Stowarzyszenie Administratorów Bezpieczeństwa Informacji

Warszawa, 4 maja 2012r.

Projekt

Art. …

W ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.) wprowadza się następujące zmiany:

1) w art. 12 pkt 4 otrzymuje brzmienie:
„4) prowadzenie rejestrów zbiorów danych oraz administratorów bezpieczeństwa informacji, a także udzielanie informacji znajdujących się w rejestrach";

2) po art. 16 dodaje się art. 16b w brzmieniu:

„Art.16b.1 Jeżeli nie sprzeciwia się to celowi lub interesowi kontroli, Generalny Inspektor może odstąpić od czynności kontrolnych, o których mowa w art. 14-16 i zwrócić się do administratora bezpieczeństwa informacji, wpisanego do rejestru, o którym mowa w art. 46b ust.2, o przeprowadzenie kontroli w określonym terminie.
2. Po przeprowadzeniu kontroli administrator bezpieczeństwa informacji przedstawia Generalnemu Inspektorowi sprawozdanie, o którym mowa w art. 36a ust.2 pkt 1.
3. Przeprowadzenie kontroli przez administratora bezpieczeństwa informacji nie wyłącza prawa Generalnego Inspektora do późniejszej kontroli, o której mowa w art. 12 pkt 1 i art. 14.";

3) w art. 36 uchyla się ust.3;

4) po art. 36 dodaje się art. 36a w brzmieniu:

„Art. 36a. 1. Administrator danych powołuje administratora bezpieczeństwa informacji, chyba że sam wykonuje zadania, o których mowa w ust.2.

2. Do zadań administratora bezpieczeństwa informacji należy:
1) przeprowadzanie kontroli przestrzegania przepisów o ochronie danych osobowych w jednostce organizacyjnej oraz opracowanie w tym zakresie sprawozdania dla administratora danych,
2) zapewnienie opracowania i aktualizowania dokumentacji, o której mowa w art. 36 ust.2, oraz nadzorowanie przestrzegania zasad w niej określonych,
3) prowadzenie rejestru zbiorów danych przetwarzanych w jednostce organizacyjnej,
4) zaznajamianie osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych.

3. Administrator danych może powierzyć administratorowi bezpieczeństwa informacji wykonywanie innych zadań, które nie naruszają prawidłowego wykonywania jego obowiązków, o których mowa w ust.2.

4. Administratorem bezpieczeństwa informacji może być osoba, która:
1) ma pełną zdolność do czynności prawnych oraz korzysta z pełni praw publicznych,
2) posiada odpowiednią wiedzę z zakresu przepisów o ochronie danych osobowych,
3) nie była karana za przestępstwo popełnione z winy umyślnej.

5. Administrator danych może powołać zastępcę lub administratora bezpieczeństwa informacji, który spełnia warunki określone w ust. 4.

6. Administrator bezpieczeństwa informacji podlega bezpośrednio kierownikowi jednostki organizacyjnej, który zapewnia niezbędne środki i organizacyjną odrębność administratora bezpieczeństwa informacji w niezależnym wykonywaniu przez niego zadań, o których mowa w ust.2.

7. Minister właściwy do spraw administracji publicznej, po zasięgnięciu opinii Generalnego Inspektora, określi w drodze rozporządzenia:
1) zasady i tryb przeprowadzania kontroli oraz opracowania i przedstawiania sprawozdania, o których mowa w ust. 2 pkt 1;
2) tryb wykonywania nadzoru, o którym mowa w ust.2 pkt 2;
3) sposób prowadzenia rejestru zbiorów danych, o którym mowa w ust.2 pkt 3;
- uwzględniając sprawność wykonywania zadań przez administratora bezpieczeństwa informacji oraz konieczność zapewnienia jego niezależności i organizacyjnej odrębności.";

5) tytuł rozdziału 6 otrzymuje brzmienie:
„Rejestracja zbiorów danych osobowych oraz administratorów bezpieczeństwa informacji";

6) art. 40 otrzymuje brzmienie:
„art. 40 Administrator danych jest zobowiązany zgłosić do rejestracji Generalnemu Inspektorowi:
1) zbiór danych, z wyjątkiem przypadków, których mowa w art. 43 ust.1 i ust.1a,
2) powołanego administratora bezpieczeństwa informacji.";

7) w art. 43 po ust.1 dodaje się ust. 1a w brzmieniu:
„1a. Niezależnie od zwolnień określonych w ust.1 obowiązkowi rejestracji zbiorów danych osobowych, z wyjątkiem zbiorów danych, o których mowa w art. 27 ust.1, nie podlega administrator danych, który powołał i zgłosił Generalnemu Inspektorowi administratora bezpieczeństwa informacji, pod warunkiem że administrator bezpieczeństwa informacji prowadzi rejestr, o którym mowa w art. 36a ust.2 pkt 3";

8) art. 46 ust.2 otrzymuje brzmienie:
„2. Administrator danych, o których mowa w art. 27 ust. 1, może rozpocząć ich przetwarzanie w zbiorze danych po zarejestrowaniu zbioru, chyba że ustawa zwalnia go z obowiązku zgłoszenia zbioru do rejestracji lub administrator bezpieczeństwa informacji wpisany do rejestru, o którym mowa w art. 46b ust.2, przedstawił, dołączoną do zgłoszenia, opinię stwierdzającą zgodność przetwarzania tych danych osobowych z ustawą.";

9) po art. 46a dodaje się art. 46b, art. 46c i art. 46d w brzmieniu:
„art. 46b.1. Administrator danych jest zobowiązany zgłosić do rejestracji Generalnemu Inspektorowi powołanie i odwołanie administratora bezpieczeństwa informacji, w terminie 14 dni od dnia powołania lub odwołania. W zgłoszeniu administrator danych podaje podstawowe dane osobowe administratora bezpieczeństwa informacji

oraz składa oświadczenie o spełnieniu ustawowych warunków powołania lub przedstawia przyczyny odwołania.
2. Generalny Inspektor prowadzi jawny rejestr administratorów bezpieczeństwa informacji, który każdy ma prawo przeglądać.
3. Na żądanie administratora danych lub administratora bezpieczeństwa informacji Generalny Inspektor wydaje zaświadczenie o zarejestrowaniu administratora bezpieczeństwa informacji.

art. 46c.1. Wykreślenie administratora bezpieczeństwa informacji z rejestru następuje po powiadomieniu o jego odwołaniu, o którym mowa w art. 46b ust.1.
2. Generalny Inspektor z urzędu wydaje decyzję o wykreśleniu administratora bezpieczeństwa informacji z rejestru, jeżeli:

1) powołanie administratora bezpieczeństwa informacji nastąpiło z naruszeniem warunków określonych w ustawie, albo
2) działalność administratora bezpieczeństwa informacji narusza zasady określone w ustawie, albo
3) administrator danych nie powiadomił w terminie, o którym mowa w art. 46b ust.1, o odwołaniu administratora bezpieczeństwa informacji.

3. Decyzja o wykreśleniu podlega natychmiastowemu wykonaniu, a do administratora danych będącego jej adresatem nie stosuje się zwolnienia, o którym mowa w art. 43 ust.1a.

4. Administrator danych może ponownie zgłosić powołanie administratora bezpieczeństwa informacji po usunięciu wad, które były powodem wykreślenia z rejestru, o którym mowa w ust.2. Generalny Inspektor, w drodze decyzji, po stwierdzeniu usunięcia wad wpisuje administratora bezpieczeństwa informacji do rejestru i dopuszcza stosowanie zwolnienia, o którym mowa w art.43 ust.1a.

art. 46d. Minister właściwy do spraw administracji publicznej, po zasięgnięciu opinii Generalnego Inspektora, określi w drodze rozporządzenia:
1) wzór zgłoszenia administratora bezpieczeństwa informacji, o którym mowa w art. 46b ust.1,
2) wzór opinii administratora bezpieczeństwa informacji, o której mowa w art. 46 ust.2,
- uwzględniając obowiązek zamieszczenia informacji niezbędnych do wykonania obowiązków określonych w ustawie.”.

Uzasadnienie

1. W ustawie o ochronie danych osobowych (u.o.d.o.) jako znaczące obciążenie administracyjne dla administratorów danych (w tym przedsiębiorców) wskazywany jest obowiązek rejestracyjny (art. 40 i nast.), tj. wymóg zgłaszania do Generalnego Inspektora Ochrony Danych Osobowych (GIODO) zbioru danych, a następnie dokonywania zgłoszeń aktualizujących informacje podane we wniosku rejestracyjnym.

W projekcie nowelizacji proponuje się kompleksowe zwolnienie z obowiązku rejestracyjnego, a także ograniczenie innych obciążeń administracyjnych związanych z kompetencjami GIODO: 1) kontroli wstępnej przetwarzania danych osobowych wrażliwych w ramach rejestracji zbiorów danych, 2) kontroli zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych.

Ze względu na wymogi prawa unijnego konstrukcja wprowadzenia wspomnianych ograniczeń opiera się na rozszerzeniu kompetencji i modyfikacji statusu administratora bezpieczeństwa informacji (ABI). Jednakże nie wymaga to wprowadzenia nowej instytucji do ustawy, ponieważ ABI funkcjonuje już w obecnym stanie prawnym.

Będąca pierwowzorem polskiej ustawy o ochronie danych osobowych Dyrektywa 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 (OJ Nr L 281 z dnia 31 listopada 1995 r.) przewiduje nałożenie na administratora danych obowiązku notyfikacji krajowemu organowi ds. ochrony danych osobowych procesu przetwarzania danych osobowych (art. 18-19, *Notification*). Na gruncie wspomnianej dyrektywy niedopuszczalne jest zrezygnowanie przez państwo członkowskie z obowiązku notyfikacji, ale możliwe jest uproszczenie bądź zwolnienie z wymogu w zakresie wyznaczonym dyrektywą.

W szczególności dyrektywa 95/46/WE dopuszcza, aby państwa członkowskie uprościły obowiązek notyfikacyjny lub z niego zwolniły, jeżeli administrator danych wyznaczy urzędnika ds. ochrony danych osobowych (*data protection official),* pod warunkiem spełnienia przez niego dwóch warunków: zapewnienia 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; zob. art. 18 ust.2). Należy podkreślić, że jest to jedyne przewidziane w dyrektywie zwolnienie o charakterze kompleksowym, ponieważ inne zwolnienia dotyczą określonych kategorii danych (art. 18 ust.4), lub też zależą od kryteriów wpływu na prawa i wolności podmiotu danych (art. 18 ust.2 tiret pierwsze) czy dostępności danych osobowych (art. 18 ust.3).

Funkcjonujący w polskiej ustawie ABI, który może być uznawany za odpowiednik urzędnika ds. ochrony danych osobowych, nie spełnia żadnego z warunków określonych w dyrektywie 95/46/WE. 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.

Proponowana w projekcie zmiana wprowadza przewidziane w dyrektywie warunki niezależności ABI w zakresie wykonywania kontroli przestrzegania przepisów o ochronie danych osobowych oraz kompetencję do uproszczonej rejestracji zbiorów danych. Dla podmiotów (administratorów danych), które spełniły w/w warunki powołania ABI przewidziano całościowe zwolnienie z obowiązku rejestracji zbiorów i ich aktualizacji (ze względu na odpowiednie stosowanie do aktualizacji przepisów o rejestracji – art. 41 ust.4 ustawy). Jednocześnie przyjęto prosty mechanizm kontroli, czy administrator danych rzeczywiście wyznaczył ABI, poprzez obowiązek powiadomienia GIODO o tym fakcie.

Przy okazji ustawa rozstrzyga status ABI, w zakresie którego trwała dotychczas dyskusja, czy jest to zawód, stanowisko pracy, czy jedynie funkcja w jednostce organizacyjnej. Projektowana nowelizacja przyjmuje, że ABI może wykonywać inne nałożone na niego zadania, które nie naruszają jego obowiązków dotyczących ochrony danych osobowych. Celowo projektowana zmiana unika regulowania kwestii zmierzającej w kierunku tworzenia nowej grupy zawodowej.

Powyższe zwolnienie z obowiązku rejestracyjnego nie dotyczy jedynie zbiorów zawierających tzw. dane wrażliwe (tj. dane wymienione w art. 27 ust.1 u.o.d.o.), ponieważ w ramach rejestracji w polskiej ustawie wykonywany jest obowiązek kontroli wstępnej (*prior checking*) operacji, które mogą stwarzać zagrożenie dla praw i wolności podmiotu danych (art. 20 dyrektywy 95/46/WE). Natomiast proponuje się w projekcie ograniczenie rygoru

administracyjnego, który obecnie polega na obowiązku powstrzymania się przez administratora danych od rozpoczęcia przetwarzania danych wrażliwych do momentu dokonania rejestracji zbioru danych przez GIODO. Według projektu pozytywna opinia ABI co do zgodności z prawem przetwarzania danych wrażliwych powodowałaby zwolnienie z warunku oczekiwania na czynność rejestracyjną Generalnego Inspektora. Oprócz tego GIODO, ze względu na niezależną kompetencję kontrolną ABI, mógłby powierzyć mu wykonywanie innych czynności kontrolnych. Stanowi to istotne odciążenie dla administratorów danych (w tym przedsiębiorców) w stosunku do stanu aktualnego, w którym w każdym wymagającym tego przypadku (np. skargi osoby trzeciej) podlegają oni bezpośredniej kontroli Generalnego Inspektora.

Należy podkreślić, że wszystkie zaproponowane w projekcie rozwiązania były już dyskutowane od 2008 r., z udziałem GIODO, w środowisku administratorów bezpieczeństwa informacji zrzeszonych w Stowarzyszeniu Administratorów Bezpieczeństwa Informacji oraz przedstawiane na licznych krajowych konferencjach przeznaczonych dla osób zajmujących się problematyką ochrony danych osobowych (m.in. na Kongresach Administratorów Bezpieczeństwa Informacji). Potrzeba zmiany statusu ABI w zakresie objętym projektem przedstawiana była również na wysłuchaniu publicznym w Sejmie w dniu 09.07.2008r. dotyczącym przedstawionego przez Prezydenta RP projektu ustawy o zmianie ustawy o ochronie danych osobowych (druk 488).

2. Przechodząc do poszczególnych proponowanych zmian w ustawie to w art. 12 przewiduje się rozszerzenie kompetencji rejestracyjnych GIODO na informacje o administratorach bezpieczeństwa informacji (ABI), które będą uzyskiwane przez organ na podstawie powiadomień administratorów danych. Przepis ten jest powiązany z nowymi art. 46b-46c, w których określa się warunek powiadamiania Generalnego Inspektora o powołaniu i odwołaniu ABI, jak również zadania GIODO do prowadzenia stosownego rejestru oraz wykreślania z niego w przypadku braku spełnienia wymogów ustawowych. Przewidziana konstrukcja ma w prosty sposób zapewnić kontrolę, czy administrator danych faktycznie spełnił warunki niezbędne do zwolnienia go z obowiązku rejestracyjnego.

W dodanym art. 16b przewiduje się możliwość uproszczonej kontroli przestrzegania przepisów o ochronie danych osobowych, która będzie wykonywana – na wniosek GIODO - przez niezależnego ABI, zastępując w tym zakresie bezpośrednią kontrolę Generalnego Inspektora. Taka kontrola w żaden sposób nie naruszy kompetencji samego Generalnego Inspektora, który jedynie uznaniowo – po spełnieniu określonych warunków - dopuszcza uproszczoną kontrolę i nie jest ograniczony jej przeprowadzeniem w kolejnych swoich czynnościach.

W art. 36a wprowadza się nowe przepisy dotyczące statusu i zadań ABI, które zapewnią zachowanie następujących standardów wyznaczonych dyrektywą 95/46/WE:

- niezależność w wykonywaniu zadań,
- kompetencje do kontroli wewnętrznej w zakresie przestrzegania przepisów o ochronie danych osobowych,
- prowadzenie wewnętrznego rejestru zbiorów danych.

Zadaniem dodatkowym, ale ściśle związanym z właściwą ochroną danych osobowych, będzie obowiązek zaznajamiania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych.

Jednocześnie w projekcie ustawy nowelizującej wyznaczony zostaje status ABI, na który składają się: wymogi stawiane osobie mającej pełnić omawianą funkcję, organizacyjne usytuowania funkcji oraz dopuszczenie nałożenia na ABI innych zadań niż określonych w ustawie o ochronie danych osobowych (pod warunkiem, że nie naruszą możliwości prawidłowego wykonywania zadań wyznaczonych w ustawie). Dopuszczono także

możliwość powołania zastępcy administratora bezpieczeństwa informacji, co ma znaczenie w sytuacjach, gdy sam ABI przejściowo nie może realizować swoich zadań.

W przepisach dotyczących rejestracji zbiorów danych wyłączono obowiązek rejestracyjny wobec administratorów danych, którzy powołali i zgłosili do Generalnego Inspektora administratora bezpieczeństwa informacji, pod warunkiem prowadzenia przez niego wewnętrznego, uproszczonego rejestru zbiorów danych.

Obowiązek rejestracyjny nie został natomiast wyłączony w zakresie zbiorów zawierających dane wrażliwe. Natomiast w tym przypadku administrator danych nie będzie obowiązany do powstrzymania się z czynnościami przetwarzania takich danych do momentu dokonania rejestracji, jeżeli ABI wyda pozytywną opinię stwierdzającą zgodność przetwarzania danych wrażliwych z ustawą. Takie rozwiązanie przewiduje zmieniany przepis art. 46 ust.2 ustawy.

Wzory opinii ABI dotyczące przetwarzania danych wrażliwych oraz uproszczonego rejestru zbiorów danych określone zostaną w przepisach wykonawczych do ustawy o ochronie danych osobowych.

Opracowanie na bazie projektu zmian ustawy o ochronie danych osobowych przygotowanego przez Zespół ds. roli ABI Stowarzyszenia Administratorów Bezpieczeństwa Informacji w dniu 21 maja 2009r.
Przewodniczący Zespołu – Maciej Byczkowski, Prezes Zarządu Stowarzyszenia ABI
Redakcja treści projektu oraz opracowanie uzasadnienia w odniesieniu do ustawy deregulacyjnej – dr Grzegorz Sibiga