UNIA METROPOLII POLSKICH
IM. PAWŁA ADAMOWICZA

Warszawa, 02 czerwca 2021 r.

Pan Marek Zagórski
Sekretarz Stanu
w Kancelarii Prezesa Rady Ministrów

Szanowny Panie Ministrze,

w imieniu Unii Metropolii Polskich im. Pawła Adamowicza uprzejmie przekazuję opinię do projektu Dyrektywy Parlamentu Europejskiego i Rady w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii (tzw. Dyrektywa NIS 2)[1], uchylająca dyrektywę (UE) 2016/1148.

Nowa regulacja proponuje m.in.:

1. rozszerzenie istniejących sektorów (transport, ochrona zdrowia, zaopatrzenie w wodę pitną i jej dystrybucję, finanse) o nowe obszary:
   a) Administracja publiczna,
   b) Ścieki - przedsiębiorstwa zbierające, odprowadzające lub oczyszczające ścieki komunalne, bytowe i przemysłowe, o których mowa w art. 2 pkt 1–3 dyrektywy Rady 91/271/EWG(24),
   c) Gospodarowanie odpadami - przedsiębiorstwa zajmujące się gospodarowaniem odpadami, o którym mowa w art. 3 pkt 9 dyrektywy 2008/98/WE(29), z wyłączeniem przedsiębiorstw, dla których gospodarowanie odpadami nie stanowi głównej działalności gospodarczej;
2. zmianę obecnego modelu regulacji z przedmiotowego, zogniskowanego na operatorach usług kluczowych - na podmiotowe, określające kryterium obowiązku stosowania ustawy w odpowiednim załączniku do Dyrektywy NIS 2. Zmiana będzie miała odzwierciedlenie również w treści Dyrektywy NIS 2, zawierającej definicje. Obecnie występujące pojęcie „operator usługi kluczowej", zostanie zastąpione pojęciem „podmiot niezbędny".

W świetle powyższego Unia Metropolii Polskich zgłasza do obecnej wersji projektu Dyrektywy NIS 2 niżej wymienione zastrzeżenia i postulaty.

1) W kwestii rozszerzenie zakresu podmiotowego przyszłej dyrektywy o nowe sektory, w szczególności sektor: „Administracja publiczna".

Wprowadzenie sektora „Administracja publiczna" do grupy podmiotów niezbędnych, zmieni obecny status administracji publicznej w obowiązującej ustawie z 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa (Dz.U. 2018 poz. 1560). Konsekwencją będzie konieczność realizacji przez administrację publiczną nowych obowiązków, których zakres jest znaczący i szeroki: od konieczności opracowania procedur, po stosowanie konkretnych technik zabezpieczeń np. szyfrowania. Zgodnie z przedstawioną przez KE propozycją sektor administracja ma obejmować następujące grupy podmiotów publicznych:

- podmioty administracji publicznej w ramach instytucji rządowych na szczeblu centralnym,

[1] https://eur-lex.europa.eu/legal-ontent/PL/TXT/HTML/?uri=CELEX:52020PC0823&qid=1615538645562&from=EN

BIURO: PAŁAC KULTURY I NAUKI,
POK. 1801 (XVIII PIĘTRO)
PLAC DEFILAD 1, 00-901 WARSZAWA,
TEL. 22 656 76 16 ; E-MAIL: BIURO@METROPOLIE.PL
WWW. METROPOLIE.PL

- podmioty administracji publicznej dla regionów na poziomie NUTS 1 wymienionych w załączniku I do rozporządzenia (WE) nr 1059/2003(27),
- podmioty administracji publicznej dla regionów na poziomie NUTS 2 wymienionych w załączniku I do rozporządzenia (WE) nr 1059/2003 W.

W ocenie Unii Metropolii Polskich, określenie w Załączniku nr 21 podmiotów z zakresu administracji publicznej, w oparciu o klasyfikacje NUTS - należy uznać za nietrafione. Zwłaszcza, gdy wyznaczanie ww. podmiotów ma następować na mocy wyłącznie załącznika Dyrektywy NIS a nie na indywidualnych decyzjach administracyjnych. Podział statystyczny ma na celu objęcie swoim zakresem jak największej liczby podmiotów, jednak w przypadku definiowania zakresów dla potrzeb załącznika należy stosować definicje zawężające. Dodatkowo stosowanie NUTS jest niewłaściwe z uwagi na to, iż nomenklatura ta odnosi się do obszarów a nie organów lub podmiotów publicznych. W przypadku gdy Dyrektywa NIS 2 zawiera definicję podmiotu publicznego - podobną jak w PZP - trudno znaleźć uzasadnienie dla ww. podziału na NUTS w samym załączniku.

W związku z powyższym rekomendujemy zrezygnowanie z podziału NUTS, jako mechanizmu wyznaczania podmiotów administracji publicznej – podmiotów niezbędnych. W zamian należy pozostawić dział Administracja – w oparciu o definicję podmiotu administracji publicznej w rozumieniu art. 4 pkt 23.

Ponadto, naszym zdaniem, obecny zakres podmiotowy (w tym określony w załączniku nr 1) jest za szeroki i nieadekwatny. Wydaje się, iż należy wyłączyć z pod działania dyrektywy:

a) podmioty publiczne świadczące usługi kulturalne (biblioteki, muzea, teatry itp.),

b) podmioty administracji świadczącej:
- nie udzielającej opieki medycznej,
- nie posiadające dostępu do rejestru publicznych,
- nie realizujące zadań z zakresu władztwa administracyjnego.

Cele dyrektywy nie wskazują wprost na konieczność obejmowania tych podmiotów obowiązkami dyrektywy. Zadania świadczone przez te podmioty nie powodują ryzyka braku ciągłości działania, a jeżeli taki brak nastąpi, to nie będzie bezpośrednio zagrażał bezpieczeństwu ludzi. Ww. wyłączenie pozwoli na zachowanie zasady proporcjonalności. Ponadto Państwa członkowskie – z uwagi na minimalny standard dyrektywy - będą mogły objąć te podmioty zakresem dyrektywy, jeżeli będą miały taką wolę.

Postulujemy o wprowadzenie rozwiązania alternatywnego, przyznającego uprawnienia Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) lub bezpośrednio KE do wprowadzania "wyjątków" od stosowania dyrektywy dla podmiotów, które nie wpływają na poziom bezpieczeństwa kraju (np. teatrów, bibliotek, etc.) a kwalifikują się po poprawkach dyrektywy NIS 2 jako podmioty istotne. Procedura wprowadzania ww. wyjątków powinna być elektroniczna i szybka.

2) W kwestii regulacji szczególnej dla małych jednostek (możliwość przenoszenie zadań na inne jednostki).

W świetle ww. uwag Unia Metropolii Polskich proponuje wprowadzenie regulacji, zgodnie z którą jednostki samorządu terytorialnego, mogą – jeżeli tak zdecydują[2] – zapewniać swoim jednostkom organizacyjnym obsługę i realizację obowiązków wynikających z Dyrektywy NIS 2. Fakt ten powinny notyfikować organom właściwym.

W takim przypadku powstanie możliwość wsparcia mniejszych jednostek w realizacji zadań przez np. samorządowe centra usług wspólnych lub wyspecjalizowane wydziały informatyzacji bądź cyberbezpieczeństwa w strukturach urzędów gmin i miast. Do rozważania pozostaje możliwość wzajemnego wspierania się w tym zakresie jednostek samorządu terytorialnego na podstawie porozumień lub przez powołane przez nie struktury (związki międzygminne, związki powiatowo-gminne itp[3]). W takim przypadku regulacja Dyrektywy NIS 2 powinna mieć charakter ogólny na tyle, by umożliwiała

[2] Na mocy np. aktu prawa miejscowego.

[3] Należy wskazać, że prawo do współpracy jednostek samorządu terytorialnego jest jednym z praw zapewnionych przez Europejską Kartę Samorządu Terytorialnego (Dz. U. z 1994 Nr 124 poz. 607)

wprowadzenie takich rozwiązań różnym podmiotom samorządu terytorialnego w Europie, przy uwzględnieniu ich modeli ustrojowych.

3) **W kwestii niewystarczającego oszacowania kosztów wdrożenia Dyrektywy NIS 2 dla administracji lokalnej**.

W dokumencie opisującym analizę wpływy przyszłej regulacji Dyrektywy NIS 2 „Impact assesment" [4] wskazano m.in., że nie podjęto próby oszacowania liczby poszczególnych instytucji publicznych objętych regulacją, ponieważ celem jest dokonanie globalnego oszacowania całkowitego kosztu dla sektora publicznego. Wskazano natomiast, że dane dla administracji publicznej dotyczą kosztów operacyjnych. Wydatki na ICT w sektorze publicznym są zazwyczaj wyrażane jako odsetek wydatków operacyjnych, a nie przychodów lub obrotów. W 2019 r. według Eurostatu łączne wydatki na szczeblu rządu centralnego w UE-27 wynosiły 22% PKB, podczas gdy całkowite dochody wyniosły 21,7% PKB. **Na poziomie jednostek samorządu terytorialnego wydatki ogółem odpowiadały dochodom ogółem: 10,9% PKB.**

W ocenie Unii Metropolii Polskich wskazana metodologia jest nieprawidłowa. Nie obrazuje wszystkich elementów związanych z wdrożeniem nowych obowiązków wynikających z przyszłej regulacji. W analizie zrównano wszystkie szczeble i wielkości samorządu lokalnego, gdy tymczasem istnieją duże różnice w możliwościach zapewnienia sprawnej realizacji zadań z zakresu cyberbezpieczeństwa w poszczególnych jednostkach samorządu terytorialnego, wynikające m.in. z odmiennej jakości infrastruktury, kompetencji oraz struktury zatrudnienia. Zróżnicowanie ma charakter pionowy (rodzaje jednostek samorządu terytorialnego) oraz horyzontalny (regiony UE). Uważamy, że oszacowania kosztów wdrożenia dyrektywy NIS 2 należy dokonać na etapie prac nad aktem. Ocenianie kosztów dopiero na etapie prac nad ustawą wdrażającą będzie działaniem spóźnionym dla jednostek samorządu terytorialnego, które będą ponosić niewspółmiernie duże koszty dostosowania się do przepisów nowej regulacji.

4) **W kwestii zgłaszanie naruszeń.**

Obecne brzmienie projektu dyrektywy wskazuje (w motywie 55 w zw. z art. 20 ust. 4), że w przypadku gdy podmioty powezmą wiedzę o incydencie, powinny mieć obowiązek dokonania wstępnego zgłoszenia w ciągu 24 godzin, a następnie przedłożenia – w terminie nie dłuższym niż miesiąc – sprawozdania końcowego.

Unia Metropoli Polskich postuluje przedłużenie terminu do max. 72 h dla podmiotów nie świadczących usług w trybie ciągłym (non stop np. 24/7 lub podobnym). Uspójnienie terminów zgłaszania z incydentami GPRD (po polsku RODO) pozwoli na niezwiększanie kosztów osobowych za tzw. dyżury weekendowe. Zmniejszy to obciążenia przedsiębiorstw, ułatwi i usprawni zgłaszanie informacji wymaganych zgodnie z prawem Unii. Taki tryb powinien być zgodny z unijnymi przepisami o ochronie danych w zakresie danych osobowych.

5) **W kwestii doprecyzowania przepisów dotyczących audytów.**

W ocenie Unii Metropolii Polskich obecne przepisy dotyczące projektowanych terminów dla określonych w art. 30 ust. 4 lit. f oraz art. 32 ust. 1 propozycji dyrektywy powinny zostać doprecyzowane. W szczególności wskazany w art. 30 ust. 4 lit. f „rozsądny termin" powinien zostać zmieniony na „ terminie niezwłocznym, nie dłuższym niż 6 miesięcy".

6) **W kwestii administracyjnych kar pieniężnych.**

Propozycja przyszłej Dyrektywy NIS 2 zakłada prawo do nakładania administracyjnych kar pieniężnych za nieprzestrzeganie obowiązków. W przypadku przedsiębiorstw są one bardzo duże (do 2 procent). Kary mają być proporcjonalne ale i odstraszające. Przewidziane są również regulacje pozwalające na wprowadzenie szczegółowych zasad nakładania kar (wysokości i zakresu).

W odniesieniu do powyższego Unia Metropolii Polskich zgłasza następujące propozycje zmian:

a) w przypadku kar administracyjnych nakładanych na podmioty administracji publicznej należy zastosować rozwiązania funkcjonujące w RODO,

[4] Brussels, 16.12.2020 SWD(2020) 345 final

b) na gruncie dyrektywy należy doprecyzować czy w przypadku, w którym podmiot spełnia definicje administracji publicznej i jednocześnie jest przedsiębiorcą – istnieje możliwość zwolnienia go z obowiązku zapłaty kary,
c) na poziomie dyrektywy należy rozwiązać kwestię zróżnicowania kar w stosunku do podmiotów z tych samych sektorów i obowiązków a o różnym statusie (prywatny - publiczny). Pozwoli to na uniknięcie zarzutów niekonstytucyjności prawa, jak w przypadku RODO.
d) administracyjne kary pieniężne powinny być nakładane na organy a nie na osoby indywidualne.

W naszej ocenie należy zastanowić się nad wprowadzeniem mechanizmu wspierania podmiotów objętych zakresem regulacji. Jednym z rozwiązań może być przeznaczanie wyegzekwowanych administracyjnych kar pieniężnych na fundusz pożyczkowo - wspierający dla podmiotów, których sytuacja finansowa nie pozwala na wystarczające inwestowanie w obszary regulacji. Wsparcie z takiego mechanizmu miałoby charakter preferencyjny z możliwością umorzenia, w przypadku spełnienia wymagań.

Alternatywnie proponujemy, by w miejsce odstraszających kar finansowych wobec osób odpowiedzialnych w podmiotach, wprowadzić zachęty dla podmiotów do wspólnego wykorzystywania ich indywidualnej wiedzy i praktycznego doświadczenia na szczeblu strategicznym, taktycznym oraz operacyjnym, w celu wzmocnienia zdolności w zakresie odpowiedniego oceniania i monitorowania cyberzagrożeń, obrony przed nimi i reagowania na nie.

W tym celu rekomendujemy:

e) wprowadzenie i stosowanie tzw. ratingu cybersecurity, czyli publicznie dostępnych informacji o stanie ochrony przed cyberzagrożeniami (oraz stosowanie weryfikacji tych kryteriów w procesach gospodarczych),
f) uruchomienie jako nagrody, usługi EU cybersecurity support, dostępnej za abonamentem dla podmiotów pomyślnie stosujących się do zaleceń i audytów (może być jeszcze zróżnicowany poziom np. gold, silver, etc.), która by dawała wsparcie 24/7 albo ochronę typu "cloud cybersecurity" dla routerów, firewali.

Szanowny Panie Ministrze,

w imieniu miast Unii Metropolii Polskich uprzejmie prosimy o rozważenie zasadności wprowadzenia zaproponowanych uwag, w tym potrzebę dokładnego oszacowania wpływu przyszłej regulacji na sektor samorządu terytorialnego. Nasze postulaty zgłaszamy również na forum Europejskiego Komitetu Regionów, by zostały rozpatrzone na jak najwcześniejszym etapie prac nad tym ważnym i potrzebnym aktem prawnym.

Jednocześnie deklarujemy gotowość współpracy z Rządem Rzeczypospolitej Polskiej nad wypracowaniem ostatecznego brzmienia przepisów przedmiotowej regulacji.

Z wyrazami szacunku

DYREKTOR BIURA
UNII METROPOLII POLSKICH

Tomasz Fijołek