Administrator bezpieczeństwa informacji (ABI), jako urzędnik do spraw ochrony danych osobowych

1 stycznia 2015 r. ABI zmienił status w organizacji. Jest tzw. wewnętrznym urzędnikiem ds. ochrony danych osobowych, podległym bezpośrednio kierownikowi jednostki.

FOTOLIA

STANISŁAW HADY-GŁOWIAK

specjalista prawa pracy, ABI, doktorant Uniwersytetu Śląskiego, członek Instytutu Analizy Ryzyka w Rzeszowie i ACFE Polska

Abstract

The paper presents the Community and national regulations concerning the institution Administrator of Information Security (ABI). The work is of legal and comparative nature and seeks to identify the need to standardize the rules and new legal solutions in this respect. In addition, the study shows the need for clear and transparent rules for the functioning of ABI, its legal position, the range of tasks it performs, as well as the statutory requirements necessary to perform the tasks in this position.

Wstęp

W niniejszym artykule przedstawiono regulacje wspólnotowe i krajowe dotyczące instytucji Administratora Bezpieczeństwa Informacji, zwanego dalej „ABI". Praca ma charakter prawno – porównawczy, jej celem jest wskazanie konieczności ujednolicenia przepisów oraz wskazanie nowych rozwiązań prawnych w przedmiotowym zakresie. Ponadto w pracy wskazano potrzebę wprowadzenia jasnych i czytelnych zasad dotyczących funkcjonowania instytucji ABI, jego pozycji prawnej, zakresu wykonywanych przez niego zadań, jak również wymogów ustawowych niezbędnych do wykonywania zadań na tym stanowisku.

Instytucja ABI nie jest nową konstrukcją w polskim porządku prawnym. Dotychczas ABI, jako osoba pełniąca funkcję w jednostce, w przypadku jego powołania przez administratora danych, był ustawowo odpowiedzialny jedynie za nadzór nad przestrzeganiem zasad ochrony danych osobowych, co w związku ze zmianą przepisów ustawy o ochronie danych osobowych od dnia 1 stycznia 2015 roku spowodowało zmianę jego statusu w organizacji. Stał się tzw. wewnętrznym urzędnikiem ds. ochrony danych osobowych, podległym bezpośrednio kierownikowi jednostki[1].

Pozycja ABI wyznaczona została przepisami obowiązującej aktualnie Dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych[2].

W dyrektywie o ochronie danych umożliwiono wprowadzenie w prawie krajowym przepisów przewidujących wyznaczenie przez administratorów osoby, pełniącej funkcję urzędnika do spraw ochrony danych osobowych. Ma on obowiązek zapewnić niskie prawdopodobieństwo wywierania przez czynności przetwarzania niekorzystnego wpływu na prawa i wolności osób, których dane dotyczą[3].

Zgodnie z powyższym urzędnik do spraw ochrony danych osobowych odpowiedzialny jest w świetle art. 18 ust. 2 dyrektywy w szczególności za zapewnienie w niezależny sposób wewnętrznego stosowania przepisów prawa krajowego, przyjętych na mocy ww. dyrektywy oraz za prowadzenie rejestru operacji przetwarzania danych wykonywanych przez administratora danych, zapewniając przy tym, że nie zostaną naruszone prawa i wolności osób, których dane dotyczą.

Niemiecka ustawa o ochronie danych stanowi doskonały przykład wdrożenia w ustawodawstwie krajowym ww. przepisu. I tak zgodnie z § 4 f ust. 1 ustawy federalnej prywatne przedsiębiorstwa mają obowiązek wyznaczyć wewnętrznego urzędnika do spraw ochrony danych osobowych, jeżeli zatrudniają na stałe 10 lub więcej osób zajmujących się zautomatyzowanym przetwarzaniem danych osobowych. Jak wyraźnie wskazano w dyrektywie, zdolność do osiągnięcia tego celu wymaga pewnej niezależności stanowiska urzędnika w ramach organizacji administratora[4].

Przyjęte rozwiązania mają również na celu przygotowanie administratorów danych do unormowań zapowiadanych w projekcie rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych[5].

1. P. Kowalik, Administrator Bezpieczeństwa Informacji [w:] A. Gałach, S. Hoc i inni, Ochrona danych osobowych i informacji niejawnych w sektorze publicznym, C.H. Beck, Warszawa 2015, str. 35.
2. Komunikat w sprawie regulacji ABI, http://www.giodo.gov.pl/1520224/.
3. Podręcznik europejskiego prawa o ochronie danych osobowych, Agencja Praw Podstawowych UE, 2014, str. 106-107.
4. Podręcznik europejskiego prawa …, op .cit., str. 106-107.

Zdaniem ministra Andrzeja Lewińskiego, szczególnie istotne będzie uchwalenie nowych przepisów na poziomie Unii Europejskiej, które będą miały formę rozporządzenia, zatem we wszystkich państwach członkowskich będą stosowane bezpośrednio. Gdy wejdą w życie, powinny wzmocnić przysługujące każdemu z nas prawa, zapewnią realne gwarancje, że nasze prawo do ochrony danych osobowych i prawo do prywatności będą przestrzegane. Dla administratorów danych oznacza to większe obostrzenia dotyczące wykorzystywania naszych danych. Podkreślił przy tym, że przedsiębiorcy już teraz powinni zacząć przygotowywać się do tych zmian, m.in. rozważyć powołanie administratora bezpieczeństwa informacji (ABI), do czego unijne rozporządzenie będzie zobowiązywało, a co znowelizowane od 1 stycznia 2015 r. przepisy ustawy o ochronie danych osobowych umożliwiają. Jak mówił, ABI to pomocnik administratora, stojący na straży przestrzegania wykorzystywania danych osobowych zgodnie z prawem, by nie dochodziło do jego naruszenia[6].

ABI w świetle przepisów obowiązujących w Polsce

Jak wspomniano już na wstępie instytucja ABI nie jest nową konstrukcją w polskim porządku prawnym. Na mocy noweli z 22 stycznia 2004 r. do poprzednio obowiązującej wersji ustawy o ochronie danych osobowych z 29 sierpnia 1997 r.[7] (zwanej dalej u.o.d.o.) w art 36 ust. 3 ustawy została zawarta możliwość wyznaczenia administratora bezpieczeństwa informacji (ABI), którego zadaniem było nadzorowanie przestrzegania zasad ochrony danych, chyba że administrator danych sam wykonywał czynności nadzorcze.

W związku z powyższym przed dniem wejścia w życie zmian wprowadzonych nowelizacją z 7 listopada 2014 r., a wchodzących w życie 1 stycznia 2015 r. obowiązek wyznaczenia administratora bezpieczeństwa informacji dotyczył nie tylko administratorów, którzy przetwarzają dane w systemach informatycznych (jak było to pod rządami poprzedniego rozporządzenia), ale także administratorów przetwarzających dane w tradycyjnych zbiorach danych (ręcznie). W przepisach dotychczas obowiązującej ustawy nie określono jednak szczegółowo zakresu obowiązków administratora bezpieczeństwa informacji. Ustawodawca ograniczył się tylko do ogólnego stwierdzenia, że administrator bezpieczeństwa informacji ma nadzorować przestrzeganie zasad ochrony, o których mowa w art. 36 ust. 1 u.o.d.o. Z tego sformułowania można było jedynie wyprowadzić wniosek, iż obowiązkiem administratora bezpieczeństwa informacji było nadzorowanie stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych. Administrator bezpieczeństwa informacji powinien nadzorować przede wszystkim zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem[8].

W związku z powyższym należy tutaj przytoczyć definicję nadzoru, który polega na kontroli połączonej z możliwością stosowania środków władczych, a więc wiążącego oddziaływania. Zatem administrator bezpieczeństwa informacji powinien mieć zapewnioną możliwość reagowania w sytuacjach zagrożenia czy też naruszenia zasad ochrony danych osobowych. Administrator bezpieczeństwa informacji mógł być pracownikiem administratora danych, ale mogła to być również osoba zatrudniona na podstawie umowy cywilnoprawnej (np. zlecenia) – przepisy nie rozstrzygały tej kwestii. Niewątpliwie jednak bezpieczniejsze dla administratora było pierwsze ze wskazanych powyżej rozwiązań. W praktyce funkcja ABI jest i była niekiedy łączona ze sprawowaniem innych funkcji, np. pełnomocnika ds. ochrony informacji niejawnych. Choć formalnie nie ma przeszkód do przyjmowania takiego rozwiązania, jednak niekiedy może prowadzić to do sytuacji, w której ABI będzie musiał nadzorować własne działania. Szczególnie wyraźnie widoczne jest to w sytuacji, gdy administratorem bezpieczeństwa informacji jest administrator systemu informatycznego. Z tego względu lepszym rozwiązaniem jest wyznaczanie ABI spośród pracowników, którzy nie są

5. Komunikat w sprawie regulacji ABI, op. cit.
6. Nowe prawo i edukacja odpowiedzią na wyzwania w ochronie danych osobowych, 28.01.2015 r., http://www.giodo.gov.pl/1520222/id_art/8367/j/pl.
7. Dz. U. z 2002 r., nr 101, poz. 926 z późn zm.
8. Barta J., Fajgielski P., Markiewicz R., Ochrona danych osobowych. Komentarz., http://lex.online.wolterskluwer.pl/WKPLOnline/index.rpc?#content.rpc--ASK--nro=587309235&wersja=-1&localNroPart=0&reqId=1425149914753_1508197224&class=CONTENT&loc=4&full=1&hId=3.

zatrudnieni przy przetwarzaniu danych. W literaturze postuluje się, aby przyznać ABI pozycję niezależną od pionu służb informatycznych i podległość np. bezpośrednio dyrektorowi, a nie kierownikowi działu informatyki. Są to niewątpliwie postulaty uzasadnione, lecz w praktyce niekiedy trudne do spełnienia, głównie ze względów finansowych[9].

Wątpliwości pojawiały się także w dotychczas obowiązującej ustawie, m.in. gdy chodziło o to, czy administrator danych mógł wyznaczyć więcej niż jednego administratora bezpieczeństwa informacji. Na tak sformułowane pytanie odpowiedzi negatywnej udzielali P. Barta i P. Litwiński, uznając, że wykładnia językowa jednoznacznie przemawia za wyznaczeniem jednego ABI, natomiast powołanie więcej niż jednego ABI nie jest dopuszczalne. Wskazani autorzy opowiadali się natomiast za tworzeniem "wewnętrznej struktury podległej ABI-emu". Taka wykładnia nie wydaje się jednak prawidłowa. Sformułowanie zawarte w komentowanym przepisie nie wykluczało możliwości powoływania więcej niż jednego administratora bezpieczeństwa informacji, a w praktyce wyznaczenie kilku osób, jako pełniących tę funkcję, było rozwiązaniem zasadnym (np. w sytuacji, gdy w rozbudowanej strukturze organizacyjnej administratora, procesy przetwarzania danych dokonywane są w miejscach znacznie od siebie oddalonych bądź w przypadku, gdy jedna osoba miała nadzorować zabezpieczenia tradycyjnie przetwarzanych danych, a inna osoba sprawować nadzór nad przetwarzaniem danych w systemach informatycznych). W takiej sytuacji istotne jest jednak, aby zakres zadań poszczególnych osób sprawujących funkcję ABI był określony precyzyjnie, by nie dochodziło między nimi do sporów kompetencyjnych (zarówno pozytywnych, jak i negatywnych). Oczywiście komentowany przepis nie wykluczał możliwości tworzenia wewnętrznej struktury organizacyjnej podległej ABI. Wyznaczenie administratora bezpieczeństwa informacji powinno mieć formę pisemną, choć przepisy nic na ten temat nie mówią. Warto o to zadbać ze względów dowodowych. Wyznaczenie ABI powinno znaleźć także odzwierciedlenie w indywidualnym zakresie czynności – obowiązków – osoby wyznaczonej.[10] W związku z ogłoszeniem tekstu ustawy z 7 listopada 2014 r. o ułatwieniu wykonywania działalności gospodarczej (Dz. U. z 2014 r. poz. 1662, dalej zwanej ustawą), na mocy art. 9, który wszedł w życie 1 stycznia 2015 r., doszło do zmiany przepisów ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r., poz. 1182, z późn. zm., dalej zwaną u.o.d.o.), m.in. w zakresie funkcjonowania administratora bezpieczeństwa informacji[11].

Nowelą, o której mowa powyżej, do ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych[12] wprowadzono zmiany dotyczące m.in. pozycji prawnej administratora bezpieczeństwa informacji, zakresu wykonywanych przez niego zadań, jak również wymogów ustawowych, niezbędnych do wykonywania zadań na tym stanowisku. Jeżeli chodzi o zakres wykonywanych zadań, to zostały one w porównaniu do dotychczas obwiązującej regulacji szczegółowo określone w art. 36 a ust 2 powołanej ustawy. I tak do o zadań administratora bezpieczeństwa informacji należy:

1. Zapewnianie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez:
   a. sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla administratora danych,
   b. nadzorowanie opracowania i aktualizowania dokumentacji, o której mowa w art. 36 ust. 2, oraz przestrzegania zasad w niej określonych,
   c. zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych.
2. Prowadzenie rejestru zbiorów danych przetwarzanych przez administratora danych, z wyjątkiem zbiorów, o których mowa w art. 43 ust. 1, zawierającego nazwę zbioru oraz informacje, o których mowa w art. 41 ust. 1 pkt 2-4a i 7. Rejestr, o którym mowa powyżej jest jawny.

Sprawdzenie, o którym mowa powyżej, jest dokonywane:

1. Gdy zwróci się o to Generalny Inspektor Ochrony Danych Osobowych.
2. Cyklicznie, na podstawie rocznego programu sprawdzeń opracowanego przez administrato-

9. Barta J., Fajgielski P., Markiewicz R., Ochrona danych osobowych. Komentarz……, op. cit.
10. J. Barta, P. Fajgielski, R. Markiewicz Ochrona danych osobowych. Komentarz……, op. cit.
11. Komunikat w sprawie regulacji ABI, http://www.giodo.gov.pl/1520224/.
12. Dz. U. z 2014 r., poz. 1182 z późn. zm.

ra bezpieczeństwa informacji i przedkładanego do zatwierdzenia administratorowi danych.
3. Doraźnie, jeżeli administrator bezpieczeństwa informacji uzyska informacje wskazujące na występowanie istotnych zagrożeń naruszenia ochrony danych osobowych, w szczególności bezpieczeństwa tych danych[13].

Zgodnie z ust. 4 ww. przepisu administrator danych może powierzyć administratorowi bezpieczeństwa informacji wykonywanie innych obowiązków, jeżeli nie naruszy to prawidłowego wykonywania zadań, o których mowa wyżej. W związku z powyższym, poprzez dodanie ww. zapisu zostały rozwiane wątpliwości, co do możliwości powierzenia ABI wykonywania innych obowiązków. Jednakże, jak już wcześniej wspomniano, łączenie funkcji ABI i administratora systemu nie jest rozwiązaniem właściwym, ponieważ prowadziłoby to do sytuacji, w której ABI nadzorowałby własne działania. Zmianie uległa również pozycja prawna ABI, który dotychczas był osobą wyznaczoną do pełnienia funkcji, a jego pozycja w strukturze organizacyjnej nie była prawnie uregulowana. Pomimo wykonywania czynności nadzorczych w zakresie ochrony danych osobowych, w praktyce spotykał się z różnymi przeszkodami organizacyjno-prawnymi, wobec braku jednoznacznej pozycji prawnej ABI w strukturze organizacyjnej. Obecnie ABI podlega bezpośrednio kierownikowi jednostki organizacyjnej lub osobie fizycznej będącej administratorem danych. Administrator danych zapewnia środki i organizacyjną odrębność administratora bezpieczeństwa informacji, niezbędne do niezależytego wykonywania przez niego zadań. Dotychczas istniejące wątpliwości, co do możliwości powołania zastępców ABI zostały również uregulowane w ust. 6 ww. przepisu ustawy i w przedmiotowym zakresie w razie zaistnienia takiej potrzeby administrator danych może powołać zastępców ABI. Jeżeli zaś chodzi o wymagania niezbędne do wykonywania zadań na stanowisku ABI, to spełnia je osoba, która:

1. Ma pełną zdolność do czynności prawnych oraz korzysta z pełni praw publicznych.
2. Posiada odpowiednią wiedzę w zakresie ochrony danych osobowych.
3. Nie była karana za umyślne przestępstwo.

Wymagania określone na stanowisku ABI-ego wymagają jednak doprecyzowania, bowiem wskazane kryteria nie mają żadnego przełożenia na charakterystykę wykonywanych zadań. Zdecydowanie powinna to być osoba, legitymująca się specjalistyczną wiedzą w przedmiotowym zakresie i doświadczeniem zawodowym, związanym z ochroną danych osobowych. Kryterium posiadania odpowiedniej wiedzy w zakresie ochrony danych osobowych nie ma bowiem żadnego przełożenia na wykonywane przez ABI czynności. Każda osoba może legitymować się takim kryterium, chociażby poprzez ukończenie szkolenia z zakresu ochrony danych osobowych, które może świadczyć każdy podmiot zajmujący się zawodowo szkoleniami pracowników lub edukacją.

Résumé

Instytucja Administratora Bezpieczeństwa Informacji uległa znacznym zmianom od 1 stycznia 2015 roku. Jak wspomniano już wcześniej, powołanie ABI-ego nadal jest dobrowolne, aczkolwiek tylko do czasu uchwalenia nowego rozporządzenia na poziomie Unii Europejskiej, które będzie obowiązywało we wszystkich krajach członkowskich z mocy samego prawa.
Ponadto, już w niektórych krajach członkowskich takie rozwiązanie przyjęto na podstawie samej dyrektywy, np. w Niemczech, o czym była mowa na wstępie. Dlatego powołanie ABI -ego należałoby traktować, jako rozwiązanie przejściowe, do czasu wprowadzenia bardziej szczegółowych rozwiązań prawnych w tym zakresie, bowiem dotychczas uchwalone zapisy ustawy, nawet po zmianach wprowadzonych 1 stycznia 2015 r. pozostawiają wiele do życzenia.

W pierwszej kolejności w niniejszym artykule wskazano, iż w świetle obecnie obowiązujących przepisów prawnych od 1 stycznia 2015 roku istnieją wątpliwości interpretacyjne, dotyczące możliwości powołania więcej niż jednego ABI -ego w jednostce, bądź stworzenia wewnętrznej struktury podległej ABI -emu. W mojej ocenie oba rozwiązania wydają się być dopuszczalne, szczególnie w przypadku, gdy mamy do czynienia z podmiotem o istotnie rozbudowanej strukturze organizacyjnej. Należy jednak pamiętać, by zakres obowiązków poszczególnych osób był precyzyjnie i jednoznacznie określony, a z kolei struktura wewnętrzna precyzyjnie zdefiniowana, by nie dochodziło do sporów kompetencyjnych, a zapisy były zgodne z obowiązującą ustawą.

Jeżeli chodzi zaś o pozycję prawną ABI -ego i zakres wykonywanych przez niego zadań, to zostały one precyzyjnie określone w ustawie i nie powinny budzić żadnych wątpliwości.

Kolejnym zapisem budzącym wątpliwości interpretacyjne jest możliwość powierzenia ABI -emu wykonywania

13. P. Fajgielski, Nowelizacja ustawy o ochronie danych osobowych, prezentacja z dnia 7 XI.2014 r., KUL.

innych obowiązków, jeżeli nie naruszy to prawidłowego wykonywania przez niego zadań ustawowych. I tutaj zapis jest jasny, jednakże należy zaznaczyć, że ABI nie może być osobą, która nadzorowałaby własne zadania, jak np. administrator systemu informatycznego.

Na koniec należy podkreślić pewną nieudolność ustawodawcy, który wskazał, iż do wykonywania zadań na stanowisku ABI -ego może być dopuszczona osoba, która m.in. posiada odpowiednią wiedzę w zakresie ochrony danych osobowych. Ww. kryterium wymaga doprecyzowania chociażby poprzez wskazanie doświadczenia na wskazanym stanowisku lub wskazanie posiadania niezbędnych uprawnień do wykonywania zadań na wskazanym stanowisku.

Bibliografia

1. P. Kowalik Administrator Bezpieczeństwa Informacji [w:] A. Gałach, S. Hoc i inni Ochrona danych osobowych i informacji niejawnych w sektorze publicznym, C.H. Beck, Warszawa 2015.
2. Podręcznik europejskiego prawa o ochronie danych osobowych, Agencja Praw Podstawowych UE, 2014.
3. J. Barta, P. Fajgielski, R. Markiewicz Ochrona danych osobowych. Komentarz.
4. Komunikat w sprawie regulacji ABI, http://www.giodo.gov.pl/1520224.
5. P. Fajgielski Nowelizacja ustawy o ochronie danych osobowych, prezentacja z 7 XI.2014 r., KUL.
6. Nowe prawo i edukacja odpowiedzią na wyzwania w ochronie danych osobowych, 28.01.2015r., http://www.giodo.gov.pl/1520222/id_art/8367/j/pl.
7. Ustawa z 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2015 r., poz. 2135, z późn. zm.)