Warszawa, dnia 21 listopada 2024 r.

Sz. P. Dariusz Standerski
Sekretarz Stanu
Ministerstwo Cyfryzacji

STANOWISKO

ZWIĄZKU PRACODAWCÓW BRANŻY INTERNETOWEJ IAB POLSKA
W SPRAWIE PROJEKTU NOWELIZACJI USTAWY O KRAJOWYM SYSTEMIE CYBERBEZPIECZEŃSTWA (PROJEKT Z 3 PAŹDZIERNIKA 2024 ROKU)

Szanowni Państwo,

w związku z publikacją 7 października 2024 roku nowego projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (dalej: **projekt nowelizacji**) Związek Pracodawców Branży Internetowej Interactive Advertising Bureau Polska (dalej: **IAB Polska**), który brał udział w dotychczasowych konsultacjach publicznych dotyczących projektu nowelizacji, jest zainteresowany przedstawieniem nowego stanowiska do projektowanych przepisów.

Należy bowiem zauważyć, że choć w treści nowego projektu uwzględniono wiele uwag zgłoszonych w trakcie dotychczasowych konsultacji publicznych, to równocześnie wprowadzano do niego wiele nowych i tym samym niekonsultowanych wcześniej rozwiązań. Jednocześnie wiele ze zgłaszanych uwag nie zostało uwzględnionych w treści nowego projektu nowelizacji.

I. Uwagi ogólne

Przede wszystkim należy zauważyć, że w projekcie nowelizacji **w dalszym ciągu nie wyjaśniono, czym jest „świadczona usługa" oraz „system informacyjny wykorzystywany w procesie świadczenia usługi"**, mimo że pojęcia te będą kluczowe dla praktyki stosowania znowelizowanej ustawy o krajowym systemie cyberbezpieczeństwa (dalej: **UKSC**).

Na skutek przyjęcia proponowanej koncepcji „usługi" **nie jest możliwe zastosowanie tego pojęcia choćby do działalności podmiotów z sektorów produkcyjnych**, takich jak np. produkcja wyrobów medycznych lub chemikaliów. Produkcji nie można bowiem utożsamiać ze świadczeniem usług. W konsekwencji nie można ustalić, jaki system informatyczny powinien być w tym przypadku utożsamiany z „świadczoną usługą" – przykładowo: czy powinien to być system powiązany z procesem zbierania zamówień, obsługi maszyn przemysłowych, dystrybucji gotowego produktu itd.

Co więcej, w nowym projekcie nowelizacji rozszerzono zakres tych pojęć, **zastępując zwrot „wykorzystywany do świadczenia usługi" o wiele szerszym i bardziej wieloznacznym zwrotem „wykorzystywany w procesie świadczenia usługi"**. Tak szeroki zakres regulacji może doprowadzić do objęcia wymaganiami wynikającymi z projektu nowelizacji każdego systemu informatycznego działającego w danym podmiocie, niekoniecznie powiązanego z wąsko rozumianym „świadczeniem usługi".

Współcześnie „w procesie" świadczenia usług wykorzystuje się wiele różnych systemów informacyjnych – jak np. systemy do komunikacji, oprogramowanie biurowe czy programy antywirusowe – które są niezbędne do prowadzenia działalności gospodarczej, ale nie są technologicznie powiązane z celem „świadczenia usługi". Zgodnie z obecnym brzmieniem projektu nowelizacji zachodzi jednak obawa, że również tego rodzaju systemy będą stanowić element „procesu" świadczenia usługi, wobec czego również do nich będą się odnosić regulacje nowelizowanej UKSC.

Z kolei realizacja wielu obowiązków wynikających z projektu nowelizacji w kontekście tego rodzaju systemów (np. w zakresie obowiązku audytowego) może się okazać niewykonalna z uwagi na warunki licencyjne narzucane przez międzynarodowych dostawców tych systemów.

Tym samym IAB Polska postuluje dokonanie modyfikacji komentowanych przepisów poprzez jednoznaczne **wyjaśnienie pojęcia „świadczonej usługi"** (lub jego zastąpienie regulacją bardziej oddającą cele dyrektywy NIS 2[1]), a także wskazanie, **jakich konkretnie systemów mają dotyczyć obowiązki** wynikające z projektu nowelizacji.

II. Uwagi szczegółowe

1. Zakres podmiotowy regulacji, problemy definicyjne.

[art. 1 ust. 2 projektu nowelizacji / art. 2 nowelizowanego UKSC]

Definiując poszczególne podmioty działające w branży ICT, projekt nowelizacji wielokrotnie **wykracza poza regulacje dyrektywy NIS 2, definiuje poszczególne pojęcia w sposób niezrozumiały lub nie definiuje ich wcale**. Prowadzi to do niezgodności projektu nowelizacji z dyrektywą NIS 2 w tak kluczowym aspekcie, jakim jest jej zakres podmiotowy.

W tym kontekście należy przede wszystkim zwrócić uwagę na:

1. **Niezrozumiałe pojęcie** „dostawcy chmury obliczeniowej", **które umożliwia bardzo szeroką interpretację tego pojęcia**. Zgodnie z obecnym projektem nowelizacji, wobec nieprecyzyjności definicji stwarza ryzyko, że praktycznie każda usługa świadczona w modelu SaaS może zostać uznana za usługę chmury obliczeniowej, co należy uznać za działanie nieproporcjonalne.

[1] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2)

2. **Brak ograniczenia działalności** „dostawców usług zarządzanych” **oraz** „dostawców usług zarządzanych w zakresie cyberbezpieczeństwa” **do usług świadczonych wyłącznie w modelu B2B** (między przedsiębiorcami).

   Choć w załączniku nr 1 do dyrektywy NIS 2 wprost wskazano, że o zarządzaniu usługami ICT jest mowa wyłącznie w relacjach między przedsiębiorcami, to projekt nowelizacji nie zawiera takiego ograniczenia. Również wprost w definicjach „dostawców usług zarządzanych” oraz „dostawców usług zarządzanych w zakresie cyberbezpieczeństwa” wskazano, że w tej definicji zaliczają się również osoby fizyczne.

3. **Włączenie w zakres sektora infrastruktury cyfrowej** „podmiotów świadczących usługi rejestracji nazw domen”, a także **nieproporcjonalne rozszerzenie definicji tego rodzaju podmiotów**.

   W myśl dyrektywy NIS 2 „podmioty świadczące usługi rejestracji nazw domen” stanowią autonomiczną grupę podmiotów, odrębną od podmiotów kluczowych oraz ważnych. Natomiast proponowana definicja tego rodzaju podmiotów obejmuje również podmioty, które w dowolny sposób pośredniczą w usłudze rejestracji nazw domen, mimo że tak szerokie rozumienie tego pojęcia nie wynika z dyrektywy NIS 2.

4. **Brak zdefiniowania pojęcia** „dostawcy punktu wymiany ruchu internetowego”.

Tym samym IAB Polska postuluje:

1. **wprowadzenie jasnych i czytelnych przesłanek**, które umożliwią rozgraniczenie, którzy „dostawcy chmury obliczeniowej” – zwłaszcza w kontekście usług świadczonych w modelu SaaS – będą podlegali nowej regulacji;
2. **ograniczenie działalności** „dostawców usług zarządzanych” oraz „dostawców usług zarządzanych w zakresie cyberbezpieczeństwa” **do usług świadczonych wyłącznie w modelu B2B** (między przedsiębiorcami);
3. **ograniczenie zakresu pojęcia** „podmiotów świadczących usługi rejestracji nazw domen”, a także **wykreślenie tego rodzaju podmiotów z załącznika nr 1** do projektu nowelizacji;
4. zdefiniowania pojęcia „dostawców punktu wymiany ruchu internetowego” zgodnie z definicją zawartą w dyrektywie NIS 2.

2. Podmioty działające w ramach grupy kapitałowej.
[art. 1 ust. 8 projektu nowelizacji / art. 5 ust. 6 i 7 nowelizowanego UKSC]

Do nowego projektu nowelizacji dodano regulację, zgodnie z którą podmiot wskazany w załączniku nr 1 lub 2, który spełnia kryteria dla co najmniej średniego przedsiębiorstwa, ale którego system informacyjny jest niezależny od systemów jego przedsiębiorstw powiązanych lub przedsiębiorstw partnerskich, nie będzie uznany za podmiot kluczowy ani ważnym.

W nowej regulacji **nie wyjaśniono jednak, czym jest „niezależny” system informacyjny**. „Niezależność” systemu informacyjnego nie została powiązana z pojęciem „świadczonej

usługi", co budzi wątpliwości, w jakich sytuacjach ten przepis znajdzie zastosowanie. Z analizowanego przepisu nie wynika – przykładowo – czy oprogramowanie biurowe nabywane łącznie dla wszystkich podmiotów z grupy kapitałowej będzie mogło zostać uznane za „niezależny" system informacyjny.

Co więcej, nowa regulacja odnosi się **wyłącznie do podmiotów spełniających wymogi dla co najmniej średniego przedsiębiorstwa**. Oznacz to, że jeżeli określony podmiot zostanie uznany za podmiot kluczowy lub ważny na innej podstawie niż art. 5 ust. 1 pkt 1 lub art. 5 ust. 2 pkt 1 (dotyczy to przykładowo „małych" przedsiębiorców telekomunikacyjnych), to **nie będzie można zastosować wobec takiego przedmiotu projektowanego wyłączenia**.

Należy również zauważyć, że projekt nowelizacji w dalszym ciągu **nie przewiduje żadnych wyłączeń dla podmiotów wchodzących w skład grupy kapitałowej, które świadczą usługi wyłącznie na rzecz innych podmiotów z grupy**. Przyjęcie takiego rozwiązania prowadzi do faktycznego rozszerzenia zakresu podmiotowego regulacji na niemożliwą do zidentyfikowania liczbę podmiotów, działających we wszystkich sektorach gospodarki. Jeśli bowiem w ramach grupy kapitałowej działającej w dowolnym sektorze gospodarki będzie funkcjonował wyodrębniony podmiot odpowiedzialny za zarządzanie procesami biznesowymi lub technologicznymi, **w praktyce cała grupa kapitałowa będzie musiała wypełnić wymagania wynikające z projektu nowelizacji**.

Takie podejście należy uznać za nieproporcjonalne oraz sprzeczne z przepisami dyrektywy NIS 2, co zostało szczegółowo opisane we wcześniejszym stanowisku złożonym przez IAB Polska (uwagi szczegółowe, pkt II)[2].

Tym samym IAB Polska postuluje:

1. wyjaśnienie pojęcia **„niezależnego" systemu informacyjnego**;
2. doprecyzowanie nowych przepisów **w kontekście progów wielkościowych dla przedsiębiorców**;
3. **wyłącznie spod regulacji podmiotów** (w szczególności dostawców usług zarządzanych oraz dostawców usług zarządzanych w zakresie cyberbezpieczeństwa), **które świadczą usługi wyłącznie na rzecz podmiotów wchodzących w skład własnej grupy kapitałowej**. Przykładowo poprzez dodanie art. 5 ust. 7a o treści:

   „*Jeżeli podmiot spełnia wymogi do uznania za podmiot ważny lub podmiot kluczowy w ramach działalności prowadzonej w sektorze infrastruktury cyfrowej lub w sektorze zarządzania usługami ICT, ale jego działalność w ramach tych sektorów jest realizowana wyłącznie na rzecz jego przedsiębiorstw powiązanych lub przedsiębiorstw partnerskich, to podmiot ten nie jest podmiotem ważnym ani podmiotem kluczowym*".

3. Zakres stosowania projektu nowelizacji do podmiotów zagranicznych.

[art. 1 ust. 8 projektu nowelizacji / art. 5a ust. 3-5 nowelizowanego UKSC]

[2] https://legislacja.gov.pl/docs//2/12384504/13055201/13055204/dokument671776.pdf

W nowym projekcie nowelizacji zmodyfikowano zasady stosowania UKSC wobec podmiotów z sektorów „cyfrowych", co było jednym z postulatów IAB Polska. Sposób wprowadzania tych zamian budzi jednak liczne wątpliwości interpretacyjne i uniemożliwia jednoznaczne określenie, jakie podmioty będą podlegały przepisom polskiej ustawy.

Projekt nowelizacji w dalszym ciągu posługuje się **niejasnymi i niedookreślonymi pojęciami** „kierownika podmiotu podejmującego decyzje w sprawie systemu zarządzania bezpieczeństwem informacji" czy „realizowania zadań związanych z systemem zarządzania bezpieczeństwem informacji", co rodzi szerokie możliwości interpretacji tych przepisów i nie pozwala na ich jednoznacznie stosowanie.

Projekt nowelizacji nie wyjaśnia również sytuacji podmiotów, które **choć posiadają spółkę zarejestrowaną w Polsce i pośredniczą w świadczeniu usług na terytorium RP, to nie mają wpływu na sposób czy bezpieczeństwo świadczenia usług**.

Taka sytuacja dotyczy – przykładowo – dostawców chmury obliczeniowej, którzy w Polsce są jedynie „pośrednikiem" spółki zarejestrowanej w innym państwie członkowskim UE. Tego rodzaju dostawcy posiadają jednostki organizacyjne w Polsce (więc powinni podlegać regulacji na podstawie projektowanego art. 5a ust. 1) i zarządzają własnym systemem bezpieczeństwa informacji, ale jednocześnie na terytorium RP nie znajduje się osoba odpowiedzialna za zarządzanie bezpieczeństwa faktycznie świadczonej usługi chmurowej.

Tym samym IAB Polska postuluje uzupełnienie analizowanego przepisu w sposób, **który umożliwi jednoznaczną identyfikację podmiotów, do których ma on zastosowanie**.

4. **Audyty bezpieczeństwa systemu informatycznego.**
   [art. 1 ust. 21 lit. a) projektu nowelizacji / art. 15 ust. 1 nowelizowanego UKSC]

W nowym projekcie nowelizacji zmodyfikowano przepis nakładający obowiązek regularnego przeprowadzania audytu bezpieczeństwa systemu informacyjnego wykorzystywanego w procesie świadczenia usługi.

W tym miejscu należy jednak przypomnieć **sygnalizowane już wcześniej wątpliwości dotyczące posługiwania się w projekcie nowelizacji pojęciem „świadczonej usługi" i „systemu informacyjnego wykorzystywanego w procesie świadczenia usługi"**. Nie jest bowiem jasne, jakiego systemu miałyby dotyczyć obowiązek audytowy.

Tym samym IAB Polska postuluje, **aby obowiązek audytowy dotyczył** nie „systemu informacyjnego wykorzystywanego do świadczenia usługi", a raczej „**systemu zarządzania bezpieczeństwem informacji**".

5. **Organy właściwe do sprawowania nadzoru**
   [art. 1 ust. 41 projektu nowelizacji / art. 41 nowelizowanego UKSC]

Nowy projekt nowelizacji w dalszym ciągu **nie rozwiązuje przyszłego sporu kompetencyjnego w sytuacji, gdy określony podmiot będzie podmiotem kluczowym lub**

ważnym jednocześnie w kilku sektorach gospodarki. Natomiast wielość organów właściwych może w znaczący sposób **utrudnić stosowanie przepisów**, dublować obowiązki nakładane przez te organy na podmioty kluczowe i ważne, a także **doprowadzić do sporów kompetencyjnych** pomiędzy właściwymi organami.

Zdaniem IAB Polska proponowane w art. 53a nowelizowanego UKSC uprawnienie (ale nie obowiązek) do tworzenia metodyk nadzoru będzie nieskuteczne, a **rozgraniczenie kompetencji właściwych organów okaże się niemożliwe**. I choć w uzasadnieniu do projektu nowelizacji wskazano, że organ właściwy może stosować środki nadzorcze tylko w zakresie obejmującym sektor, który został mu przypisany, to **jeżeli ten sam system informacyjny będzie wykorzystywany do świadczenia usługi obejmującej kilka sektorów, to pojawi się spór kompetencyjny, którego istnienia nie przewiduje obecny projekt nowelizacji**. To z kolei negatywnie wpłynie na możliwość prowadzenia działalności przez podmioty kluczowe i ważne, które będą zobowiązane równocześnie współpracować z wieloma organami nadzoru – często w kontekście realizacji tego samego obowiązku lub funkcjonowania tego samego systemu informacyjnego.

Przykładowo: dla podmiotu będącego jednocześnie dostawcą platformy sieci usług społecznościowych oraz przedsiębiorcą komunikacji elektronicznej organem właściwym będzie zarówno minister właściwy do spraw informatyzacji jak i Prezes Urzędu Komunikacji Elektronicznej, **mimo że podmiot będzie świadczył jedną usługę przy wykorzystaniu jednego systemu informacyjnego** (komunikatora w ramach platformy społecznościowej).

Tym samym IAB Polska postuluje wprowadzenie przepisów jednoznacznie regulujących zasady wykonywania nadzoru nad podmiotem kluczowym lub ważnym, **który jednocześnie działa w kilku sektorach gospodarki**, w stosunku do których zostały wyznaczone różne organy właściwe (np. poprzez wyznaczanie **wiodącego organu nadzoru**).

III. Uwagi dodatkowe

IAB Polska zwraca również uwagę, że w nowym projekcie nowelizacji nie uwzględniono szeregu uwag, które były podnoszone przez IAB Polska w stanowisku zgłoszonym we wcześniejszym etapie konsultacji publicznych. Biorąc pod uwagę istotność tych uwag, IAB Polska pragnie raz jeszcze zwrócić uwagę na konieczność:

1. **Wyłączenia spod podlegania** projektowanej regulacji dostawców usług zarządzanych w zakresie cyberbezpieczeństwa, **którzy spełniają wymogi dla małych** przedsiębiorców (uwagi szczegółowe, pkt II wcześniejszego stanowiska).

2. Wprowadzania **dodatkowych wymogów proceduralnych**, które będą musiały zostać spełnione przed **wydaniem przez Radę Ministrów niektórych rozporządzeń** (uwagi szczegółowe, pkt VII wcześniejszego stanowiska).

3. **Ograniczenia obowiązku publikowanie określonych rodzajów informacji przez dostawców usług zarządzanych w zakresie cyberbezpieczeństwa** na swoich stronach internetowych (uwagi szczegółowe, pkt VIII wcześniejszego stanowiska).

4. Wprowadzenia **dodatkowych wymogów związanych z badaniem produktów, usługi i procesów ICT przez właściwe CSIRT** w celu identyfikacji podatności (uwagi szczegółowe, pkt XI wcześniejszego stanowiska).

5. **Doprecyzowania zasad przeprowadzania oceny bezpieczeństwa** oraz **wyłączenia stosowania przepisów dotyczących oceny bezpieczeństwa** w stosunku do podmiotów, które regularnie przeprowadzają ocenę bezpieczeństwa we własnym zakresie (uwagi szczegółowe, pkt XII wcześniejszego stanowiska).

6. **Wykreślenia** lub co najmniej gruntowej zmiany **przepisów dotyczących procedury uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka** (uwagi szczegółowe, pkt XIV wcześniejszego stanowiska).

7. **Wykreślenia** lub co najmniej gruntowej zmiany **przepisów dotyczących wydawania polecenia zabezpieczającego** (uwagi szczegółowe, pkt XV wcześniejszego stanowiska).

8. **Wykreślenia przepisów wprowadzających możliwą do nałożenia karę pieniężną w wysokości nawet 100 mln zł** lub co najmniej doprecyzowania przesłanek do nałożenia tej kary (uwagi szczegółowe, pkt XVI wcześniejszego stanowiska).

9. **Obniżenia maksymalnej wysokości okresowej kary pieniężnej** (uwagi szczegółowe, pkt XVII wcześniejszego stanowiska).

10. **Wykreślenia przepisów zezwalających na nadanie decyzji o nałożeniu kary pieniężnej rygoru natychmiastowej wykonalności** (uwagi szczegółowe, pkt XVIII wcześniejszego stanowiska).

11. **Wykreślenia** z załączników nr 1 i nr 2 **podmiotów, które zostały równocześnie przyporządkowane do kilku sektorów** – w szczególności w kontekście dostawców usług zarządzanych w zakresie cyberbezpieczeństwa (uwagi dodatkowe, pkt II wcześniejszego stanowiska).

Z poważaniem

Włodzimierz Schmidt
Prezes Zarządu