Wersja z 06.04.2020

**Uwagi 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**

**II TURA KONSULTACJI**

Uwagi zgłosili:

* Polska Izba Informatyki i Telekomunikacji (PIIT)
* Polska Izba Komunikacji Elektronicznej (PIKE)
* Krajowa Izba Komunikacji Ethernetowej (KIKE)
* Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji (KIGEIT)
* Związek Pracodawców Mediów Elektronicznych i Telekomunikacji MEDIAKOM (MEDIAKOM)
* Izba Rzeczoznawców Polskiego Towarzystwa Informatycznego (PTI)
* Związek Importerów i Producentów Sprzętu Elektrycznego i Elektronicznego – ZIPSEE Cyfrowa Polska (ZIPSEE)
* Polskie Towarzystwo Przesyłu i Rozdziału Energii Elektrycznej (PTPiREE)

|  |  |  |  |
| --- | --- | --- | --- |
| Jednostka redakcyjna | Podmiot zgłaszający uwagę | Treść uwagi | Stanowisko MC |
| Ogólna | PIKE | PIKE uprzejmie dziękuje za możliwość udziału w procesie legislacyjnym i wyraża nadzieję, że opisane w niniejszym piśmie uwagi i propozycje zostaną przez Ministra Cyfryzacji uwzględnione w toku dalszych prac. Izba pragnie zwrócić uwagę przede wszystkim na wskazaną w art. 13a dyrektywy 2009/140/WE zasadę proporcjonalności środków w stosunku do istniejącego ryzyka. Z tego względu minimalny zestaw środków określony w projekcie rozporządzenia powinien być jak najmniejszy, aby pozwolić przedsiębiorcom elastyczne reagowanie na zagrożenia. | Uwaga uwzględniona.  W opinii projektodawcy, propozycje przepisów spełniają wymóg proporcjonalności.  „Minimalny zestaw środków” nie oznacza, że środki mają zostać dopasowane do przedsiębiorców, tylko że jest to faktycznie minimalny zestaw środków niezbędnych do zapewnienia bezpieczeństwa. |
| Ogólna | KIKE | Projekt rozporządzenia reguluje istotną z punktu widzenia rynku telekomunikacyjnego kwestię, jaką jest zabezpieczenia sieci telekomunikacyjnych i usług telekomunikacyjnych przed poważnymi naruszeniami bezpieczeństwa lub integralności sieci lub usług telekomunikacyjnych.  Należy zwrócić uwagę na zasadniczą kwestię jaką jest brak proporcjonalności proponowanych środków organizacyjnych oraz metod zapobiegania zagrożeniom zarówno pod kątem tych zagrożeń jak i skali wielkości operatora. Zdaniem KIKE większość obowiązków wskazanych w projekcie rozporządzenia nie powinna być kierowana do mikro i małych przedsiębiorców, gdyż będzie stanowiła dla nich zbyt duże obciążenie w stosunku do osiąganych przez nich dochodów. Na uwagę zwracają zapisy art. 66 i 67 ustawy Prawo przedsiębiorców należy zmniejszać obciążenia obowiązkami nakładanymi na mikroprzedsiębiorców oraz małych przedsiębiorców, zwłaszcza w sferze obowiązków informacyjnych takich jak w projekcie rozporządzenia.  KIKE zwraca również uwagę na zapisy art. 13 a dyrektywy ramowej, którego realizacji służy m.in. projektowane rozporządzenie. W art. 13a ust. 1 dyrektywy ramowej jest również mowa o zapewnieniu poziomu bezpieczeństwa proporcjonalnego do istniejącego ryzyka. Izba wskazuje, ze w przypadku małych sieci telekomunikacyjnych poziom ryzyka dla bezpieczeństwa jest znacznie mniejszy niż w przypadku dużych sieci telekomunikacyjnych. Nie chodzi tu o sam fakt wystąpienia zagrożenia, ale jego skutki. Zakłócenie funkcjonowania małej sieci telekomunikacyjnej pociąga dla siebie skutki dla małej ilości abonentów co nie ma dużego wpływu na rynek telekomunikacyjny i jest łatwe do usunięcia. Takie rozróżnienie poziomów ryzyka wynika pośrednio z treści dyrektywy 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (dyrektywa ds. cyberbezpieczeństwa), gdzie w art. 14 ust. 4 wskazano, że na istotność wpływu danego incydentu wpływa liczba użytkowników objęta incydentem oraz zasięg geograficzny. Choć zgodnie z art. 1 ust. 3 dyrektywy ds. cyberbezpieczeństwa wymogów z tej dyrektywy nie stosuje się do operatorów telekomunikacyjnych, ale zdaniem Izby należy przyjąć analogiczne mechanizmy oceny zagrożenia i podjętych środków.  Biorąc powyższe pod uwagę, zdaniem Izby mikroprzedsiębiorcy w ogóle powinni być wyłączeni ze stosowania przepisów rozporządzenia tak jak to zostało wprowadzone w projekcie rozporządzenia z art. 176a ust. 5 Pt w zakresie planów działań na wypadek szczególnych zagrożeń. | Uwaga częściowo uwzględniona.  W opinii projektodawcy, propozycje przepisów spełniają wymóg proporcjonalności.  „Minimalny zestaw środków” nie oznacza, że środki mają zostać dopasowane do przedsiębiorców, tylko że jest to faktycznie minimalny zestaw środków niezbędnych do zapewnienia bezpieczeństwa.  Jak podnoszono w poprzednich pismach oraz podczas konferencji uzgodnieniowej, upoważnienie ustawowe nie pozwala na zróżnicowanie traktowania przedsiębiorców wg ich wielkości – odmiennie niż w przypadku rozporządzenia z art. 176a PT. |
| Ogólna / § 2 | KIKE | Z kolei katalog obowiązków dla małych przedsiębiorców powinien zostać zmniejszony do następujących najważniejszych obowiązków:   1. opracowuje i aktualizuje wykaz elementów infrastruktury telekomunikacyjnej i systemów informatycznych, których naruszenie bezpieczeństwa lub integralności będzie miało istotny wpływ na funkcjonowanie sieci lub usług o znaczeniu kluczowym dla funkcjonowania przedsiębiorcy, zwanych dalej „kluczową infrastrukturą”; 2. identyfikuje zagrożenia bezpieczeństwa lub integralności sieci lub usług; 3. zapewnia i stosuje środki minimalizujące skutki wystąpienia oddziaływań zagrożeń na bezpieczeństwo lub integralność sieci lub usług; 4. zabezpiecza dostęp do kluczowej infrastruktury i wskazuje środki reagowania na nieuprawniony dostęp lub próbę takiego dostępu; 5. stosuje, wynikające z oceny prawdopodobieństwa wystąpienia oddziaływania zagrożeń, środki zabezpieczające dla poszczególnych kategorii przetwarzanych przez niego danych; 6. zapewnia dokumentowanie naruszenia bezpieczeństwa i ustalenie przyczyn takiego naruszenia; 7. przeprowadza ocenę bezpieczeństwa sieci i usług telekomunikacyjnych raz na trzy lata.   Pozostałe obowiązki, jakie znajdują się w projekcie rozporządzenia są zbyt dużym obciążeniem finansowym dla małego przedsiębiorcy. Ich wykonanie będzie nieproporcjonalne w stosunku do celu jakim jest zapewnienie bezpieczeństwa. Należy wskazać, ze mali przedsiębiorcy telekomunikacyjni nie dysponują zasobami kadrowymi umożliwiającymi wykonanie części obowiązków z projektu rozporządzenia, ani nie posiadają niezbędnych zasobów finansowych na ich wykonanie. Należy również wskazać na niewielką skalę działalności tych podmiotów na rynku telekomunikacyjnym, co powinno się przełożyć na proporcjonalne zmniejszenie obowiązków w zakresie stosowanych środków technicznych oraz procedur organizacyjnych jakie te podmioty powinny stosować. Nie jest bowiem celowe aby mały operator o niecałym tysiącu abonentów miał takie same obowiązki zabezpieczania sieci jak duży operator posiadający kilka milionów abonentów.  Bezcelowe jest nakładanie na małego operatora (a tym bardziej na mikroprzedsiębiorcę) obowiązek w zakresie identyfikacji zagrożeń związanych z zawieranymi umowami międzyoperatorskimi. Mali operatorzy nie mają żadnego wpływu na treść zawieranych przez siebie umów międzyoperatorskich z większymi podmiotami.  Mali operatorzy wykonując obowiązki w zakresie monitorowania dostępu do swojej infrastruktury kluczowej oraz monitorowania całej sieci poniosą tak wysokie nakłady finansowe, ze przewyższą one korzyści ze wzmocnionej ochrony. Spowodują te obowiązki właściwie znaczące zmniejszenie opłacalności prowadzonej przez nich działalności gospodarczej.  Okresowa ocena bezpieczeństwa sieci powinna dla małych przedsiębiorców być zredukowana wyłącznie do okresu 3 letniego, a jej ponowne wykonywanie po naruszeniu bezpieczeństwa powinno być dobrowolną decyzja biznesową tego operatora.  Podsumowując, KIKE wskazuje na konieczność zmiany filozofii projektu rozporządzenia na mniejsze obciążanie operatorami obowiązkami w zakresie organizacyjnym i technicznym. | Uwaga nieuwzględniona.  Pominięcie wybranych arbitralnie elementów w propozycji (nie jest jasne, dlaczego „ocena prawdopodobieństwa wystąpienia oddziaływania zagrożeń” czy też „ustanawianie zasad bezpiecznego zdalnego przetwarzania danych” zostały pominięte) powoduje że środki przestają działać – przykładowo, bez oceny prawdopodobieństwa nie jest możliwe stosowanie odpowiednich środków bezpieczeństwa.  Obowiązki są skalowalne i mimo iż sformułowane tak samo, w procesie wdrażania będą się znacząco różnić. Zatem nie można zgodzić się z zarzutem, że duży operator z infrastrukturą rozrzuconą po całym kraju będzie miał taką samą ocenę zagrożeń co mały podmiot, działający lokalnie i bez własnej infrastruktury.  Propozycja, aby oceny były raz na trzy lata – i to bez powtarzania ocen w przypadku naruszeń bezpieczeństwa –przy dzisiejszym rozwoju technologicznym nie spełni swojej roli.  Ocena bezpieczeństwa jest istotnym elementem doskonalenia organizacji, poprawy procedur, środków bezpieczeństwa, radzenia sobie z incydentami, ale też oceny skuteczności podjętych decyzji zarządczych. Dokonywanie oceny raz na trzy lata pozbawia jej tych cech. |
| Ogólna | MEDIAKOM | Ponawiam stanowisko, że w ocenie mikro, małych i średnich przedsiębiorców rozporządzenie jest zbędne. Obowiązek podjęcia środków technicznych i organizacyjnych w celu zapewnienia bezpieczeństwa i integralności sieci, usług i przekazów komunikatów w związku ze świadczonymi usługami wynika z art. 175 ustawy Prawo telekomunikacyjne, który to przepis obowiązuje od 2004 r. i mimo, iż dotąd nie zostało wydane rozporządzenie wykonawcze w oparciu o art. 175d PT, operatorzy obowiązki te realizowali środkami, które w ich ocenie wystarczają dla ich realizacji. W interesie każdego przedsiębiorcy telekomunikacyjnego leży zagwarantowanie bezpieczeństwa sieci i usług. Każda przerwa czy zakłócenie w świadczeniu usług rodzi roszczenia odszkodowawcze po stronie odbiorców usług i koszty związane z usuwaniem awarii. W tej sytuacji wdrożenie właściwych środków technicznych i procedur mających na celu zapobieganie wszelkim niebezpieczeństwom i awariom jest niezbędne i kluczowe dla zapewnienia ciągłości usług, zabezpieczenia przed przerwami w ich świadczeniu i minimalizowania skutków ewentualnych przerw. Jednak każdy z operatorów jest w stanie samodzielnie ocenić na ryzyko jakich zagrożeń narażona jest jego sieć i usługi i wdrożyć odpowiednie środki techniczne i organizacyjne, które odpowiednio do skali ryzyka zagrożeń, technologii usług, rozmiarów sieci – zabezpieczą sieć i usługi. Rozporządzenie nie wnosi w tym zakresie żadnych szczególnych, odmiennych od już stosowanych, rozwiązań. | Uwaga nieuwzględniona.  Należy się zgodzić, że w obecnej sytuacji przedsiębiorcy telekomunikacyjni sami decydują, jakie rodzaje środków technicznych i organizacyjnych chcą zastosować, aby zapewnić bezpieczeństwo sieci i usług telekomunikacyjnych. Nie jest to jednak sytuacja pożądana. Brakuje jednolitych standardów prawnych, które działając w interesie obywateli, obligowałyby przedsiębiorców telekomunikacyjnych do stosowania konkretnych rodzajów rozwiązań w zakresie bezpieczeństwa. Niniejsze rozporządzenie wprowadza wyrównane zasady dla wszystkich przedsiębiorców – prawdą jest, że nie są to nowe rozwiązania. Taka była intencja projektodawców – przedstawiana zresztą podczas konferencji uzgodnieniowej. |
| Ogólna | PTI | Projekt rozporządzenia nie wypełnia delegacji ustawowej do jego wydania, bowiem nie przewiduje w zasadzie żadnych „środków technicznych i organizacyjnych” jakie powinni zastosować przedsiębiorcy telekomunikacyjni, a jedynie zawiera zasadnicze wymagania dot. wytwarzania dokumentacji oraz obowiązków związanych z rozpoznawaniem zagrożeń dla bezpieczeństwa lub integralności sieci. Projekt nie konsumuje publikacji Grupy Współpracy NIS Nr 01/2020 zatytułowanej „Cybersecurity of 5G networks EU Toolbox of risk mitigating measures” (zwanym dalej „5G Toolbox”). W dokumencie, będącym źródłem prawa dla krajów członkowskich, sformułowano skoordynowany raport z szacowania ryzyka oraz zabezpieczenia (załącznik 1, tabela 1) w podziale na:   * strategiczne – od SM01 do SM08; * techniczne – od TM01 do TM11 oraz * wspierające – od SA01 do SA10.   Dla każdego z dziewięciu zidentyfikowanych obszarów ryzyka opracowano plany postępowania z ryzykiem w horyzoncie krótko, średnio i długoterminowym (załącznik 1, tabela 2). Opracowany projekt aktu prawnego powinien te plany implementować, a niestety tego nie robi w stopniu wystarczającym.  „5G Toolbox” zaleca (str. 18) aby wszystkie państwa członkowskie zapewniły stosowanie zabezpieczeń (w tym silną rolę regulatorów krajowych) właściwych i proporcjonalnych w odpowiedzi do obecnie zidentyfikowanych, jak i przyszłych ryzyk. W szczególności w zakresie:   * wzmocnienia wymagań bezpieczeństwa dla operatorów (np. dokładnego/precyzyjnego zarządzania dostępem, zasad bezpiecznych działań operacyjnych i monitorowania, ograniczenia outsourcingu specyficznych funkcji, itp.); * oszacowania profilu ryzyka dla dostawców, a jako konsekwencja wdrożenia właściwych restrykcji dla dostawców wysokiego ryzyka włącznie z ich wykluczeniem dla złagodzenia ryzyka dla kluczowych aktywów (np. funkcje szkieletu sieci, zarządzanie siecią i funkcje orkiestracji oraz funkcje dostępu do sieci); * zapewnienie, że każdy operator posiada właściwą strategię wielu źródeł (ang. multi-vendor) w celu ograniczenia uzależnienia od pojedynczego dostawcy. | Uwaga nieuwzględniona.  Wdrożenie rozwiązań określonych w Toolboxie 5G wymaga szerszych działań – głównie zmian legislacyjnych na poziomie ustawowym, które będą wdrażane do nowego Prawa Komunikacji Elektronicznej.  Propozycje zapisów w tej kwestii zostaną przedstawione pod koniec kwietnia 2020. |
| Ogólna | ZIPSEE | Przede wszystkim musimy podkreślić, iż przygotowany projekt rozporządzenia nie przewiduje w zasadzie żadnych „środków technicznych i organizacyjnych” jakie powinni zastosować przedsiębiorcy telekomunikacyjni, a jedynie zawiera zasadnicze wymagania dot. wytwarzania dokumentacji oraz obowiązków związanych z rozpoznawaniem zagrożeń dla bezpieczeństwa lub integralności sieci. | Uwaga nieuwzględniona.  Projektodawca stoi na stanowisku, że projekt rozporządzenie zawiera środki techniczne i organizacyjne, a ich przykładowe wskazanie zawarte jest w uzasadnieniu. |
| Ogólna | ZIPSEE | Co więcej, naszym zdaniem projekt nie uwzględnia zapisów „Cybersecurity of 5G networks EU Toolbox of risk mitigating measures” (zwanym dalej „5G Toolbox”). W dokumencie, będącym źródłem prawa dla krajów członkowskich, sformułowano skoordynowany raport z szacowania ryzyka oraz zabezpieczenia. Dla każdego z dziewięciu zidentyfikowanych obszarów ryzyka opracowano plany postępowania z ryzykiem w horyzoncie krótko, średnio i długoterminowym. Niestety procedowany projekt nie implementuje tych zapisów.  „5G Toolbox” zaleca aby wszystkie państwa członkowskie zapewniły stosowanie zabezpieczeń w odpowiedzi do obecnie zidentyfikowanego, jak i przyszłego ryzyka. W szczególności w zakresie:   * wzmocnienia wymagań bezpieczeństwa dla operatorów   + oszacowania profilu ryzyka dla dostawców, a jako konsekwencja wdrożenia właści-wych restrykcji dla dostawców wysokiego ryzyka włącznie z ich wykluczeniem dla złagodzenia ryzyka dla kluczowych aktywów   + zapewnienie, że każdy operator posiada właściwą strategię wielu źródeł (ang. multi-vendor) w celu ograniczenia uzależnienia od pojedynczego dostawcy.   Wymagania w § 2 projektu Rozporządzenia są bardzo ogólne i pomijają większość zagadnień z „5G Toolbox” wskazanych powyżej. Kwestie outsourcingu są całkowicie pominięte, podobnie jak strategia zarządzania dostawcami i łańcuchem dostaw.  Pominięto również całkowicie aspekt nadzoru nad stosowaniem niniejszego rozporządzenia, a w szczególności wzmocnienia regulatora i jego roli w tym procesie. A jest to jedna z kluczowych kwestii. | Uwaga nieuwzględniona.  Toolbox 5G jest dokumentem, który wymaga wdrożenia poprzez zmianę prawa na poziomie ustawy – wymaga nowych uprawnień dla regulatora i nowych obowiązków dla przedsiębiorców. Obecnie trwają prace nad nowym Prawem komunikacji elektronicznej – zastępującego obecne Prawo telekomunikacyjne – które wdroży m.in. postanowienia Toolboxa 5G. |
| Ogólna | ZIPSEE | Dodatkowo pragnę zwrócić uwagę, iż przedmiotowe Rozporządzenie powinno zabezpieczać zdalny dostęp do zarządzania siecią czyli tzw. customer service. Brak kontroli może pozwolić na wyłączenie sygnału w sieci telekomunikacyjnej czyli doprowadzić do rzeczywistego paraliżu gospodarki lub nawet całego państwa. | Uwaga nieuwzględniona.  Pragnę zauważyć, że § 2 pkt 8 projektu rozporządzenia wskazuje ustanawianie zasad bezpiecznego zdalnego przetwarzania danych jako jeden ze środków do uwzględnienia. |
| Ogólna | ZIPSEE | Podsumowując jeszcze raz odwołam się do kluczowego, z europejskiego punktu widzenia dokumentu, tzw. „5G Toolbox”, który zachęca poszczególne państwa członkowskie do stosowania konkretnych obowiązków adekwatnych do zdiagnozowanych obecnie i przyszłego ryzyka. Wedle ostatnich szacunków, w Polsce od 40-80% sieci pochodzi od jednego dostawcy. „5G Toolbox” stanowi, że: "Strengthening the role of national authorities", "Restrict the use of high risk suppliers and strengthen access controls, network monitoring and patch management processes", "ensure diversity of supply within each operator and geographical balance at national level and promote long-term sustainability of 5G supply chain".  Pozostaje to w ścisłym związku, z wielokrotnie wskazywanymi w stanowiskach Rządu, zagrożeniami związanymi z uzależnieniem naszej sieci od jednego dostawcy. Skuteczną kontrolę tego dostępu powinno zawierać przedmiotowe rozporządzenie, a obecnie procedowany projekt, w naszej opinii, ich nie zawiera. | Uwaga nieuwzględniona.  Toolbox 5G jest dokumentem, który wymaga wdrożenia poprzez zmianę prawa na poziomie ustawy – wymaga nowych uprawnień dla regulatora i nowych obowiązków dla przedsiębiorców. Obecnie trwają prace nad nowym Prawem komunikacji elektronicznej – zastępującego obecne Prawo telekomunikacyjne – które wdroży m.in. postanowienia Toolboxa 5G. |
| § 2 | PIKE | Projekt rozporządzenia po ostatnich konsultacjach uwzględnia większość poprzednich postulatów PIKE. Nie został jedynie uwzględniony jeden postulat, przez co projekt rozporządzenia nie jest spójny z dokonanymi zmianami.  W § 2 pkt 11 projektu rozporządzenia wprowadza się obowiązek zapewnienia monitorowania i dokumentowania funkcjonowania sieci i usług telekomunikacyjnych mający na celu wykrycie naruszenia bezpieczeństwa oraz ustalenie przyczyn naruszenia. Punkt ten znacząco wykracza poza delegację ustawową i jest nieproporcjonalny do celu jakim jest zwalczanie zagrożeń. Projekt bowiem nakazuje ciągłe monitorowanie stanu sieci i jego dokumentowania. Taka jego konstrukcja może być rozumiana jako konieczność ciągłego monitorowania wszelkich elementów jego sieci (nawet tych nieistotnych) i sporządzania z tego niepotrzebnej dokumentacji. Tymczasem obowiązek ten powinien się skupić wyłącznie na monitorowaniu kluczowych elementów sieci (takie zawężenie wprowadzono w pozostałych elementach projektu rozporządzenia) i dokumentowaniu wyłącznie naruszeń bezpieczeństwa i integralności, mających istotny wpływ na funkcjonowanie sieci lub usług. | Uwaga uwzględniona.  Propozycja zmiany treści § 2 pkt 11 na następującą:  *„11) zapewnia monitorowanie i dokumentowanie funkcjonowania sieci i usług telekomunikacyjnych mające na celu wykrycie naruszenia bezpieczeństwa lub integralności sieci lub usług, o których mowa w art. 175a ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne i ustalenie przyczyn takiego naruszenia”*  W ten sposób należy monitorować sieć tylko pod kątem „poważnych naruszeń”. |
| § 2 | PIKE | Wyjaśnienia wymaga również kwestia ustalenia przyczyn naruszenia bezpieczeństwa. Według Izby operator powinien jedynie określać rodzaj naruszenia, wszelkie bardziej szczegółowe dane powinien przekazywać jedynie w wypadku posiadania ich przy okazji świadczenia usług. Nie może ten przepis zmuszać przedsiębiorców telekomunikacyjnych do prowadzenia samodzielnego dochodzenia w celu wykrycia szczegółowych źródeł naruszenia bezpieczeństwa sieci, zwłaszcza tych pochodzących spoza jego sieci. | Uwaga nieuwzględniona.  Ustalenie przyczyn naruszenia bezpieczeństwa jest niezbędne, aby ocenić naturę problemu konfiguracyjnego lub lukę w zabezpieczeniach.  Bezrefleksyjne odhaczanie kolejnych przypadków naruszeń bez przyjrzenia się przyczynie nie doprowadzi do podwyższenia poziomu bezpieczeństwa. |
| § 2 | PTI | Wymagania w § 2 są bardzo ogólne i pomijają większość zagadnień opisanych powyżej. Kwestie outsourcingu są całkowicie pominięte, podobnie jak strategia zarządzania dostawcami i łańcuchem dostaw. | Uwaga nieuwzględniona.  Kwestie outsourcingu mieszczą się w § 2 pkt 6-11. Zarządzanie dostawcami i łańcuchem dostaw mieści się w § 2 pkt 10 (bezpieczeństwo prawne) i, nieco ogólniej, w § 2 pkt 3-5 (zarządzanie ryzykiem). |
| § 2 | PTI | Pominięto również całkowicie aspekt nadzoru nad stosowaniem niniejszego rozporządzenia, a w szczególności wzmocnienia regulatora i jego roli w tym procesie. | Uwaga nieuwzględniona.  Pozycja regulatora i zasady nadzoru nad rynkiem określa ustawa – Prawo telekomunikacyjne. |
| § 2 | PTPiREE | par. 2 ust. 13 rozporządzenia określa obowiązek dokonywania „oceny bezpieczeństwa sieci i usług telekomunikacyjnych”, ale nie zawiera wskazówek co należy przez taką ocenę rozumieć. Uzasadnienie do projektu zawiera informację czym taka ocena być nie musi, ale wydaje się rozsądne, aby rozporządzenie określało też elementy konieczne takiej oceny. | Uwaga nieuwzględniona.  Ocena bezpieczeństwa jest istotnym elementem doskonalenia organizacji, poprawy procedur, środków bezpieczeństwa, radzenia sobie z incydentami, ale też oceny skuteczności podjętych decyzji zarządczych. Ma ona służyć przede wszystkim przedsiębiorcy. Nie uznaje się za wskazane ograniczać swobody przedsiębiorcy w zakresie doboru środków koniecznych do przeprowadzenia oceny bezpieczeństwa. |
| § 3 | PIIT | **Odnośnie brzmienia §3, PIIT podtrzymuje swoje dotychczasowe uwagi,** przy czym wskazujemy, że: o krytycznie oceniamy zmianę – jak się wydaje niezamierzoną – w zdaniu wprowadzającym w § 3 projektu rozporządzenia, która powoduje, że przedsiębiorca telekomunikacyjny musiałby stosować środki przewidziane w § 3 w stosunku do sieci wszystkich generacji (przewodowych oraz radiowych 2G, 3G, 4G i 5G oraz następnych), podczas gdy z pierwotnego tekstu rozporządzenia jasno wynikało – i tak należało rozumieć intencje Projektodawcy – aby te środki były stosowane wyłącznie w odniesieniu do sieci piątej generacji. Zwracamy bowiem uwagę, że zdanie wprowadzające w § 3 w pierwszej opublikowanej wersji projektu rozporządzenia brzmiało (podkreślenie własne):  *§ 3. 1. Przedsiębiorca telekomunikacyjny dostarczający sieć piątej generacji (5G), określoną w dokumencie technicznym – Raporcie ETSI TR 121 915 V.15.0.0. (2019-10)* ***w ramach tej sieci*** *identyfikuje zagrożenia, ocenia prawdopodobieństwo ich wystąpienia, zapewnia i stosuje środki minimalizujące skutki wystąpienia zagrożeń, w zakresie bezpieczeństwa i integralności sieci i usług, uwzględniając:* […]  W najnowszej wersji projektu rozporządzenia ze zdania wprowadzającego w § 3 usunięto stwierdzenie „w ramach tej sieci”, co powoduje fundamentalną, choć jak rozumiemy niezamierzoną zmianę zakresu stosowania § 3 rozporządzenia, która przeczyłaby dotychczasowym ustaleniom poczynionym w toku konsultacji publicznych i uzgodnień międzyresortowych. Skutki takiej zmiany mogłyby powodować, że przedsiębiorcy telekomunikacyjni, dostarczający sieci piątej generacji, byliby zmuszeni stosować środki przewidziane w § 3 rozporządzenia do zarządzanych przez siebie sieci wszystkich generacji, a nie - jak to było planowane i uzgadniane – tylko do sieci 5G.  Biorąc powyższe pod uwagę uważamy za konieczne takie przeredagowanie zdania wprowadzającego do § 3 projektu rozporządzenia, aby tekst rozporządzenia powrócił do pierwotnych założeń Projektodawcy, a środki przewidziane w § 3 znajdowały zastosowanie wyłącznie do sieci 5G. W tym celu możliwe jest przywrócenie zwrotu „*w ramach tej sieci*” lub nadanie zdaniu wstępnemu brzmienia rozpoczynającego się od: „*Przedsiębiorca telekomunikacyjny w zakresie w jakim dostarcza* dostarczający *sieć piątej generacji (…)”.* | Uwaga uwzględniona.  Tak, § 3 ma się odnosić tylko do sieci 5G.  Propozycja zmiany zapisu:  *„§ 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 przedsięwzięć, o których mowa w § 2 pkt 3-5, uwzględnia* ***w ramach tej sieci****: (…)”* |
| § 3 | PIIT | Ponownie wskazujemy, że w ocenie PIIT nie jest zasadne wprowadzanie wymogu uwzględniania Rekomendacji Pełnomocnika ds. Cyberbezpieczeństwa, które zostały wprowadzone do krajowego porządku prawnego w ramach ustawy o krajowym systemie cyberbezpieczeństwa. Jest to narzędzie odrębne i nieobejmujące 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. | Uwaga nieuwzględniona  Przedsiębiorcy telekomunikacyjni nie będą ich adresatami, a jedynie będą zobowiązani do uwzględniania ich podczas szacowania ryzyka w swojej organizacji. |
| § 3 | KIGEIT | **1. Uwaga do § 3**. Krytycznie oceniamy zmianę – jak się wydaje niezamierzoną – w zdaniu wprowadzającym w § 3 projektu rozporządzenia, która powoduje, że przedsiębiorca telekomunikacyjny będzie musiał stosować środki przewidziane w § 3 w stosunku do sieci wszystkich generacji (2G, 3G, 4G i 5G oraz następnych), podczas gdy z pierwotnego tekstu rozporządzenia jasno wynikało – i taka była intencja Projektodawcy – aby te środki były stosowane wyłącznie w odniesieniu do sieci piątej generacji. Zwracamy uwagę, że zdanie wprowadzające w § 3 w pierwszej opublikowanej wersji projektu rozporządzenia brzmiało (podkreślenie własne):  *§ 3. 1. Przedsiębiorca telekomunikacyjny dostarczający sieć piątej generacji (5G), określoną w dokumencie technicznym – Raporcie ETSI TR 121 915 V.15.0.0. (2019-10) w ramach tej sieci identyfikuje zagrożenia, ocenia prawdopodobieństwo ich wystąpienia, zapewnia i stosuje środki minimalizujące skutki wystąpienia zagrożeń, w zakresie bezpieczeństwa i integralności sieci i usług, uwzględniając: […]*  W najnowszej wersji projektu rozporządzenia ze zdania wprowadzającego w § 3 usunięto stwierdzenie „w ramach tej sieci”, co powoduje fundamentalną i niezamierzoną zmianę zakresu stosowania § 3 rozporządzenia, przeczącą wszystkim dotychczasowym ustaleniom poczynionym w toku konsultacji publicznych i uzgodnień międzyresortowych. Skutki takiej zmiany są oczywiste, mianowicie przedsiębiorcy telekomunikacyjni, dostarczający sieci piątej generacji, będą zmuszeni stosować środki przewidziane w § 3 rozporządzenia do zarządzanych przez siebie sieci wszystkich generacji, a nie - jak to było planowane  i uzgadniane – tylko do sieci 5G.  Biorąc powyższe pod uwagę uważamy za konieczne takie przeredagowanie zdania wprowadzającego do § 3 projektu rozporządzenia, być może przez przywrócenie stwierdzenia „w ramach tej sieci”, aby tekst rozporządzenia powrócił do pierwotnych założeń Projektodawcy, a środki przewidziane w § 3 znajdowały zastosowanie wyłącznie do sieci 5G. | Uwaga uwzględniona.  Tak, § 3 ma się odnosić tylko do sieci 5G.  Propozycja zmiany zapisu:  *„§ 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 przedsięwzięć, o których mowa w § 2 pkt 3-5, uwzględnia* ***w ramach tej sieci****: (…)”* |
| § 3 | PTI | W przypadku sieci 5G określono dodatkowe wymagania w formie § 3.  W ust. 1 odwołano się do 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.  Ust. 3 jest ogólny, nie ma żadnej miary i nic nie wnosi, zatem może zostać wykreślony, natomiast ust. 2 nie zawiera sformułowań wystarczająco jednoznacznych i tym samym wymaga przeredagowania zgodnie z poniższą uwagą szczegółową. | Uwaga częściowo uwzględniona.  Przedsiębiorcy telekomunikacyjni nie będą ich adresatami, a jedynie będą zobowiązani do uwzględniania ich podczas szacowania ryzyka w swojej organizacji.  Zapis ust. 3 został zmieniony - rozwinięto ust. 2. |
| § 3 | PTI | **Jest:**  *2) unikanie uzależnienia 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:**  Obecne brzmienie proponowanego przepisu par 3 ust.2 wydaje się niewystarczająco precyzyjne. “Unikanie uzależnienia” jest terminem zbliżonym do należytej staranności i może być rozumiany niejednoznacznie. W efekcie, bezpieczeństwo może być różnie rozumiane na poziomie poszczególnych operatorów (MNO), podczas gdy celem jest stworzenie minimalnego poziomu bezpieczeństwa w skali kraju, a nawet całej UE. Dodatkowo, nieprecyzyjny zapis może skutecznie uniemożliwić egzekwowanie obowiązków nałożonych na operatorów.  Naszym zdaniem właściwszy byłby wskazany wprost w rozporządzeniu obowiązek zachowania niezależności od jednego dostawcy (lub grupy dostawców “ryzykownych”) oraz szeroko rozumianej dywersyfikacji dostaw. W takim kierunku zmierzają też rozwiązania zawarte w dokumencie “5G Toolbox”, który Polska, jako państwo członkowskie UE powinna uwzględniać tworząc przepisy wykonawcze oraz procedury weryfikacji sposobu wdrożenia 5G w kraju. “5G Toolbox” pozwala na zdefiniowanie, czym jest “uzależnienie od jednego dostawcy” a także wskazuje proponowane rozwiązania na poziomie prawnym i technicznym. Propozycja brzmienia par 3 ust.2 odzwierciedla konkretne rozwiązania zawarte w “5G Toolbox”: SM05, SM06 i SM07.  Proponowana treść podpunktu 2a) stanowi przeniesienie zasady strategii “multi-vendor”. Zapewnienie, że każdy MNO posiada odpowiednią strategię wykorzystania wielu dostawców w różnych częściach sieci 5G (w tym w ramach Radio Access Network, Transmisyjnych Sieci Dostępowych oraz Core Network) w zakresie ograniczeń technicznych oraz wymogów interoperacyjności:   * W celu uniknięcia zależności od pojedynczego dostawcy (lub dostawców o podobnym poziomie ryzyka) * W celu uniknięcia zależności od dostawców uznanych jako tych o zwiększonym poziomie ryzyka (w rozumieniu SM03)   wydaje się kluczowe w zapewnieniu bezpieczeństwa sieci 5G. Jako priorytet jest też wskazywane w “5G Toolbox”. (SM05)  Zapewnienie odpowiedniej równowagi w udziale dostawców na poziomie narodowym w celu zagwarantowania elastyczności i ciągłości dostaw (usług telekomunikacyjnych ale też samej infrastruktury i jej elementów składowych) w przypadku niespodziewanych wydarzeń z udziałem jednego operatora lub jednego dostawcy, biorąc pod uwagę zmienne warunki geograficzne i populacyjne każdego z krajów członkowskich (SM06) zaadresowane zostało w proponowanym punkcie 2 b).  Dodatkowo, punkt 2c) stanowi odzwierciedlenie reguły konkurencyjności, która jest jednym z najlepszych środków zapobiegających nadmiernemu uzależnieniu od jednego dostawcy. Ważnym jest, aby ta konkurencyjność dotyczyła nie całej sieci, ale jej poszczególnych elementów składowych lub wręcz komponentów. Jest to propozycją zapobiegania tzw. “Vendor lock”, a więc przywiązaniu operatorów do rozwiązań jednego dostawcy dla wszystkich składowych danego elementu. Polscy operatorzy, inwestując duże środki w infrastrukturę 5G powinni obligatoryjnie stosować rozwiązania, które dadzą im (a nie dostawcom elementów) pełna kontrolę nad siecią i możliwość budowania jej w oparciu o rozwiązania różnych dostawców.  Punkt 2d) proponowanego rozwiązania jest odpowiedzią na najnowsze trendy w branży telekomunikacyjnej, w tym takich jak promowane 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 zakup tych składowych 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 uzasadnione. | Uwaga uwzględniona. |
| § 3 | ZIPSEE | W przypadku sieci 5G kluczowe zapisy określono w formie § 3.  W ust. 1 znajdujemy odwołanie do art. 33 ust. 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Odwołanie to budzi poważną wątpliwość, gdyż przedsiębiorstwa telekomunikacyjne są wyłączone z jej stosowania na podstawie art. 1 ust. 2 pkt 1. Poza tym, odwołanie to nie wyczerpuje zaleceń GC 01/2020 w zakresie certyfikacji.  Ust. 3 jest ogólny, nie ma żadnej miary i nic nie wnosi, zatem może zostać wykreślony. Szczególną uwagę zwracamy na treść ust. 2, który nie zawiera sformułowań wystarczająco jednoznacznych i tym samym wymaga przeredagowania. W związku z powyższym pozwalamy sobie zaproponować odpowiednie przeredagowanie przedmiotowego fragmentu projektowanego Rozporządzenia:  **Obecnie proponowany zapis ust. 2 brzmi:**  *2) unikanie uzależnienia od jednego producenta poszczególnych elementów sieci telekomunikacyjnej przy jednoczesnym zapewnieniu interoperacyjności usług;*  **W celu zapewnienia odpowiedniego jednoznacznego zapisu i uniknięcie ewentualnych sporów interpretacyjnych w tym zakresie, proponujemy:**  *2) obowiązek dywersyfikacji dostawców poszczególnych elementów sieci 5G, realizowany poprzez:*   1. *a) unikanie ryzyka zależności od jednego dostawcy lub zależności od grupy dostawców o zwiększonym poziomie ryzyka,* 2. *b) zapewnienie odpowiedniej równowagi w udziale dostawców na poziomie narodowym w celu zagwarantowania elastyczności i ciągłości dostaw,* 3. *c) zapewnienie konkurencyjności i otwartości rynku na dostawców poszczególnych elementów sieci,* 4. *d) stosowanie innowacyjnego i bezpiecznego oprogramowania funkcji sieciowych, nieza-leżnego od dostawców sprzętu, przy jednoczesnym zapewnieniu interoperacyjności usług.* 5. Tak jak wspomniałem powyżej, proponowany przez Ministerstwo Cyfryzacji przepis ust.2 wydaje się niewystarczająco precyzyjny. “Unikanie uzależnienia” jest terminem zbliżonym do należytej staranności i może być rozumiany niejednoznacznie. W efekcie, bezpieczeństwo może być różnie rozumiane na poziomie poszczególnych operatorów, podczas gdy celem jest stworzenie minimalnego poziomu bezpieczeństwa w skali kraju, a nawet całej UE. 6. Dodatkowo, nieprecyzyjny zapis może skutecznie uniemożliwić egzekwowanie obowiązków nałożonych na operatorów. Podniesione przez nas wątpliwości utrudnia stosowanie proponowanego zapisu zarówno operatorom telekomunikacyjnym jak i regulatorowi rynku. 7. Naszym zdaniem właściwszy byłby wskazany wprost w rozporządzeniu obowiązek zachowania niezależności od jednego dostawcy oraz szeroko rozumianej dywersyfikacji dostaw. Zaproponowana prze nas modyfikacja przedmiotowego ustępu jest naszym zdaniem zbieżna również z intencją dokumentu “5G Toolbox”, który Polska, jako państwo członkowskie UE powinna uwzględniać tworząc przepisy wykonawcze oraz procedury weryfikacji sposobu wdrożenia 5G w kraju. 8. Zapewnienie, że każdy MNO posiada odpowiednią strategię wykorzystania wielu dostawców w różnych częściach sieci 5G (w tym w ramach Radio Access Network, Transmisyjnych Sieci Dostępowych oraz Core Network) w zakresie ograniczeń technicznych oraz wymogów interoperacyjności w celu uniknięcia zależności od pojedynczego dostawcy oraz uznanych jako tych o zwiększonym poziomie ryzyka, wydaje się kluczowe w zapewnieniu bezpieczeństwa sieci 5G. 9. Proponowana przez nas lit. b) ust. 2 ma na celu zapewnienie odpowiedniej równowagi w udziale dostawców na poziomie narodowym w celu zagwarantowania elastyczności i ciągłości dostaw w przypadku niespodziewanych wydarzeń z udziałem jednego operatora lub jednego dostawcy 10. Z kolei lit. c) stanowi odzwierciedlenie reguły konkurencyjności, która jest jednym z najlepszych środków zapobiegających nadmiernemu uzależnieniu od jednego dostawcy. Ważnym jest, aby ta konkurencyjność dotyczyła nie całej sieci, ale jej poszczególnych elementów składowych lub wręcz komponentów. Jest to propozycja zapobiegania tzw. “Vendor lock”, a więc przywiązaniu operatorów do rozwiązań jednego dostawcy dla wszystkich składowych danego elementu. Polscy operatorzy, inwestując duże środki w infrastrukturę 5G powinni obligatoryjnie stosować rozwiązania, które dadzą im pełną kontrolę nad siecią i możliwość budowania jej w oparciu o rozwiązania różnych dostawców. 11. Proponowane przez nas zapisy mają na celu doprowadzić proponowane przez Ministerstwo zapisy do zbieżności z najnowszymi trendami w branży telekomunikacyjnej. Model, w którym cały sprzęt, oprogramowanie i integracja do danego elementu infrastruktury sieciowej dostarczane są od jednego dostawcy, jest sukcesywnie wypierany przez zakup tych składowych 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 szczególnie uzasadnione. Rozporządzenie powinno także nakładać wymóg dostosowywania rozwiązań do Open RAN oparty o jeden z powszechnie akceptowanych standardów np. w warunkach podpisania stosownych porozumień z jednostką samorządu terytorialnego, przedsiębiorstwem komunalnym, parkiem naukowo-technologicznym lub ośrodkami R&D itp. | Uwaga uwzględniona.  Przepis ust. 2 został zmieniony. |
| § 3 | PTPiREE | par. 3 ust. 1 pkt 1 nakazuje uwzględniać rekomendacje, o których mowa w art. 33 ust. 4 ustawy o KSC, ale nie przewiduje możliwości zgłaszania zastrzeżeń, o których mowa w art. 33 ust. 5 tej ustawy. Przedsiębiorcy telekomunikacyjni, o ile nie są operatorami usług kluczowych w rozumieniu KSC, zostaną więc pozbawieni możliwości dyskusji z rekomendacjami i wnioskowania o ich zmianę bądź uchylenie. Ponadto treść uzasadnienia projektu wskazuje, że stosowanie rekomendacji nie będzie w żaden sposób weryfikowane. | Uwaga nieuwzględniona.  Różnica wynika z faktu, że przedsiębiorcy telekomunikacyjni nie są częścią krajowego systemu cyberbezpieczeństwa i nie będą zobowiązani do stosowania rekomendacji, a jedynie do uwzględniania ich treści w ramach szacowania ryzyka i podejmowania działań na rzecz zabezpieczania swojej infrastruktury. |
| § 4 | PIIT | **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.  De facto spowoduje to opóźnienie stosowania rozporządzenia o 18 miesięcy, co nie jest intencją projektodawcy. |
| § 4 | KIGEIT | **Uwaga do § 4.** Proponujemy aby wydłużyć czas wejścia w życie przepisów § 2, tak aby wynosił 24 miesiące. | Uwaga nieuwzględniona.  Nie jest to zgodne z intencją projektodawcy. |
| § 4 | MEDIAKOM | Postulujemy zmianę § 4 rozporządzenia i ustalenie, że wchodzi ono w życie z upływem 12 miesięcy od dnia ogłoszenia. Należy zauważyć, że równolegle toczą się prace nad nową ustawą Prawo komunikacji elektronicznej, która zastąpi Prawo telekomunikacyjne. Z tą zmianą wiązać się będzie szereg obowiązków dla operatorów telekomunikacyjnych, w tym konieczność dostosowania prowadzonej działalności do nowych wymogów prawnych. Istnieje poważne ryzyko, że zbiegnie się w czasie konieczność wdrożenia nowych regulacji wynikających z nowej ustawy i niniejszego rozporządzenia. Będzie to poważne obciążenie dla operatorów, angażujące siły ludzkie i być może także finansowe. Stąd konieczność rozłożenia w czasie wdrożenia obowiązków wynikających z rozporządzenia. | Uwaga nieuwzględniona.  Nie jest to zgodne z intencją projektodawcy. |