**Zestawienie zgłoszonych uwag do projektu rozporządzenia Rady Ministrów rozporządzenie w sprawie planu działań przedsiębiorcy telekomunikacyjnego w sytuacjach szczególnych zagrożeń – konsultacje publiczne**

Uwagi zgłoszone przez:

* Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji
* Polska Izba Informatyki i Telekomunikacji
* Polska Izba Komunikacji Elektronicznej
* Krajowa Izba Komunikacji Ethernetowej
* Pracodawcy RP
* Konfederacja Lewiatan
* Urząd Komunikacji Elektronicznej

| **Jedn. red. projektu z dn. 29.06.2020** | **Treść uwag** | **Stanowisko MC**  (odniesienia do jedn. red. po przeredagowaniu projektu) | **Uzgodnienia** |
| --- | --- | --- | --- |
| **KIGEiT** | | | |
| § 6 ust. 1 pkt 2 | Przychylamy się do dotychczas zgłaszanych przez innych uczestników konsultacji uwag odnośnie braku podstaw prawnych do wprowadzenia do projektu rozporządzenia odniesienia do zagrożeń cyberbezpieczeństwa, w rozumieniu ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560 oraz 2019 r., poz. 2020) („u.k.s.c.”). Zgodnie bowiem z brzmieniem art. 1 ust. 2 pkt 1 u.k.s.c., ustawy o krajowym systemie cyberbezpieczeństwa nie stosuje się – w zakresie wymogów dotyczących bezpieczeństwa i zgłaszania incydentów – do przedsiębiorców telekomunikacyjnych, w wypadku których kwestie te regulują przepisy ustawy Prawo telekomunikacyjne (art. 175-175d p.t.). W tym kontekście należy również wskazać na bezpodstawność obowiązku nakładanego na przedsiębiorcę telekomunikacyjnego przeprowadzania analiz i ocen na podstawie „informacji o zagrożeniach cyberbezpieczeństwa publikowanych przez zespoły reagowania na incydenty bezpieczeństwa komputerowego działające na poziomie krajowym”. Wprawdzie przepis projektu rozporządzenia w § 6 ust. 1 pkt 2 odnosi się do „informacji” a nie „rekomendacji”, w praktyce te pojęcia mogą być używane zamiennie i granica między nimi może się zatrzeć. W szczególności, że w uzasadnieniu Projektu na s. 12 wyjaśnia się, że wprawdzie u.k.s.c. nie obejmuje przedsiębiorców telekomunikacyjnych, co oznacza, że nie są oni elementem krajowego systemu cyberbezpieczeństwa i nie mają obowiązków związanych z uczestnictwem w tym systemie, to jednak, przedsiębiorcy telekomunikacyjni powinni uwzględniać informacje z analizy incydentów. | Uwaga uwzględniona.  Treść przepisu dostosowano do brzmienia art. 176a ust. 2 pkt 4 ustawy – Prawo telekomunikacyjne. |  |
| § 6 ust. 1 pkt 2 | Nadto postanowienia § 6 ust. 1 pkt 2 Projektu zostały poszerzone o konieczność uwzględniania w analizie „raportów Agencji Unii Europejskiej do spraw Cyberbezpieczeństwa (ENISA)”. W tym miejscu należy podkreślić, że rozszerzenie przewidziane w § 6 ust. 1 pkt 2 Projektu wykracza poza delegację ustawową przewidzianą w art. 176a ust. 5 p.t. W treści przepisu art. 176a ust. 5 p.t. brak jest bowiem odniesienia do ENISA, analogicznie jak w treści art. 175d p.t. Należy jednak pokreślić, że delegacja zawarta w art. 175d p.t. odnosi się do innego aktu prawnego, tj. Rozporządzenie 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 i nie ma zastosowania do upoważnienia ustawowego obejmującego wydanie Projektu przez Radę Ministrów. Z uwagi na powyższe postulujemy wykreślenie z projektu rozporządzenia odwołania do zagrożeń cyberbezpieczeństwa uregulowanych u.k.s.c. oraz odniesienia do raportów ENISA jako czynników uwzględnianych przy analizie ryzyk przy sporządzaniu planów działań przedsiębiorcy telekomunikacyjnego w sytuacjach szczególnych zagrożeń. | Uwaga uwzględniona.  Zaproponowano brzmienie: „ … na podstawie dostępnych informacji o zagrożeniach cyberbezpieczeństwa” |  |
| § 7 ust. 1 pkt 9 | W nawiązaniu do uwag zgłoszonych do wcześniejszych wersji projektu przedmiotowego rozporządzenia, należy podkreślić, że projekt rozporządzenia z dnia 29.06.2020 w zaproponowanej postaci zobowiązywałby przedsiębiorcę telekomunikacyjnego do powielania w planie procedury udostępniania urządzeń telekomunikacyjnych przedsiębiorcy innym przedsiębiorcom telekomunikacyjnym lub właściwym podmiotom i służbom, niezbędnych do przeprowadzenia akcji ratowniczych, ustanowionej wcześniej i posiadanej już przez przedsiębiorcę telekomunikacyjnego. Wydaje się, że jeżeli przedsiębiorca telekomunikacyjny posiada taką procedurę w postaci dokumentu określającego tę procedurę, to nie ma potrzeby powielania tego dokumentu w planie, wystarczy w planie wskazać ten dokument i odwołać się do tego dokumentu. Proponowana zmiana spowoduje, że przedsiębiorca telekomunikacyjny nieposiadający dokumentu określającego tę procedurę, będzie obowiązany opisać ją w planie, natomiast przedsiębiorca telekomunikacyjny posiadający taki dokument, będzie obowiązany wskazać go w planie. Przedmiotowa procedura może być istotna dla organów uzgadniających plan, co jednak nie przesądza o potrzebie, czy wręcz obowiązku narzucanym przepisem prawa, powielania dokumentów przez przedsiębiorcę. Wydaje się, że nie ma przeszkód udostępnienia takiej procedury podmiotom zainteresowanym, a w szczególności właściwym podmiotom i służbom, których ta procedura dotyczy.  W tej sytuacji proponuje się nadać § 7 ust. 1 pkt 9 projektu rozporządzenia następujące brzmienie:  *„9) procedurę udostępniania urządzeń telekomunikacyjnych przedsiębiorcy innym przedsiębiorcom telekomunikacyjnym lub właściwym podmiotom i służbom, niezbędnych do przeprowadzenia akcji ratowniczych albo wskazanie dokumentu określającego tę procedurę*;”. | Uwaga nieuwzględniona.  Samo wskazanie w planie dokumentu określającego procedurę nie jest wystarczające dla organów uzgadniających plan. Nie będą one w ten sposób posiadały wiedzy co ta procedura zawiera; będą znać tylko nazwę dokumentu, który tę procedurę zawiera. |  |
| § 7 ust. 1 pkt 15 | W § 7 ust. 1 pkt 15 projektu rozporządzenia określono, że „…Plan zawiera: … 15) wykaz umów dotyczących realizacji zadań na rzecz obronności państwa”. Jak należy się domyślać wykaz ten powinien być zamieszczany w planie przedsiębiorcy, który zawarł takie umowy, bowiem w przeciwnym razie przedsiębiorca nie ma co zamieścić w przedmiotowym wykazie. Oczywiście przepis ten można rozumieć w ten sposób, że jeśli przedsiębiorca nie ma umów, to ich nie wykazuje, ale jeżeli tak jest rozumiany ten przepis, to tym bardziej można przepis doprecyzować tak, aby był jednoznaczny i nie dawał możliwości innej interpretacji. W tej sytuacji proponuje się nadać § 7 ust. 1 pkt 15 projektu rozporządzenia następujące brzmienie:  „*15) wykaz umów dotyczących realizacji zadań na rzecz obronności państwa, o ile zostały zawarte*” | Uwaga nieuwzględniona.  Nie sporządza się wykazu umów, które nie zostały zawarte (w odpowiednim miejscu planu proponuje się wskazać: „*Brak umów dotyczących zadań na rzecz obronności państwa*”.  Ponadto wprowadzono poprawkę, że obowiązek ten dotyczy tylko przedsiębiorców o szczególnym znaczeniu gospodarczo-obronnym. |  |
| § 11 pkt 2 | W § 11 projektu rozporządzenia określono termin sporządzania planu, jako 12 miesięcy: 1) od dnia wejścia w życie rozporządzenia albo 2) od aktualizacji okresowej wynikającej z przepisów dotychczasowych. Wydaje się, że punkt 2 tego paragrafu jest nieprecyzyjny, bowiem nie określa terminu. W związku z powyższym proponuje się nadać § 11 pkt 2 projektu rozporządzenia następujące brzmienie:  *„2) od terminu aktualizacji okresowej wynikającej z przepisów dotychczasowych*” | Uwaga uwzględniona.  Propozycja: „od dnia upływu terminu aktualizacji okresowej planu sporządzonego przez przedsiębiorcę na podstawie przepisów dotychczasowych” |  |
| **Polska Izba Informatyki i Telekomunikacji** | | | |
| § 6 ust. 1 pkt 2 | PIIT na poprzednich etapach konsultacji publicznych postulował usunięcie z projektu odwołania do konieczności analizowania informacji o zagrożeniach cyberbezpieczeństwa, które znajdowało się w ówczesnym § 4 ust. 1 pkt 2.  Uwaga ta nie została uwzględniona i podtrzymujemy ją, przedstawiając w tym zakresie dodatkową, dalej idącą argumentację:  • Brak jest podstaw prawnych do wprowadzenia do Projektu rozporządzenia odniesienia do „zagrożeń cyberbezpieczeństwa”, w rozumieniu ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560 oraz 2019 r., poz. 2020) („u.k.s.c.”).  • Upoważnienie ustawowe, w zakresie, w jakim nawiązuje do siatki pojęciowej używanej w u.k.s.c. nie odnosi się bowiem do pojęcia „zagrożeń cyberbezpieczeństwa”, ale wyłącznie do pojęcia „incydentów”.  • Dla rozszerzającego podejścia do wykonania upoważnienia, nie uprawniają jednocześnie przesłanki racjonalności, do których odniesiono się w uzasadnieniu wskazując, że wprawdzie u.k.s.c. nie obejmuje przedsiębiorców telekomunikacyjnych, co oznacza, że nie są oni elementem krajowego systemu cyberbezpieczeństwa i nie mają obowiązków związanych z uczestnictwem  w tym systemie, to jednak racjonalnym wydaje się jednak, aby wykonując swoją działalności telekomunikacyjną przeprowadzali analizy incydentów i zabezpieczali swoje sieci i usługi.  • Szczególnie, że zgodnie z brzmieniem art. 1 ust. 2 pkt 1 u.k.s.c., ustawy o krajowym systemie cyberbezpieczeństwa nie stosuje się – w zakresie wymogów dotyczących bezpieczeństwa  i zgłaszania incydentów – do przedsiębiorców telekomunikacyjnych, w wypadku których kwestie te regulują przepisy ustawy Prawo telekomunikacyjne (art. 175-175d p.t.).  • Ponadto także, kwestie identyfikacji i adresowania pełnego spektrum zagrożeń są już uwzględnione w ramach obowiązków wynikających z aktu wykonawczego do art. 175d PT, do którego zresztą nawiązuje także samo projektowane rozporządzenie do art. 176a PT.  • W tym kontekście, należy tym bardziej wskazać na bezpodstawność obowiązku nakładanego na przedsiębiorcę telekomunikacyjnego w zakresie przeprowadzania analiz i ocen na podstawie  „informacji o zagrożeniach cyberbezpieczeństwa publikowanych przez zespoły reagowania na incydenty bezpieczeństwa komputerowego działające na poziomie krajowym”.  • Dodatkowo, należy zauważyć, że postanowienia § 6 ust. 1 pkt 2 Projektu zostały poszerzone  o konieczność uwzględniania w analizie „raportów Agencji Unii Europejskiej do spraw Cyberbezpieczeństwa (ENISA)”. W tym miejscu należy podkreślić, że rozszerzenie przewidziane w § 6 ust. 1 pkt 2 Projektu także wykracza poza delegację ustawową przewidzianą w art. 176a ust. 5 p.t. W treści przepisu art. 176a ust. 5 p.t. brak jest bowiem odniesienia do ENISA, analogicznie, jak w treści art. 175d p.t. Należy jednak pokreślić, że delegacja zawarta w art. 175d p.t. odnosi się do innego aktu prawnego, tj. 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 i nie ma zastosowania do upoważnienia ustawowego obejmującego wydanie Projektu przez Radę Ministrów.  Z uwagi na powyższe:  • Wnosimy o doprowadzenie do pełnej zgodności projektowanego rozporządzenia z upoważnieniem ustawowym, co można zrealizować poprzez usunięcie nadmiarowego odwołania do „zagrożeń cyberbezpieczeństwa”, w szczególności w sytuacji, gdy pojęcie to odnoszone jest do siatki pojęciowej ustawy KSC.  • Równolegle, podtrzymujemy uwagę przedstawioną w stanowisku PIIT z lutego oraz maja br. dotyczącą odwołania do konieczności uwzględniania w toku analiz także informacji o zagrożeniach publikowanych przez CSIRT, a w wersji z 29.06.2020 także oraz raportów Agencji Unii Europejskiej do spraw Cyberbezpieczeństwa (ENISA). Tym samym postulujemy usunięcie z pkt 2 frazy: „w szczególności na podstawie informacji o zagrożeniach cyberbezpieczeństwa publikowanych przez zespoły reagowania na incydenty bezpieczeństwa komputerowego działające na poziomie krajowym oraz raportów Agencji Unii Europejskiej do spraw Cyberbezpieczeństwa (ENISA).”.  W naszej ocenie, poza wyżej sygnalizowanymi uwagami o charakterze formalnym i prawnym, zapis będzie stwarzał poważne trudności w uwzględnianiu publikowanych przez te zespoły informacji w ramach procedur przygotowania i uzgadniania planu. Informacje te nie są bowiem ściśle unormowane, w takim sensie, że nie pojawiają się w jasno określonych i przewidywalnych okresach i dotyczą szerokiego spektrum zagadnień. Mogą mieć natomiast charakter wpadkowy, dotyczący występujących w danym momencie zagrożeń. Plany działania są natomiast dokumentami generalnymi o długotrwałej i skomplikowanej procedurze przygotowania i przyjmowania. Tym samym na poziomie wymagań prawnych w naszej ocenie takie wymaganie należy usunąć, zakładając jednocześnie, że kompleksowa analiza zagrożeń cyberbezpieczeństwa, o której mowa w ust. 1 pkt 2 zostanie wykonana z uwzględnieniem wszelkich źródeł, a sam fakt, możliwości publikowania informacji o zagrożeniach przez zespoły reagowania na incydenty i reagowania na takie publikacje, o ile dotyczą działalności przedsiębiorców telekomunikacyjnych, może być uwzględniany przez przedsiębiorców w planie w zakresie, w jakim dotyczy on cyberbezpieczeństwa. | Uwaga uwzględniona.  Treść przepisu dostosowano do brzmienia art. 176a ust. 2 pkt 4 ustawy – Prawo telekomunikacyjne.  Zaproponowano brzmienie: „ … na podstawie dostępnych informacji o zagrożeniach cyberbezpieczeństwa” |  |
| § 7 ust. 1 pkt 9 | W nawiązaniu do uwag zgłoszonych do wcześniejszych wersji projektu przedmiotowego rozporządzenia, należy podkreślić, że projekt rozporządzenia z dnia 29.06.2020 w zaproponowanej postaci zobowiązywałby przedsiębiorcę telekomunikacyjnego do powielania w planie procedury udostępniania urządzeń telekomunikacyjnych przedsiębiorcy innym przedsiębiorcom telekomunikacyjnym lub właściwym podmiotom i służbom, niezbędnych do przeprowadzenia akcji ratowniczych, ustanowionej wcześniej i posiadanej już przez przedsiębiorcę telekomunikacyjnego. Wydaje się, że jeżeli przedsiębiorca telekomunikacyjny posiada taką procedurę w postaci dokumentu określającego tę procedurę, to nie ma potrzeby powielania tego dokumentu w planie, wystarczy  w planie wskazać ten dokument i odwołać się do tego dokumentu. Proponowana zmiana spowoduje, że przedsiębiorca telekomunikacyjny nieposiadający dokumentu określającego tę procedurę, będzie obowiązany opisać ją w planie, natomiast przedsiębiorca telekomunikacyjny posiadający taki dokument, będzie obowiązany wskazać go w planie. Przedmiotowa procedura może być istotna dla organów uzgadniających plan, co jednak nie przesądza o potrzebie, czy wręcz obowiązku narzucanym przepisem prawa, powielania dokumentów przez przedsiębiorcę. Wydaje się, że nie ma przeszkód udostępnienia takiej procedury podmiotom zainteresowanym, a w szczególności właściwym podmiotom i służbom, których ta procedura dotyczy.  W tej sytuacji proponuje się nadać § 7 ust. 1 pkt 9 projektu rozporządzenia następujące brzmienie:  „*9) procedurę udostępniania urządzeń telekomunikacyjnych przedsiębiorcy innym przedsiębiorcom telekomunikacyjnym lub właściwym podmiotom i służbom, niezbędnych do przeprowadzenia akcji ratowniczych albo wskazanie dokumentu określającego tę procedurę*;” | Uwaga nieuwzględniona.  Samo wskazanie w planie dokumentu określającego procedurę nie jest wystarczające dla organów uzgadniających plan. Nie będą one w ten sposób posiadały wiedzy co ta procedura zawiera; będą znać tylko nazwę dokumentu, który tę procedurę zawiera. |  |
| § 7 ust. 1 pkt 15 | W § 7 ust. 1 pkt 15 projektu rozporządzenia określono, że „…Plan zawiera: … 15) wykaz umów dotyczących realizacji zadań na rzecz obronności państwa”. Jak należy się domyślać wykaz ten powinien być zamieszczany w planie przedsiębiorcy, który zawarł takie umowy, bowiem  w przeciwnym razie przedsiębiorca nie ma co zamieścić w przedmiotowym wykazie. Oczywiście przepis ten można rozumieć w ten sposób, że jeśli przedsiębiorca nie ma umów, to ich nie wykazuje, ale jeżeli tak jest rozumiany ten przepis, to tym bardziej można przepis doprecyzować tak, aby był jednoznaczny i nie dawał możliwości innej interpretacji.  W tej sytuacji proponuje się nadać § 7 ust. 1 pkt 15 projektu rozporządzenia następujące brzmienie:  „*15) wykaz umów dotyczących realizacji zadań na rzecz obronności państwa, o ile zostały zawarte*”. | Uwaga nieuwzględniona.  Nie sporządza się wykazu umów, które nie zostały zawarte (w odpowiednim miejscu planu proponuje się wskazać: „*Brak umów dotyczących zadań na rzecz obronności państwa*”.  Ponadto wprowadzono poprawkę, że obowiązek ten dotyczy tylko przedsiębiorców o szczególnym znaczeniu gospodarczo-obronnym. |  |
| § 10 ust. 2 pkt 3 | W projektowanym brzmieniu § 8 ust. 2 pkt 3 zaproponowano bardzo istotną zmianę przesłanek aktualizacji planu. Dotychczas (obecne przepisy i projekt z dnia 24.01.2020) przesłanką była „istotna zmiana danych dotyczących szczególnych zagrożeń”.  Proponowane jest natomiast wprowadzenie zapisu wskazującego na istotną zmianę:  • danych dotyczących zagrożeń, o których mowa w § 6 ust. 1 pkt 1, czyli szczególnych zagrożeń środowiskowych lub fizycznych na obszarze, na którym wykonuje działalność telekomunikacyjną, oraz oceny ich wpływu na bezpieczeństwo i integralność wykorzystywanej infrastruktury telekomunikacyjnej i świadczonych usług, na podstawie danych udostępnionych przez właściwych terytorialnie wojewodów;  • zagrożeń cyberbezpieczeństwa,  • sytuacji w zakresie występowania naruszeń bezpieczeństwa lub integralności infrastruktury telekomunikacyjnej lub świadczonych usług;  W naszej ocenie w sposób zbyt szeroki i oceny dookreślono nowe przesłanki aktualizacji planu.  W praktyce zapis wskazujący, że plan podlega aktualizacji w przypadku wystąpienia okoliczności wpływających na jego zawartość, a w szczególności istotnej zmiany zagrożeń cyberbezpieczeństwa, oznaczać może, że każdy nowy rodzaj występowania ataku DDoS czy phishningu w sieci przedsiębiorcy telekomunikacyjnego jest istotny i powinien podlegać aktualizacji. Powodować to może stan permanentnej aktualizacji planu związany z zagrożeniami w zakresie cyberbezpieczeństwa. Postulujemy przywrócenie brzmienia z dotychczasowego rozporządzenia. | Uwaga uwzględniona.  Skreślono „zagrożenia cyberbezpieczeństwa”.  Odniesiono się do: „sytuacji w zakresie występowania naruszeń bezpieczeństwa lub integralności infrastruktury telekomunikacyjnej lub świadczonych usług, w tym związanych z wystąpieniem incydentów, o których mowa w art. 6 ust. 1 pkt 2;”, zgodnie z intencją art. 176a ust. 2 pkt 4 ustawy – Prawo telekomunikacyjne |  |
| § 10 ust. 3 | § 10 ust. 3 projektu proponuje się nadać brzmienie:  „*3. Przedsiębiorca dokonuje aktualizacji planu po wystąpieniu okoliczności, o których mowa w ust. 2 oraz udostępnia zaktualizowaną część planu zainteresowanym organom uzgadniającym plan, zgodnie z § 9*.”.  Uzasadnienie:  Po dokonaniu aktualizacji bieżącej planu należy udostępnić zaktualizowaną część planu tym organom, których ta aktualizacja dotyczy i które są zainteresowane tą aktualizacją, tj. na zasadach określonych w § 9 projektu. Nie ma natomiast potrzeby udostępniania zaktualizowanej części planu wszystkim organom uzgadniającym plan. | Uwaga nieuwzględniona.  Aktualizacja dotyczy różnych obszarów. Każdy z organów uzgadniających powinien otrzymać zaktualizowany plan, gdyż nie będzie wiedział, że podlegał on aktualizacji. |  |
| § 11 | W § 11 projektu rozporządzenia określono termin sporządzania planu, jako 12 miesięcy: 1) od dnia wejścia w życie rozporządzenia albo 2) od aktualizacji okresowej wynikającej z przepisów dotychczasowych.  Opracowanie planu zgodnie z nowymi wymaganiami będzie wymagało uprzedniego i szerokiego przygotowania nowych analiz zagrożeń, co powoduje realne zagrożenie, że dla przedsiębiorców telekomunikacyjnych którzy będą musieli uwzględnić dodatkowe zagadnienia w zakresie zagrożeń cyberbezpieczeństwa po wejściu w życie nowelizacji rozporządzenia, termin 12 miesięcy będzie terminem zbyt krótkim na sporządzenie, uwzględnienie i wprowadzenie do stosowania wymaganych zmian. Z uwagi na spodziewane wydłużenie procesu uzgadniania planów związane z rozszerzeniem ich zakresu, Izba postuluje wydłużenie okresu do 18 miesięcy.  Ponadto, zdaniem Izby dookreślenia wymaga wyrażenie „sporządza plan”. Czytając literalnie termin 12 miesięcy może być rozumiany jedynie w znaczeniu sporządzenia planu po stronie przedsiębiorcy telekomunikacyjnego, bez konieczności uzgodnieni i wprowadzenia do stosowania. I może nie obejmować swym zakresem, oprócz czynności „sporządzenia planu”, czynności na „uzgodnienia” i „wprowadzenia do stosowania” planu. W sytuacji, w której działanie związane ze sporządzeniem planu ma obejmować zarówno: sporządzenie, uzgodnienie i wprowadzenie do stosowania planu, termin 12 miesięcy jest stanowczo za krótki, a ponadto wymaga dookreślenia, co obejmuje swoim zakresem wyrażenie sporządza plan.  Wydaje się także, że punkt 2 tego paragrafu § 11 jest nieprecyzyjny, bowiem nie określa terminu. Izba proponuje doprecyzowanie w tym punkcie.  PIIT proponuje także, aby wprowadzić normę do rozporządzenia wskazującą, że obecny plan zachowuje ważność do czasu sporządzenia nowego planu zgodnie z przepisami projektowanego rozporządzenia. Przedsiębiorcy chcą mieć pewność w drodze rozporządzenia, że obecne plany nie stracą aktualności do czasu sporządzenia nowych. Wynika to z faktu, że proces przygotowania jest bardzo czasochłonny i aby przygotować plan, który kończy się w np. w lutym 2021 należy z ponad rocznym wyprzedzeniem podjąć czynności procesowe do jego sporządzenia.  W związku z powyższym PIIT proponuje nadać dotychczasowemu § 11 projektu rozporządzenia ust. 1 oraz dodać ust. 2 w brzmieniu jak poniżej:  „§ 11. 1. Przedsiębiorca sporządza plan, uzgadnia i wprowadza do stosowania, zgodnie  z przepisami niniejszego rozporządzenia w terminie 18 miesięcy:  1) od dnia wejścia w życie rozporządzenia albo  2) od terminu aktualizacji okresowej wynikającej z przepisów dotychczasowych  – w zależności od tego, który z tych terminów nastąpi później.  **2. Plany przedsiębiorców sporządzone, uzgodnione i wprowadzone do stosowania, przed wejściem w życie niniejszego rozporządzenia zachowują aktualność do upływu terminu ich sporządzenia, o którym mowa w ust. 1.”.** | Uwaga uwzględniona.  Przepisy zostały przeredagowane. |  |
| **PIKE** | | | |
| § 6 | Analizę zagrożeń cyberbezpieczeństwa z ustawy o krajowym systemie cyberbezpieczeństwa (KSC). PIKE w dalszym ciągu podkreśla, że przedsiębiorcy telekomunikacyjni w zakresie zagrożenia dot. cyberbezpieczeństwa i świadczenia przez siebie usług telekomunikacyjnych są uregulowani w Dziale VIIA Pt „Bezpieczeństwo i integralność sieci i usług telekomunikacyjnych”, a nie w KSC. Projektowana regulacja de facto rozszerza obowiązki przedsiębiorców telekomunikacyjnych o kwestie związane z cyberbezpieczeństwem z KSC. Tymczasem przepisy KSC wyraźnie wskazują, że nie mają one zastosowania do większości przedsiębiorców telekomunikacyjnych (tylko do tych, którzy świadczą dodatkowo usługi wskazane w KSC). Cyberzagrożenia z KSC nie dotyczą działalności telekomunikacyjnej, o której mowa w art. 176a Pt, tak więc ten zapis projektu rozporządzenia (i inne związane z nim propozycje przepisów) powinny być usunięte jako sprzeczne zarówno z Pt jak i z KSC. W zakresie cyberbezpieczeństwa sieci telekomunikacyjnych oraz usług telekomunikacyjnych właściwe jest odesłanie do art. 175-175d Pt. Z tego względu podtrzymuję poprzednie stanowisko Izby o konieczności usunięcia z projektu rozporządzenia postanowień związanych z cyberbezpieczeństwem. | Uwaga uwzględniona.  Treść przepisu dostosowano do brzmienia art. 176a ust. 2 pkt 4 ustawy – Prawo telekomunikacyjne. |  |
| § 6 | Za szczególnie niekorzystną zmianę należy uznać rozszerzenie prac nad planem działań z infrastruktury telekomunikacyjnej stanowiącej własność przedsiębiorcy telekomunikacyjnego na infrastrukturę telekomunikacyjną przez niego wykorzystywaną. Zmiana ta powoduje, że przedsiębiorca musi uwzględnić w planach również cudze sieci, które np. dzierżawi lub korzysta z kolokacji. To rozszerzenie jest błędne, gdyż przedsiębiorca telekomunikacyjny w ramach realizacji planu działań może jedynie wykonywać zadania na własnej sieci, a nie wolno mu modyfikować czy naprawiać cudzej infrastruktury telekomunikacyjnej. Zapis ten narusza wszystkie umowy międzyoperatorskie, które nie przewidują takiego rozszerzenia udostępniania sieci telekomunikacyjnych. Ponadto, należy wziąć pod uwagę także fakt, że koszty zapewnienia cyberbezpieczeństwa tych elementów infrastruktury stanowią koszt jej utrzymania. Operator korzystający z infrastruktury pokrywa w odpowiedniej części koszty utrzymania infrastruktury, dlatego zapewnienie cyberbezpieczeństwa powinno należeć do obowiązków operatora odpowiedzialnego za utrzymanie sieci. | Uwaga nieuwzględniona.  Przedsiębiorca, który dzierżawi sieć (wykorzystuje ją) powinien brać pod uwagę zagrożenia, które mogą dotyczyć takiej sieci i wpływać na bezpieczeństwo świadczonych przez siebie usług (z wykorzystaniem takiej dzierżawionej sieci). Nie chodzi o jej modyfikację czy naprawę, ale o uwzględnienie czynników, które mogą wpływać na świadczone usługi i ich bezpieczeństwo. Kwestie dotyczące utrzymania sieci i ich bezpieczeństwa powinny być przedmiotem umowy pomiędzy przedsiębiorcami: właścicielem sieci i dzierżawiącym sieć. Niemniej jednak to przedsiębiorca dzierżawiący odpowiada za jakość usług i ich bezpieczeństwo. |  |
| § 7 ust. 2 | W projekcie rozporządzenia wprowadzono nowe zapisy o rozszerzeniu planów działań opracowywanych przez przedsiębiorców o szczególnym znaczeniu gospodarczo-obronnym w § 7 ust. 2. Zdaniem Izby brak jest powodu do wprowadzenia tej nowej regulacji zwłaszcza na obecnym poziomie uzgodnień projektu rozporządzenia. PIKE wskazuje, że ten nowy obowiązek jest znaczącym obciążeniem dla przedsiębiorców telekomunikacyjnych i nie powinien on być wykazywany w planie działań, lecz w indywidualnych relacjach tych przedsiębiorców telekomunikacyjnych z organami. Nowe obowiązki to:  - wykaz elementów sieci telekomunikacyjnej oraz sposób ich przygotowania do zapewnienia telekomunikacji na potrzeby właściwych podmiotów i służb wraz z procedurami uruchamiania tych elementów,  - wykaz obiektów i elementów infrastruktury telekomunikacyjnej dostosowanych do współpracy z ruchomymi urządzeniami telekomunikacyjnymi używanymi przez podmioty z art. 4 Pt wraz z procedurami ich użycia.  Jak widać są to ogromne nowe obowiązki, w dodatku tak szczegółowe, że nie ma możliwości ich uzgodnienia w terminie 30 dni z organami, ani nawet opracować w rozsądnym terminie samego planu działań z tymi zadaniami. Co więcej, zadania te są tak rozległe, że będą często podlegały zmiano, przez co cały plan działań będzie musiał bezustannie podlegać aktualizacji.  Ponadto w projekcie rozporządzenia wprowadzono nowy obowiązek w § 7 ust. 1 pkt 4, który budzi sprzeciw Izby. W przepisie tym nakazuje się przedsiębiorcy opisywać dodatkowo przewidzianych skutków zakłócenia działania elementów kluczowych infrastruktury. Zdaniem Izby obowiązek ten jest nadmiarowy i nie ma żadnego merytorycznego uzasadnienia. Plan działań ma opisywać podejmowane przez operatora działania w wypadku wystąpienia określonych sytuacji, a nie opisywać przypuszczenia przedsiębiorcy telekomunikacyjnego jakie skutki mogą wywołać awarie elementów jego infrastruktury. | Uwaga nieuwzględniona.  Wprowadzone zapisy nie są nowe w świetle istniejących przepisów. Obecnie przepisy te są zawarte w § 5 pkt 9 i 13 rozporządzenia Rady Ministrów z dnia 4 stycznia 2010 r. w sprawie planu działań przedsiębiorcy telekomunikacyjnego w sytuacjach szczególnych zagrożeń (Dz. U. poz. 77, z późn. zm.).  Zostały ponownie wprowadzone do projektu na wniosek MON. |  |
| § 8 | Izba pozytywnie odnosi się do redukcji liczby organów, z którymi należy uzgadniać plany działań w § 6 projektu rozporządzenia. W dalszym ciągu zdaniem PIKE należy jednak doprecyzować formułę tych uzgodnień, poprzez wskazanie skutków przewlekłości działań organów. Właściwe wydaje się przyjęcie, że w przypadku niezgłoszenia uwag przez te organy w ciągu 30 dni należy traktować jako akceptację przez nich planu działań. Obecnie bezczynność tych organów pozostaje bez konsekwencji dla nich, a utrudnia działalność operatorów, narażają ich na kary za brak aktualnych planów działań. | Uwaga nieuwzględniona.  Brak jest konkretnych przykładów/informacji dotyczących bezczynności organów w związku z uzgadnianiem planów. Ponadto jest to materia ustawowa. |  |
| § 10 | Izba popiera wprowadzone zmiany w zakresie ujednolicenia mechanizmu aktualizacji planów działań. Nowy zapis rezygnuje z podziału aktualizacji okresowych i bieżących, przez co przedsiębiorcy telekomunikacyjni będą mogli elastycznie dokonywać koniecznych aktualizacji bez obaw, że będą musieli dublować swoją pracę z powodu upływu terminu trzech lat ostatniej aktualizacji.  Jednocześnie izba popiera wprowadzenie obowiązku przekazywania przez organy przedsiębiorcom telekomunikacyjnym informacji niezbędnych do przygotowania tych planów działań. | To jest opinia (pozytywna). |  |
| **KIKE** | | | |
| § 2 ust. 1 pkt 1) | Izba ponownie podkreśla konieczność zwiększenia pułapu zwolnień od wykonywania planów działań dla małych i średnich przedsiębiorców. Proponowany próg 10 mln zł jest krokiem w dobrą stronę (obecny próg to zaledwie 4 mln zł rocznego przychodu), ale niewystarczającym. Takiej wielkości przychód wyłącza z obowiązku właściwie tylko mikroprzedsiębiorców, podczas gdy powinien objąć również małych przedsiębiorców (10 mln euro obrotu netto), a w stosunku do średnich przedsiębiorców (50 mln euro obrotu netto) być stosowany częściowo. W opinii Izby taka zmiana byłaby jak najbardziej zgodna z przepisami Konstytucji biznesu, w tym art. 67 i 68 ustawy Prawo przedsiębiorców (Prawo przedsiębiorców). Większa część przychodu przedsiębiorców telekomunikacyjnych jest pochłaniana przez koszty zarówno utrzymania sieci telekomunikacyjnej czy opłaty międzyoperatorskie i z nadawcami jak i podatki i opłaty publiczne oraz ogólne koszty prowadzenia przedsiębiorstwa. Stąd w telekomunikacji dochody są relatywnie niskie w porównaniu do przychodów. Dlatego też pułap 10 mln zł zwolnienia z obowiązku można uznać za wysoki tylko w stosunku do przedsiębiorstw telekomunikacyjnych właściwie nie posiadających swoich sieci (a te są i tak zwolnione z tego obowiązku na podstawie § 2 ust. 1 pkt 3, 4 i 7 projektu rozporządzenia). | Uwaga nieuwzględniona.  Zastosowane kryteria pozwalają obniżyć liczbę przedsiębiorców zobowiązanych do sporządzenia planu do ok. 100. Progi oparto na faktycznych danych UKE. |  |
| § 6 ust. 1 pkt 1) | Analiza zagrożeń środowiskowych i fizycznych oraz ich wpływu na bezpieczeństwo  i integralność własnej sieci a także świadczonych usług, w tym usług polegających na rozprowadzaniu i rozpowszechnianiu programów radiofonicznych lub telewizyjnych oraz usługi dostarczania udogodnień towarzyszących. Usługi te są wyłączone z regulacji jedynie w sytuacji, gdy są jedynymi usługami świadczonymi przez przedsiębiorcę telekomunikacyjnego, co wskazuje wyraźnie, że ich świadczenie nie jest związane z planem działań w sytuacji szczególnych zagrożeń. Z tego względu regulacja działań podejmowanych w sytuacji szczególnych zagrożeń powinna być ograniczona do usług telefonicznych oraz dostępu do sieci Internet. | Uwaga uwzględniona.  Wprowadzono nowy przepis § 3 pkt 1. |  |
| § 6 ust. 1 pkt 2) | Analiza zagrożeń cyberbezpieczeństwa z ustawy o krajowym systemie cyberbezpieczeństwa (KSC). Izba ponownie podkreśla, że przedsiębiorcy telekomunikacyjni w zakresie zagrożenia dot. cyberbezpieczeństwa i świadczenia przez siebie usług telekomunikacyjnych są uregulowani w Dziale VIIA Pt „Bezpieczeństwo i integralność sieci i usług telekomunikacyjnych”, a nie w KSC. Projektowana regulacja de facto rozszerza obowiązki przedsiębiorców telekomunikacyjnych o kwestie związane z cyberbezpieczeństwem z KSC. Tymczasem przepisy KSC wyraźnie wskazują, że nie mają one zastosowania do większości przedsiębiorców telekomunikacyjnych (tylko do tych, którzy świadczą dodatkowo usługi wskazane w KSC). Cyberzagrożenia z KSC nie dotyczą działalności telekomunikacyjnej, o której mowa w art. 176a Pt. Co więcej nowa wersja projektu przywróciła zapis o dokonywaniu analizy cyberzagrożeń w oparciu o raporty ENISA co jest działalnie nadmiarowym dla małych i średnich przedsiębiorców, gdyż zagrożenia tam opisane mogą nie występować na polskim rynku. | Uwaga uwzględniona.  Treść przepisu dostosowano do brzmienia art. 176a ust. 2 pkt 4 ustawy – Prawo telekomunikacyjne. |  |
| § 6 ust. 1 pkt 3) | Analiza potrzeb w zakresie odtwarzania i utrzymania usług telekomunikacyjnych  i dostępu telekomunikacyjnego dla podmiotów i służb związanych z ratownictwem, obronnością, cyberbezpieczeństwem, bezpieczeństwem i porządkiem oraz z zarządzaniem kryzysowym, która powinna uwzględniać stopniowalność tego obowiązku w zależności od wielkości operatora. | Uwaga nieuwzględniona.  Brak jest merytorycznych i racjonalnych przesłanek do stopniowalności przedsiębiorców zobowiązanych do sporządzania planu obowiązku wobec podmiotów i służb związanych z a ratownictwem. Ponadto taka regulacja byłaby wykroczeniem poza upoważnienie ustawowe. |  |
| § 5 | Zakres planu działań z § 5 projektu rozporządzenia powinien być dostosowany do wielkości przedsiębiorcy telekomunikacyjnego. Nie powinno być tak, że mały i średni przedsiębiorca musi przygotować plan działań taki sam jak operator zasiedziały Orange Polska S.A. KIKE w dalszym ciągu postuluje zwolnienie małych i średnich operatorów  z obowiązków w zakresie: procedur współpracy z organami uzgadniającymi; wyników analiz  i ocen; udostępniania urządzeń telekomunikacyjnych innym przedsiębiorcom telekomunikacyjnym lub właściwym podmiotom i służbom w zakresie akcji ratowniczych; wdrożonych systemów monitorowania i zabezpieczania, w tym ochrony fizycznej, infrastruktury telekomunikacyjnej oraz świadczonych usług przed zakłóceniami i skutkami naruszenia bezpieczeństwa lub integralności; zapewnieniem dostarczania energii elektrycznej dla urządzeń telekomunikacyjnych. | Uwaga nieuwzględniona.  Plan działania przedsiębiorcy powinien być adekwatny do prowadzonej przez niego działalności. Nie jest wymagane sporządzenie planu wykraczającego poza możliwości przedsiębiorcy. Ponadto, ograniczono liczbę zobowiązanych przedsiębiorców do ok. 100. |  |
| § 7 ust. 1 pkt 4 | Izba nie popiera wprowadzonej zmiany w § 7 ust. 1 pkt 4 projektu nakazującego przedsiębiorcy opisywać dodatkowo przewidzianych skutków zakłócenia działania elementów kluczowych. Informacje te są zbędne i stanowią nadmiarowe obciążenie dla przedsiębiorcy. | Uwaga nieuwzględniona.  Przedsiębiorca dokonując analiz i oceny, o których mowa w § 6 musi wziąć pod uwagę skutki zakłócenia działania swojej kluczowej infrastruktury. Jeśli tego nie zrobi to analiza będzie niepełna i będzie skutkować brakiem kontroli nad działaniem tej infrastruktury w sytuacji szczególnego zagrożenia. |  |
| § 8 | W dalszym ciągu w opinii KIKE należy jednak doprecyzować formułę tych uzgodnień, poprzez wskazanie skutków przewlekłości działań organów. Właściwe wydaje się przyjęcie, że w przypadku niezgłoszenia uwag przez te organy w ciągu 30 dni należy traktować jako akceptację przez nich planu działań. Obecnie bezczynność tych organów pozostaje bez konsekwencji dla nich, a utrudnia działalność operatorów. | Uwaga nieuwzględniona.  Brak jest konkretnych przykładów/informacji dotyczących bezczynności organów w związku z uzgadnianiem planów. Ponadto jest to materia ustawowa. |  |
| **Pracodawcy RP** | | | |
| § 6 ust. 1 pkt 2 | W projekcie rozporządzenia w §6 ust. 1 pkt 2 następuje odwołanie dotyczące konieczności uwzględniania w toku analiz informacji o zagrożeniach publikowanych przez CSIRT oraz raportów Agencji Unii Europejskiej do spraw Cyberbezpieczeństwa (ENISA). Postulujemy usunięcie zwrotu pkt 2. w brzmieniu: „w szczególności na podstawie informacji o zagrożeniach cyberbezpieczeństwa publikowanych przez zespoły reagowania na incydenty bezpieczeństwa komputerowego działające na poziomie krajowym oraz raportów Agencji Unii Europejskiej do spraw Cyberbezpieczeństwa (ENISA)”.  W naszej ocenie projektowany przepis stwarza duże trudności w uwzględnianiu publikowanych przez te zespoły informacji w ramach procedur przygotowania i uzgadniania planu. Informacje te nie są unormowane i nie pojawiają się w jasno określonych i przewidywalnych okresach. Dotyczą też szerokiego spektrum zagadnień. Plany działania są natomiast dokumentami generalnymi o długotrwałej i skomplikowanej procedurze przygotowania i przyjmowania. Tym samym wymaganie to należy usunąć, zakładając jednocześnie, iż kompleksowa analiza zagrożeń cyberbezpieczeństwa, o której mowa w ust. 1 pkt 2, zostanie wykonana z uwzględnieniem wszelkich źródeł, a sam fakt możliwości publikowania informacji o zagrożeniach przez zespoły reagowania na incydenty i reagowania na takie publikacje, o ile dotyczą działalności przedsiębiorców telekomunikacyjnych, może być uwzględniany przez przedsiębiorców w planie w zakresie, w jakim dotyczy on cyberbezpieczeństwa. | Uwaga uwzględniona.  Treść przepisu dostosowano do brzmienia art. 176a ust. 2 pkt 4 ustawy – Prawo telekomunikacyjne. |  |
| § 10 ust. 2 pkt 3 | W projektowanym brzmieniu §10 ust. 2 pkt 3 zaproponowano istotną zmianę przesłanek aktualizacji planu. Dotychczas przesłanką była „istotna zmiana danych dotyczących szczególnych zagrożeń” i postulujemy przywrócenie tego brzmienia.  Proponowane jest natomiast wprowadzenie zapisu wskazującego na istotną zmianę tej przesłanki:  • danych dotyczących zagrożeń, o których mowa w § 6 ust. 1 pkt 1, czyli szczególnych zagrożeń środowiskowych lub fizycznych na obszarze, na którym wykonuje działalność telekomunikacyjną, oraz oceny ich wpływu na bezpieczeństwo i integralność wykorzystywanej infrastruktury telekomunikacyjnej i świadczonych usług, na podstawie danych udostępnionych przez właściwych terytorialnie wojewodów;  • zagrożeń cyberbezpieczeństwa,  • sytuacji w zakresie występowania naruszeń bezpieczeństwa lub integralności infrastruktury telekomunikacyjnej lub świadczonych usług;  W naszej opinii, w sposób bardzo szeroki określono nowe przesłanki aktualizacji planu, co w praktyce będzie oznaczało, że plan może podlegać częstej aktualizacji, np. w przypadku wystąpienia okoliczności wpływających na jego zawartość, w tym istotnych zmian opisanych w pkt. 1. Powyższe może powodować stan ciągłej aktualizacji planu, związany z istotnymi zmianami. Aktualizacja powinna się odbywać nie rzadziej niż raz na trzy lata. | Uwaga uwzględniona.  Skreślono „zagrożenia cyberbezpieczeństwa”.  Odniesiono się do: „sytuacji w zakresie występowania naruszeń bezpieczeństwa lub integralności infrastruktury telekomunikacyjnej lub świadczonych usług, w tym związanych z wystąpieniem incydentów, o których mowa w art. 6 ust. 1 pkt 2;”, zgodnie z intencją art. 176a ust. 2 pkt 4 ustawy – Prawo telekomunikacyjne |  |
| § 11 | W §11 projektu rozporządzenia określono termin sporządzania planu na 12 miesięcy od dnia wejścia w życie rozporządzenia albo od aktualizacji okresowej wynikającej z przepisów dotychczasowych. Przygotowanie całego procesu związanego z przygotowaniem planu i opracowanie planu zgodnie z nowymi wymaganiami powoduje konieczność uprzedniego przygotowania, i to w szerokim zakresie, nowych analiz zagrożeń. Dla przedsiębiorców telekomunikacyjnych, uwzględniając dodatkowe zagadnienia, termin 12 miesięcy może okazać się zbyt krótki. Postulujemy zatem o wydłużenie terminu do 18 miesięcy.  Ponadto dookreślenia wymaga wyrażenie „sporządza plan”. Czytając literalnie, pojęcie może być rozumiane w znaczeniu sporządzenia planu bez konieczności uzgodnień i wprowadzenia do stosowania. Powoduje to, że oprócz czynności „sporządzenia planu”, pojęcie to nie obejmuje swym zakresem, czynności takich jak „uzgodnienia” czy „wprowadzenia do stosowania” planu. Jeżeli działanie związane ze sporządzeniem planu ma obejmować zarówno: sporządzenie, uzgodnienie i wprowadzenie do stosowania planu, termin 12 miesięcy jest stanowczo za krótki. Co więcej, wymaga dookreślenia wyrażenie „sporządza plan”.  Proponujemy również, by wprowadzić do rozporządzenia normę wskazującą, iż obecny plan zachowuje ważność do czasu sporządzenia nowego planu zgodnie z przepisami projektowanego rozporządzenia. Przedsiębiorcy chcą mieć pewność, że obecne plany nie stracą aktualności do czasu sporządzenia nowych. Wynika to z faktu, że proces przygotowania jest bardzo czasochłonny.  Dlatego proponujemy zmiany jak poniżej:  „§ 11. 1. Przedsiębiorca sporządza plan, uzgadnia i wprowadza do stosowania, zgodnie z przepisami niniejszego rozporządzenia w terminie 12 18 miesięcy:  1) od dnia wejścia w życie rozporządzenia albo  2) od terminu aktualizacji okresowej wynikającej z przepisów dotychczasowych  – w zależności od tego, który z tych terminów nastąpi później.  2. Plany przedsiębiorców sporządzone, uzgodnione i wprowadzone do stosowania, przed wejściem w życie niniejszego rozporządzenia zachowują aktualność do upływu terminu, o którym mowa w ust. 1”. | Uwaga uwzględniona. |  |
| **Konfederacja Lewiatan** | | | |
| § 6 ust. 1 pkt 2 | Kluczowym na tym etapie prac zagadnieniem jest weryfikacja i doprowadzenie do pełnej zgodności projektowanego rozporządzenia z upoważnieniem określonym w art. 176a ust. 5 ustawy Prawo telekomunikacyjne. Nasze wątpliwości związane są w szczególności z przywołaniem w § 6 ust. 1 pkt 2 „zagrożeń cyberbezpieczeństwa, w rozumieniu ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560 oraz z 2019 r. poz. 2020 i 2248 oraz z 2020 r. poz. 695 i 875), oraz oceny ich wpływu na bezpieczeństwo i integralność wykorzystywanej infrastruktury telekomunikacyjnej i świadczonych usług, w szczególności na podstawie informacji o zagrożeniach cyberbezpieczeństwa publikowanych przez zespoły reagowania na incydenty bezpieczeństwa komputerowego działające na poziomie krajowym oraz raportów Agencji Unii Europejskiej do spraw Cyberbezpieczeństwa (ENISA)”.  Wysoka precyzja i jednoznaczność mają tutaj znaczenie podstawowe, szczególnie, że zgodnie z brzmieniem art. 1 ust. 2 pkt 1 ustawy o krajowym systemie cyberbezpieczeństwa nie stosuje się –w zakresie wymogów dotyczących bezpieczeństwa i zgłaszania incydentów – do przedsiębiorców telekomunikacyjnych, co w szczególności dotyczy przypadków, w których kwestie te regulują wprost przepisy ustawy Prawo telekomunikacyjne (art. 175-175d p.t.).  W tym kontekście musimy zauważyć, że ustawa prawo telekomunikacyjne, w art. 176a ust. 5 konstruując nieprzekraczalne upoważnienie ustawowe nie odnosi się do konieczności uwzględniania przez przedsiębiorców telekomunikacyjnych kwestii „zagrożeń cyberbezpieczeństwa” w rozumieniu KSC. Naturalnie, nie odnosi się również do konieczności uwzględniania publikowanych w tym zakresie informacji przez CSIRT-y czy ENIS-ę. W zakresie wspólnym z ustawą KSC, wspomniany wyżej art. 176a ust. 5 PT, w zw. z ust. 2 pkt 4 pozwala Radzie Ministrów na określenie w rozporządzeniu jedynie technicznych i organizacyjnych środków zapewnienia bezpieczeństwa i integralności infrastruktury telekomunikacyjnej i świadczonych usług, w tym ochrony przed wystąpieniem incydentów w rozumieniu ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.  Jakkolwiek kwestie incydentów i zagrożeń cyberbezpieczeństwa są w pewien sposób powiązane, tak jednak na gruncie ustawy KSC są to pojęcia bardzo silnie ugruntowane i z których użyciem wiążą się z określone konsekwencje. Tym samym przepis ten stanowi w naszej ocenie przekroczenie upoważnienia ustawowego, a tym samym można wskazać na bezpodstawność obowiązku nakładanego na przedsiębiorcę telekomunikacyjnego przeprowadzania analiz i ocen na podstawie „informacji o zagrożeniach cyberbezpieczeństwa publikowanych przez zespoły reagowania na incydenty bezpieczeństwa komputerowego działające na poziomie krajowym”, a także konieczność uwzględniania w analizie „raportów Agencji Unii Europejskiej do spraw Cyberbezpieczeństwa (ENISA)”. Co więcej, przepis projektu w § 6 ust. 1 pkt 2 odnosi się do „informacji” a nie „rekomendacji”, w praktyce te pojęcia mogą być używane zamiennie i granica między nimi może się zatrzeć.  W związku z powyższym, korekty wydaje się wymagać także uzasadnienie projektu rozporządzenia, które na str. 12 wskazuje, że Ponadto potrzebę analizy rozszerzono o zagrożenia cyberbezpieczeństwa i ich wpływ na powyższe bezpieczeństwo i integralność. Takie podejście wynika z przepisów ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560, z późn. zm.), zwanej dalej „KSC”, zmieniających przepisy art. 176a ust. 1 pkt 3 i ust. 2 pkt 4 ustawy. KSC nie obejmuje przedsiębiorców telekomunikacyjnych, co oznacza, że nie są oni elementem krajowego systemu cyberbezpieczeństwa i nie mają obowiązków związanych z uczestnictwem w tym systemie. Racjonalnym wydaje się jednak, aby wykonując swoją działalności telekomunikacyjną przeprowadzali analizy incydentów i zabezpieczali swoje sieci i usługi.  Odnosząc się do powyższego fragmentu uzasadnienia w pierwszej kolejności należy potwierdzić, że reżimy ustaw PT i KSC są rozłączne w zakresie wymagań bezpieczeństwa i zgłaszania incydentów. W drugiej kolejności Rada Ministrów, konstruując rozporządzenie do art. 176a musi poruszać się w ramach upoważnienia, a nie posługiwać się dodatkowymi, subiektywnie ocenianymi przesłankami racjonalności, które nie mogą stanowić samodzielnej podstawy do określania zakresu zapisów rozporządzenia ponad upoważnienie ustawowe. Co więcej, odwołanie do wskazanych w art. 176a ust. 1 pkt 3 sytuacji szczególnych zagrożeń, jest odwołaniem do ugruntowanej w reżimie Prawa telekomunikacyjnego instytucji, a nie odwołaniem do zagrożeń cyberbezpieczeństwa w rozumieniu KSC. Wreszcie, zauważyć należy, że wymagania w zakresie kompleksowej identyfikacji zagrożeń bezpieczeństwa lub integralności są już wskazane w rozporządzeniu wydanym do art. 175d PT tj. rozporządzenie 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, gdzie w §2 pkt 3-4), 9-10) wskazano, że:  - „przedsiębiorca telekomunikacyjny identyfikuje zagrożenia bezpieczeństwa lub integralności sieci lub usług”,  -„ocenia prawdopodobieństwo wystąpienia oddziaływania zagrożeń na bezpieczeństwo lub integralność sieci lub usług”  - „zawierając umowy mające istotny wpływ na funkcjonowanie sieci lub usług, identyfikuje zagrożenia dla bezpieczeństwa tych sieci lub usług, związane z zawieranymi umowami;”  -„stosuje, wynikające z oceny prawdopodobieństwa wystąpienia oddziaływania zagrożeń, środki zabezpieczające dla poszczególnych kategorii danych”  Istotne jest również, że na podstawie projektowanego §7 ust. 1 pkt 10 opis działań realizowanych na potrzeby wykonania przepisów wydanych do art. 175d będzie także elementem planu działania w sytuacjach szczególnych zagrożeń.  Biorąc jednocześnie pod uwagę wyjątkowość skierowania do przedsiębiorców telekomunikacyjnych w poważnieniu niektórych zagadnień związanych z systemem ustawy KSC (incydent) nie można rozszerzająco, obejmować reżimem ustawy KSC także kwestii zagrożeń cyberbezpieczeństwa rozumianych ściśle zgodnie z systematyką ustawy KSC.  Podsumowując, w naszej ocenie przywołanie w §6 ust. 1 pkt 2) „zagrożeń cyberbezpieczeństwa” w rozumieniu ustawy KSC stanowi istotne przekroczenie upoważnienia ustawowego. W oczywisty sposób zagraża to stabilności przyjmowanego, istotnego dla bezpieczeństwa aktu prawnego. Tym bardziej usunięcia wymagają doprecyzowujące (tym samym pogłębiające niezgodność z upoważnieniem) odwołania do informacji publikowane przez CSIRT-y lub ENIS-ę.  Niezależnie od nieprawidłowości na poziomie formalnym i legislacyjnym, w naszej ocenie utrzymanie tego obowiązku stanowiło będzie niepotrzebne dublowanie obowiązków operatorów, którzy już na gruncie aktu wykonawczego do art. 175d PT (procedowanych równolegle do omawianego rozporządzenia do art. 176a) zobowiązani są do szczegółowych analiz i wdrożeń w obszarze zagrożeń bezpieczeństwa.  Tym samym § 6 ust. 1 pkt 2 powinien zostać usunięty z projektu.  W tym miejscu należy podkreślić, że rozszerzenie przewidziane w § 6 ust. 1 pkt 2 Projektu wykracza poza delegację ustawową. | Uwaga uwzględniona.  Treść przepisu dostosowano do brzmienia art. 176a ust. 2 pkt 4 ustawy – Prawo telekomunikacyjne. |  |
| § 10 ust. 2 pkt 3 | W projektowanym brzmieniu § 10 ust. 2 pkt 3 zaproponowano bardzo istotną zmianę przesłanek aktualizacji planu. W dotychczasowych przepisach przesłanką była „istotna zmiana danych dotyczących szczególnych zagrożeń”, w związku z czym postulujemy przywrócenie brzmienia z dotychczasowego rozporządzenia.  Proponowane jest natomiast wprowadzenie zapisu wskazującego na istotną zmianę tej przesłanki:  danych dotyczących zagrożeń, o których mowa w § 6 ust. 1 pkt 1, czyli szczególnych zagrożeń środowiskowych lub fizycznych na obszarze, na którym wykonuje działalność telekomunikacyjną, oraz oceny ich wpływu na bezpieczeństwo i integralność wykorzystywanej infrastruktury telekomunikacyjnej i świadczonych usług, na podstawie danych udostępnionych przez właściwych terytorialnie wojewodów zagrożeń cyberbezpieczeństwa,  sytuacji w zakresie występowania naruszeń bezpieczeństwa lub integralności infrastruktury telekomunikacyjnej lub świadczonych usług.  W naszej opinii, w sposób bardzo szeroki określono nowe przesłanki aktualizacji planu, co w praktyce będzie oznaczało, że plan może podlegać częstej aktualizacji np. w przypadku wystąpienia okoliczności wpływających na jego zawartość, w tym istotnych zmian opisanych pkt. 1. Powyższe może powodować stan ciągłej aktualizacji planu związany z istotnymi zmianami, Aktualizacja powinna się odbywać nie rzadziej niż raz na trzy lata. | Uwaga uwzględniona.  Skreślono „zagrożenia cyberbezpieczeństwa”.  Odniesiono się do: „sytuacji w zakresie występowania naruszeń bezpieczeństwa lub integralności infrastruktury telekomunikacyjnej lub świadczonych usług, w tym związanych z wystąpieniem incydentów, o których mowa w art. 6 ust. 1 pkt 2;”, zgodnie z intencją art. 176a ust. 2 pkt 4 ustawy – Prawo telekomunikacyjne |  |
| § 11 | W § 11 projektu rozporządzenia określono termin sporządzania planu na 12 miesięcy, od dnia wejścia w życie rozporządzenia albo od aktualizacji okresowej wynikającej z przepisów dotychczasowych.  Przygotowanie całego procesu związanego z przygotowaniem planu i opracowanie planu zgodnie z nowymi wymaganiami powoduje uprzednie i bardzo szerokie przygotowanie nowych analiz zagrożeń.  Powyższe powoduje realne zagrożenie, że dla przedsiębiorców telekomunikacyjnych, że uwzględniając dodatkowe zagadnienia termin 12 miesięcy będzie terminem zbyt krótkim na sporządzenie planu. Postulujemy o wydłużenie okresu do 18 miesięcy.  Ponadto, dookreślenia wymaga wyrażenie „sporządza plan”. Czytając literalnie pojęcie może być rozumiane w znaczeniu sporządzenia planu bez konieczności uzgodnień i wprowadzenia do stosowania. Powoduje to, że oprócz czynności „sporządzenia planu”, pojęcie to nie obejmuje swym zakresem, czynności na „uzgodnienia” i „wprowadzenia do stosowania” planu. Jeżeli działanie związane ze sporządzeniem planu ma obejmować zarówno: sporządzenie, uzgodnienie i wprowadzenie do stosowania planu, termin 12 miesięcy jest stanowczo za krótki, a ponadto wymaga dookreślenia wyrażenie co należy rozumieć pod wyrażeniem sporządza plan.  KL proponuje także, aby wprowadzić normę do rozporządzenia wskazującą, że obecny plan zachowuje ważność do czasu sporządzenia nowego planu zgodnie z przepisami projektowanego rozporządzenia. Przedsiębiorcy chcą mieć pewność w drodze rozporządzenia, że obecne plany nie stracą aktualności do czasu sporządzenia nowych. Wynika to z faktu, że proces przygotowania jest bardzo czasochłonny i aby przygotować plan, który kończy się w np. w lutym 2021 należy z ponad rocznym wyprzedzeniem podjąć czynności procesowe do jego sporządzenia.  W związku proponujemy zmiany jak poniżej:  „§ 11. 1. Przedsiębiorca sporządza plan, uzgadnia i wprowadza do stosowania, zgodnie z przepisami niniejszego rozporządzenia w terminie 12 18 miesięcy:  1) od dnia wejścia w życie rozporządzenia albo  2) od terminu aktualizacji okresowej wynikającej z przepisów dotychczasowych  – w zależności od tego, który z tych terminów nastąpi później.  2. Plany przedsiębiorców sporządzone, uzgodnione i wprowadzone do stosowania, przed wejściem w życie niniejszego rozporządzenia zachowują aktualność do upływu terminu, o którym mowa w ust. 1.”. | Uwaga częściowo uwzględniona.  Przepis został przeredagpwany. |  |
| **UKE** | | | |
| § 3 ust. 1 | W projektowanym przepisie jest mowa o sporządzaniu przez przedsiębiorcę planu dla „faktycznego” obszaru wykonywania działalności telekomunikacyjnej, podczas gdy np. w § 6 ust. 1 pkt 1 oraz w § 7 ust. 1 pkt 4 jest mowa odpowiednio o „obszarze, na którym wykonuje działalność telekomunikacyjną” oraz „obszarze działalności” (z pominięciem wyrazu „faktycznym”). W związku z tym projektowane przepisy wymagają odpowiedniego ujednolicenia w tym zakresie. | Uwaga uwzględniona. |  |
| § 4 ust. 3 | W ramach zapisu „i przekazuje Prezesowi UKE te informacje” należy sprecyzować, o które „informacje” chodzi w tym przypadku. | Uwaga uwzględniona. |  |
| § 5 ust. 3 | Należy wskazać moment od którego rozpoczyna bieg wskazany w projektowanym przepisie termin 14 dni. | Uwaga uwzględniona. |  |
| § 6 ust. 1 pkt 3 | W lit. a, b i c należy skreślić wyraz „dla”, bowiem przedsiębiorca sporządzający plan de facto ma dokonywać analizy „potrzeb podmiotów lub służb”, nie zaś (jak wynika z brzmienia projektowanego przepisu) analizy „potrzeb dla podmiotów lub służb”. | Uwaga uwzględniona. |  |
| § 7 ust. 1 pkt 3 | Po wyrazach „organy uzgadniające” należy dodać wyraz „plan” (zgodnie z wprowadzonym w § 5 ust. 1 określeniem „organy uzgadniające plan”). | Uwaga uwzględniona. |  |
| § 7 ust. 1 pkt 4 | W ramach zapisu „opis świadczonych usług z uwzględnieniem zakresu współpracy z podmiotami zewnętrznymi, niezbędnej do świadczenia tych usług” niejasne jest określenie „podmioty zewnętrzne” oraz o jakie rodzaje współpracy z podmiotami zewnętrznymi chodzi w projektowanym przepisie (czy np. o outsourcing?). Odpowiedzi na niniejsze wątpliwości nie dostarcza również uzasadnienie do projektowanego rozporządzenia. | Określenie „podmioty zewnętrzne” należy rozumieć jako podmiot wykonujący zadania w ramach outsourcingu. Wyjaśnienie zostanie ujęte w uzasadnieniu. |  |
| § 7 ust. 1 pkt 9 | W celu zapewnienia przejrzystości redakcyjnej projektowanemu przepisowi proponuje się nadać brzmienie „9) procedurę udostępniania innym przedsiębiorcom telekomunikacyjnym lub właściwym podmiotom i służbom urządzeń telekomunikacyjnych przedsiębiorcy, niezbędnych do przeprowadzania akcji ratowniczych, wraz ze wskazaniem dokumentu określającego tę procedurę;”. | Uwaga uwzględniona. |  |
| § 7 ust. 1 pkt 10 | W projektowanym przepisie należy skreślić wyrazy „albo wskazanie dokumentu określającego stosowanie tych środków i metod, o ile został ustanowiony”. | Uwaga nieuwzględniona.  W rozporządzeniu wydanym na podstawie art. 175d ustawy – Prawo telekomunikacyjne, przedsiębiorcy telekomunikacyjni sporządzają dokumentację dotyczącą wdrożonych środków i metod zapobiegania zagrożeniom.  Zawarcie w planie opisu tych środków i metod jest dublowaniem dokumentacji i nie wydaje się racjonalne. |  |
| § 7 ust. 1 pkt 11 | W projektowanym przepisie po wyrazie „naprawczych” należy dodać wyrazy „zgodnie z umowami zawartymi z dostawcami” (podobnie jak miało to miejsce w wersji projektowanego rozporządzenia z dnia 18.05.2020 r.) | Uwaga nieuwzględniona.  Odniesienie do „umów zawartych z dostawcami” nie wnosi istotnej treści normatywnej.  Brak uzasadnienia ze strony UKE, że takie odniesienie ma istotne znaczenie na spełnienie obowiązku ujętego w pkt 11.  W uzasadnieniu wskazano, że opis sposobów współpracy z dostawcami powinien być zgodny z umowami zawartymi z tymi dostawcami. |  |
| § 7 ust. 1 pkt 12 | W projektowanym przepisie należy skreślić wyrazy „albo wskazanie dokumentu normującego wdrażanie tych systemów”. | Uwaga uwzględniona.  Obowiązkiem powinno być tylko zamieszczenie w planie wykazów systemów i procedur. |  |
| § 7 ust. 1 pkt 14 | Niejasny jest powód zmiany brzmienia projektowanego przepisu (w stosunku do projektowanego rozporządzenia w wersji z dnia 18.05.2020) w części poprzedzającej zapis „wraz ze wskazaniem dokumentu normującego wprowadzenie takich przedsięwzięć”. Należy bowiem zauważyć, że brzmienie projektowanego przepisu w wersji z dnia 18.05.2020 zostało ustalone w wyniku prac roboczych przedstawicieli MC oraz UKE nad projektem rozporządzenia. Co więcej, brzmienie to jest analogiczne do brzmienia § 5 pkt 15 aktualnie obowiązującego rozporządzenia w sprawie planu działań przedsiębiorcy telekomunikacyjnego w sytuacjach szczególnych zagrożeń, którego praktyczny aspekt funkcjonowania nigdy nie był podważany, w szczególności przez przedsiębiorców telekomunikacyjnych. W związku z tym proponuje się przywrócić brzmienie projektowanego przepisu w wersji z dnia 18.05.2020. | Uwaga nieuwzględniona.  Zgodnie z opinią RCL uspójnienia z art. 176a ust. 2 pkt 6 wymaga § 7 pkt 14 – upoważnienie ustawowe wskazuje na „przygotowania” techniczne i organizacyjne w razie ograniczeń działalności telekomunikacyjnej wprowadzonych ustawą, zaś projekt rozporządzenia posługuje się pojęciem „przedsięwzięcia”. |  |
| § 8 ust. 4 oraz § 9 ust. 4 | W ramach projektowanych przepisów należy wskazać momenty od których rozpoczynają bieg wskazane w nich terminy (30 i 14 dni – w przypadku § 8 ust. 4 oraz 14 dni – w przypadku § 9 ust. 4) | Uwaga częściowo uwzględniona. |  |
| § 10 ust. 1 i 2 | W ramach projektowanych przepisów proponuje się użyć (podobnie jak miało to w wersji projektowanego rozporządzenia z dnia 18.05.2020) określeń „aktualizacja okresowa” (w przypadku ust. 1) oraz „aktualizacja bieżąca” (w przypadku ust. 2). Należy bowiem zauważyć, że ww. określenia i ich znaczenie zostały utrwalone w ramach dotychczasowej działalności przedsiębiorców telekomunikacyjnych, jak również pozwalają na jednoznaczne rozróżnienie tych dwóch rodzajów aktualizacji. | Uwaga nieuwzględniona.  Celem zmiany było uproszczenie przepisów i nomenklatury. Ponadto podział ten rodził wątpliwości ze strony RCL co do spójności aktualizacji planu w trybie „bieżącym” i „okresowym” |  |
| § 10 ust. 3 | Użyty w projektowanym przepisie wyraz „udostępnia” proponuje się zastąpić wyrazem „przesyła” (stosownie do zawartego na str. 15 fragmentu uzasadnienia do projektowanego przepisu, zgodnie z którym „Po dokonaniu aktualizacji planu, przedsiębiorca „przesyła” zaktualizowaną część planu organom uzgadniającym plan”). | Uwaga uwzględniona.  W stosunku do planu projekt używa wszędzie pojęcia „przesyła”. |  |
| § 10 ust. 4 | W pkt 1 i 2 po oznaczeniu „§ 7” należy dodać oznaczenie „ust. 1”. | Uwaga uwzględniona. |  |
| § 11 | Projektowany przepis nie reguluje statusu planów sporządzonych przez przedsiębiorców na podstawie przepisów dotychczasowych (w przeciwieństwie do § 12 ust. 2 obowiązującego rozporządzenia w sprawie planu działań przedsiębiorcy telekomunikacyjnego w sytuacjach szczególnych zagrożeń).  Ponadto przepis ten jest rozbieżny względem projektowanego § 3 pkt 2 w zakresie określenia terminu do sporządzenia planu przez przedsiębiorcę, który rozpoczął działalność w okresie krótszym niż rok przed wejściem projektowanego rozporządzenia w życie (na podstawie projektowanego § 3 pkt 2 przedsiębiorca będzie musiał sporządzić plan w terminie 12 miesięcy od dnia rozpoczęcia świadczenia usług telekomunikacyjnych lub dostarczania sieci telekomunikacyjnej, zaś na podstawie projektowanego § 11 pkt 1 przedsiębiorca będzie musiał sporządzić plan w terminie 12 miesięcy od dnia wejścia w życie projektowanego rozporządzenia).  Jednocześnie proponuje się, aby przedsiębiorcy którzy w dniu wejścia w życie projektowanego rozporządzenia posiadają plan sporządzony na podstawie przepisów dotychczasowych (w tym także ci którzy działają na rynku krócej niż 3 lata i ich plany nie podlegały jeszcze aktualizacji okresowej) byli obowiązani do sporządzenia nowego planu w terminie przewidzianym na aktualizację planu, o którym mowa w projektowanym § 10 ust. 1. | Uwaga uwzględniona  Uwaga uwzględniona  W projekcie nie występuje pojęcie „nowego” planu. Plan jest sporządzany, a potem aktualizowany.  Przedsiębiorca ma obowiązek zaktualizować plan jeśli pojawią się czynniki wpływające na jego zawartość. |  |