LEWIATAN

Warszawa, 16 lutego 2021 r.
KL/55/29/AM/2022

Pani
**Justyna Romanowska**
Kierowniczka Referatu ds. Cyfryzacji
Attaché ds. cyfrowych

Pani
**Katarzyna Prusak - Górniak**
Radczyni
Attaché ds. cyberbezpieczeństwa
Referat ds. Cyfryzacji

*Szanowni Państwo,*

W związku z rozpoczęciem trilogów dot. projektu dyrektywy Parlamentu Europejskiego i Rady w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, uchylającej dyrektywę (UE) 2016/1148 (dalej: projekt dyrektywy NIS2), nawiązując do dyskusji na spotkaniu firm członkowskich Konfederacji Lewiatan z przedstawicielami Referatu ds. Cyfryzacji w Stałym Przedstawicielstwie RP przy UE w Brukseli w dniu 31 stycznia br., Konfederacja Lewiatan, poniżej, przedstawia stanowisko do art. 20 projektu dyrektywy.

Z poważaniem,

Maciej Witucki
Prezydent Konfederacji Lewiatan

**Załącznik:** Stanowisko Konfederacji Lewiatan do art. 20 projektu dyrektywy NIS2 (w oparciu o tekst czterokolumnowy Rady UE z dnia 11 stycznia 2022, sygn. 5163/22)



member of BUSINESSEUROPE

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 art. 20 projektu dyrektywy NIS2 (w oparciu o tekst czterokolumnowy Rady UE z dnia 11 stycznia 2022, sygn. 5163/22)**

## Zgłaszanie incydentów – art. 20 projektu Dyrektywy NIS2

W aktualnym stanie dyskusji dysponujemy faktycznie trzema tekstami propozycji, tj. propozycją KE, Parlamentu i Rady. Są one zawarte w dokumencie Rady z 11 stycznia 2022 r.[1] zawierającym:

- wniosek Komisji z dnia 16 grudnia 2020 r.,
- zmiany przyjęte przez Parlament Europejski 4 listopada 2021 r.,
- mandat Rady przyjęty przez Radę 3 grudnia 2021 r.

W poniższych uwagach referujemy do przedstawionego tam tekstu w oryginale. Zauważamy jednocześnie, że w opublikowanym tekście ITRE (A9-0313/2021) tłumaczonym na jęz. polski wystąpił błąd w zakresie tłumaczenia art. 20 ust. 1, który istotnie zmienia jego wydźwięk:

- *Member States shall ensure that essential and important entities notify, without undue delay, the CSIRT in accordance with paragraphs 3 and 4 of any **significant incident**.*
- *Państwa członkowskie zapewniają, aby podmioty niezbędne i istotne bez zbędnej zwłoki zgłaszały **CSIRT każdy incydent** zgodnie z ust. 3 i 4.*

W zakresie art. 20 dotyczącego raportowania przedstawiamy następujące stanowisko:

1. Art. 20 ust. 1 (pkt 335 tabeli)

Popieramy proponowane przez Radę doprecyzowanie wskazujące, że samo zgłoszenie istotnego incydentu nie może rodzić negatywnych skutków dla zgłaszającego:

- *The act of the notification in itself shall not make the notifying entity subject to increased liability.*

Postulujemy zachowanie znajdującego się w tekście KE i Rady wskazania, że istotność incydentu jest rozpatrywana przede wszystkim z perspektywy usług podmiotów zgłaszających – „significant impact on the provision of their services".

2. Art. 20 ust. 2 (pkt 336 I 337 tabeli)

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=consil%3AST_5163_2022_INIT



member of BUSINESSEUROPE

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

Popieramy proponowane przez PE doprecyzowanie, że informowanie użytkowników ma odbywać się na zasadzie „best effort", z zachowaniem zasady braku dodatkowej odpowiedzialności związanej z tym informowaniem:

- *Informing of recipients shall take place on a 'best efforts' basis and shall not subject the notifying to an increase in liability.*

3. Art. 20 ust. 3

Odnosząc się ogólnie do kryteriów klasyfikacji incydentu jako istotnego podkreślamy, że wszystkie dyskutowane propozycje są pozbawione konkretnych informacji pozwalających na zakwalifikowanie danego zdarzenia jako istotnego lub nie. Na poziomie krajowym, zarówno w PT jak i uKSC na poziomie rozporządzeń dookreślono jak definiowany jest skutek zakłócający, tj. określono konkretne, liczbowe przesłanki – np. czas niedostępności, czy liczba użytkowników. To pozwala świadczącym usługi dokonywać prostej i skutecznej klasyfikacji. Wszelkie inne, miękkie sposoby określenia tych przesłanek będą skutkować ocennością i niejednolitym podejściem obowiązanych do zgłaszania, organów nadzorujących oraz użytkowników.

Celem przepisów powinno być na tyle precyzyjne określanie wszystkich wymagań, a także określenie progów zgłaszania incydentów, żeby podmioty niezbędne i istotne mogły, korzystając z wcześniej przygotowanych już scenariuszy lub ustalonych wzorców w ramach analizy ryzyka, określać istotność incydentu. W przeciwnym przypadku określanie istotności danego incydentu, bez wyraźnego zdefiniowania parametrów tej istotności, może mieć efekt odwrotny od zamierzonego, i tak np. dla świadomego podmiotu niezbędnego lub istotnego istotność incydentu może mieć istotność przy liczbie odbiorców 5 mln, a dla innego 5 tys., podobnie z czasem trwania lub zasięgiem geograficznym, czy też wpływem incydentu na funkcjonowanie i ciągłość usług.

Rozumiemy, że ten cel mógłby zostać osiągnięty przez wydanie przewidzianych aktów delegowanych. Na tą chwilę nie są one jednak znane co zupełnie pozbawia nas możliwości merytorycznego odniesienia się do faktycznych kryteriów oceny incydentów.

Zgodnie z definicją zawartą w art. 4 pkt 1) propozycji dyrektywy KE mówi z kolei, że 'incydent' *oznacza każde zdarzenie naruszające dostępność, autentyczność, integralność lub poufność przechowywanych, przekazywanych lub przetwarzanych danych lub związanych z nimi usług oferowanych przez sieci i systemy informatyczne lub dostępnych za ich pośrednictwem*.

Zatem zakres definicji 'incydentu' jest dosyć ogólny i bardzo szeroki, a więc także zakres ewentualnego obowiązku dla podmiotów niezbędnych i istotnych będzie bardzo obciążający. W praktyce zawiera większość zdarzeń jakie mogą potencjalnie wystąpić u podmiotu niezbędnego lub istotnego i być powiązane z incydentem. To z kolei oznacza stworzenie całego zestawu nowych narzędzi analitycznych, zatrudnienia odpowiedniego personelu w trybie 24 godzin i jego przeszkolenia, jedynie w zakresie określania istotności danego incydentu na cele 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

do CSIRT. Wszystko to składa się na dodatkowe koszty, które będą musiały ponieść podmioty niezbędne i istotne, co zapewne spowoduje zarówno wzrost kosztów usług, jak i kosztów pracy.

Przy tak szerokim zakresie obowiązku wynikającym z art. 20(3), określenie istotności danego incydentu z uwzględnieniem tych wszystkich parametrów w 24 godziny nie będzie możliwe. Analiza istotności incydentu z uwzględnieniem wszystkich wskazywanych parametrów, przy incydentach bardzo trudnych i wymagających, często wymaga zbadania różnych współzależności, a także często kontaktu i ustaleń z dostawcami zewnętrznymi. W odniesieniu do incydentów, które znacząco zakłócają dostępność usług świadczonych przez podmiot, powiadamianie CSIRT bez zbędnej zwłoki (a więc w czasie nawet krótszym niż wymagane 24 godziny), a w każdym razie w ciągu 24 godzin od uzyskania informacji o incydencie, będzie wręcz niemożliwe i będzie narażało podmioty już na wstępie na dodatkowe sankcje ze strony administracji.

Wprawdzie w propozycji art. 20(3) zostało użyte wyrażenie zmiękczające „where available", jednakże może to nie być wystarczające, aby odpowiednio chronić podmioty niezbędne i istotne, przed nakazowym żądaniem przekazywania informacji o incydentach pod groźbą kary, a także szczegółowym weryfikowaniem terminu przekazania tych informacji. Co więcej może nie zostać to nawet odwzorowane w prawie krajowym.

4. Art. 20 ust. 3 lit a (pkt 339 tabeli)

Popieramy proponowane przez PE zastąpienie odniesienia do bardzo ocennych czynników jak „operational disruption" czy „financial loses" zawartych w propozycjach KE i Rady.

Propozycja PE odnosi się do mierzalnej przesłanki tj. liczby użytkowników dotkniętych incydentem.

5. Art. 20 ust. 3 lit b-bb (pkt 339-340b tabeli)

Popieramy proponowane przez PE doprecyzowanie kryteriów poprzez odniesienie do czasu trwania obszaru, zakresu zakłócenia. Są to relatywnie mierzalne czynniki. Propozycje KE i Rady odnosiły się natomiast do niejasnych pojęć znaczącej materialnej lub niematerialnej straty.

Kryteria te są zbliżone do kryteriów wynikających aktualnie z art. 175a ust. 2a prawa telekomunikacyjnego.

6. Art. 20 ust. 3 lit. bc (pkt 340c tabeli)

Nie popieramy proponowanego przez PE wskazania na przesłankę wpływu incydentu na ekonomiczne i społeczne aktywności. Kryterium takie jest zupełnie niemierzalne i nieprecyzyjne, a tym samym nie powinno być wykorzystywane do oceny czy dany incydent jest incydentem istotnym. Szczególnie, że do dokonania takiej oceny zasadniczo właściwy jest przede wszystkim użytkownik usługi. W naszej ocenie kwestie te mogłyby być analizowane nie na etapie klasyfikowania incydentu (szczególnie jeśli mogłaby to być jedyna przesłanka)

7. Art. 20 ust. 4 (pkt 341 tabeli)





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

Popieramy poprawki PE (także w innych miejscach) doprecyzowujące, że raportowanie powinno odbywać się tylko do CSIRT. W propozycjach Rady i KE mówi się dodatkowo także o *„competent authorities*". Zachowana powinna być jedna ścieżka kontaktu do kluczowego operacyjnie organu tj. CSIRT, który powinien dalej decydować o dystrybucji takiego zgłoszenia wśród innych podmiotów publicznych.

8. Art. 20 ust. 4 (pkt 342-342c)

W naszej ocenie podstawowym terminem przekazania „initial notification" powinny być 72 godziny.

W art. 20(4) akapit 2 znalazł się także zapis, że państwa członkowskie przewidują – w należycie uzasadnionych przypadkach i w porozumieniu z CSIRT – możliwość odstąpienia przez dany podmiot od określonych terminów, jednak nie należy spodziewać się szerokich odstępstw w tym zakresie, ponieważ jednym właśnie z celów NIS2 jest podniesienie poziomu harmonizacji w zakresie wymogów dotyczących bezpieczeństwa i zgłaszania incydentów.

Jednym z głównych celów NIS2 jest zapewnienie wyższego poziomu cyberbezpieczeństwa poprzez możliwość szybkiego reagowania na cyberincydenty. Nie uda się tego osiągnąć w inny sposób, jak poprzez szybkie reagowanie i przeciwdziałanie incydentom przez podmioty niezbędne i kluczowe. Właściwym więc podejściem powinno być takie, w którym podmioty niezbędne i istotne, w pierwszej kolejności skupiają się na określeniu wektorów ataku i jego odparciu, a w drugiej na zaraportowaniu incydentu z określeniem jego istotności do właściwego CSIRT.

W ślad za powyższym, wstępne zgłoszenie znaczącego incydentu w ciągu 24 godzin, określenie jego istotności w oparciu o tak szczegółowy katalog parametrów jak z art. 20(3), może być trudne, i powinno następować co najmniej w terminie 72 godzin.

Jeżeli prawodawcy zależy, aby notyfikacja o incydencie była przekazywana do CSIRT bez zbędnej zwłoki i w ciągu 24 godzin od uzyskania informacji o incydencie, może to być informacja która jest w danej chwili dostępna przekazywana przez podmiot zgłaszający (niezbędny lub istotny) na zasadzie „best effort" (tj. na zasadzie sygnalizowania incydentu). Powinno to zostać wyraźnie dookreślone w przepisach. W tym kierunku wydaje się iść propozycja Rady określająca, że takie „initial notification" stanowi „early warning". Ta mogłaby zostać uzupełniona o wskazanie na wykonywanie go zgodnie z zasadą „best effort" oraz oczywiście bez negatywnych skutków dla zgłaszającego, również jeśli przekazane informacje byłyby korygowane na kolejnych etapach.

Propozycja PE również wydaje się lepsza od pierwotnej propozycji KE, ponieważ odnosi się do zasady „best effort" i przynajmniej dla incydentów nieskutkujących przerwaniem ciągłości działania usług podmiotu zgłaszającego wprowadza termin 72 godzin.

9. Art. 20 ust. 4a (pkt 348a tabeli)





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

Popieramy propozycje PE dot. wyraźnego wskazania, że dla wszelkich zgłoszeń powinien istnieć jeden punkt oraz wspólne formularze i wytyczne w celu ograniczenia obciążeń podmiotów raportujących.

10. Art. 20 ust. 5 (pkt 349 tabeli)

Popieramy propozycję KE i PE w zakresie terminu 24 godzin na reakcję CSIRT dot. przekazanego zgłoszenia. Popieramy propozycję PE w zakresie wskazania, że udzielane na wniosek wsparcie ma mieć charakter „actionable advice". Powinno to zapobiegać udzielaniu porad, które nie są adekwatne do sytuacji.

11. Art. 20 ust. 7a (pkt 351a tabeli)

Popieramy propozycję PE dot. stworzenia przez CSIRT jednego punktu kontaktu dla innych jednostek publicznych („competent authorities") zawierającego informacje o istotnych incydentach.

12. Art. 20 ust. 8 (pkt 352 tabeli)

Popieramy poprawki PE dot. zapewniania poufności i ochrony informacji przekazywanych przez zgłaszającego incydent, w wypadkach ich dzielenia z innymi państwami członkowskimi.

***KL/55/29/AM/2022***





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