FEDERACJA
PRZEDSIĘBIORCÓW
POLSKICH

RPW/98866/2017 P
Data:2017-11-21

Warszawa, 17 listopada 2017 r.

Ministerstwo Cyfryzacji
Ulica Królewska 27
00—060 Warszawa

Dokument dotyczy: Konsultacji Społecznych do projektu ustawy o krajowym systemie cyberbezpieczeństwa z dnia 31 października 2017 roku (dalej: Projekt)

Szanowna Pani Minister,

w imieniu przedsiębiorców skupionych w Federacji Przedsiębiorców Polskich, w związku przedstawieniem projektu ustawy o krajowym systemie cyberbezpieczeństwa z dnia 31 października 2017 roku (dalej: Projekt) uprzejmie przekazuję następujące uwagi.

Uwagi do projektu ustawy o krajowym systemie cyberbezpieczeństwa z dnia 31 października 2017 roku

Jak wynika z uzasadnienia Projektu oraz uzasadnienia do niego, celem regulacji jest rozbudowa systemu cyberbezpieczeństwa państw członkowskich Unii Europejskiej. W pierwszej kolejność należy sobie zadać pytanie co jest przedmiotem ochrony tej ustawy. Nikt nie atakuje ani nie utrzymuje systemów informacyjnych dla samych siebie, ale po to, aby przy ich użyciu przetwarzać dane. Tym samym faktycznym przedmiotem ochrony są dane przetwarzane w systemach informacyjnych.

Wskazać należy, że incydenty bezpieczeństwa w systemach informacyjnych, takie jak ujawnienie, przejęcie lub utrata danych, wywołują w przeważającej mierze skutki niemożliwe do usunięcia. Jest to o tyle istotne, że w dzisiejszych czasach przetwarza się w ten sposób zdecydowaną większość danych.

Poufność raz przejętych lub ujawnionych danych nigdy nie zostanie przywrócona. Dlatego też najważniejsze jest położenie nacisku na prewencyjny charakter ustawy.

W projekcie ustawy widoczne są rozbudowane przepisy dotyczące kwestii formalnych i instytucjonalnych. Faktem jest, że kwestie formalne i instytucjonalne nie odegrają istotnej, a może nawet żadnej, roli prewencyjnej w zakresie cyberbezpieczeństwa.

W tym celu należy wprowadzić surowe przepisy sankcjonujące naruszenia, włącznie z przepisami karnymi (prewencja poprzez odstraszenie) oraz doprecyzować przepisy dotyczące wymaganych zabezpieczeń systemów informacyjnych (prewencja poprzez techniczne zabezpieczenie).

1. Doprecyzowanie przepisów dotyczących zabezpieczeń systemów informacyjnych.

Zgodnie z art. 10 ust. 2 pkt 3 Projektu operatorzy usług kluczowych wdrażają system zarządzania bezpieczeństwem zapewniający w szczególności odpowiednie i proporcjonalne środki techniczne i organizacyjne w celu analizowania i zarządzania ryzykami, na jakie narażone są systemy informacyjne wykorzystywane przez nich do świadczenia usług kluczowych uwzględniając najnowszy stan wiedzy oraz zapewniając poziom bezpieczeństwa systemów informacyjnych odpowiedni do istniejącego ryzyka.

Analogiczne postanowienie dotyczy dostawców usług cyfrowych w zakresie świadczonych przez nich usług cyfrowych (*vide* art. 18 ust. 2 Projektu).

Takie ujęcie sprawy podyktowanej jest prawdopodobnie słusznym przyjęciem przez ustawodawcę, że wprowadzenie konkretnych sposobów zabezpieczeń do porządku prawnego nie jest rozwiązaniem idealnym. Nie sposób bowiem nowelizować ustawę za każdym razem jak pojawią się nowe sposoby zabezpieczania systemów informacyjnych.

Z drugiej strony zatrzymanie się na sformułowaniu „odpowiednie i proporcjonalne środki techniczne (...) uwzględniając najnowszy stan wiedzy" jest dalece niewystarczające.

Jak wynika z doświadczeń, zebranych m. in. na kanwie ustawy o ochronie danych osobowych z 1997 roku, gdzie przyjęto podobne rozwiązanie (*vide* art. 36 tejże ustawy), tak ogólne sformułowanie wymagań stawianych podmiotom przetwarzającym dane jest rozwiązaniem błędnym. Po pierwsze podmioty zobowiązane nie mają informacji, a jedynie mogą się domyślać, jak należy zabezpieczać dane. W celu dookreślenia ich obowiązków muszą samodzielnie, albo poprzez zewnętrznych konsultantów, dokonywać interpretacji na pograniczu prawa i techniki, co i tak nie daje im pewności co do zgodności z ustawą.

Po drugie ustawodawca, który wprowadza tak ogólne postanowienia, ma problem z egzekucją celu jakiemu one służą. To jest ochroną danych. Spektrum możliwych interpretacji takiego postanowienia jest bowiem zbyt rozległe.

Przyjmując, że doprecyzowanie tej kwestii nie może odbywać się poprzez narzucenie obowiązanym konkretnego rozwiązania, wskazać należy na dwa sposoby rozwiązania tego problemu.

Po pierwsze można do Projektu wprowadzić przykładowe techniczne sposoby zabezpieczeń, które ponad wszelką wątpliwość zapewniają realizację celów ustawodawcy. Alternatywnie, można wprowadzić do Projektu delegację

ustawową do wydania rozporządzenia w tym zakresie, co zapewniałoby większą elastyczność regulacji prawnych, przy jednoczesnej realizacji celu.

Idąc dalej, wskazać należy, że odpowiednimi sposobami zabezpieczeń, jakie mogłyby znaleźć się w katalogu otwartym na poziomie Projektu lub rozporządzenia są szyfrowanie lub anonimizacja danych, przy czym szyfrowanie jest możliwe do zastosowania w szerszym zakresie.

Pamiętając o celu, jakim jest ochrona danych przed nieuprawnionym dostępem lub usunięciem, nie ulega wątpliwości, że odpowiednim sposobem ochrony tych danych jest szyfrowanie. Utrata kontroli nad zaszyfrowanymi danymi nie powoduje bowiem ujawnienia ich treści. Do tego wymagany jest dodatkowo dostęp do klucza szyfrującego, który dla bezpieczeństwa powinien być przechowywany w innym miejscu niż systemy informacyjne, w których dane są przetwarzane.

Dlatego też należy postulować dodanie katalogu otwartego środków technicznych zapewniających cyberbezpieczeństwo, w którym znajdzie się szyfrowanie.

Cyberbezpieczeństwo dotyczy zarówno przesyłu jak i przechowywania danych, w tym w usługach przetwarzania w chmurze, zdefiniowanych w Projekcie jako część usług cyfrowych (*vide* art. 1 pkt 20 i 21 Projektu), co Projekt powinien uwzględniać.

2. Rozszerzenie przepisów penalizujących.

Mając na uwadze powagę zagadnienia, postanowienia zawarte w Rodziale 10 Projektu „Przepisy o karach pieniężnych" są zdecydowanie niewystarczające. Maksymalną karą pieniężną przewidzianą Projektem jest 200.000,00 (dwieście tysięcy) złotych. Maksymalna wysokość kar pieniężnych jest rażąco niska. Porównać je można chociażby z karami finansowymi przewidzianymi w projekcie ustawy o ochronie danych osobowych z 12 września 2017 roku, który odsyła do Rozporządzenia ogólnego o ochronie danych osobowych z 27 kwietnia 2016 roku, które przewiduje kary pieniężne aż do 20 mln EURO lub do 4 % światowego obrotu podmiotu dokonującego naruszenia.

Zważywszy na istotę regulacji wprowadzanych Projektem, w tym dla bezpieczeństwa obywateli i Państwa, w pełni uzasadnione jest twierdzenie, że naruszenia obowiązków nakładanych Projektem, w tym przez operatorów usług kluczowych, powinny penalizowane przepisami karnymi. Szeroko rozumiane bezpieczeństwo obywateli i Państwa jest ponad wszelką wątpliwość przedmiotem ochrony Projektu.

Zauważyć należy, że przewidziane w Projekcie kary pieniężne są niewielkie. Przekładać się to będzie na marginalne traktowanie omawianych regulacji przez podmioty, które powinny stać na straży cyberbezpieczeństwa.

Po drugie, kary finansowe mają być nakładane na instytucje, nie zaś osoby, które sprawują w nich funkcje kierownicze. Tym samym, brutalnie rzecz ujmując, osoby pełniące te funkcje, co do zasady, będą miały mniejszą motywację rzetelnego stosowania się do postanowień Projektu niż, gdyby przewidywał on sankcje karne, które z natury swojej dotykałyby te właśnie osoby.

Wprowadzenie penalizacji działań i zaniechań, których skutkiem będzie lub może być uniemożliwienie wzrostu albo zamach na cyberbezpierzeństwo Rzeczpospolitej Polski wydaje się konieczne, zważywszy na doniosłość tego zagadnienia dla przyszłości kraju. Przepisy Kodeksu karnego, w tym dotyczące przestępstw przeciwko bezpieczeństwu powszechnemu (art. 163 i n. Kodeksu karnego) w żadnym stopniu nie przystają do istniejących zagrożeń płynących z cyberprzestrzeni.

Przykładowymi przestępstwami, jakie mogłyby zostać ujęte w Projekcie są: (i) nieprawidłowe zabezpieczenie danych, zwłaszcza przez operatorów usług kluczowych lub sprowadzenie zagrożenia ujawnienia lub utraty danych przetwarzanych w systemach informacyjnych; (ii) umyślne (celowe lub poprzez rażące zaniechania) ujawnienie danych przetwarzanych w systemach informacyjnych. Rolę prewencyjną w tym zakresie ustawodawca prawdopodobnie zamierza zrealizować poprzez art. 57 ust. 3 Projektu, lecz kara w nim przewidziana wydaje się zbyt niska, biorąc pod uwagę przedmiot ochrony.

Z poważaniem,

Marek Kowalski

Przewodniczący FPP

Członek Rady Dialogu Społecznego