Ministerstwo
Cyfryzacji

Sekretarz Stanu
Paweł Olszewski

BM.WP.057.72.2024
Warszawa, 05 sierpnia 2024 r.

Szanowna Pani
Małgorzata Kidawa - Błońska
Marszałek Senatu RP

Dot. pisma z 2 lipca 2024 r. w sprawie oświadczenia złożonego przez Senatora RP Pana Andrzeja Kaletę podczas 14 posiedzenia Senatu RP w dniu 26 czerwca 2024 r. (BPS/043-14-290-MC/24)

Szanowna Pani Marszałek,

poniżej przedstawiam odpowiedzi na złożone przez Senatora oświadczenie.

Ad 1) Czy jeśli chodzi o podmioty objęte ustawą, to zakłady i prywatne firmy działające w powiatach żywieckim i cieszyńskim będą objęte nowymi przepisami? Chodzi o następujące zakłady i firmy: Celma Indukta SA, producent silników elektrycznych, będący częścią grupy Cantoni Motor, posiadający zakład w Cieszynie; PPG Polifarb Cieszyn SA z siedzibą w Cieszynie; Elektrometal SA z siedzibą w Cieszynie; Grupa Żywiec SA z zakładami w Żywcu; Hutchinson Poland Sp. z o.o. z siedzibą i zakładami w Żywcu; Famed Żywiec Sp. z o.o.; Sews-Cabind Poland Sp. z o.o. z zakładami w Żywcu, będąca częścią Grupy Sumitomo; Perrot Polska Sp. z o.o.; Orex Rotomoulding Sp. z o.o.; Nordflam HS Sp. z o.o.

Projektowana ustawa określa kryteria, jakie podmiot musi spełnić, aby być objęty jej regulacjami. Wprowadzenie zasady samoidentyfikacji oznacza, że podmioty, w tym przedsiębiorcy z powiatu żywieckiego i cieszyńskiego, ustalą czy spełniają przesłanki do bycia podmiotem kluczowym lub ważnym w rozumieniu projektowanej ustawy, a tym samym czy są objęci jej regulacjami.

Ad 2) Czy Ministerstwo Cyfryzacji przeprowadziło analizę zgodności nowych przepisów z dyrektywą UE 2022/2555? Jeżeli tak, to proszę o udostępnienie wyników tej analizy.

Wynikiem analizy jest zamieszczona w Biuletynie Informacji Publicznej tabela zgodności projektowanych przepisów z wdrażaną dyrektywą. Przedmiotowe dokumenty dostępne są na stronie internetowej Rządowego Procesu Legislacyjnego.

Ad 3) Czy istnieją plany wsparcia finansowego dla podmiotów w celu zminimalizowania wpływu kosztów? Ile podmiotów z powiatów żywieckiego i cieszyńskiego zostanie objętych nowymi przepisami? Czy Ministerstwo Cyfryzacji posiada szczegółowe dane dotyczące liczby tych podmiotów? Czy przeprowadzono weryfikację wpływu kosztów na j.s.t.? Jaka była metodologia? Skąd j.s.t. mają mieć środki na dostosowanie się do nowych wymogów cyberbezpieczeństwa?

Ministerstwo Cyfryzacji nie dysponuje szczegółowymi danymi dotyczącymi liczby podmiotów objętych ustawą z powiatów żywieckiego i cieszyńskiego. Związane jest to z brakiem informacji w tabelach REGON dotyczących wielkości podmiotu – wielkość ta jest określana przez pryzmat liczby pracowników, tymczasem do oceny wielkości podmiotu należy wziąć pod uwagę roczny obrót albo roczną sumę bilansową. Ponadto tablice REGON nie obejmują podziału na powiaty.

Odnośnie wpływu finansowego projektu ustawy na jednostki samorządu terytorialnego to

telefon +48 22 245 54 42
adres email sekretariat.BM@cyfra.gov.pl
www.gov.pl/web/cyfryzacja

ul. Królewska 27
00-060 Warszawa

podmioty publiczne, w tym jednostki samorządu terytorialnego już obecnie są obowiązane do zgłaszania incydentów w podmiocie publicznym oraz do zarządzania incydentami, co wynika z art. 22 ustawy o krajowym systemie cyberbezpieczeństwa. Ponadto podmioty publiczne mają obowiązek wdrożenia systemu zarządzania bezpieczeństwem informacji i przeprowadzania m.in. audytów (co wynika z § 19 rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[1]). Podsumowując, już obecnie jednostki samorządu terytorialnego mają obowiązki z zakresu cyberbezpieczeństwa i powinny uwzględniać koszty z tym związane w ramach standardowego planowania budżetowego. Dostosowanie się podmiotów publicznych, w tym jednostek samorządu terytorialnego, do wymogów dyrektywy NIS2 będzie polegało na przeglądzie już wdrożonych systemów zarządzania bezpieczeństwem informacji i uzupełnienia dokumentacji oraz środków technicznych i organizacyjnych. Skala zmian będzie zależna od obecnej dojrzałości organizacyjnej poszczególnych podmiotów publicznych.

W ramach inwestycji C3.1.1 Cyberbezpieczeństwo - CyberPL, infrastruktura przetwarzania danych i dostarczania usług cyfrowych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo – Komponent Cyberbezpieczeństwo (subinwestycja C3.1.1.1), planowane jest uruchomienie czterech projektów dedykowanych dla wybranych grup podmiotów krajowego systemu cyberbezpieczeństwa, w tym dla jednostek sektora finansów publicznych.

Aktualnie trwają prace do przygotowania naborów, z uwzględnieniem ich celu określonego w Krajowym Planie Odbudowy i zwiększania odporności. Docelowe grupy odbiorców wsparcia będą wynikały bezpośrednio z tych założeń. Uruchamianie naborów dla tych projektów planowane jest sukcesywnie w kolejnych kwartałach bieżącego roku.

Ad 4) W jaki sposób nowe przepisy wpłyną na funkcjonowanie małych i średnich przedsiębiorstw z powiatów cieszyńskiego i żywieckiego? Czy ministerstwo zamierza uzupełnić te informacje? Jeśli tak, to kiedy można się tego spodziewać? Czy ministerstwo przewiduje dodatkowe wsparcie dla tych firm, aby pomóc im w dostosowaniu się do nowych wymogów?

Dyrektywa podzieliła podmioty na podmioty kluczowe (co najmniej duzi przedsiębiorcy) i podmioty ważne (co najmniej średni przedsiębiorcy). Istnieje od tego kilka wyjątków, przykładowo wszyscy przedsiębiorcy telekomunikacyjni, bez względu na wielkość, podlegają obowiązkom z dyrektywy 2022/2555.

Nałożono obowiązki na podmioty kluczowe i podmioty ważne zgodnie z wykazem tych podmiotów wskazanych w załączniku nr 1 i 2 do dyrektywy NIS2. Będą one obowiązane dokonać samorejestracji w wykazie podmiotów kluczowych i ważnych, co umożliwi ich identyfikację, aktywne wsparcie ich przez zespoły CSIRT sektorowe i zespoły CSIRT poziomu krajowego oraz wykonywanie czynności nadzorczych przez organy właściwe do spraw cyberbezpieczeństwa.

Podmioty kluczowe i podmioty ważne będą obowiązane wprowadzić system zarządzania bezpieczeństwem informacji w procesach służących świadczeniu usług przez te podmioty. Odpowiada to zakresowi wymogów co do środków zarządzania ryzykiem wskazanych w art. 21 dyrektywy.

Kierownik podmiotu kluczowego lub podmiotu ważnego będzie odpowiedzialny za realizację tych zadań przez podmiot – i będą mogły być nałożone na niego kary.

[1] Dz. U. poz. 773

Będzie miał też obowiązek przejścia stosownego szkolenia z zakresu cyberbezpieczeństwa.

Projektowana ustawa w zakresie zgłaszania incydentów zwiększa liczbę obowiązków nakładanych na podmioty objęte jej regulacją. Podmioty kluczowe i ważne będą w pierwszej kolejności zgłaszać wczesne ostrzeżenie o incydencie poważnym. Zgłoszenia będą kierowane do CSIRT sektorowego. Wczesne ostrzeżenie będzie mogło zawierać wniosek o wskazanie wytycznych dotyczących możliwych do wdrożenia środków ograniczających skutki incydentu poważnego lub o udzielenie dodatkowego wsparcia technicznego przy obsłudze incydentu. Po otrzymaniu takiego wniosku CSIRT sektorowy zobowiązany będzie do udzielenia stosownego wsparcia podmiotowi zgłaszającemu taki wniosek. Następnie dokonywane będzie zgłoszenie incydentu. W trakcie obsługi incydentu, na wniosek właściwego CSIRT sektorowego, przekazywane będzie sprawozdanie okresowe, a po zakończeniu obsługi incydentu – sprawozdanie końcowe.

Podmioty, które mogą spełniać kryteria uznania za podmioty kluczowe lub podmioty ważne będą mogły być „odpytywane" przez organy właściwe do spraw cyberbezpieczeństwa o informacje, które pozwolą ustalić ich status. Brak udzielenia odpowiedzi będzie skutkował nałożeniem administracyjnej kary pieniężnej.

W związku z nałożeniem na podmioty krajowego systemu cyberbezpieczeństwa szeregu obowiązków istotne zmiany zachodzą w przepisach dotyczących nadzoru i egzekwowania przepisów, a także wymierzania kar administracyjnych. Projektowane regulacje wyposażają organy właściwe do spraw cyberbezpieczeństwa w szerokie kompetencje nadzoru i egzekwowania przepisów, takie jak wydawanie ostrzeżeń, nakazów, decyzji administracyjnych nakazujących podjęcie lub zaniechanie określonego działania. Organy te zostaną również wyposażone w środki, które znajdą zastosowanie w sytuacji, w której podmiot kluczowy lub podmiot ważny nie wykonał w terminie postanowień określonych w ostrzeżeniu, nakazie, czy decyzji. Wśród obowiązków nakładanych na organy właściwe do spraw cyberbezpieczeństwa należy wymienić w szczególności obowiązek brania pod uwagę określonych kryteriów, które należy przeanalizować w celu podjęcia działań nadzorczych i egzekowania przepisów, a także wymierzając karę pieniężną.

Rozbudowany został również katalog przypadków określających kiedy podmioty kluczowe lub podmioty ważne podlegają karze pieniężnej. Oznacza to co do zasady zwiększenie zadań dla organów właściwych do spraw cyberbezpieczeństwa, które będą musiały wymierzać kary pieniężne za określone działania lub zaniechania, których dopuszczać się będą podmioty kluczowe lub podmioty ważne. Ponownie należy podkreślić, że wymierzając karę pieniężną organy właściwe do spraw cyberbezpieczeństwa obligatoryjnie będą musiały dokonywać analizy określonych w projektowanych przepisach przesłanek.

Podkreślić należy, że wobec podmiotów ważnych zastosowano słabsze środki nadzoru – podmioty te będą nadzorowane dopiero po uzyskaniu informacji o naruszeniu ustawy (ex post).

Odnosząc się do pytania Pana Senatora o planowanych działaniach w stworzeniu lepszego klimatu dla działalności małych i średnich przedsiębiorstw to przygotowywane jest rozporządzenie w sprawie udzielania pomocy de minimis na rozwój produktów i usług z zakresu cyberbezpieczeństwa w ramach programu „Cyfrowa Europa". Projektowane rozporządzenie ma umożliwić ministrowi właściwemu do spraw informatyzacji udzielanie pomocy *de minimis* na inwestycje z zakresu cyberbezpieczeństwa. Dzięki projektowanym

przepisom minister właściwy do spraw informatyzacji będzie mógł udzielać wsparcia mikro-, małym i średnim przedsiębiorcom na:

1) rozwój istniejącego produktu z zakresu cyberbezpieczeństwa;
2) rozwój istniejącej usługi z zakresu cyberbezpieczeństwa;
3) stworzenie nowego produktu lub nowej usługi z zakresu cyberbezpieczeństwa;
4) zwiększenie rozpoznawalności produktów lub usług z zakresu cyberbezpieczeństwa na rynku, m. in. poprzez udział w zagranicznych misjach handlowych, konferencjach, targach, działaniach wspierających promocję oferowanych rozwiązań czy nawiązywanie współpracy biznesowej;
5) certyfikację produktu lub usługi pod kątem ich cyberbezpieczeństwa, w tym na pokrycie kosztów związanych z przygotowaniem do procesu certyfikacji.

Ad 5) Jakie kroki podjęło ministerstwo, aby uwzględnić specyfikę regionu Beskidu Śląskiego, gdzie wiele międzynarodowych grup i koncernów posiada swoje oddziały lub siedzibę? Czy istnieją plany konsultacji z lokalnymi przedsiębiorcami w celu lepszego zrozumienia ich potrzeb i obaw? Jak nowe przepisy będą się miały do pogarszającego się otoczenia inwestycyjnego? Czy nie spowodują wzrostu kosztów i przeniesienia produkcji do innych krajów UE lub poza UE?

Ministerstwo Cyfryzacji zawsze jest otwarte na robocze spotkania z przedsiębiorcami. Zwracam uwagę, że w całej Unii Europejskiej będą obowiązywać jednolite wymogi z zakresu cyberbezpieczeństwa. Analogiczne warunki, wymagania i standardy będą obowiązywać w każdym państwie członkowskim UE.

Z wyrazami szacunku,
Paweł Olszewski
Sekretarz Stanu
/dokument podpisany elektronicznie/

Do wiadomości:
Kancelaria Prezesa Rady Ministrów - Departament Spraw Parlamentarnych

telefon +48 22 245 54 42
adres email sekretariat.BM@cyfra.gov.pl
www.gov.pl/web/cyfryzacja

ul. Królewska 27
00-060 Warszawa