 Warszawa, /*elektroniczny znacznik czasu*/

MINISTER DO SPRAW UNII EUROPEJSKIEJ

***Konrad Szymański***

Sygn. KPDPUE.920.1030.2020.AR(2)

dot.: DP-III.0211.4.2020 z 7.09.2020 r.

**Pan Mateusz Morawiecki**

**Prezes Rady Ministrów**

**Minister Cyfryzacji**

**Opinia**

**o zgodności z prawem Unii Europejskiej *projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy – Prawo zamówień publicznych,* wyrażona przez ministra właściwego do spraw członkostwa Rzeczypospolitej Polskiej w Unii Europejskiej**

*Szanowny Panie Premierze,*

w związku z przedłożonym projektemustawy pozwalam sobie wyrazić poniższą opinię.

1. W projektowanym art. 1 pkt 2 lit. b (dodawany do *ustawy o krajowym systemie cyberbezpieczeństwa* pkt 8a w art. 2) wprowadzono definicję incydentu telekomunikacyjnego, zgodnie z którą incydentem telekomunikacyjnym jest incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi komunikacji elektronicznej. W tym kontekście chciałbym wskazać na *dyrektywę 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*, która zawiera definicję pojęcia „incydent”. Zgodnie z tą definicją incydentem jest każde zdarzenie, które ma rzeczywiście niekorzystny wpływ na bezpieczeństwo sieci i systemów informatycznych.

Projektowana ustawa przewiduje odrębny od obecnie obowiązującego reżim postepowania w przypadku wystąpienia incydentu telekomunikacyjnego. Wskazać należy, że incydent telekomunikacyjny może być objęty zakresem stosowania dyrektywy 2016/1148, w szczególności jeśli ma istotny wpływ na świadczenie usługi cyfrowej w rozumieniu art. 4 *rozporządzenia wykonawczego Komisji (UE) 2018/151 z dnia 30 stycznia 2018 r. ustanawiającego zasady stosowania dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 w odniesieniu do dalszego doprecyzowania elementów, jakie mają być uwzględnione przez dostawców usług cyfrowych w zakresie zarządzania istniejącymi ryzykami dla bezpieczeństwa sieci i systemów informatycznych, oraz parametrów służących do określenia, czy incydent ma istotny wpływ*. Z projektowanych przepisów nie wynika jednak, że przedsiębiorca komunikacji elektronicznej, w przypadku gdy incydent telekomunikacyjny jest również incydentem w rozumieniu dyrektywy 2016/1148 oraz rozporządzenia wykonawczego 2018/151, powinien podjąć działania właściwe dla danej kategorii incydentu.

W związku z powyższym obowiązki przedsiębiorcy komunikacji elektronicznej powinny zostać rozszerzone o obowiązki wynikające z *ustawy o krajowym systemie cyberbezpieczeństwa* w odniesieniu do każdej z kategorii incydentu, a w szczególności do incydentu istotnego, zgodnie z rozporządzeniem wykonawczym 2018/151.

1. Jeśli przedsiębiorca komunikacji elektronicznej świadczy usługi kluczowe (usługi DNS, prowadzi punkt wymiany ruchu internetowego (IXP) oraz zarządza rejestracją internetowych nazw domen w ramach domeny najwyższego poziomu (TLD)), powinien spełniać wymogi w zakresie bezpieczeństwa i zgłaszania incydentów, o których mowa w art. 14 dyrektywy 2016/1148. W szczególności obowiązki w odniesieniu do wdrożenia systemu zarządzania bezpieczeństwem w systemie informacyjnym wykorzystywanym do świadczenia usługi kluczowej (art. 8 *ustawy o krajowym systemie cyberbezpieczeństwa*), obowiązki operatora usługi kluczowej (art. 9, 10, 11 *ustawy o krajowym systemie cyberbezpieczeństwa*), które wdrażają art. 14 dyrektywy. W projektowanej ustawie nie przewidziano jednak przepisu, zgodnie z którym, w sytuacji gdy przedsiębiorca komunikacji elektronicznej jest operatorem usługi kluczowej, powinien wypełniać powyższe obowiązki.

Ponadto, przedsiębiorca komunikacji elektronicznej, jako dostawca usług cyfrowych, powinien podejmować właściwe i proporcjonalne środki techniczne i organizacyjne określone w rozporządzeniu wykonawczym 2018/151 w celu zarządzania ryzykiem, na jakie narażone są systemy informacyjne wykorzystywane do świadczenia usługi cyfrowej. Z projektowanych przepisów nie wynika jednak, że przedsiębiorca komunikacji elektronicznej powinien również spełniać te wymogi.

Wobec powyższego projektowana ustawa powinna zostać uzupełniona o wskazanie, że przedsiębiorca komunikacji elektronicznej, w przypadku uznania go za operatora usługi kluczowej, jest zobowiązany do wypełnienia obowiązków, o których mowa w rozdziale 3 *ustawy o krajowym systemie cyberbezpieczeństwa* (wdrożenie art. 14 dyrektywy 2016/1148), a jako dostawca usług cyfrowych obowiązków, o których mowa w rozdziale 4 ustawy (wdrożenie art. 16 dyrektywy 2016/1148).

1. Z projektowanego art. 1 pkt 12 projektu (dodawany do ustawy art. 20c ust. 1 pkt 2) wynika, że do zgłoszenia incydentu telekomunikacyjnego zobowiązany jest przedsiębiorca komunikacji elektronicznej, sporządzający plan, o którym mowa w art. 47 ust. 1 *ustawy – Prawo komunikacji elektronicznej*. Tymczasem z art. 47 ust. 1 *projektu ustawy Prawo komunikacji elektronicznej* wynika, że do sporządzenia planu działań w sytuacji szczególnego zagrożenia zobowiązany jest przedsiębiorca telekomunikacyjny. Należy zauważyć, że pojęcie przedsiębiorcy telekomunikacyjnego jest węższe niż pojęcie przedsiębiorcy komunikacji elektronicznej, które obejmuje również podmioty świadczące usługę komunikacji interpersonalnej niewykorzystującą numerów.

Takie sformułowanie przepisów może prowadzić do interpretacji, zgodnie z którą ta kategoria przedsiębiorców, tj. podmioty świadczące usługę komunikacji interpersonalnej niewykorzystującą numerów, nie będzie zobowiązana do zgłaszania incydentów telekomunikacyjnych.

Powyższe rozwiązanie budzi wątpliwości w kontekście zgodności z art. 40 ust. 2 *dyrektywy 2018/1972 ustanawiającej Europejski kodeks łączności elektronicznej*. Przepis ten nakłada bowiem na podmioty udostępniające publiczne sieci łączności elektronicznej lub świadczące publicznie dostępne usługi łączności elektronicznej obowiązek zgłaszania incydentów. Zgodnie z definicją usługi łączności elektronicznej określoną w art. 2 pkt 4 dyrektywy 2018/1972 w kategorii podmiotów zobowiązanych do zgłaszania incydentów mieszczą się również podmioty świadczące usługę komunikacji interpersonalnej niewykorzystującą numerów.

Wobec powyższego obowiązek zgłaszania incydentów należy rozszerzyć na podmioty świadczące usługę komunikacji interpersonalnej niewykorzystującą numerów.

1. W projektowanym art. 1 pkt 12 (dodawany do ustawy o krajowym systemie cyberbezpieczeństwa rozdział 4a) określono obowiązki przedsiębiorców komunikacji elektronicznej. Zwracam uwagę, że zawarte w nim przepisy mogą zostać uznane za zasady dotyczące usług społeczeństwa informacyjnego w rozumieniu art. 1 ust. 1 lit. e) *dyrektywy (UE) 2015/1535 ustanawiającej procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego*, podlegające obowiązkowi notyfikacji. Przywołany przepis dyrektywy definiuje bowiem zasady dotyczące usług jako wymogi o charakterze ogólnym odnoszące się w szczególności do podejmowania i wykonywania działalności usług społeczeństwa informacyjnego, takie jak przepisy dotyczące dostawcy usług, usług i odbiorców usług.

Należy również zwrócić uwagę na dodawane art. 66a-66c (art. 1 pkt 29 projektu) i art. 67a-67c (art. 1 pkt 30 projektu), które wprowadzają możliwość ustanowienia ograniczeń w swobodnym przepływie towarów i usług społeczeństwa informacyjnego polegających w szczególności na zakazie wprowadzania do użytkowania sprzętu, oprogramowania i usług, nakazie ich wycofania z użytkowania, nakazie wprowadzenia określonych zmian w sprzęcie lub oprogramowaniu, zakazie korzystania albo nakazie wstrzymania dystrybucji. Wydaje się, że wskazane jest powiadomienie Komisji również o tych przepisach, niezależnie od konieczności notyfikowania konkretnych decyzji, w przypadku gdyby zawierały przepisy techniczne w rozumieniu art. 1 ust. 1 lit. f) dyrektywy 2015/1535.

Niezależnie od powyższego przypominam, że w przypadku, gdyby decyzje podejmowane na podstawie wskazanych przepisów ustawy miały skutkować ograniczeniem usługi społeczeństwa informacyjnego świadczonej przez usługodawcę mającego siedzibę na terytorium innego państwa członkowskiego Europejskiego Obszaru Gospodarczego, konieczne będzie także zastosowanie procedury powiadomienia Komisji i państwa siedziby, określonej w art. 3 ust. 4-6 *dyrektywy 2000/31/WE Parlamentu Europejskiego i Rady w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym)*.

Jednocześnie informuję, że decyzję o konieczności notyfikacji na gruncie dyrektywy 2015/1535 podejmuje projektodawca, w przypadku wątpliwości możliwe jest zasięgnięcie w tej kwestii opinii ministra właściwego do spraw gospodarki, który pełni funkcję koordynatora krajowego systemu notyfikacji norm i aktów prawnych.

1. Zgodnie art. 1 pkt 24 lit. c projektu (zmieniany art. 44 ust. 6 *ustawy o krajowym systemie cyberbezpieczeństwa*) „w przypadku braku możliwości realizacji zadań CSIRT sektorowego w trybie określonym w ust. 1 lub ust. 5 art. 44 ustawy zmienianej, organ właściwy może, po zasięgnięciu opinii Pełnomocnika, powierzyć realizację zadań CSIRT sektorowego podmiotowi, o którym mowa w art. 4 *ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych*”. Mając na uwadze to, że przepis ten nie określa trybu powierzenia realizacji wspomnianych zadań ani nie odsyła w tym zakresie do przepisów *ustawy – Prawo zamówień publicznych*, wydaje się, że może on stanowić podstawę wyłączenia stosowania przepisów o zamówieniach publicznych do powierzenia realizacji zadań CSIRT. Mając na uwadze to, że w uzasadnieniu projektu nie odniesiono się tej kwestii, niezbędne jest jej wyjaśnienie.

Należy w tym kontekście zauważyć, że organy właściwe, o których mowa w art. 41 *ustawy o krajowym systemie cyberbezpieczeństwa,* wpisują się w definicję instytucji zamawiającej, określoną w art. 2 ust. 1 pkt 1 *dyrektywy 2014/24/UE w sprawie zamówień publicznych* i jako takie, zobowiązane są, na podstawie art. 1 ust. 1 tej dyrektywy, do dokonywania zamówień zgodnie z trybami określonymi w dyrektywie.

Dyrektywa 2014/24/UE przewiduje co prawda wyjątki od jej stosowania. W tym kontekście należy jednak podkreślić, że zgodnie z utrwalonym orzecznictwem Trybunału Sprawiedliwości UE wszelkie wyjątki od stosowania przepisów dyrektyw dotyczących zamówień publicznych są nie tylko wyczerpująco określone w tych dyrektywach, ale również podlegają wykładni zawężającej (por. wyrok TSUE w sprawie Teckal, C-107/98, pkt 43-44; wyrok TSUE w sprawie C-385/02, Komisja/Włochy, pkt 19).

Przykładowo art. 12 ust. 1-3 dyrektywy 2014/24/UE pozwala na wyłączenie stosowania jej przepisów do zamówień publicznych dokonywanych między niektórymi podmiotami sektora publicznego, natomiast zgodnie z jej art. 15 ust. 2 nie ma ona zastosowania do zamówień publicznych i konkursów, w stopniu, w jakim stosowanie tej dyrektywy zobowiązywałoby państwo członkowskie do dostarczania informacji, których ujawnienie państwo to uważa za sprzeczne z jego podstawowymi interesami w zakresie bezpieczeństwa.

Projektodawca powinien zatem wyjaśnić, czy spełnione zostały przesłanki skorzystania z tych lub innych wyłączeń dopuszczalnych na gruncie dyrektywy 2014/24/UE.

Możliwe jest też rozważenie, czy wspomniany przepis nie mieści się w zakresie regulacji dyrektywy 2009/81/WE z dnia 13 lipca 2009 r. w sprawie koordynacji procedur udzielania niektórych zamówień na roboty budowlane, dostawy i usługi przez instytucje lub podmioty zamawiające w dziedzinach obronności i bezpieczeństwa, która zgodnie z art. 13 ust. 1 lit a) nie ma zastosowania do zamówień, w przypadku których stosowanie przepisów tej dyrektywy zobowiązałoby państwo członkowskie do dostarczenia informacji, których ujawnienie uznaje ono za sprzeczne z jego podstawowymi interesami bezpieczeństwa. Do skorzystania z tego wyłączenia niezbędne jest jednak wykazanie przez projektodawcę po pierwsze, że projektowany przepis mieści się w zakresie regulacji dyrektywy 2009/81/WE, po drugie zaś, że spełnione zostały przesłanki wyłączenia jej stosowania.

1. W projektowanej ustawie przewidziano zmianę w art. 109 ust. 1 *ustawy – Prawo zamówień publicznych* polegająca na dodaniu wśród podstaw wykluczenia wykonawcy przesłanki odnoszącej się do tego, że jest on „dostawcą sprzętu lub oprogramowania, wobec którego stwierdzono wysokie ryzyko, w ramach oceny, o której mowa w art. 66a ust. 1 *ustawy o krajowym systemie cyberbezpieczeństwa*” (art. 2 pkt 2 projektu, projektowany art. 109 ust. 1 pkt 11). Zmieniany przepis art. 109 ust. 1 *ustawy – Prawo zamówień publicznych* stanowi z kolei transpozycję art. 57 dyrektywy 2014/24/UE, w którym określono podstawy wykluczenia wykonawcy. W kontekście projektowanego wyłączenia zastosowanie mogłaby ewentualnie znaleźć przesłanka określona w art. 57 ust. 4 lit. c), zgodnie z którym instytucje zamawiające mogą wykluczyć lub zostać zobowiązane przez państwa członkowskie do wykluczenia wykonawcy z udziału w postępowaniu o udzielenie zamówienia, jeśli mogą wykazać za pomocą stosownych środków, że wykonawca jest winny poważnego wykroczenia zawodowego, które podaje w wątpliwość jego uczciwość. Skorzystanie ze wspomnianego wyłączenia wymagałoby jednak wykazania przez projektodawcę, że wysokie ryzyko, o którym mowa w tym przepisie, stwierdza się na podstawie wykroczeń zawodowych.

**Projekt ustawy, z zastrzeżeniem uwag zgłoszonych w niniejszej opinii, nie jest sprzeczny z prawem Unii Europejskiej.**

*Z poważaniem*

Konrad Szymański

Minister do Spraw Unii Europejskiej

*/podpisano kwalifikowanym podpisem elektronicznym/*