Stowarzyszenie
Administratorów
Bezpieczeństwa
Informacji

Warszawa, dn. 13.10.2017 r.

Szanowna Pani
Anna Streżyńska
Minister Cyfryzacji

Szanowna Pani Minister,

W odpowiedzi na pismo nr DP-WLI.0211.2.2017 z dnia 14 września 2017 r. przesyłamy w załączeniu uwagi Stowarzyszenia Administratorów Bezpieczeństwa Informacji (SABI) do projektu ustawy o ochronie danych osobowych oraz projektu ustawy - Przepisy wprowadzające ustawę o ochronie danych osobowych.

Ze względu na trwające wewnątrz Stowarzyszenia ABI konsultacje uprzejmie informujemy o możliwości przesłania w najbliższych dniach dalszych uwag Stowarzyszenia.

z wyrazami szacunku

Maciej Byczkowski
Prezes Zarządu Stowarzyszenia ABI

Załącznik: Wykaz uwag do projektu ustawy o ochronie danych osobowych oraz projektu ustawy - Przepisy wprowadzające ustawę o ochronie danych osobowych .

Wykaz uwag do projektu ustawy o ochronie danych osobowych oraz projektu ustawy - Przepisy wprowadzające ustawę o ochronie danych osobowych

I. Nazwy projektów ustaw

Zwracamy uwagę, że nazwa „ustawa o ochronie danych osobowych" może wprowadzać w błąd czytelnika w tym znaczeniu, że powtarza nazwę obecnej ustawy z dnia 29 sierpnia 1997 r., a znacząco różni się od niej przedmiotem regulacji. Projektowana ustawa normuje jedynie niektóre kwestie ochrony danych osobowych w zakresie dopuszczonym ogólnym rozporządzeniem o ochronie danych (dalej „RODO"). Tymczasem obecnie obowiązująca ustawa o ochronie danych osobowych w sposób całościowy reguluje problematykę ochrony danych osobowych. Wobec tego nazwa ustawy powinna zostać zmieniona w ten sposób, żeby wskazywać, że określa jedynie niektóre aspekty ochrony danych.

Nazwa drugiej ustawy wskazuje, że jej przedmiotem są jedynie przepisy wprowadzające projektowaną ustawę o ochronie danych osobowych, podczas gdy znacząca większość jej przepisów dostosowuje prawo polskie do ogólnego rozporządzenia o ochronie danych. Również w uzasadnieniu projektu wskazuje się, że jest to dostosowanie krajowego porządku prawnego do nowych norm prawnych zawartych w rozporządzeniu[1]. Dlatego nazwa powinna zostać zmieniona w ten sposób, aby również odnosiła się do dostosowania do RODO.

II. Inspektorzy ochrony danych

W **art. 5 ust. 4 i 5 projektu ustawy o ochronie danych osobowych** (dalej „***projekt u.o.d.o***.") przewiduje się wyłącznie zgłoszenia elektroniczne wyznaczenia inspektora ochrony danych (dalej „IOD") poprzez system teleinformatyczny Prezesa Urzędu Ochrony Danych Osobowych (dalej „PUODO") z użyciem funkcjonalności ePUAP. Ograniczenie zgłoszenia tylko do dokonania tej czynności w systemie teleinformatycznym PUODO może doprowadzić do niewykonywania obowiązku zgłoszeniowego określonego w RODO, jeżeli nie zostanie przygotowany do dnia 25 maja 2018 r. system przez Biuro Generalnego Inspektora Ochrony Danych Osobowych (dalej GIODO). Z uzasadnienia projektu nie wynika, aby między projektodawcą oraz GIODO zostały poczynione uzgodnienia dotyczące przygotowania systemu. Dlatego też alternatywnym trybem dokonywania zgłoszeń, przynajmniej przez pierwsze miesiące obowiązywania RODO, powinno być zawiadamianie w sposób tradycyjny, np. z użyciem urzędowo określonego formularza.

W **art. 5 ust. 6 projektu u.o.d.o.** użyto zwrotu, że ewidencja zawiadomień IOD jest „wewnętrzna", co nie przesądza, czy dane w ewidencji są jawne czy też nie mają takiego charakteru. Pomimo że w

[1] Uzasadnienie, s. 1; dostępne pod adresem:
http://legislacja.rcl.gov.pl/docs//2/12302951/12457700/12457701/dokument308370.pdf

orzecznictwie sądowym dotyczącym przepisów o dostępie do informacji publicznej funkcjonuje pojęcie „dokumentu wewnętrznego", to w samej ustawie o dostępie do informacji publicznej prawodawca nie posługuje się tym pojęciem, a ograniczenia w dostępie są wprost wymienione w ustawie, przede wszystkim opierając się na konstrukcji tajemnicy. Po wejściu w życie projektowanych przepisów, może to prowadzić do sporów w przedmiocie udostępniania danych o IOD z ewidencji prowadzonej przez organ nadzorczy.

W art. 70 ust. 1 projektu u.o.d.o. przewiduje się kompetencję kontrolującego do przesłuchiwania pracownika kontrolowanego w charakterze świadka. W przypadku IOD będącego pracownikiem kontrolowanego, projektowanemu rozwiązaniu sprzeciwiają się przepisy ogólnego rozporządzenia dotyczące zadań IOD zawarte w art. 39 ust. 1 lit. d) i lit. e) RODO. Z przepisów tych wynika szczególny charakter współdziałania między IOD oraz organem nadzorczym, ponieważ inspektor współpracuje z organem i pełni dla niego funkcję punktu kontaktowego, czego nie można pogodzić z proponowaną władczą relacją wzywania. Dlatego też projektowany przepis powinien zawierać wyłączenie, że nie dotyczy osoby pełniącej funkcję IOD w zakresie wykonywania tej funkcji.

III. Certyfikacja

Zwracamy uwagę, że przewidziane **w rozdziale 3 projektu u.o.d.o.** przekazanie bezpośrednio organowi nadzorczemu (PUODO) kompetencji certyfikacyjnych może negatywnie wpływać na proces certyfikacyjny i znaczenie tej instytucji. PUODO jest bowiem jednocześnie organem administracji publicznej nakładającym sankcje administracyjne (nakazy oraz kary pieniężne). W tym kontekście negatywnie ocenić należy połączenie roli podmiotu certyfikującego mającego wgląd w działalność sprawdzanego (certyfikowanego) z kompetencjami organu nadzorczego, który może uzyskane podczas certyfikacji informacje wykorzystać do nakładania sankcji lub zawiadamia organów ścigania. W związku z tym zwracamy się o ponowne przenalizowanie modelu certyfikacji w Polsce i rozważenie wprowadzenia w tym zakresie rozwiązania opartego na akredytacjach.

IV. Zgłaszanie naruszeń ochrony danych

W **art. 41 projektu u.o.d.o.** nakłada się na PUODO obowiązek prowadzenia systemu teleinformatycznego umożliwiającego administratorom dokonywanie zgłoszenia naruszenia ochrony danych osobowych. Ten jedyny w projekcie przepis nie określa w ogóle sytuacji adresatów obowiązków zgłaszania naruszeń (tj. administratorów). Nie wiadomo, czy zgłaszanie naruszeń w systemie PUODO będzie jedynym trybem dokonywania tej czynności, jak również nieznane są szczegóły techniczne (np. sposób e-identyfikacji zgłaszającego). Wobec tego zwracamy się o dookreślenie tych kwestii technicznych w projekcie ustawy. Podobnie jak w przypadku systemu obsługującego zgłoszenia wyznaczenia IOD, w przypadku, gdy system nie zacznie funkcjonować od

25 maja 2018 r., a będzie wyłącznym trybem zgłaszania naruszeń to dojdzie do niewykonywania obowiązku wskazanego w art. 33 RODO.

V. Rekomendacje w zakresie środków zabezpieczenia technicznego i organizacyjnego –

Negatywnie oceniamy przewidzianą w **art. 43 projektu u.o.d.o.** kompetencję PUODO do przedstawiania rekomendacji określających środki techniczne i organizacyjne stosowane w celu zapewnienia bezpieczeństwa przetwarzania danych osobowych. Przedstawiona propozycja stanowi zanegowanie wyrażonej w RODO zasady podejścia opartego na ryzyku w zakresie bezpieczeństwa danych. W podejściu opartym na ryzyku aktywność w zakresie doboru środków zabezpieczenia technicznego i organizacyjnego danych spoczywa na administratorach i podmiotach przetwarzających w zależności od przeprowadzonego szacowania ryzyka. Tymczasem proponowane rozwiązanie potencjalnie może doprowadzić do bierności administratorów, którzy zamiast samodzielnie szacować ryzyko będą oczekiwali na rekomendacje organu nadzorczego wskazujące konkretne środki do zastosowania. Przedmiotowa kompetencja nie jest przewidziana w RODO i nie będą istniały żadne mechanizmy zapewaniające spójność konkretnych rekomendacji polskiego organu z podejściem do problematyki bezpieczeństwa w pozostałych państwach Unii Europejskiej. Wreszcie nie wiadomo jakie konsekwencje prawne będą miały rekomendacje i jaka będzie sytuacja podmiotu, który się do nich nie zastosował. W dodatku rekomendacje pod względem merytorycznym nie będą podlegały żadnej kontroli. Wobec powyższego wnioskujemy o usunięcie tego rozwiązania z projektu.

VI. Postępowanie administracyjne prowadzone przez PUODO

Zastrzeżenie budzi przewidziany w **art. 53 projektu u.o.d.o.** nowy rodzaj postanowienia wydawanego przez PUODO w trakcie postępowania administracyjnego. Według wspomnianego przepisu w postanowieniu organ może zobowiązać adresata do ograniczenia przetwarzania danych osobowych i to na czas trwania całego postępowania (tj. do momentu wydania decyzji). Zgodnie z art 60 projektu u.o.d.o. postanowienie to będzie dopiero zaskarżalne w decyzji. Powyższe rozwiązanie oznacza, że strona postępowania (adresat nakazu zawartego w postanowieniu) będzie ponosił dolegliwości, polegające np. na braku możliwości korzystania z danych osobowych w swojej działalności, bez możliwości prawa do skarżenia do sądu tego nakazu. Wątpliwości pogłębia dotychczasowa praktyka długotrwałego prowadzenia postępowań administracyjnych przez GIODO, co oznacza – w odniesieniu do omawianego postanowienia – długi okres obowiązywania nakazu zawartego w postanowieniu. Naszym zdaniem przedmiotowe postanowienie może znaleźć się jedynie wówczas w ustawie, jeżeli zostanie wprowadzone prawo do skarżenia tego aktu indywidualnego, a przepisy będą przewidywały skrócone terminy rozpatrzenia skargi przez sąd (np. termin dla sądu do rozstrzygnięcia mógłby wynosić 14 dni od daty otrzymania skargi, a dla PUODO – 7 dni na przekazanie skargi do sądu wraz z odpowiedzią i aktami sprawy).

Przewidziane **w art. 60 projektu u.o.d.o.** rozwiązanie, że postanowienia wydane przez Prezesa Urzędu strona może zaskarżyć w skardze na decyzję Prezesa Urzędu oznacza, że nie można postanowień wydanych przez PUODO skarżyć odrębnie i to także w przypadku postanowień kończących postępowanie, tzn. takich, w których nie jest wydawana decyzja. W naszej ocenie takie rozwiązanie oznacza naruszenie prawa do sądu gwarantowanego w art. 45 Konstytucji RP w przypadku wydawania postanowienia kończącego postępowanie.

Należy także pamiętać, że jednym z postanowień kończących postępowanie jest postanowienie o odmowie wszczęcia postępowania administracyjnego (art. 61a k.p.a.). Jeżeli takie postanowienie zapadnie w wyniku wniosku (skargi) podmiotu danych to brak możliwości jego zaskarżenia, który przewiduje art. 60 projektu u.o.d.o. oznacza naruszenie prawa określonego w art. 78 ust. 2 RODO. Organ bowiem merytorycznie nie rozpatrzył skargi poprzez odmowę wszczęcia postępowania, a skarżący jest pozbawiony środka ochrony prawnej przed sądem.

Inny przepis, który może naruszać art. 45 Konstytucji RP - w przypadku postanowień kończących postępowanie - znajduje się w **art. 139 ust. 4 projektu ustawy – Przepisy wprowadzające u.o.d.o**. Przewiduje on umorzenie z mocy prawa postanowień wszczętych przez GIODO w wyniku złożenia zażalenia na postanowienie. Wydanie takiego postanowienia umarzającego może uniemożliwić sądowi, do którego trafi skarga na postanowienie, merytoryczne ustosunkowanie się do przedmiotu sporu.

Przepis **art. 59 projektu u.o.d.o.** przewiduje automatycznie natychmiastową wykonalność każdej decyzji, a wniesienie skargi do sądu wstrzymuje wykonalność jedynie decyzji nakładającej karę pieniężną. W naszej opinii jest to rozwiązanie nakładające zbyt daleko idącą dolegliwość na adresata decyzji, w przypadku uwzględnienia przez sąd skargi na decyzję powodującą nieuzasadnioną odpowiedzialność Skarbu Państwa za szkody wyrządzone wykonaniem decyzji. Proponujemy aby ustanowić w ustawie stosowne przesłanki nałożenia rygoru natychmiastowej wykonalności (np. związanego z istotnymi, negatywnymi konsekwencjami dla praw i wolności podmiotu danych dalszego przetwarzania danych osobowych przez adresata decyzji) albo też zrezygnować z tego przepisu, ponieważ wówczas PUODO będzie mógł nakładać rygor natychmiastowej wykonalności decyzji na ogólnych zasadach określonych w art. 108 k.p.a.

VII. Kontrola PUODO

W **art. 67 ust. 1 – 2 projektu u.o.d.o.** wprowadza się możliwość wyłączenia kontrolującego z kontroli, w tym na wniosek kontrolowanego, w szczególności w sytuacji, gdy zachodzą uzasadnione wątpliwości co do jego bezstronności. To istotna gwarancja prawidłowego wykonywania kontroli. Jednak w **art. 67 ust. 4 projektu u.o.d.o**. przewiduje się, że nie przysługuje skarga na postanowienie o odmowie wyłączenia kontrolującego. Czyni to ochronę kontrolowanego czysto iluzoryczną i nie różni się od obecnej sytuacji, w której pomimo braku formy postanowienia można się zwrócić do

GIODO o wyłączenie kontrolera, a ten odpowie pismem nie podlegającym kontroli. W związku z tym zwracamy się o zmianę przepisu w ten sposób, żeby postanowienie o odmowie wyłączenia kontrolującego było zaskarżalne zażaleniem.

Przepis **art. 69 ust. 5 projektu u.o.d.o**. dopuszcza możliwość nagrywania obrazu podczas kontroli przez kontrolującego. Rejestracja obrazu ma dotyczyć przebiegu kontroli lub poszczególnych czynności. Należy zwrócić uwagę, że rejestracja obrazu może daleko ingerować w sferę dóbr nagrywanych osób fizycznych, a w przypadku przedsiębiorców – w ich tajemnicę przedsiębiorstwa. Dlatego też należy wprowadzić dodatkowe przepisy gwarancyjne, które tylko za zgodą osób nagrywanych powalałyby rejestrować ich wizerunek i nagrywać inne obrazy wkraczające w sferę prywatności. Natomiast w przypadku obrazu ujawniającego tajemnicę przedsiębiorstwa nagrywanie mogłoby następować tylko w zakresie niezbędnym dla celów kontroli.

Według **art. 73 projektu u.o.d.o**. w przypadku kontroli wyłącza się stosowanie przepisów art. 79, art. 82 i art. 83 ustawy o swobodzie działalności gospodarczej. W naszej ocenie to zbyt daleko idące ograniczenie praw kontrolowanego, ponieważ wymienione przepisy pełnią funkcje gwarancyjne dla kontrolowanego. Naszym zdaniem ograniczenie stosowania tych przepisów mogłoby mieć miejsce tylko w przypadku, gdy ich respektowanie przez organ powodowałoby negatywne konsekwencje dla celów kontroli, ale w takim wypadku w ustawie należy szczegółowo określić takie sytuacje.