LEWIATAN

Warszawa, 9 lipca 2020 r.
KL/339/245/AM/2020

Pan
Marek Zagórski
Minister Cyfryzacji

Szanowny Panie Ministrze,

W odpowiedzi na zaproszenie Ministerstwa Cyfryzacji do konsultacji projektu rozporządzenia Rady Ministrów w sprawie planu działań przedsiębiorcy telekomunikacyjnego w sytuacjach szczególnych zagrożeń (nr z wykazu RD528), Konfederacja Lewiatan przedstawia poniżej stanowisko do projektu ustawy.

Z poważaniem,

Maciej Witucki
Prezydent Konfederacji Lewiatan

Załącznik:
Stanowisko Konfederacji Lewiatan wobec projektu rozporządzenia Rady Ministrów w sprawie planu działań przedsiębiorcy telekomunikacyjnego w sytuacjach szczególnych zagrożeń (nr z wykazu RD528).

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS

LEWIATAN

Stanowisko Konfederacji Lewiatan wobec projektu rozporządzenia Rady **Ministrów w sprawie planu działań przedsiębiorcy telekomunikacyjnego w sytuacjach szczególnych zagrożeń (nr z wykazu RD528)**

W związku z publikacją do ponownych konsultacji rozporządzenia Rady Ministrów w sprawie planu działań przedsiębiorcy telekomunikacyjnego w sytuacjach szczególnych z dnia 29 czerwca 2020 r. (dalej: „Projekt") Konfederacja Lewiatan przedstawia następujące stanowisko.

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

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS

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*"

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS

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.

Przesłanki aktualizacji planu - § 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;

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS

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.

Termin sporządzania nowego planu i przepisy przejściowe - § 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.

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS

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.”.

Konfederacja Lewiatan, KL/339/245/AM/2020

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS