Warszawa, dnia 25 maja 2022 r.

**Departament Cyberbezpieczeństwa**
**Kancelaria Prezesa Rady Ministrów**

**STANOWISKO**

**ZWIĄZKU PRACODAWCÓW BRANŻY INTERNETOWEJ INTERACTIVE ADVERTISING BUREAU (IAB POLSKA) WS. PROJEKTU USTAWY O ZMIANIE USTAWY O KRAJOWYM SYSTEMIE CYBERBEZPIECZEŃSTWA ORAZ NIEKTÓRYCH INNYCH USTAW (WERSJA Z 15 MARCA 2022 R.)**

*Szanowni Państwo,*

W związku z publikacją 25 marca 2022 r. nowego projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (dalej „**nowelizacja ustawy o KSC**") Związek Branży Internetowej IAB Polska (dalej „**IAB Polska**") zrzeszający ponad 200 członków, wśród których znajdują się m.in. największe portale internetowe, sieci reklamowe, domy mediowe i agencje interaktywne, jest zainteresowane przedstawieniem stanowiska do projektu nowelizacji ustawy o KSC, jako że regulacja ta może wpływać na członków IAB i mieć do nich bezpośrednie zastosowanie.

## Uwagi ogólne

Projekt nowelizacji ustawy o KSC przedstawiony 25 marca 2022 r. przede wszystkim uzupełnia brakujące przepisy dyrektywy Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiającej Europejski kodeks łączności elektronicznej (dalej „**EKŁE**"), które nie zostały dotychczas uwzględnione w projekcie ustawy Prawo komunikacji elektronicznej (dalej „**PKE**").

Pomysł regulacji obowiązków przedsiębiorców komunikacji elektronicznej w taki sposób, aby część z nich znalazła się poza PKE w wyniku przeniesienia do odrębnej ustawy, zdaniem IAB Polska stanowi **kontynuację niewłaściwych praktyk legislacyjnych prowadzących do pogłębiania chaosu prawnego**. Na skutek przedstawionej 25 marca 2022 r. propozycji nowelizacji ustawy o KSC doszło do naruszenia jednolitego sposobu regulacji dotyczącej przedsiębiorców komunikacji elektronicznej, która wynika z EKŁE. Negatywnie należy ocenić również pomysł wydzielania poszczególnych elementów tej regulacji do ustawy o KSC.

IAB Polska jednocześnie negatywnie ocenia propozycję jednoznacznego włączenia przedsiębiorców komunikacji elektronicznej do krajowego systemu cyberbezpieczeństwa. IAB Polska uznaje **propozycję tej zmiany za zbyt daleko idącą**.

Ustawa o KSC jako akt prawny prawa krajowego uchwalony w wyniku transpozycji dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 16 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (dalej „**dyrektywa NIS**") nie obejmuje swoim zakresem przedsiębiorców komunikacji elektronicznej. Dyrektywa NIS wymaga od państw członkowskich, aby zidentyfikowały działające na ich terytorium podmioty z określonych w dyrektywie sektorów jako operatorów usług kluczowych lub dostawców usług cyfrowych i zobowiązały je do podejmowania odpowiednich działań zmierzających do zapewniania odpowiedniego poziomu cyberbezpieczeństwa.

Próbę włączenia przedsiębiorców komunikacji elektronicznej do krajowego systemu cyberbezpieczeństwa IAB Polska uznaje **za nadmierne w stosunku do wymogów, jakie stawia krajom członkowskim dyrektywa NIS**, i nie spowoduje ono realnego wzrostu ogólnego poziomu cyberbezpieczeństwa.

## 1. Uwagi szczegółowe

*[Obowiązek udostępniania tajemnicy prawnie chronionej]*

IAB Polska pragnie zwrócić uwagę na sposób uregulowania zakresu uprawnień, jakie – na podstawie projektu nowelizacji ustawy o KSC – uzyska właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV oraz CSIRT Telco. Zgodnie z art. 20e ust. 5 każdy z tych organów może zwrócić się do przedsiębiorcy komunikacji elektronicznej o uzupełnienie zgłoszenia o informacje, w tym informacje stanowiące tajemnice prawnie chronione, w zakresie niezbędnym do obsługi incydentu telekomunikacyjnego.

Ustawa o KSC nie definiuje, czym są informacje stanowiące tajemnice prawnie chronione, natomiast ogranicza się do informacji, że tajemnicą prawnie chronioną jest m.in. tajemnica przedsiębiorstwa. Pojęcie tajemnicy prawnie chronionej może być rozumiane szeroko i może obejmować wszystkie informacje, których poufność powinna być przestrzegana przez przedsiębiorcę komunikacji elektronicznej, w szczególności tajemnicę telekomunikacyjną (art. 159 i kolejne Prawa telekomunikacyjnego)/tajemnicę komunikacji elektronicznej (art. 381 i kolejne PKE).

W ocenie IAB Polska **propozycja nowelizacji ustawy o KSC w zakresie przekazywania właściwym organom informacji prawnie chronionej jest nieprecyzyjna i powinna wprost wykluczyć możliwość przekazywania informacji stanowiącej tajemnicę telekomunikacyjną/tajemnicę komunikacji elektronicznej** ze względu na zakaz przetwarzania tych informacji przez osoby inne niż nadawca i odbiorca tych informacji. Ponieważ ujawnienie tajemnicy telekomunikacyjnej/tajemnicy komunikacji elektronicznej jest

możliwe wyłącznie w przypadkach wyraźnie dopuszczonych przez prawo, treść art. 20e ust. 5 ustawy o KSC nie może stanowić podstawy do ujawnienia tajemnicy telekomunikacyjnej/tajemnicy komunikacji elektronicznej.

Powyższe zastrzeżenie jest o tyle ważne, że brak współpracy przedsiębiorcy komunikacji elektronicznej z właściwymi organami przy obsłudze incydentu telekomunikacyjnego i incydentu krytycznego będzie stanowić podstawę do nałożenia na niego kary pieniężnej zgodnie z art. 76a ust. 1 pkt 8 ustawy o KSC. **Wykluczenie wprost możliwość przekazywania informacji stanowiącej tajemnicę telekomunikacyjną/tajemnicę komunikacji elektronicznej pozwoli uniknąć wątpliwości co do zakresu przekazywanych danych**.

*[Zasady odpowiedzialności przedsiębiorców telekomunikacyjnych]*

IAB Polska pragnie dodatkowo zauważyć na przedstawione propozycje ustanowienia w projekcie nowelizacji ustawy o KSC zasad odpowiedzialności przedsiębiorców komunikacji elektronicznej za naruszenie określonych w ustawy o KSC obowiązków (projektowany art. 76a i art. 76b ustawy o KSC).

W ocenie IAB Polska zastrzeżenia budzi określenie obowiązków, których naruszenie będzie powodowało obowiązkową odpowiedzialność przedsiębiorcy komunikacji elektronicznej (art. 76a ust. 1 ustawy o KSC) lub jego fakultatywną odpowiedzialnością, jeśli przemawia za tym charakter lub zakres naruszenia (art. 76a ust. 2 ustawy o KSC).

Przede wszystkim pojawia się wątpliwość, czy **w każdym przypadku niewypełnienia obowiązków wskazanych w projektowanym art. 76a ust. 1 ustawy o KSC przedsiębiorca komunikacji elektronicznej powinien podlegać karze pieniężnej**. Należy zwrócić przede wszystkim uwagę na następujące obowiązki:

1. brak współpracy z Prezesem UKE przy ocenie zastosowanych środków technicznych i organizacyjnych, w szczególności nieprzekazanie w terminie wskazanym przez Prezesa UKE żądanych przez niego informacji;
2. nieusunięcie w wyznaczonym przez Prezesa UKE terminie podatności, która doprowadziła lub mogła doprowadzić do incydentu;
3. nieprzestrzeganie zaleceń pokontrolnych Prezesa UKE przekazanych przedsiębiorcy komunikacji elektronicznej w wyniku przeprowadzonej kontroli stosowania przepisów ustawy o KSC.

IAB Polska stoi na stanowisku, że w powyższych przypadkach odpowiednie organy powinny dokonać oceny zakresu naruszenia obowiązków i ewentualnie nałożyć karę dopiero, jeśli przemawia za tym charakterem lub zakres takiego naruszenia. Niewypełnianie powyższych obowiązków może przybierać różne formy i nie zawsze można stwierdzić, że działania przedsiębiorcy komunikacji elektronicznej jest naganne i powinien on podlegać karze pieniężnej.

## 2. Uwagi dodatkowe

IAB Polska pragnie jednocześnie powtórzyć zastrzeżenia do tych propozycji w nowelizacji ustawy o KSC, które pojawiły się na wcześniejszych etapach pracy legislacyjnych, które w większości pozostają nadal aktualne ze względu na ich nieuwzględnienie w najnowszej wersji nowelizacji ustawy o KSC.

*[Postępowanie w sprawie uznania za dostawcę wysokiego ryzyka – art. 66a i nast. ustawy o KSC]*

IAB Polska zwraca ponownie uwagę na – jego zdaniem – **niewłaściwą regulację dotyczącą postępowania w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka** (projektowane art. 66a i nast. ustawy o KSC). Należy przede wszystkim przypomnieć najważniejsze zastrzeżenia dotyczące tej propozycji:

1. brak informacji na temat wytycznych, kryteriów, przesłanek na podstawie których dostawca ten miałby być uznany za stanowiący poważne zagrożenie dla obronności, bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego, lub życia i zdrowia ludzi, co wiąże się z ryzykiem arbitralności decyzji ministra oraz faktyczną niemożnością podjęcia przez danego dostawcę działań mających zapobiec uznaniu go za dostawcę wysokiego ryzyka;
2. niewskazanie rodzaju sprzętu lub oprogramowania, które miałoby stanowić poważne zagrożenie dla obronności, bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego, lub życia i zdrowia ludzi, co oznacza, że nawet mało znaczące dla bezpieczeństwa narodowego elementy infrastruktury IT wykorzystywane w jednostkach publicznych mogą być przedmiotem wykluczenia;
3. brak mechanizmów dających szansę dostawcy, wobec którego prowadzone jest postępowania, uniknięcia uznania go za dostawcę wysokiego ryzyka poprzez dokonania działań naprawczych;
4. nadanie z mocy ustawy decyzji o uznaniu za dostawcę wysokiego ryzyka rygoru natychmiastowej wykonalności oraz wyłączenie możliwości wstrzymania tego rygoru przez sąd.

*[Polecenie zabezpieczające – art. 67b ustawy o KSC]*

IAB Polska przypomina również pojawiające się uwagi dotyczące propozycji uregulowania polecenia zabezpieczającego (projektowany art. 67b ustawy o KSC), które, w drodze decyzji administracyjnej, będzie wydawać minister właściwy do spraw informatyzacji w przypadku wystąpienia incydentu krytycznego. Tym, co budzi największe zastrzeżenia, jest **niepewność, kogo dokładnie miałoby dotyczyć polecenie zabezpieczające – zgodnie z projektowanym przepisem, w poleceniu mają być wskazane „rodzaj lub rodzaje podmiotów, których dotyczy”**. Odbiorcami takiego polecenia mogą być dostawcy usług cyfrowych, którzy muszą już obecnie dokonywać autoidentyfikacji jako podmiotu posiadającego ten status. Może to doprowadzić do sytuacji, w której wysokie kary pieniężne będą stosowane wobec podmiotów, które polecenia nie wykonały z uwagi na brak świadomości obowiązku wykonania określonego zachowania nakazanego przez ministra.

Również kara pieniężna do 3% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, jaka może zostać nałożona na dostawcę cyfrowego, w świetle innych kar przewidzianych na gruncie ustawy o KSC wydaje się **zdecydowanie wygórowana i nieadekwatna.**

*[Wyłączenie stosowania Prawa zamówień publicznych – art. 76h ustawy o KSC]*

W celu stworzenia strategicznej sieci bezpieczeństwa przy zawieraniu umów dotyczących realizacji zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego przepisy ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych („PZP") nie będą stosowane (projektowany art. 76h ustawy o KSC).

Zdaniem IAB Polska projektowany art. 76e ustawy KSC określa zakres szerszy niż w art. 12 PZP, ale przedmiotowo podobny. Warto zatem, aby **w projektowanym art. 76e ustawy KSC dodać podobne zastrzeżenie jak z art. 12 PZP tj. zezwolenie na wyłącznie PZP dopiero po wykazaniu przez Zamawiającego (np. w wewnętrznej notatce służbowej) nie da się w inny sposób niż przez wyłączenie stosowania ustawy PZP zapewnić bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego**, w zakresie telekomunikacji, w szczególności, że nie wystarczy w tym zakresie zastosować procedury z Działu VI PZP. Innym rozwiązaniem może być wprowadzenie dodatkowego wyłączenia wprost do PZP.

Z poważaniem,

Włodzimierz Schmidt

Prezes Zarządu