Do druku nr 3457

KRASP Konferencja Rektorów Akademickich Szkół Polskich

Warszawa, 24 lipca 2023 r.
KRASP/152/2023

Szanowny Pan
Dariusz Salamończyk
Zastępca Szefa
Kancelarii Sejmu

SEKRETARIAT Z-CY SZEFA KS
L.dz. DS.175.473.2023
Data wpływu 27.07.2023

Szanowny Panie Ministrze,

w odpowiedzi na pismo nr SPS-WP.020.188.4.2023 z 6 lipca 2023 r. w załączeniu przesyłam opinię Komisji ds. Infrastruktury informatycznej Konferencji Rektorów Akademickich Szkół Polskich w sprawie rządowego projektu ustawy o zmianie ustawy o krajowym systemie ceberbezpieczeństwa oraz niektórych innych ustaw.

WYDZIAŁ OBSŁUGI PREZYDIUM SEJMU
L. dz. SPS-WP.020.188.12.2023
Data wpływu 27.07.23r.

Z wyrazami szacunku,

prof. dr hab. inż. Arkadiusz Mężyk
Przewodniczący KRASP

Biuro KRASP

Uniwersytet Warszawski
ul. Krakowskie Przedmieście 26/28, 00-927 Warszawa
tel.: 22 55 20 352
biuro@krasp.org.pl | www.krasp.org.pl

Przewodniczący KRASP

prof. dr hab. inż. Arkadiusz Mężyk
Rektor Politechniki Śląskiej
president@krasp.org.pl

Katowice, 21.07.2023

Opinia Komisji ds. Infrastruktury Informatycznej KRASP
na temat projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (Druk sejmowy 3457) w zakresie jej wpływu na uczelnie

I. Zgodnie z przesłanym projektem ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa uczelnie są podmiotami krajowego systemu cyberbezpieczeństwa na podstawie art.4 pkt.8 projektu ustawy jako podmioty wymienione w art.7 ust.1 pkt.1 ustawy z dnia 20 lipca 2018 roku Prawo o szkolnictwie wyższym.

Uczelnie jako podmioty objęte krajowym systemem cyberbezpieczeństwa będą podlegały nowym obowiązkom oraz ograniczeniom przewidzianym w projektowanych przepisach ustawy, w tym:

1) obowiązkowi wyznaczenia dwóch osób odpowiedzialnych za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa (zgodnie z obecnie obowiązującą ustawą obowiązek dotyczył wyznaczenia jednej osoby);
2) zakazowi wprowadzania do użytkowania typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT w zakresie objętym decyzją o uznaniu dostawcy za „dostawcę wysokiego ryzyka" (pojęcie, które będzie wprowadzone do porządku prawnego) dostarczanych przez tego dostawcę (art.66b ust.1 pkt 2);
3) obowiązkowi wycofania z użytkowania typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT w zakresie objętym decyzją dostarczanych przez dostawcę wysokiego ryzyka nie później niż 7 lat od dnia ogłoszenia lub udostępnienia informacji o decyzji Ministra właściwego do spraw cyfryzacji (art.66b ust.1 pkt 2);
4) zakazowi nabywania sprzętu, oprogramowania i usług określonych w decyzji o uznaniu dostawy sprzętu lub oprogramowania od „ dostawcy wysokiego ryzyka" (art.66b ust.4);
5) obowiązkowi udzielania informacji na wniosek uprawnionych podmiotów wymienionych w ust.2 art.66c o wycofanych produktach ICT, rodzajach usług ICT i konkretnych procesach ICT objętych decyzją o uznaniu dostawcy za „dostawcę wysokiego ryzyka" (art.66c ust.1);
6) obowiązkowi odrzucenia oferty wykonawcy wybieranego w procedurze zamówienia publicznego, w przypadku, gdy obejmuje ona produkt ICT , którego typ został określony w decyzji o uznaniu dostawcy za dostawcę wysokiego ryzyka lub usługę ICT lub proces ICT określonych w decyzji (proponowane dodanie pkt. 19 do art.226 ust.1 ustawy Prawo zamówień publicznych).

Z tytułu niewypełnienia obowiązków wymienionych powyżej pod pkt.1-5 na podmiot zobowiązany mogą zostać nałożone kary pieniężne w drodze decyzji administracyjnych

określone w art. 73 ust.2a-2c proponowanych przepisów zmieniających. Proponowany przepis art.73 ust.6 i 7 ustawy przewiduje niezależnie od kar nałożonych na podmiot możliwość nałożenia kar pieniężnych na kierującego podmiotem publicznym za brak wyznaczenia osób odpowiedzialnych za utrzymanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa oraz za brak udzielenia informacji o wycofanych produktach, usługach oraz procesach ICT, o którym mowa w art.66c projektu ustawy.

II. Uwagi do przepisów projektu ustawy:
Należy zauważyć, że w uzasadnieniu projektu ustawy oraz określeniu wpływu ustawy na uczelnie, projektodawca wymienił jedynie obowiązek wyznaczenie dwóch przedstawicieli uczelni odpowiedzialnych za kontakty z podmiotami krajowego systemu bezpieczeństwa. Jeśli taki jest zamiar projektodawcy to w ustawie powinien zostać dodany zapis wyłączający stosowanie przepis art.66b i 66c w stosunku do uczelni (analogiczny zapis art.67b dotyczy NPB). Dodanie ustawowego wyłączenia jest uzasadnione w świetle konsekwencji, w tym finansowych dla uczelni z tytułu obowiązku stosowania art.66b oraz 66c.

Biorąc pod uwagę, że w przedstawionym projekcie ustawy nie ma proponowanego wyłączenia, poniższe uwagi dotyczą tekstu aktu prawnego nie zawierającego powyższego wyłączenia:

1) w związku z propozycją wprowadzenia pojęcia „ dostawcy wysokiego ryzyka" na mocy decyzji administracyjnej Ministra właściwego do spraw informatyzacji oraz obowiązków z tym związanych dla podmiotów - łącznie z zakazem nabywania produktów, sprzętu i usług określonych w decyzji lub obowiązkiem ich wycofania z użytkowania- właściwym byłoby, aby w przedmiotowej decyzji były one precyzyjnie wymienione. Natomiast przepis art.66a ust.13 stanowi, że decyzja zawiera w szczególności wskazanie typów produktów ICT, rodzajów usług ICT. Biorąc pod uwagę konsekwencje decyzji, wskazanie poprzez typy produktów lub rodzaje usług może prowadzić do konieczności interpretacji przed podmiot, czy konkretny oferowany produkt ICT jest objęty decyzją. Poza tym w art.66b ust.4 mowa jest o zakazie nabywania sprzętu, oprogramowania i usług określonych w decyzji, o której mowa w art.66a ust.12. Porównanie tych zapisów wskazuje na niespójność pojęciową, która może skutkować trudnością w stosowaniu przepisów przez podmioty zobowiązane;
2) w związku z kompetencją Ministra do spraw informatyzacji do wydawania decyzji o uznaniu dostawców za „dostawców wysokiego ryzyka" i określeniu w decyzji typów produktów, rodzajów usług lub konkretnych procesów ICT wskazanym byłoby, aby „Lista" prowadzona przez Ministra, o której mowa w art.66e była uzupełniona o termin wydania/ogłoszenia decyzji, która jest dla podmiotów zobowiązanych szczególnie istotna pod kątem obowiązku wycofania ich z użytkowania lub zakazie nabywania;
3) w proponowanej zmianie ustawy w art.73 dotyczącym kar pieniężnych wprowadzono zmiany skutkujące możliwością nałożenia kar pieniężnych na dodatkowa grupę podmiotów określonych w art.66a ust.1 pkt.1-3 ustawy (w której mieszczą się uczelnie) za niedochowanie obowiązków nałożonych ustawą. Przepisy te przewidują poza nałożeniem kar pieniężnych na podmiot możliwość jednoczesnego nałożenia kary pieniężnej na osobę kierującą podmiotem. Proponuje się rezygnację z tego systemu

karania. Analiza przepisów dotyczących kar prowadzi także do wniosku, iż nie zostały one odpowiednio zróżnicowane w stosunku do rodzaju podmiotów oraz skutków naruszeń. W związku z tym wskazana byłaby rezygnacja z ich stosowania wobec uczelni lub znaczne obniżenie ich wysokości w stosunku do uczelni i osób kierujących nimi;

4) w uzasadnieniu projektu ustawy wskazano, że nie oszacowano kosztów wycofywania sprzętu/ usług objętych decyzjami Ministra o uznaniu dostawcy za dostawcę wysokiego ryzyka. Ustawodawca przyjął, że podmioty są zobowiązane wycofać te produkty w okresie 7 lat od ogłoszenia decyzji. W uzasadnieniu ustawy argumentuje się, że 7 lat to termin średniego życia tego typu produktu, natomiast w przypadku uczelni ten termin może być dłuższy. W tym wypadku koszty obligatoryjnego wycofania produktu, a w konsekwencji konieczności nabycia produktu zastępczego faktycznie poniesie uczelnia. W związku z powyższym powinny być zabezpieczone środki publiczne na pokrycie tych kosztów, które będą skutkiem wydawanych decyzji przez Ministra do spraw cyfryzacji.

Przewodnicząca Komisji
ds. Infrastruktury Informatycznej KRASP
Prof. dr hab. inż. Celina M. Olszak

Celina Olszak