PT**, **który ma jednocześnie charakter nienormatywny i może być w dowolny sposób kształtowany i zmieniany przez Pełnomocnika ds. Cyberbezpieczeństwa**, a co więcej nie odpowiada w żaden sposób zasadom przygotowywania, konsultowania i przyjmowania aktów nakładających określone obowiązki na przedsiębiorców. Szczególnie w przypadku,  w którym Rekomendacje nie powinny nawet zostać przywołane w rozporządzeniu stosowanym do przedsiębiorców telekomunikacyjnych. * **Obowiązek „stosowania” Rekomendacji jest wprost sprzeczny z naturą rekomendacji,** które są formą określenia pewnych zaleceń, wskazań lub opinii, a nie sztywnych wymagań. Sam projektodawca wyraźnie, bowiem wskazuje w rozporządzeniu ***Nie oznaczają one automatycznie konieczności pozbycia się sprzętu z sieci*** *– wskazują jedynie na możliwe zagrożenia wynikające ze stosowania określonych urządzeń. Rekomendacje mogą mieć również charakter pozytywny (wskazywać zalecany sprzęt) oraz wskazywać określony sposób korzystania (np. rodzaje systemów, w których zaleca się korzystać z określonego sprzętu lub oprogramowania).* Należy wskazać, że takie uzasadnienie było w pewnym zakresie aktualne wobec pierwotnej propozycji brzmienia projektu, natomiast obecny tekst nakazujący stosowanie jest, przynajmniej potencjalnie, sprzeczny z intencją wyrażoną w uzasadnieniu. Wszak, gdyby rekomendacje (których tekst nie jest znany) taki wymóg sformułowały, wówczas przedsiębiorca telekomunikacyjny byłyby obowiązany się do nich zastosować. * **Wprowadzenie obowiązku „stosowania” rekomendacji w przypadku przedsiębiorców telekomunikacyjnych jest tym bardziej niedopuszczalne, że brak jest nawet możliwości, które posiadają podmioty krajowego systemu cyberbezpieczeństwa, które w przypadku skierowania wobec nich Rekomendacji mają wyraźnie zapewnioną możliwość reakcji**  **i sprzeciwu**. Wynika to wprost z art. 33 ust. 5-8 ustawy o krajowym systemie cyberbezpieczeństwa, który wskazuje, że:   *5.* ***Podmiot*** ***krajowego*** ***systemu*** ***cyberbezpieczeństwa może wnieść do Pełnomocnika zastrzeżenia do rekomendacji*** *dotyczących stosowania urządzeń informatycznych lub oprogramowania, z uwagi na ich negatywny wpływ na świadczoną usługę lub realizowane zadanie publiczne, nie później niż w terminie 7 dni od dnia otrzymania rekomendacji.*  *6.* ***Pełnomocnik odnosi się do zastrzeżeń*** *otrzymanych w trybie ust. 5 niezwłocznie, jednak nie później niż w terminie 14 dni od dnia ich otrzymania, i podtrzymuje rekomendacje dotyczące stosowania urządzeń informatycznych lub oprogramowania albo wydaje zmienione rekomendacje.*  *7.* ***Podmiot*** ***krajowego*** ***systemu*** ***cyberbezpieczeństwa informuje Pełnomocnika, na jego wniosek, o sposobie i zakresie uwzględnienia*** *rekomendacji dotyczących stosowania urządzeń informatycznych lub oprogramowania.*  *8.* ***Nieuwzględnienie rekomendacji dotyczących stosowania urządzeń informatycznych lub oprogramowania stanowi podstawę do wystąpienia przez Pełnomocnika do organu sprawującego nadzór nad podmiotem, o którym mowa***  ***w ust. 7, z informacją o ich nieuwzględnieniu****.*  Projektodawca nawet w uzasadnieniu wyraźnie wskazuje, że „*Ujęcie rekomendacji w tym punkcie nie oznacza, że przedsiębiorcy są włączani w procedurę dotyczącą uwzględniania stosowania rekomendacji i nadzoru określoną w ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa*”.  W praktyce **przyjęta konstrukcja oznacza, więc, że przedsiębiorcy telekomunikacyjni, zostaną objęci jedynie jedną z bardziej represywnych form działania dostępnych instytucjom krajowego systemu cyberbezpieczeństwa, nie będąc jego uczestnikami,**  **a jednocześnie nie posiadając żadnych form obrony przed tymi obowiązkami**, jakie mogą zostać określone w przyszłych Rekomendacjach, a które dzisiaj nie są znane nawet  w ogólnym zarysie.   * **Obowiązek stosowania Rekomendacji, jest sprzeczny z ideą normy zawartej w §3, wg, której to rolą przedsiębiorcy jest dokonanie odpowiednich analiz i wdrożeń**, tj. czynności obejmujących obszary wskazane w §2 pkt 3-5:   *3) identyfikuje zagrożenia bezpieczeństwa lub integralności sieci lub usług;*  *4) ocenia prawdopodobieństwo wystąpienia oddziaływania zagrożeń na bezpieczeństwo lub integralność sieci lub usług;*  *5) zapewnia i stosuje środki minimalizujące skutki wystąpienia oddziaływań zagrożeń na bezpieczeństwo lub integralność sieci lub usług;*  W sytuacji, gdy narzucone zostanie stosowanie Rekomendacji podmiotu zewnętrznego, który ww. analiz dokona wg własnych standardów i założeń, podstawowy sens może stracić słusznie dotychczas przyjmowana logika przepisu oparta na zobowiązaniu przedsiębiorców telekomunikacyjnych (jako najwłaściwszych do tego podmiotów) do wykonania odpowiednich analiz i dostosowania do nich wdrażanych środków. Rekomendacje byłoby niezbędne do stosowania nawet, gdyby nie znajdowały potwierdzenie w analizach przeprowadzonych przez przedsiębiorcę telekomunikacyjnego.   * Wreszcie, wskazać należy, że **Prawo telekomunikacyjne przewiduje już szczególne tryby nakładania na przedsiębiorców telekomunikacyjnych, przez właściwy dla nich organ, tj. Prezesa Urzędu Komunikacji Elektronicznej, dodatkowych wymagań w zakresie bezpieczeństwa**, które wynikają wprost z art. 178 dot. decyzji w sytuacjach szczególnych zagrożeń.   Podsumowując musimy wskazać, że **w naszej ocenie, aż nadto wyraźne jest, że taka konstrukcja nie powinna utrzymać się w tekście projektu** rozporządzenia.  Postulujemy, więc, ponownie **wykreślenie z projektu odwołania do rekomendacji Pełnomocnika Rządu ds. Cyberbezpieczeństwa, a przynajmniej usunięcie wskazania na bezwzględny obowiązek ich stosowania.**  Ewentualnie, biorąc pod uwagę fakt, że Rekomendacje faktycznie mogą mieć charakter pozytywny (jak wskazano w uzasadnieniu) i stanowić użyteczne źródło wiedzy (nie obowiązków) dla przedsiębiorców, możemy ponownie zaproponować przyjęcie konstrukcji postulowanej w stanowisku PIIT przedstawionym do pierwotnego brzmienia projektu rozporządzenia z 24 stycznia br. tj. w §3 proponujemy treść pkt 1 w ust. 1 oznaczyć, jako ust. 2 i nadać mu następujące brzmienie:  *„2. Przedsiębiorca telekomunikacyjny, realizując działania, o których mowa w ust. 1 może uwzględniać również rekomendacje, o których mowa w art. 33 ust. 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560 oraz z 2019 r. poz. 2020 i 2248);”* | Uwaga częściowo uwzględniona.  Zmieniono przepis w ten sposób, że należy „uwzględniać” rekomendacje Pełnomocnika w ramach swojego procesu szacowania ryzyka. Nie będą obowiązani stosować rekomendacji na równi z podmiotami krajowego systemu cyberbezpieczeństwa.  Na konferencji:  Przedstawiciel PIIT przyjął wyjaśnienia MC. Uwagę uznano za uzgodnioną. |
|  | §3 | PIIT | **Dywersyfikacja**  W zmodyfikowanej propozycji przepisów przyjęto konstrukcję wskazującą na obowiązek zagwarantowania braku uzależnienia od jednego dostawcy.  **Według uzasadnienia przyczyną dla takiej modyfikacji miało być uwzględnienie propozycji „*strony społecznej*** *zgłoszone w trakcie konsultacji wskazywały na konieczność doprecyzowania kwestii unikania uzależnienia od jednego producenta*”**. Sformułowanie to sugeruje jakoby istniał wobec takiej propozycji konsensus** i wszystkie organizacje popierały doprecyzowanie przedmiotowego zapisu. Tymczasem, chociażby **Polska Izba Informatyki i Telekomunikacji, która jest jedynym podmiotem, który zrzesza wszystkich operatorów sieci mobilnych, którzy będą faktycznie obowiązani do stosowania przedmiotowych przepisów, na żadnym etapie konsultacji nie sygnalizowała konieczności doprecyzowania wymagania odnoszącego się do dywersyfikacji dostawców**.  Biorąc powyższe pod uwagę, **zakładamy, że wprowadzenie przedmiotowego doprecyzowania opierało się na niewłaściwej diagnozie oczekiwań strony społecznej**, która przynajmniej w naszej ocenie powinna być definiowana przez pryzmat podmiotów bezpośrednio zobowiązanych do stosowania konsultowanych przepisów.  Tym samym:   * Postulujemy przywrócenie zawartego w projekcie z dnia 5 marca 2020 r. brzmienia **§ 3 ust. 1 pkt 2, który wskazywał na potrzebę „*unikania uzależnienia od jednego producenta*”** oraz wprowadzenie odpowiednich modyfikacji w uzasadnieniu projektu. * **W przypadku braku uwzględnienia naszego postulatu,** wnioskujemy o modyfikacje uzasadnienia projektu poprzez:   + wskazanie, że doprecyzowanie zostało wprowadzone na wniosek części podmiotów ze strony społecznej;   + wyraźne określenie jakie podmioty postulowały przedmiotowe rozwiązanie;   + podkreślenie, że Polska Izba Informatyki i Telekomunikacji nie postulowała, ani nie popierała wprowadzenia omawianych zmian projektu rozporządzenia. | Uwaga częściowo uwzględniona.  Zmieniono brzmienie przepisu, nie będzie się odnosić do „gwarantowania braku uzależnienia”.  Usunięto także zbyt szczegółowe doprecyzowanie obowiązku dywersyfikacji.  Uznano, że jest o tyle utrudnione, że zawiera wiele niedookreślonych zapisów (“odpowiednia równowaga”) jak i reguluje kwestie, które nie powinny być rozstrzygane przez indywidualnych przedsiębiorców (czym jest dostawca o zwiększonym poziomie ryzyka, zapewnianie otwartości rynku). Odstąpiono zatem od tego brzmienia.  Na konferencji:  Przedstawiciel PIIT przyjął wyjaśnienia MC. Uwagę uznano za uzgodnioną. |
|  | § 4 | PIIT | **Termin wejścia w życie**  **Podtrzymujemy również uwagi w zakresie terminu wejścia w życie oraz wprowadzenia precyzyjnego terminu pierwszego przygotowania dokumentacji**. Tym samym wnioskujemy o przyjęcie następującej konstrukcji:  *„§ 3a. Dokumentacja, o której mowa w §2 pkt 1) przygotowywana jest po raz pierwszy w terminie 18 miesięcy od wejścia w życie niniejszego rozporządzenia.”*  *§ 4. Rozporządzenie wchodzi w życie po upływie 12 miesięcy od dnia ogłoszenia.”* | Uwaga nieuwzględniona.  Termin 6 miesięcy pozostaje bez zmian. Przedłużenie terminu na sporządzenie dokumentacji oznacza de facto przedłużenie do 18 miesięcy wejścia w życie rozporządzenia.  Na konferencji:  Przedstawiciel PIIT przyjął wyjaśnienia MC. Uwagę uznano za uzgodnioną. |
|  | § 4 | KIGEIT | Podtrzymujemy aby wydłużyć czas wejścia w życie przepisów § 2, tak aby wynosił 24 miesiące. | Uwaga nieuwzględniona.  Termin 6 miesięcy pozostaje bez zmian.  Na konferencji:  Przedstawiciel KIGEIT przyjął wyjaśnienia MC. Uwagę uznano za uzgodnioną. |
|  | § 4 | Związek Cyfrowa Polska | W chwili obecnej niezbędnym wydaje mi się doprecyzowanie zapisu o dywersyfikacji dostawców, który wydaje mi się kluczowy.  Obecnie przedmiotowy par. 3, ust.1 pkt. 2 projektowanego Rozporządzenia przyjął brzmienie:  *"2) gwarantuje brak uzależnienia się od jednego producenta poszczególnych elementów sieci telekomunikacyjnej przy jednoczesnym zapewnieniu interoperacyjności usług"*  W mojej ocenie zaproponowany zapis jest nadal mocno nieprecyzyjny. "Uzależnienie" nie jest terminem biznesowym, prawniczym czy też technologicznym, a przede wszystkim jest to pojęcie niemierzalne. W związku z powyższym istnieje ryzyko, iż użycie takiego nieprecyzyjnego pojęcia będzie polem do bardzo różnego interpretowania przedmiotowego zapisu. Stąd jestem zwolennikiem użycia w przedmiotowym zapisie słowa „obowiązek”.  Co spowodowałoby nabranie przez przedmiotową część Rozporządzenia brzmienia:  *"2) obowiązek braku uzależnienia się od jednego producenta poszczególnych elementów sieci telekomunikacyjnej przy jednoczesnym zapewnieniu interoperacyjności usług "*  Jednocześnie podtrzymuję swoja propozycję, przedłożoną Panu Ministrowi w poprzedniej fazie konsultacji przedmiotowego Rozporządzenia, aby doprecyzować powyższy zapis poprzez brzmienie:  *2) obowiązek dywersyfikacji dostawców poszczególnych elementów sieci 5G, realizowany poprzez:*   1. *unikanie ryzyka zależności od jednego dostawcy lub zależności od grupy dostawców  o zwiększonym poziomie ryzyka,* 2. *zapewnienie odpowiedniej równowagi w udziale dostawców na poziomie narodowym w celu zagwarantowania elastyczności i ciągłości dostaw,* 3. *zapewnienie konkurencyjności i otwartości rynku na dostawców poszczególnych elementów sieci,*   *stosowanie innowacyjnego i bezpiecznego oprogramowania funkcji sieciowych, niezależnego od dostawców sprzętu, przy jednoczesnym zapewnieniu interoperacyjności usług* | Uwaga nieuwzględniona.  Zbyt szczegółowe doprecyzowanie obowiązku dywersyfikacji jest o tyle utrudnione, że zawiera wiele niedookreślonych zapisów (“odpowiednia równowaga”) jak i reguluje kwestie, które nie powinny być rozstrzygane przez indywidualnych przedsiębiorców (czym jest dostawca o zwiększonym poziomie ryzyka, zapewnianie otwartości rynku).  Na konferencji:  Przedstawiciel Związku Cyfrowa Polska przyjął wyjaśnienia MC. Uwagę uznano za uzgodnioną. |

1. <https://www.kso3c.pl/> [↑](#footnote-ref-2)