Stowarzyszenie
Administratorów
Bezpieczeństwa
Informacji

KANCELARIA OGÓLNA
MINISTERSTWA GOSPODARKI
wpłynęło dnia 2012 -07- 20 15⁵⁰
Nr pisma

Warszawa, dn. 19.07.2012 r.

Pan
Mariusz Haładyj
Podsekretarz Stanu
w Ministerstwie Gospodarki

Szanowny Panie Ministrze,

W związku ze skierowaniem do konsultacji społecznych „Projektu założeń projektu ustawy o redukcji niektórych obciążeń" Stowarzyszenie Administratorów Bezpieczeństwa Informacji przedstawia swoją opinię do pkt 2.30 i 2.31 projektu, tj. w zakresie zmian w przepisach ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2002 r. Nr 101, poz. 926 ze zm.; dalej także „*u.o.d.o.*").

Powstałe w 2007 r. Stowarzyszenie Administratorów Bezpieczeństwa Informacji zrzesza administratorów bezpieczeństwa informacji oraz inne osoby zajmujące się – najczęściej zawodowo – ochroną danych osobowych. Do statutowych celów Stowarzyszenia należy w szczególności opiniowanie aktów prawnych z zakresu ochrony danych osobowych i współpraca z organami administracji publicznej. W trakcie dotychczasowej działalności Stowarzyszenie brało aktywny udział m.in. w pracach sejmowych zakończonych uchwaleniem ustawy z dnia 29 października 2010 r. o zmianie ustawy o ochronie danych osobowych oraz niektórych innych ustaw (Dz.U. Nr 229, poz. 1497), a także w pracach nad przepisami wykonawczymi do ustawy o ochronie danych osobowych.

Stowarzyszenie Administratorów Bezpieczeństwa Informacji
Al. Jana Pawła II 34 lok. 6, 00-141 Warszawa, tel.: 022 620 64 58, e-mail: info@sabi.org.pl, www.sabi.org.pl

Stowarzyszenie Administratorów Bezpieczeństwa Informacji z głębokim zadowoleniem przyjmuje, przedstawione przez Ministra Gospodarki we wspomnianych założeniach, propozycje zmian w ustawie o ochronie danych osobowych, w których wprowadza się zwolnienie z obowiązku rejestracji zbiorów danych osobowych (zgłoszenia zbioru danych i aktualizacji informacji podanych w zgłoszeniu), połączone ze zmianą zasad funkcjonowania administratorów bezpieczeństwa informacji. W sposób zgodny z wymogami prawa unijnego wyłącza się w projekcie obowiązek rejestracyjny, który stanowi znaczne obciążenie administracyjne dla administratorów danych (w tym przedsiębiorców), czyniąc to jednak bez uszczerbku dla właściwego poziomu ochrony danych osobowych w jednostce organizacyjnej (w tym w przedsiębiorstwie). Taki właściwy poziom zapewni bowiem niezależny administrator bezpieczeństwa informacji (ABI) działający we współpracy z GIODO. Inną pozytywną konsekwencją przyjęcia zaproponowanych przepisów nowelizujących będzie doprecyzowanie lakonicznej i niejasnej obecnej regulacji ustawowej dotyczącej ABI, która aktualnie prowadzi do niejednolitego wykonywania tej funkcji w skali naszego kraju.

Równocześnie prosimy o przyjęcie uwag naszego Stowarzyszenia do projektu założeń, w szczególności związanych z potrzebą doprecyzowania rozwiązań znajdujących się w propozycji Ministra Gospodarki.

I. Na wstępie warto zauważyć, że po raz pierwszy od uchwalenia w 1997 r. ustawy o ochronie danych osobowych zaproponowano rozwiązanie, które przewiduje całościowe zwolnienie z obowiązków rejestracyjnych, zgodne ze przepisami Dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych. Dotychczas nie wykorzystano w polskim prawodawstwie stworzonej w dyrektywie 95/46/WE możliwości uproszczenia bądź zwolnienia z obowiązku rejestracyjnego (notyfikacyjnego) w przypadku wyznaczenia urzędnika ds. ochrony danych osobowych (*data protection official*), będącego pierwowzorem dla funkcji administratora bezpieczeństwa informacji (ABI) unormowanej w u.o.d.o. Należy jednak przypomnieć, że unijna dyrektywa przewiduje możliwość takiego zwolnienia (uproszczenia) tylko pod warunkiem spełnienia przez urzędnika dwóch warunków: zapewnienia w jednostce organizacyjnej w sposób niezależny przestrzegania krajowych przepisów o ochronie danych osobowych (opartych

na dyrektywie 95/46/WE) oraz prowadzenie rejestru operacji związanych z przetwarzaniem danych dokonywanych przez administratora danych, zawierającego takie same elementy jak rejestr ogólnokrajowy prowadzony przez państwowy organ ds. ochrony danych osobowych (tzw. uproszczona rejestracja).

Funkcjonujący w polskiej ustawie ABI nie spełnia żadnego z warunków określonych w dyrektywie 95/46/WE odnoszących się do urzędnika ds. ochrony danych osobowych. Ustawa nie gwarantuje mu niezależności, jak również nie przyznaje kompetencji w zakresie uproszczonej rejestracji. Aktualnie w ustawie o ochronie danych osobowych znajduje się tylko jeden przepis dotyczący ABI (art. 36 ust. 3), według którego zadaniem tegoż administratora jest nadzorowanie przestrzegania zasad w zakresie bezpieczeństwa techniczno -organizacyjnego przetwarzanych danych osobowych, podczas gdy dyrektywa rozciąga kompetencje urzędnika na wszystkie krajowe przepisy o ochronie danych osobowych.

Według art. 36 ust. 3 u.o.d.o. *„Administrator danych wyznacza administratora bezpieczeństwa informacji, nadzorującego przestrzeganie zasad ochrony, o których mowa w ust. 1, chyba że sam wykonuje te czynności.”*. Lakoniczna treść regulacji prowadzi obecnie do niejednolitego wykonywania tej funkcji w skali naszego kraju. Podstawowe problemy dotyczą zakresu kompetencji ABI oraz jego usytuowania organizacyjnego. **W opinii Stowarzyszenia przedstawiona przez Ministra Gospodarki w projekcie regulacja zapewni rozwiązanie aktualnych problemów związanych z działalnością administratorów bezpieczeństwa informacji.**

II. Podstawowym celem ustawy o ochronie danych osobowych jest zagwarantowanie stosownych mechanizmów (materialnych i proceduralnych) w celu realizacji wyznaczonego Konstytucją RP prawa osoby fizycznej do ochrony swoich danych osobowych, stanowiącego przejaw prawa do prywatności. **Dlatego też ograniczenia lub zwolnienia z obowiązków ustawowych w omawianym zakresie nie mogą negatywnie wpłynąć na poziom gwarancji praw podmiotu danych.** Ten właśnie kierunek potwierdza wspomniana dyrektywa 95/46/WE, która dopuszcza całościowe zwolnienie z obowiązku rejestracyjnego (notyfikacyjnego) tylko w przypadku funkcjonowania wewnątrz struktury organizacyjnej administratora danych funkcji urzędnika zapewniającej niezależne przejęcie kompetencji organu państwowego.

Kierunek zmian powinien zawierać właściwe wyważenie potrzeb administratorów danych (w tym przedsiębiorców) związanych z przetwarzaniem danych osobowych oraz praw osób,

których dane dotyczą i mechanizmów gwarantujących te prawa (np. rejestracji zbiorów danych osobowych), z tym zastrzeżeniem, że priorytetem jest ochrona interesu podmiotów danych.

W ocenie Stowarzyszenia takie właśnie prawidłowe podejście w stosunku do zmian prawnych zasad ochrony danych osobowych prezentowane jest w projekcie założeń przedstawionym przez Ministra Gospodarki oraz piśmie w tym przedmiocie Generalnego Inspektora Ochrony Danych Osobowych, o którym mowa w pkt IV niniejszego pisma.

III. Zaproponowane w założeniach rozwiązania dotyczące administratora bezpieczeństwa informacji (ABI) należy także odnieść do przedstawionego w dniu 25 stycznia 2012 r. przez Komisje Europejską projektu rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (*ogólne rozporządzenie o ochronie danych*) (art. 35-37). **W tym kontekście zmiany w ustawie dotyczące ABI będą krokiem przygotowującym do wdrożenia w Polsce rozwiązań przewidzianych w projekcie rozporządzenia, tj. obowiązku administratora danych wyznaczenia – w przypadkach określonych rozporządzeniem – inspektora ds. ochrony danych osobowych (inspektora).**

Projektowane rozporządzenie od inspektora ochrony danych będzie wymagać kwalifikacji zawodowych oraz wiedzy specjalistycznej z zakresu prawa ochrony danych. Inspektor będzie wykonywał swoje obowiązki i zadania niezależnie i podlegał bezpośrednio kierownictwu administratora (lub podmiotu przetwarzającego). Wyznaczający inspektora (administrator danych lub przetwarzający) mają go wspierać w wykonywaniu przez niego zadań i zapewnić personel, pomieszczenia, sprzęt i zasoby niezbędne realizacji obowiązków i zadań. Oprócz tego wprowadza się obowiązek powiadomienia organu nadzorczego (w Polsce GIODO) w zakresie imienia, nazwiska i innych danych kontaktowych inspektora.

Do zadań inspektora będzie należało w szczególności monitorowanie wykonania i stosowania przepisów rozporządzenia i polityk w zakresie ochrony danych osobowych (w tym szkolenie personelu zaangażowanego w operacje przetwarzania), zapewnienie prowadzenia dokumentacji ochrony danych osobowych oraz współpraca z organem nadzorczym na wniosek tego organu lub z inicjatywy samego inspektora.

Jak wskazano powyżej projektowane rozporządzenie unijne zawiera rozwiązania zbliżone lub pokrywające się z tymi przedstawionymi w projekcie założeń Ministra

Gospodarki, chociaż oczywiście obydwu regulacji nie można traktować, jako tożsamych treściowo, choćby z tego powodu, że rozporządzenie przewiduje znacznie szerszy zakres zadań inspektora.

IV. Jednocześnie prosimy o przyjęcie pewnych zmian w przedstawionym projekcie, w szczególności czyniących zadość propozycjom zawartym w piśmie Generalnego Inspektora Ochrony Danych Osobowych do Ministra Mariusza Haładyja, Podsekretarza Stanu w Ministerstwie Gospodarki z dnia 29 maja 2012 r. (GI-030-1/12/33720) i stanowiących załącznik do tego pisma projekcie ustawy wraz z uzasadnieniem.

1. W projekcie przedstawionym przez Generalnego Inspektora zasadnie zaproponowano uszczegółowienie kompetencji administratora bezpieczeństwa informacji polegające na: sprawdzeniu przez ABI zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych, zapewnieniu przez niego opracowania i aktualizowania dokumentacji przetwarzania i ochrony danych osobowych i nadzorowaniu przestrzegania zasad w niej określonych, jak również zaznajamianiu osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych i prowadzeniu jawnego rejestru zbiorów danych przetwarzanych w jednostce organizacyjnej.

2. Ponadto w projekcie zawarto upoważnienie dla ministra właściwego do spraw administracji publicznej do określenia w drodze rozporządzenia trybu wykonywania wspomnianych czynności sprawdzających oraz nadzoru, jak również sposobu prowadzenia przez ABI wewnętrznego rejestru.

3. Wreszcie według propozycji GIODO powołanie ABI nie jest obowiązkiem, a tylko możliwością przewidzianą dla administratora danych. Jednak wyłącznie wówczas gdy administrator danych zdecyduje się na takie powołanie będzie uprawniony do zwolnienia z obowiązku rejestracyjnego. W przypadku niepowołania ABI administrator danych nadal będzie zobligowany do realizacji wymogu rejestracyjnego, a jednocześnie będzie samodzielnie wykonywał kontrolę wewnętrzną, według trybu przewidzianego w przepisach wykonawczych.

Wspomniane rozwiązanie jest o tyle istotne, ponieważ wyklucza znaczenie argumentu o dodatkowych, obowiązkowych kosztach związanych z funkcją ABI. Każdy z administratorów danych stanie przed wyborem, czy chce powołania administratora bezpieczeństwa informacji (ABI) czy tez decyduje się na dalsze wykonywanie obowiązku rejestracyjnego, które może zostać połączone z istnieniem dotychczasowych struktur organizacyjnych zajmujących się ochroną danych osobowych w jego jednostce organizacyjnej.

4. W projekcie Generalnego Inspektora przewiduje się także zapewnienie przez administratora danych, który zdecydował się na powołanie ABI, niezbędnych środków i organizacyjnej odrębności administratora bezpieczeństwa informacji w niezależnym wykonywaniu przez niego zadań.

V. Niezależnie od powyższych uwag zdaniem Stowarzyszenia występuje potrzeba zmian przepisów wykonawczych do ustawy o ochronie danych osobowych, stanowiących wykonanie upoważnienia zawartego w art. 39a u.o.d.o. Obecnie aktem wykonawczym realizującym wspomnianą delegację jest rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024).

Określone w tym rozporządzeniu z 2004 r. środki zabezpieczenia technicznego i organizacyjnego nie przystają już do wyzwań współczesnych technologii i do globalnego charakteru przetwarzania danych osobowych. Co ważne, rozporządzenie nie różnicuje obowiązków w zależności od skali przetwarzania danych i związanych z tym zagrożeń. Powoduje to nałożenie jednakowych obowiązków na wszystkie podmioty przetwarzające dane (zarówno na duże podmioty, jak i na małych przedsiębiorców). Oprócz tego, rozporządzenie w jakimkolwiek zakresie nie odnosi do administratora bezpieczeństwa informacji, co nie ułatwi wykonywania nowych, projektowanych kompetencji ABI.

W opinii Stowarzyszenia nowe brzmienie art. 39a u.o.d.o. powinno zawierać wytyczne wskazujące, iż rozporządzenie ma bardziej regulować cele i zasady, jakim na odpowiadać system zarządzania przetwarzaniem danych niż kazuistycznie normować jego poszczególne

elementy. Ponadto, wytyczne zawierają fakt, iż stopień sformalizowania zasad zarządzania bezpieczeństwem przetwarzania danych osobowych musi uwzględniać skalę przetwarzania danych, a w przypadkach gdy skala tego przetwarzania jest niewielka, wymogi formalne powinny być wprowadzone tylko w niezbędnym zakresie.

Wobec powyższego proponujemy zmianę art. 39a u.o.d.o. Przedstawione poniżej brzmienie przepisu zapewni wydanie nowych przepisów wykonawczych spełniających podane powyżej warunki:

„Art. 39a *Minister właściwy do spraw administracji publicznej, po zasięgnięciu opinii Generalnego Inspektora, określi, w drodze rozporządzenia zasady zarządzania bezpieczeństwem przetwarzania danych osobowych i wynikające z tego środki techniczne i organizacyjne, o których mowa w art. 36 ust. 1, sposób prowadzenia i zakres dokumentacji, o której mowa w art. 36 ust. 2 i sposób wykonywania kontroli, o której mowa w art. 38, uwzględniając zapewnienie ochrony przetwarzanych danych osobowych odpowiedniej do zagrożeń oraz kategorii danych objętych ochroną, a także skalę przetwarzania danych osobowych przez różne kategorie administratorów danych.*".

Mamy nadzieję na uwzględnienie uwag naszego Stowarzyszenia.

Z wyrazami szacunku

PREZES ZARZĄDU

Maciej Byczkowski