LEWIATAN

Warszawa, 20 stycznia 2021 r.
KL/27/19/AM/2021

Pan
Mateusz Morawiecki
Prezes Rady Ministrów
Minister Cyfryzacji

Pan
Marek Zagórski
Sekretarz Stanu
Pełnomocnik Rządu ds. Cyberbezpieczeństwa
Kancelaria Prezesa Rady Ministrów

Pan
Krzysztof Szubert
Pełnomocnik Prezesa Rady Ministrów
do spraw Europejskiej Polityki Cyfrowej
Kancelaria Prezesa Rady Ministrów

Szanowni Państwo,

w nawiązaniu do zaproszenia Kancelarii Prezesa Rady Ministrów do konsultacji projektu dyrektywy *on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148* (dyrektywa NIS2), Konfederacja Lewiatan, w załączeniu, przedstawia stanowisko do projektu.

Z poważaniem,

Maciej Witucki
Prezydent Konfederacji Lewiatan

Załącznik:
Stanowisko Konfederacji Lewiatan do projektu dyrektywy *on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148* (dyrektywa NIS2).

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 do projektu dyrektywy *on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148* (dyrektywa NIS2)

Konfederacja Lewiatan zgadza się z potrzebą wprowadzenia zmian w stosunku do obecnie obowiązujących przepisów dyrektywy NIS, tak, aby unijne regulacje w zakresie cyberbezpieczeństwa adresowały realne zagrożenia i realne potrzeby państw członkowskich, przedsiębiorców i obywateli w tym zakresie. Zmiany te powinny doprowadzić do stworzenia efektywnego, elastycznego i zdolnego do szybkiej reakcji systemu identyfikacji zagrożeń, mitygacji ryzyka oraz minimalizowania i usuwania szkód, bez tworzenia rozbudowanej, zbiurokratyzowanej i kosztownej struktury, skupionej na jednostronnym gromadzeniu informacji i egzekwowaniu wobec przedsiębiorców coraz to nowych wymagań i obowiązków, przy coraz bardziej restrykcyjnych terminach, zagrożonych drakońskimi karami pieniężnymi. Ponadto, projektowane przepisy wydają się pomijać jedno z najważniejszych wyzwań związanych z cyberbezpieczeństwem, mianowicie aspekt wykrywania, ścigania i karania cyberprzestępców przez organy i służby państw członkowskich UE. Projektowane przepisy skupiają się na stałym zwiększaniu zakresu wymagań wobec przedsiębiorców, w zasadzie całkowicie pomijając fundament, jakim powinno być skuteczne zwalczanie cyberprzestępczości przez organy i służby państw członkowskich UE. W ocenie Konfederacji Lewiatan projektowana dyrektywa nie spełnia pokładanych w niej oczekiwań. Chcielibyśmy zaznaczyć, że obecny etap konsultacji uznajemy za początek dobrego i konstruktywnego współdziałania rządu i przemysłu na rzecz podniesienia cyberbezpieczeństwa w Polsce i Europie. Jesteśmy do dyspozycji dla omówienia dalszych uwag i szczegółów.

W związku konsultacjami projektu dyrektywy *on measures fora high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148* ("dyrektywa NIS2"), prowadzonymi przez Kancelarię Prezesa Rady Ministrów, przedstawiamy następujące stanowisko w sprawie, z prośbą o jego uwzględnienie w toku prac nad stanowiskiem Rządu wobec projektowanej dyrektywy.

I. Propozcja rozciągnięcia zakresu stosowania NIS2 na przedsiębiorców telekomunikacyjnych

W pierwszej kolejności należy zwrócić uwagę na fakt, że projektowana dyrektywa NIS2, w przeciwieństwie do obowiązującej obecnie dyrektywy NIS, zakłada objęcie zakresem jej zastosowania przedsiębiorców telekomunikacyjnych, zarówno operatorów sieci jak i dostawców usług telekomunikacyjnych, i to bez względu na wielkość i skalę działalności przedsiębiorcy telekomunikacyjnego, podczas gdy dostawcy wielu innych usług będą poza zakresem stosowania dyrektywy NIS2 ze względu na swoją wielkość (patrz art. 2 ust. 1 projektu dyrektywy NIS2).
Objęcie przedsiębiorców telekomunikacyjnych przepisami dyrektywy NIS2 nie jest zasadne i nie powinno mieć miejsca, z uwagi na fakt, że cyberbezpieczeństwo w sektorze telekomunikacyjnym jest od lat skutecznie regulowane w ramach telekomunikacyjnej regulacji sektorowej. Unijny system cyberbezpieczeństwa, którego trzon stanowi obowiązująca dyrektywa NIS, jest osiągnięciem bardzo młodym, w porównaniu do unijnych przepisów w zakresie bezpieczeństwa sieci i usług telekomunikacyjnych, przewidzianych w dyrektywach sektorowych, dedykowanych rynkowi telekomunikacyjnemu. Odzwierciedleniem wieloletniej historii sektorowej regulacji bezpieczeństwa na rynku telekomunikacyjnym są art. 40 i 41 dyrektywy 2018/1972 z dnia 11 grudnia 2018 r. ustanawiającej Europejski kodeks łączności elektronicznej, który w chwili obecnej jest

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

transponowany do porządków prawnych państw członkowskich UE, również w zakresie wymagań dotyczących bezpieczeństwa sieci i usług telekomunikacyjnych. Objęcie przedsiębiorców telekomunikacyjnych przepisami NIS2 dorowadziłoby do poważnego zaburzenia istniejącego obecnie systemu i porządku prawnego, wyznaczonego zarówno na poziomie regulacji unijnych jak i krajowych. Doprowadziłoby to do zdemontowania funkcjonującego obecnie, na poziomie unijnym jak i krajowym, zrozumiałego i czytelnego podziału na system cyberbezpieczeństwa, który obejmuje operatorów usług kluczowych i dostawców usług cyfrowych (dyrektywa NIS i ustawa o krajowym systemie cyberbezpieczeństwa) oraz system bezpieczeństwa sieci i usług telekomunikacyjnych, obejmujący przedsiębiorców telekomunikacyjnych (Europejski Kodeks Łączności Elektronicznej i ustawa – Prawo telekomunikacyjne, którą niebawem zastąpi ustawa – Prawo komunikacji elektronicznej). Zniesienie istniejącego podziału nie znajduje żadnego uzasadnienia w poziomie incydentów, czy wzroście zagrożeń w obszarze sieci telekomunikacyjnych. Polscy przedsiębiorcy telekomunikacyjni od co najmniej dwóch dekad skutecznie dbają o bezpieczeństwo swoich sieci telekomunikacyjnych oraz o bezpieczeństwo świadczonych przez siebie usług telekomunikacyjnych, na gruncie dedykowanych sektorowi telekomunikacyjnego regulacji unijnych i krajowych, z wykorzystaniem ugruntowanych, najlepszych praktyk i gromadzonej latami wiedzy eksperckiej. Natomiast system opisany dyrektywą NIS, ustawą o krajowym systemie cyberbezpieczeństwa oraz projektowaną dyrektywą NIS2 tak naprawdę dopiero powstaje, o czym świadczy również fakt, że dyrektywa NIS2 ma zastąpić dyrektywę NIS zaledwie kilka lat jej przyjęciu.

Ponadto, zgodnie z art. 2 ust. 2 projektowanej dyrektywy wymagania i obowiązki wynikające z dyrektywy NIS2 ciążyłyby na wszystkich przedsiębiorcach telekomunikacyjnych, a więc również tych będących mikro, małymi albo średnimi przedsiębiorcami. Dyrektywa NIS2 nakłada na przedsiębiorców telekomunikacyjnych daleko idące, kosztowne i organizacyjnie wymagające obowiązki, którym wielu przedsiębiorców telekomunikacyjnych może nie sprostać. Nie sposób zapomnieć również, że przedsiębiorstwa telekomunikacyjne zaliczone mają być do grupy *essential entities*, która to grupa ma podlegać dalej idącej regulacji i obowiązkom, w tym obowiązkom *ex-ante*, niż podmioty, które mają zostać zaliczone do grupy *important entities*, do której mają należeć m.in. dostawcy elektronicznych platform handlowych, usług społecznościowych czy usług wyszukiwania. W efekcie, mali i średni dostawcy usług telekomunikacyjnych zostaną poddani reżimowi regulacyjnemu w zakresie cyberbezpieczeństwa surowszemu niż najwięksi gracze usług społeczeństwa informacyjnego. Z takim rozwiązaniem nie można się zgodzić, w szczególności, że prowadzi ono do zaburzenia konkurencji na rynku pomiędzy podmiotami oferującymi substytucyjne usługi.

Co istotne, nałożenie na wszystkich przedsiębiorców telekomunikacyjnych, w tym małych i średnich, daleko idących, kosztownych i uciążliwych obowiązków wynikających z dyrektywy NIS2 może skutkować wymuszoną regulacyjnie konsolidacją rynku telekomunikacyjnego, zarówno w ujęciu krajowym jak i unijnym. Stojąc w obliczu stale zwiększanego zakresu obowiązków regulacyjnych i ciężarów quasifiskalnych rynek telekomunikacyjny będzie się konsolidował, co w dłuższej perspektywie czasu może doprowadzić do tego, że zarówno na poziomie krajowym jak i europejskim pozostaną jedynie najwięksi dostawcy usług telekomunikacyjnych. I o ile konsolidacja wynikająca z własnych decyzji biznesowo-ekonomicznych przedsiębiorców uczestniczących w konsolidacji jest procesem zrozumiałym i naturalnym, o tyle za szkodliwą należy uznać regulację, której niezamierzonym skutkiem może być regulacyjne przymuszenie wielu małych i średnich podmiotów do wymuszonej przeregulowaniem rynku konsolidacji, która będąc efektem wzrostu kosztów prowadzenia takiej działalności, zaowocuje

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

także wzrostem cen usług i ograniczeniem dostępności nowoczesnych usług dla użytkowników końcowych.
Ponadto oczywistym jest, że do wykonania wielu z nakładanych na przedsiębiorców obowiązków konieczne jest zatrudnienie odpowiednio wykwalifikowanego personelu. W tym przypadku nie ulega wątpliwości, że personel ten musiałby być wysoko wykwalifikowany w obszarze kompetencji, który już obecnie cierpi na deficyt pracowników. Pomijając już kwestię kosztów zatrudnienia specjalistów z zakresu cyberbezpieczeństwa (czego przedsiębiorcy naturalnie pominąć nie mogą) należy zauważyć, że już w chwili obecnej w Polsce brakuje około 2 tysięcy specjalistów z zakresu cyberbezpieczeństwa i z dużą dozą prawdopodobieństwa można przyjąć, że objęcie przedsiębiorców telekomunikacyjnych obowiązkami wynikającymi z NIS2 spowodowałoby, że tych brakujących specjalistów będzie co najmniej 4 tysiące. Wobec braku wykwalifikowanych specjalistów wywiązanie się przez wszystkich polskich przedsiębiorców telekomunikacyjnych (których jest kilka tysięcy) z nowych obowiązków może okazać się po prostu niewykonalne z uwagi na obiektywny brak osób posiadających niezbędne kwalifikacje. Jest to szczególnie niebezpieczne biorąc pod uwagę, że za niewykonanie obowiązków wynikających z dyrektywy NIS maja grozić drakońskie kary finansowe. W efekcie nowe obowiązki regulacyjne, w połączeniu z brakiem wykwalifikowanej kadry, będą stanowiły kolejną, poważną barierę wejścia na rynek usług telekomunikacyjnych, jednocześnie zmuszając obecnych już na tym rynku przedsiębiorców, zwłaszcza małych i średnich, do weryfikacji i oceny czy są w stanie podołać planowanym obowiązkom regulacyjnym w obszarze cyberbezpieczeństwa.
Warto przypomnieć, że unijne prace nad Europejskim Kodeksem Łączności Elektronicznej zostały zainicjowane i były prowadzone w duchu ograniczania obowiązków i ciężarów administracyjnych spoczywających na przedsiębiorcach telekomunikacyjnych. Nawet jeśli Kodeks Łączności Elektronicznej nie spełnia wszystkich pokładanych w nim nadziei, to NIS2 obejmując swoim zakresie przedsiębiorców telekomunikacyjnych zniweczy wszystkie wysyłki prawodawcy unijnego i unijnych przedsiębiorców, w tym polskich, do zracjonalizowania zakresu obowiązków i ciężarów administracyjnych spoczywających na przedsiębiorcach telekomunikacyjnych.
Poza powyższym, informujemy, że podtrzymujemy nasze uwagi dot. włączenia sektora telekomunikacyjnego do krajowego systemu cyberbezpieczeństwa zgłoszone na etapie konsultacji projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa. W związku z procedowanym już projektem dyrektywy NIS 2 tym bardziej należy wstrzymać się ze zmianą przepisów krajowych. Jest to szczególnie istotne dla zapewnienia długofalowej przewidywalności otoczenia prawnego dla sektora komunikacji elektronicznej, stabilności przepisów krajowych, a także uniknięcia konieczności ponoszenia nadmiarowych wydatków związanych ze zbyt częstymi zmianami przepisów.

II. Zakres regulacji dyrektywy

W naszej ocenie projektowana Dyrektywa NIS2 w sposób zbyt szeroki obejmuje podmioty z sektorów uznanych za kluczowe i istotne. W naszej ocenie należy wprowadzić dodatkowe kryteria, bazujące tj. obecnie na ocenie skutku zakłócającego ewentualnych incydentów. Pod tym kątem należy dla wszystkich z przedstawionych w załącznikach obszarów wskazać także kryteria według których podmioty będą obejmowane obowiązkami. Aktualna propozycja może bowiem prowadzić do zbyt szerokiego objęcia obowiązkami oraz zagrożeniem karami podmiotów których działalność nie ma kluczowego, ani istotnego wpływu na cyberbezpieczeństwo.

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

III. Harmonizacja pojęć i definicji w aktach prawnych dotyczących rynku cyfrowego – art. 3

W ciągu ostatnich miesięcy i tygodni ma miejsce ofensywa regulacyjna dotyczącą bezpośrednio lub mającą znaczący wpływ na rynek cyfrowy i rynek danych. W ciągu ostatnich lat pojawiło się kilka znaczących regulacji jak np.

- RODO (Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE),
- Dyrektywa NIS (Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii)
- Europejski Kodeks Łączności Elektronicznej (EKŁE, Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiająca Europejski kodeks łączności elektronicznej, zastępująca dyrektywy 2002/19/WE, 2002/20/WE, 2002/21/WE, 2002/22/WE)

wraz z krajowymi aktami wdrażającymi dyrektywy oraz aktami prawnymi dopełniającymi zapisy rozporządzeń unijnych (dla RODO były to zmiany w ponad 150 ustawach). Warto zaznaczyć także obecność ogólnoeuropejskich wytycznych związanych np. z wykorzystaniem chmury obliczeniowej w segmentach takich jak finansowe (wytyczne EBA, EIOPA czy ESMA).

Obecnie zaś oprócz omawianej w tych konsultacjach propozycji zmian Dyrektywy NIS (NIS2) pojawiło się wiele projektów nowych aktów prawnych, które w znacznej części dotyczą tych samych podmiotów. Wymieńmy kilka z nich:

- Digital Services Act
- Digital Markets Act
- Digital Operational Resilience Act (dla rynków finansowych)
- Data Governance Act
- Directive on the resilience of critical entities
- (ENISA) Cloud Certification Scheme: Building Trusted Cloud Services Across Europe
- (ENISA) Cybersecurity Certification: EUCC Candidate Scheme

Wiele z tych aktów zawiera różniące się między sobą definicje dotyczące tych samych zdarzeń (np. incydentów) lub zapisy procedur w podobnych sytuacjach. Możemy wskazać jako przykład niejednoznaczność w określaniu dostawców chmury obliczeniowej. Wiele z wymienionych aktów powoduje zmienność odpowiedzialności wobec regulatorów. Objęte tymi aktami podmioty z jednej strony będą odpowiedzialne wobec jednego regulatora europejskiego (np. poprzez powiązanie z tzw. *main establishment*), ale w niemal identycznej sytuacji będzie to inny europejski lub lokalny regulator.

Postulujemy ujednolicenie i harmonizację w maksymalnym zakresie pojęć i procedur we wszystkich aktach, istniejących i planowanych. Tylko wówczas Unia Europejska będzie mogła wykorzystać gospodarkę cyfrową dla dobra obywateli, przedsiębiorstw i państw członkowskich.

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

IV. Dzielenie się informacjami i współpraca z przemysłem – art. 14.

Lewiatan z zadowoleniem wita możliwość angażowania przemysłu ICT w procesy związane z cyberbezpieczeństwem w Europie (Rozdział III, *Cooperation*), gdyż jak wskazują doświadczenia z wieloma incydentami, taka współpraca będzie niezbędna. Oczekujemy jednak dalszego sprecyzowania w jaki sposób fimy IT mogą uczestniczyć zarówno w pracach *Cooperation Group*, czy w ćwiczeniach lub przygotowaniach organizowanych przez EU-CyCLONEe tak jak zostało to opisane w Art. 14 p.3 (a).

Lewiatan uważa, że włączenie przemysłu jest niezbędne dla poprawy cyberbezpieczeństwa i powinno się to odbyć w dobrze określonych, partnerskich ramach.

V. Upoważnienie Komisji Europejskiej do kształtowania zakresu obowiązków na rzecz cyberbezpieczeństwa aktami delegowanymi

Niepokojące są również zapisy, które dają Komisji Europejskiej narządzenie do nakładania na przedsiębiorców obowiązków wykraczających ponad obowiązki i wymagania wynikające z projektowanej dyrektywy NIS2, jak również do przyjmowania aktów delegowanych, które *de facto* określą zakres obowiązków wynikających z dyrektywy NIS2. Przykładowo, zgodnie z art. 18 ust. 5 projektowanej dyrektywy NIS2 Komisja Europejska ma mieć uprawnienie do określania, jakie wymagania techniczne i organizacyjne ma spełniać przedsiębiorca, co oznacza, że *de facto* to Komisja Europejska, a nie państwa członkowskie UE, będzie określała, jakie konkretnie obowiązki będą ciążyły na przedsiębiorcach. Co gorsza, art. 18 ust. 6 przewiduje, że Komisja Europejska może aktem delegowanym narzucać na przedsiębiorców obowiązki wykraczające poza wymagania wynikające z projektowanej dyrektywy. Analogicznie, na gruncie art. 21 ust. 2 projektu dyrektywy Komisja Europejska ma uzyskać możliwość nakładania na przedsiębiorców obowiązku uzyskania certyfikatu. Zapewne opisane powyżej mechanizmy będą uzasadniane przez Komisję Europejską koniecznością zapewnienia elastyczności dyrektywy NIS2 i tak zapewne jest. Przy czym będzie to elastyczność osiągnięta kosztem uprawnień państw członkowskich, które w ten sposób utracą realną kontrolę nad zakresem wymagań wynikających z dyrektywy NIS2, adresowanych wobec przedsiębiorców prowadzących działalność na ich obszarze, jak również kosztem przedsiębiorców objętych dyrektywą NIS2, którzy w każdym momencie mogą doświadczyć nowych, kosztownych obowiązków wprowadzanych przez Komisję Europejską mocą aktów delegowanych. Jeśli Komisja Europejska takim aktem delegowanym wprowadzi obowiązki, które z uwagi na różny poziom zamożności w ramach UE będą uważane za wyważone w bogatszych państwach, a za bardzo kosztowne w biedniejszych, to takie narzędzie może skutkować niedopuszczalnym i nieakceptowalnym zaburzeniem konkurencyjności na europejskim rynku telekomunikacyjnym.

Podobne zastrzeżenia budzą odwołania do obowiązków raportowych i związanych z tym określeń incydentu o znaczącym oddziaływaniu, a także zagrożeń mogących potencjalnie skutkować incydentem znaczącym. Na poziomie dyrektywy określono je na tak wysokim poziomie ogólności, że mogą w efekcie dotyczyć bardzo szerokiego spektrum zdarzeń, skutkując jednocześnie trudnym do sprecyzowania rozszerzeniem odpowiedzialności podmiotów obowiązanych do raportowania. Doprecyzowanie tych kwestii również miałoby zostać zrealizowane w myśl art. 20 ust. 11 w drodze aktów wykonawczych.

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 naszej ocenie zabiegi polegające na przeniesieniu wielu istotnych kwestii na poziom aktów wykonawczych i delegowanych może skutkować ograniczeniem swobody krajów członkowskich w zakresie implementacji dyrektywy NIS 2. W poważny sposób ogranicza to również możliwość rzetelnej oceny samej treści dyrektywy. W naszej ocenie stanowisko Polski powinno wskazywać na potrzebę usunięcia wszelkich takich niejasności i albo doprecyzowania samych przepisów dyrektywy, albo pozostawienia pewnej swobody poszczególnym krajom.

VI. Obowiązki raportowe (cz. I) – art. 20 (1)

Treść Dyrektywy w art. 20 powinna oddawać w sposób jasny i klarowny fakt, że „*essential and important entity*" przekazuje informacje do systemu cyberbezpieczeństwa tylko jeden jedyny raz. Z obecnych zapisów nie jest to dostatecznie jasne, a wręcz pojawia się liczba mnoga („*competent authorities*"), co mogłoby oznaczać niezbędność raportowania w wielu punktach sieci. Jednocześnie brak odpowiedniej reakcji, ani wskazania należytej staranności, jest zagrożony karami opisanymi w art. 31.

Lewiatan wskazuje, że jednoznaczność i pewność prawna jest absolutnie konieczna dla wszystkich przedstawicieli przemysłu, nie tylko tych, którzy znajdują się w kategoriach „*essential and important entity*".

VII. Obowiązki raportowe (cz. II) – art. 20 (2)

W kontekście potencjalnych kar, o których mówi art. 31 wiele do życzenia pozostawia precyzja opisania w art. 20 poziomu i zakresu incydentów wymagających raportowania. W szczególności zapisy art. 20 p. 3 wydają się być bardzo ogólnikowe.

Zwracamy uwagę, że sprawa precyzji zapisu dotyczy nie tylko „*essential and important entities*", ale także organów właściwych ds. cyberbezpieczeństwa i CSIRTów. Zapis art. 20 ust. 6 mówi, że muszą one przekazać informacje „*where appropriate*"… kto ocenia, czy sytuacja była „*appropriate*", czy też nie? Czy ocena odbywa się a priori, czy też post factum? Co się dzieje, jeśli sytuacja zostanie oceniona jako „*not appropriate*"? Itd. itp.

Kolejna niejasność wynika z definicji „*near miss*", które to pojęcie pojawia się tylko w motywie (39), ale już nie w definicjach art. 4. Samo pojęcie można znaleźć wielokrotnie w dalszej części projektu dyrektywy m.in. w art. 11, 12, 13, 27, ale również w szczególności w art. 20 p. 9. Nie powinna mieć miejsce sytuacja, w której brak dokładnej i precyzyjnej definicji, a jednocześnie istnieje zagrożenie poważnymi karami.

Użyte w propozycji pojęcie „*a significant impact*" jest sformułowaniem bardzo ogólnym. Brakuje jasnej definicji tego terminu dyrektywie, co może spowodować, że każde państwo członkowskie przyjmie własną definicję. W konsekwencji wprowadzenie tego obowiązku w ustawodawstwach państw członkowskich będzie niejednolite i spowoduje liczne problemy, szczególnie dla podmiotów działających w kilku państwach.

Lewiatan postuluje zdecydowane doprecyzowanie tego artykułu.

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

VIII. Rozszerzenie obowiązków „Entities" w zakresie raportowania / sprawozdawczości (ar. 20).

Obowiązki z zakresie raportowania incydentów do odpowiednich organów/jednostek nie mogą przesłaniać celu nadrzędnego, jakim jest zapewnienie bezpieczeństwa systemów i usług. GDPR wymaga zgłoszenia incydentu w ciągu 72 godziny, niniejsza dyrektywa zakreśla termin 24 godzin na zgłoszenie incydentu z dodatkowym obowiązkiem przygotowania drobiazgowego raportu z obsługi incydentu w terminie miesiąca.
Proponujemy ujednolicić ww. terminy i przyjąć w Dyrektywie NIS 2 termin dłuższy (72 godzin na zgłoszenie wykrytego incydentu).
Obserwujemy z niepokojem dającą się zauważyć w ostatnich latach tendencję organów unijnych nakładania na przedsiębiorców kolejnych obowiązków raportowych (art. 20 paragraph 4: final report not later than one month after the submission of the report under point (a), including at least the following: (i) a detailed description of the incident, its severity and impact; (ii) the type of threat or root cause that likely triggered the incident; (iii) applied and ongoing mitigation measures).
Nie rozumiemy po co wymaga się od „Essential and Important entities" szczegółowych raportów z obsługi incydentów w kontekście art. 29 dyrektywy, w którym to artykule ustanawia się bardzo szerokie uprawnienia nadzorcze dla organów państwowych, w tym m.in. zapewnione prawo dostępu do pełnej dokumentacji podmiotu, wyników audytu itd.
Uszczegółowienia wymaga również naszym zdaniem „definicja" incydentu określonego w dyrektywie jako „significant" (art. 20 paragraph 3):
"An incident shall be considered significant if:
(a) the incident has caused or has the potential to cause substantial operational disruption or financial losses for the entity concerned;
(b) the incident has affected or has the potential to affect other natural or legal persons by causing considerable material or non-material losses.
Z uwagi na obowiązki, jakie prawodawca nakłada na „Entities" w sytuacji wystąpienia takiego incydentu, nie powinno być wątpliwości, co takim incydentem jest, a co nie jest. Zaproponowane podejście do definicji incydentu „significant" jest zbyt ogólne i w konsekwencji może powodować wiele praktycznych wątpliwości.

IX. Certyfikacja

Wprowadzenie obowiązkowej certyfikacji produktów, usług i procesów ICT dla „*essential and important entities*" tak jak zapisano to w Art. 21 jest znaczącą i niepotrzebną zmianą w stosunku do dotychczasowej praktyki mówiącej tylko o dobrowolnej certyfikacji.

Uważamy, że taki obligatoryjny zapis certyfikacji jest wprowadzony zbyt wcześnie. Wynika to m.in. z doświadczeń przemysłu związanego z implementacją Cybersecurity Act (Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013) i praktycznym wdrożeniem Ram Certyfikacji Cyberbezpieczeństwa. Proces ten zdecydowanie nie miał takiego przebiegu jak oczekiwany. Wymuszanie przez organ nadzorczy certyfikowania określonych rozwiązań czy usług wiąże się z kosztami

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

dla przedsiębiorcy oraz dużym ryzykiem spowolnienia zmian biznesowych w organizacji (bez certyfikacji dane rozwiązanie nie będzie mogło być wdrożone).
Warto także zaznaczyć, że istnieje działający i powszechnie uznany za skuteczny mechanizm European Cybersecurity Certification Group, który powinien być wykorzystany także przy wdrażaniu NIS2.

Obowiązkowa certyfikacja certyfikacja nie sprzyja pewności prowadzenia działalności gospodarczej. Państwa członkowskie powinny mieć możliwość rekomendowania certyfikacji, a nie jej wymuszania. Wymuszanie przez organ nadzorczy certyfikowania określonych rozwiązań czy usług wiąże się z kosztami dla przedsiębiorcy oraz dużym ryzykiem spowolnienia zmian biznesowych w organizacji (bez certyfikacji dane rozwiązanie nie będzie mogło być wdrożone). Postulujemy zatem przegląd proponowanych obowiązków, tak aby ich wykonywanie nie zakłócało prowadzenia działalności gospodarczej.

Zwracamy uwagę, że razem z zapisami o obowiązkowych certyfikatach na poziomie europejskim **dyrektywa powinna całkowicie jednoznacznie usuwać obowiązki związane z uzyskiwaniem certyfikatów wynikających z krajowych ram certyfikacji**. Uważamy, że jednym z elementów tworzenia jednolitego rynku w Europie jest także tworzenie jednolitych ram cyberbezpieczeństwa.

Jeśli chodzi o wymóg certyfikacji przewidziany w art. 21 projektowanej dyrektywy to przepis należy doprecyzować tak, aby ewentualny obowiązek uzyskania certyfikatu był jednokrotny i ciążył na podmiocie, który jest producentem lub wprowadza dany produkt na rynek UE, a nie na podmiocie, który korzysta lub wykorzystuje ten produkt. Uwaga wynika z tego, że art. 21 ust. 1 projektowanej dyrektywy może być odczytywany w sposób, który nie respektuje tej zasady, skoro przepis ten mówi, że państwa członkowskie mogą nałożyć obowiązek certyfikowania produktów, procesów lub usług ICT na „essential" lub „important entities", podczas gdy oczywistym jest, że „essential" albo „important entity" nie musi być producentem, wytwórcą albo importerem produktu, procesu lub usługi, która ma być certyfikowana; analizowany przepis art. 21 ust. 1 brzmi bowiem (podkreślenie własne): *In order to demonstrate compliance with certain requirements of Article 18, Member States may require essential and important entities to certify certain ICT products, ICT services and ICT processes under specific European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881. The products, services and processes subject to certification may be developed by an essential or important entity or procured from third parties.*

Uzupełnieniem powinna być certyfikacja w obszarze procesów organizacyjnych (np. ISO).

Certyfikacja nie powinna natomiast dotyczyć obszaru kompetencji i kwalifikacji zawodowych, gdyż praktyka zespołów cyberbezpieczeństwa uczy, że formalne certyfikaty nie gwarantują odpowiedniego poziomu kwalifikacji pracownika, a jednocześnie wprowadzenie wymagania certyfikowania kwalifikacji mogłoby pogłębić i tak już bardzo duży niedobór pracowników i spowolnić kształcenie niezbędnych kadr. Kształcenie kadr i zdobywanie niezbędnych kwalifikacji to proces długotrwały, rozłożony na lata i fakt ten musi być uwzględniony przy projektowaniu i wdrażaniu jakichkolwiek mechanizmów i wymagań w zakresie cyberbezpieczeństwa. Państwa członkowskie powinny aktywnie zaangażować się, w tym przeznaczając na ten cel wystarczające środki budżetowe, w zbudowanie systemu kształcenia i doskonalenia zawodowego specjalistów w zakresie cyberbezpieczeństwa,

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

ściśle współpracując w tym zakresie z przedsiębiorcami, tak, aby system kształcenia zapewniał wystarczającą ilość kandydatów do pracy, posiadających oczekiwane przez rynek kwalifikacje.

X. Nadzór nad podmiotami oferującymi usługi ponadgraniczne – art. 24

Przyjmujemy, że intencją dyrektywy NIS2 jest objęcie zharmonizowanym nadzorem wszystkich podmiotów, które oferują usługi ponadgraniczne. W zakresie nadzoru nad podmiotami oferującymi usługi ponadgraniczne, w szczególności podmiotami, które oferują usługi sieciowe (ECS/ECN) postulujemy wprowadzenie pojedynczego punktu nadzoru, który byłby realizowany przez właściwego regulatora w głównej siedzibie podmiotu (main establishment). Ten sam sposób nadzoru winien być realizowany także w stosunku do wszystkich podmiotów oferujących tzw. usługi OTT opisane w Europejskim Kodeksie Łączności Elektronicznej, a które także tradycyjnie są usługami ponadgranicznymi.
Takie rozwiązanie bezwzględnie wzmocni innowacyjność podmiotów sektora cyfrowego i pozwoli wszystkim podmiotom korzystającym z ich usług zachować jednolity poziom bezpieczeństwa.
Dodatkowo można przewidzieć opcję włączenia podmiotów ECS/ECN do takiego mechanizmu nadzoru (optin).

XI. Harmonizacja rejestracji – art. 25

Chcemy podkreślić wiodącą i niezwykle pozytywną rolę jaką odgrywa ENISA w europejskim systemie cyberbezpieczeństwa. Art. 25 p.1 wskazuje, że „*essential and important entities*" powinny dokonywać rejestracji w ENISA. Postulujemy – ze względu na inne wymagania wobec takich podmiotów rynków regulowanych – by taka rejestracja miała miejsce we właściwych krajowych organach ds. cyberbezpieczeństwa.

W szczególności związane jest to z podmiotami wymienionymi w art. 24 ust. 1

Mamy wątpliwości jaką dodatkową wartość wniosłaby obecność centralnego rejestru prowadzonego przez ENISA dla krajów członkowskich EU, a także dla podmiotów objętych regulacją lub samej ENISA. Proponujemy rozważyć ewentualną zmianę obecnego zapisu.

Por. uwaga II dotycząca haromonizacji pomiędzy poszczególnymi aktami prawnymi.

XII. Wymiana informacji – art. 26

Należy także wskazać na wątpliwości dotyczące notyfikacji udziału w wymianie informacji (art. 26 ust. 4). Powstaje pytanie, jaki jest cel prowadzenia tego typu list przez stosowny urząd, bądź też w jaki sposób pomoże on podnieść poziom cyberbezpieczeństwa państwa. Z punktu widzenia przedsiębiorcy jest to kolejny wymóg prawny, a korzyści z tego tytułu trudno zidentyfikować. Wnosimy zatem o przegląd tego potencjalnego obowiązki pod kątem przydatności pozyskanych w ten sposób danych dla administracji publicznej oraz proporcjonalności obowiązków nakładanych na przedsiębiorców.

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

XIII. Publiczne piętnowanie braku zgodności – art.29

Art. 29 p. 4 (h) daje możliwość przekazania do publicznej wiadomości braku zgodności „essential entities" z wymaganiami wynikającymi z tej dyrektywy. Wydaje się, że takie publiczne piętnowanie podmiotów nie budzi zaufania ani do nich, ani do organów właściwych ds. cyberbezpieczeństwa. Jednocześnie pozwalamy sobie wyrazić zaniepokojenie, czy te same zasady przekazywania do publicznej wiadomości będą obowiązywały w przypadku braku zgodności w podmiotach administracji publicznej i komercyjnych podmiotach prywatnych.

Możliwość przekazywania opinii publicznej stanu cyberbezpieczeństwa, zarówno w sensie ogólnym, jak i w odniesieniu do konkretnego podmiotu, istnieje niezależnie od przedstawionego projektu dyrektywy. **Proponujemy usunąć wskazany zapis**.

XIV. Kary pieniężne

Krytycznie należy odnieść się również do przepisów dotyczących kar pieniężnych, które mają być nakładane na przedsiębiorców za naruszenie przepisów projektowanej dyrektywy. Zgodnie z art. 31 ust. 4 państwa członkowskie mają zapewnić, że kary pieniężne za naruszenie obowiązków wynikających z art. 18 i 20 dyrektywy NIS2 mogą mieć maksymalną wysokość nie mniejszą niż 10 000 000 EUR albo 2% przychodu, przy czym podstawą do obliczania kary ma być większa z tych dwóch wartości (Member States shall ensure that infringements of the obligations laid down in Article 18 or Article 20 shall […] , be subject to administrative fines of **a maximum of at least** 10 000 000 EUR or up to 2% of the total worldwide annual turnover of the undertaking to which the essential or important entity belongs in the preceding financial year, whichever is higher). Widać zatem, że przewidziane w projekcie dyrektywy progi są przygotowywane z myślą o największych graczach cyfrowych, podczas gdy w praktyce wymagania wynikające z projektowanej dyrektywy, w tym kary za ich nieprzestrzeganie, dotkną przede wszystkim różnej wielkości, w tym małych i średnich, przedsiębiorców europejskich. Kara w wysokości do 45 000 000 PLN jest kwotą niebotyczną i nieosiągalną z perspektywy większości polskich małych i średnich przedsiębiorstwa. Biorąc pod uwagę, że kary pieniężne mogłyby dotknąć również mikro, małych i średnich przedsiębiorców pułapy kar powinny to uwzględniać i wydaje się, że pułapy kar zmniejszone dziesięciokrotnie powinny z jednej strony spełniać cele stawiane przed dyrektywą, a z drugiej strony uwzględniać fakt, że wymagania wynikające z dyrektywy dotkną również małych i średnich podmiotów z UE. Określając pułap kar nie można zapominać, że dyrektywa NIS2 jest jedną z wielu, która przewiduje kary pieniężna, a w coraz bardziej zdigitalizowanym świecie naruszenie wymogów cyberbezpieczeństwa może być jednocześnie naruszeniem wymagań w zakresie ochrony danych osobowych, przepisów konsumenckich czy wymagań dedykowanych sektorowi telekomunikacyjnemu. W efekcie jedno zdarzenie może powodować zbieg kar nakładanych przez różne organy, w polskich warunkach chodzi o kary nakładane przez organ, który będzie odpowiedziany za egzekwowanie NIS2 oraz kary nakładane przez Prezesa Urzędu Ochrony Danych Osobowych, Prezesa Urzędu Komunikacji Elektronicznej oraz Prezesa Urzędu Ochrony Konkurencji i Konsumentów.

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

Ponadto, kary przewidziane za takie samo naruszenie wymagań wynikających z dyrektywy NIS2 powinny być takie same dla wszystkich podmiotów objętych zakresem zastosowania dyrektywy, bez względu na to, czy podmiot, który dopuścił się naruszenia, jest podmiotem prywatnym czy publicznym. Naruszenie wymagań w zakresie cyberbezpieczeństwa może mieć takie same skutki, bez względu na to, czy naruszenia dopuścił się podmiot prywatny czy publiczny stąd nie można zaakceptować rozwiązania przewidzianego w art. 31 ust. 6 projektowanej dyrektywy, który pozostawia państwom członkowskim swobodę w decydowaniu o tym, czy podmioty publiczne będą podlegały karom na takich samym zasadach jak podmioty prywatne. Rozwiązanie takie jest wzorowane na RODO i doświadczenie z wdrażania RODO uczy, że rozwiązanie to nie powinno być powielane na gruncie innych aktów prawnych UE. Szereg państw UE członkowskich wdrażając RODO, skorzystało z tej „furtki" i uznało, że administracja publiczna nie będzie w ogóle podlegała karom za naruszenie RODO albo, że kary za naruszenie RODO przez administrację publiczną będą wielokrotnie niższe niż dla przedsiębiorców. Tą drogą poszła również Polska, gwarantując bezkarność za naruszenie RODO niektórym podmiotom administracji publicznej, dla innych przewidując kary wielokrotnie niższe niż kary grożące za to samo przewinienie sektorowi prywatnemu. W efekcie tworzony jest system podwójnych standardów, w którym w tych samych okolicznościach faktycznych administracja traktowana jest na preferencyjnych warunkach wobec przedsiębiorców i obywateli, bez żadnego obiektywnego uzasadnienia. Rodzi to również poczucie rosnącej niesprawiedliwości i znacznie obniża motywację przedsiębiorców do podnoszenia standardów, skoro administracja publiczna, choć formalnie poddana tym samym wymogom, może liczyć na pobłażliwość w przypadku zamierzonego albo niezamierzonego naruszenia. Jednocześnie praktyka rodzi wiele pytań o to, czym uzasadnić skalę obowiązków i kar pieniężnych za ich naruszenie, nakładanych na przedsiębiorców prywatnych, skoro administracja publiczna miałaby nie podlegać takim samym standardom.

XV. Definicja podmiotów administracji publicznej

Kontynuując wątek administracji publicznej należy krytycznie odnieść się do projektowanej definicji *public administration entity* (art. 4 pkt 23) projektu dyrektywy), z której należy usunąć kryterium posiadania przez taki podmiot osobowości prawnej (art. 4 pkt 23) lit. b) projektu dyrektywy). W warunkach polskich zdecydowana większość podmiotów, które powinny zostać uznane za *public administration entity* w rozumieniu projektowanej dyrektywy nie zostanie objęta przepisami dyrektywy wyłącznie dlatego, że nie posiada osobowości prawnej. W polskim porządku prawnym organy administracji publicznej i obsługujące je urzędy co do zasady nie mają własnej osobowości prawnej (w rozumieniu prawa cywilnego), a osobowość taką posiada abstrakcyjny Skarb Państwa. Pozostawienie w projektowanej dyrektywie kryterium osobowości prawnej może spowodować, że zdecydowana większość polskiej administracji publicznej pozostanie poza zakresem zastosowania dyrektywy NIS2, co wydaje się nie do pogodzenia z celami dyrektywy, w szczególności ze względu na zbiory danych wrażliwych, w tym osobowych, jakimi zarządza administracja publiczna. W związku z powyższym kryterium posiadania osobowości prawnej należy usunąć z projektowanej definicji podmiotu administracji publicznej.

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

XVI. Obowiązek zgłoszenia do ENISA i rejestr podmiotów objętych dyrektywą

Krytycznie należy się odnieść do art. 25 projektowanej dyrektywy, który nakłada obowiązek zgłoszenia do ENISA, wraz z sankcją za niewykonanie obowiązku, bezpośrednio na przedsiębiorców Jest to niedopuszczalne, gdyż dyrektywa może nakładać obowiązki tylko na państwa członkowskie UE i to tylko w zakresie celów (a nie środków), które państwa członkowskie mają osiągnąć implementując dyrektywę do krajowego porządku prawnego. Dyrektywa nie może nakładać obowiązków bezpośrednio na przedsiębiorców lub obywateli. Zgodnie z orzecznictwem Trybunału Sprawiedliwości Unii Europejskiej dyrektywa wyjątkowo może wywoływać skutek bezpośredni wobec przedsiębiorcy albo obywatela, |a tylko wtedy, gdy bezskutecznie minął już termin wdrożenia dyrektywy do krajowego porządku prawnego przez państwo członkowskie, a skutek bezpośredni dotyczy prawa / uprawnienia (a nie obowiązku czy obciążenia), które niewdrożona dyrektywa daje obywatelowi albo przedsiębiorcy.
Nie sposób również zauważyć, że sama istota obowiązku zgłoszenia do ENISA nie ma żadnego uzasadnienia, gdyż w przypadku polskich przedsiębiorców telekomunikacyjnych publicznie dostępny rejestr takich przedsiębiorców prowadzi Prezes Urzędu Komunikacji Elektronicznej. Nie ma uzasadnienia do nakładania na przedsiębiorców obowiązku dokonywania zgłoszenia, czy to do organu krajowego czy unijnego, jeśli wszystkie niezbędne w tym zakresie informacje są zawarte w publicznie dostępnych rejestrach, prowadzonych przez administrację publiczną.
Ponadto, doświadczenia z wdrożenia i stosowania dyrektywy NIS uczą, że lista podmiotów objętych obowiązkami wynikającymi z dyrektywy powinna mieć charakter jawnej, publicznie dostępnej informacji. Nie ma uzasadnienia do uznania za niejawną informacji o tym, że dany podmiot jest objęty obowiązkami wynikającymi z dyrektywy o cyberbezpieczeństwie. Tym samym wykaz lub rejestr takich podmiotów, bez względu na to, czy prowadzony na poziomie unijnym (np. przez ENISA jak przewiduje art. 25 projektu dyrektywy) czy na poziomie krajowym, powinien być jawny i publicznie dostępny.

XVII. Kontrola łańcucha dostaw

Projektowana dyrektywa słusznie zwraca uwagę na istotne znaczenie łańcucha dostaw oraz relacji z dostawcami w kontekście cyberbezpieczeństwa, zwracając uwagę na konieczność uwzględnienia jakości produktów oraz praktyk dostawców w zakresie cyberbezpieczeństwa, w szczególności praktyk bezpiecznego rozwoju produktów (motyw 43). Niestety w dalszej części preambuły projektu dyrektywy jako wzorzec właściwej oceny ryzyka, związanego z kluczowym łańcuchem dostaw, zostało wskazane Zalecenie Komisji (UE) 2019/534 Cyberbezpieczeństwo sieci 5G i powstała w oparciu o ten dokument skoordynowana ocena ryzyka przeprowadzona dla sieci 5G (tzw. 5G Toolbox) (motyw 46, 47). Przywołane Zalecenie jest dokumentem bardzo ogólnym, niespełna sześciostronicowym, w którym pobieżnie taktuje się temat czynników technicznych i innych (motyw 19 i 20 Zalecenia, raptem czternaście wierszy). 5G Toolbox wprawdzie stanowi obszerniejszy dokument, jednakże nadal w zakresie przesłanek oceny ryzyka wykazuje się wysokim poziomem ogólności i abstrakcji, który jest szczególnie widoczny w kontekście „dostawców uznawanych za wysokiego ryzyka" („suppliers considered to be high risks"). W efekcie przyjętego w 5G Toolbox podejścia niektóre państwa członkowskie przyjęły niejasne, nieobiektywne i wskutek tego dyskryminujące kryteria dla oceny ryzyka związanego z łańcuchem dostaw, narażając się na zarzut naruszenia elementarnych zasad krajowego i europejskiego porządku prawnego. Dodatkowo pojawiły się znaczące różnice w podejściu

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

poszczególnych krajów co do statusu poszczególnych dostawców, niweczące ideę wspólnego europejskiego rynku. Jest to również niezgodne z duchem projektu dyrektywy, który zakłada ujednolicenie podejścia państw członkowskich do problematyki cyberbezpieczeństwa. Kontrowersje powstałe w związku z wdrożeniem sieci 5G spotkały się z reakcją Europejskiego Trybunał Obrachunkowego (European Court of Auditors), który w grudniu 2020 podjął kontrolę wdrażania sieci 5G przez kraje członkowskie. Tam bardziej trudno jest uznać podejście przyjęte w przypadku sieci 5G za wzorzec.

Mając na uwadze powyższe, wskazanym jest, aby przepisy dyrektywy, dotyczące łańcucha dostaw, zostały sformułowane w sposób bardziej precyzyjny, w szczególności, aby definiowały one jednolite i obiektywne czynniki, które powinny być brane pod uwagę przy ocenie ryzyka łańcucha dostaw.

XVIII. „Supervision and enforcement for essential entities" w art. 29 Dyrektywy.

Zwracamy uwagę, że wykonywania skanów (art. 29 ust. 2 lit. (d)) może prowadzić do zachwiania działania usług, dlatego skanowania i wszelkie działania na systemach „Entities" powinny być uprzednio uzgodnione i odbywać się w porozumieniu z danym podmiotem.

PODSUMOWANIE:

Biorąc powyższe pod uwagę, głównym i zasadniczym postulatem jest, aby utrzymać obecny model regulacji wymogów w zakresie cyberbezpieczeństwa, tak, aby zagadnienia dotyczące bezpieczeństwa sieci i usług telekomunikacyjnych pozostały przedmiotem regulacji Europejskiego Kodeksu Łączności Elektronicznej, a zagadnienia dotyczące cyberbezpieczeństwa powinny pozostać przedmiotem regulacji dyrektywy NIS i NIS2. Należy jednocześnie zapewnić koordynację i wymianę informacji między tymi oboma systemami. Postulujemy zatem:

1. usunięcie przedsiębiorców telekomunikacyjnych z listy podmiotów objętych zakresem zastosowania projektowanej dyrektywy NIS2 i pozostawienie w mocy przepisów Europejskiego Kodeksu Łączności Elektronicznej dotyczących bezpieczeństwa sieci i usług telekomunikacyjnych;
2. wstrzymanie uchwalenia nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa do czasu ustalenia finalnego brzmienia dyrektywy NIS2 - ostateczne decyzje w tym zakresie powinny być bowiem spójne z podejściem na poziomie UE, które zostanie ustabilizowane po przyjęciu dyrektywy NIS 2.
3. zharmonizowanie pojęć i definicji w aktach prawnych dotyczących rynku cyfrowego;
4. doprecyzowanie przepisów dot. współpracy w zakresie cyberbezpieczeństwa;
5. ograniczenie zakresu stosowania Dyrektywy NIS2 do wszystkich podmiotów wymienionych w załącznikach w szczególności poprzez ocenę skutków potencjalnych incydentów u tych grup podmiotów i wprowadzenie na tej podstawie precyzyjnych kryteriów klasyfikacji;
6. usunięcie z projektowanej dyrektywy przepisów upoważniających Komisję Europejską do określania zakresu obowiązków w zakresie cyberbezpieczeństwa mocą aktów delegowanych;
7. jednoznaczne określenie obowiązków w zakresie raportowania;

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

8. wskazanie, że obowiązkiem certyfikacji objęty może zostać producent albo inny podmiot wprowadzający na rynek produkty ICT, bez obejmowania obowiązkiem certyfikacji obszaru kompetencji oraz rezygnacja z obowiązkowych certyfikatów;
9. wprowadzenie pojedynczego punktu nadzoru nad podmiotami oferującymi usługi ponadgraniczne;
10. harmonizacja rejestracji podmiotów objętych dyrektywą;
11. rezygnacja z notyfikacji udziału w wymianie informacji;
12. rezygnacja z publicznego piętnowanie braku zgodności;
13. zracjonalizowanie, przez dziesięciokrotne obniżenie, maksymalnego wymiaru kar, które mogą być nakładane za naruszenie wymogów w zakresie cyberbezpieczeństwa oraz zapewnienie, że wymiar kary, która może być nałożona za dane naruszenie, jest taki sam bez względu na to, czy podmiot dopuszczający się naruszenia jest przedsiębiorcą prywatnym czy podmiotem administracji publicznej;
14. zmianę definicji podmiotu administracji publicznej, tak, aby definicja ta w polskich warunkach faktycznie obejmowała podmioty administracji publicznej;
15. usunięcie przepisu dyrektywy nakładającego bezpośrednio na przedsiębiorców obowiązek zgłoszenia do ENISA oraz zapewnienie, że prowadzone na szczeblu unijnym lub krajowym wykazy lub rejestry będą jawne i publicznie dostępne;
16. doprecyzowanie przepisów dyrektywy w zakresie dotyczącym łańcucha dostaw

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