ABI/IOD – wyspecjalizowany audytor ds. bezpieczeństwa informacji

FOTOLIA

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

STANISŁAW HADY-GŁOWIAK

Wstęp

W niniejszym artykule przedstawiono regulacje wspólnotowe oraz krajowe, wprowadzone Rozporządzeniem o ochronie danych osobowych (RODO)[1]. Dotyczą one instytucji Administratora Bezpieczeństwa Informacji (ABI) i jego następcy – Inspektora Ochrony Danych (IOD), jako wyspecjalizowanego audytora ds. bezpieczeństwa informacji.

W pracy zostały omówione zarówno zmiany jego pozycji prawnej, jak i zakresu wykonywanych przez Inspektora Ochrony Danych (IOD) działań. Szczególną uwagę zwrócono na jego zadania w odniesieniu do analizy ryzyka i audytu oraz na ustawowe wymogi wobec kandydatów na to stanowisko.

Słowa kluczowe: Inspektor Ochrony Danych, audyt, analiza ryzyka, ochrona danych osobowych

Abstract

This article outlines the Community and national regulations introduced by the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679). It concern's the institution of the Administrator of Information Security (ABI) and its successor – Data Protection Officer, as a specialized auditor of security information. In article there were both discussed the changes in its legal position and the range of tasks performed by the Data Protection Officer. Particular attention has been paid to its tasks with regard to risk analysis and audit and as well to the statutory requirements for candidates for this position.

Administrator Bezpieczeństwa Informacji

Administrator Bezpieczeństwa Informacji został wprowadzony do polskiego ustawodawstwa w związku z przepisami już nieobowiązującej Dyrektywy 95/46/WE Parlamentu Europejskiego i Rady Europy z 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych.

Pozycja prawna ABI ewaluowała. Początkowo pełnił on funkcję o prawnie nieuregulowanej pozycji w strukturze organizacyjnej. Jedynym jego obowiązkiem było nadzorowanie przestrzegania zasad ochrony, o których mówił art. 36 ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych[2].

1 stycznia 2015 r. do ustawy wprowadzono zmiany, dotyczące m.in. pozycji prawnej ABI, zakresu wykonywanych przez niego zadań, jak również wymogów ustawowych wobec osób, które mogą wykonywać pracę na tym stanowisku[3].

Na gruncie obecnie obowiązującej ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych[4] (u.o.d.o.) powołanie ABI w każdym przypadku jest fakultatywne i żaden administrator danych nie ma obowiązku powołania ABI. Rozporządzenie o ochronie danych osobowych sytuację tę zmienia. W określonych przypadkach, RODO przewiduje obligatoryjne powołanie Inspektora przez administratora danych, również w podmiocie przetwarzającym dane, czyli u procesora. Ponadto, pozostawiona została „furtka"

1. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE
2. Dz. U. z 2014 r., poz. 1182 z późn. zm.
3. Więcej: Stanisław Hady-Głowiak Administrator bezpieczeństwa informacji (ABI), jako urzędnik do spraw ochrony danych osobowych [w] KontrolerINFO Nr 5 2016.
4. Dz. U z 2016 r., poz. 1182

dla państw członkowskich, które mogą wprowadzić obowiązek powoływania Inspektora Ochrony Danych również w innych podmiotach niż wskazane bezpośrednio w dokumencie. Taki obowiązek może także zostać wprowadzony prawem Unii[5].

Wyznaczanie Inspektora Ochrony Danych

Obowiązek wyznaczenia IOD wynika z art. 37 ust. 1 Rozporządzenia o ochronie danych osobowych. Inspektora Ochrony Danych powołać trzeba w sytuacji, gdy:

a. przetwarzania dokonuje organ lub podmiot publiczny. Wyjątek stanowią sądy przetwarzające dane w zakresie sprawowania przez nie wymiaru sprawiedliwości;
b. główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania danych, wymagających – ze względu na swój charakter, zakres lub cele – regularnego i systematycznego monitorowania na dużą skalę osób, których dane dotyczą;
c. główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1 (wrażliwych), oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa.

Obowiązek, wyznaczenia IOD będzie definiowany poprzez:

1. kategorię przetwarzanych danych;
2. cel przetwarzania danych na dużą skalę;
3. zawsze, gdy będzie mowa o jednostce publicznej[6].

Wymagania dotyczące bezpieczeństwa informacji

W świetle u.u.d.o. Administratorem Bezpieczeństwa Informacji może być 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.

Kryterium, o którym mowa w pkt 2 wymaga doprecyzowania, bowiem Administratorem powinna być osoba legitymująca się specjalistyczną wiedzą w przedmiotowym zakresie i doświadczeniem zawodowym związanym z ochroną danych osobowych. Powyższe zostało uregulowane precyzyjnie w art. 37 ust 5 Rozporządzenia, gdzie IOD jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności fachowej wiedzy na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia powierzonych mu zadań.

5. Unijna reforma ochrony danych osobowych. Analiza zmian, red. Anna Dmochowska, Marcin Zadrożny, https://sip.legalis.pl/document-full.seam?documentId=mjxw62zogi3damjuheydgnq
6. Op. cit., Unijna reforma…
7. Op. cit., Unijna reforma…

FOTOLIA

Oczywiście, RODO wskazuje, że IOD może wykonywać inne zadania i obowiązki, jednak nie powinny one powodować konfliktu interesów. Podobnie zostało to uregulowane w art. 36a ust 4 u.o.d.o. Pełnienie tej funkcji nie może być dodatkiem do innych obowiązków pracowniczych.

Niestety, obecnie bardzo często się zdarza, że osoby, które pełnią funkcję ABI, nie mają czasu na rzeczywisty nadzór nad systemem ochrony danych osobowych, ponieważ inne obowiązki pracownicze są zbyt czasochłonne. Administratorzy danych oraz podmioty przetwarzające muszą uświadomić sobie, że to w ich interesie leży, aby IOD dysponował odpowiednim czasem do wykonywania swoich zadań. Inspektor powinien być włączony w opiniowanie wszelkich procesów biznesowych w organizacji, wiążących się z przetwarzaniem danych osobowych.

Inspektor Ochrony Danych – nie koniecznie etat

Inspektor może być członkiem personelu administratora lub podmiotu przetwarzającego. Może też wykonywać swoje zadania na podstawie umowy o świadczenie usług, czego nie wyklucza obecna u.o.d.o.

RODO wskazuje administratorowi danych lub podmiotowi przetwarzającemu dodatkowy obowiązek wspierania IOD w wypełnianiu zadań. Nakazuje zapewnienie Inspektorowi zasobów niezbędnych do wykonania zadań, dostępu do danych osobowych i operacji przetwarzania. Jeśli IOD jest pracownikiem musi otrzymać wsparcie niezbędne do utrzymania fachowej wiedzy i kompetencji na dobrym poziomie.

Niezależność i bezstronność IOD

Inspektor Ochrony Danych nie może otrzymywać instrukcji dotyczących wykonywania swoich zadań. Spełniając warunki dotyczące wiedzy, umiejętności i kompetencji, potrafi samodzielnie wywiązać się z powierzonych obowiązków. Tylko pełna niezależność IOD daje gwarancję jego bezstronności.

RODO idzie dalej, precyzując, że IOD nie może być odwoływany ani karany przez administratora ani podmiot przetwarzający. Inspektor bezpośrednio podlega najwyższemu kierownictwu administratora lub podmiotu przetwarzającego. Z kolei zgodnie z u.o.d.o. ABI podlega bezpośrednio kierownikowi jednostki organizacyjnej lub osobie fizycznej będącej administratorem danych.

Europejski ustawodawca przewidział również możliwość wyznaczenia jednego inspektora ochrony danych przez grupę przedsiębiorstw. Warunkiem jest możliwość łatwego nawiązania kontaktu z inspektorem ochrony danych z każdej jednostki organizacyjnej[7].

Powołanie i odwołanie ABI/IOD

Administrator danych obowiązany jest zgłosić do rejestracji Głównego Inspektora Ochrony Danych Osobowych (GIODO) powołanie i odwołanie ABI w terminie 30 dni od dnia jego powołania lub odwołania. GIODO, prowadzące ogólnokrajowy, jawny rejestr administratorów bezpieczeństwa informacji, publikuje tę informację.

W RODO powyższa kwestia została znacznie uproszczona. Administrator lub podmiot przetwarzający publikują dane kontaktowe Inspektora Ochrony Danych i zawiadamiają o nich organ nadzorczy.
Różnica tych rozwiązań dotyczy zasadniczo sposobu publikacji tej informacji.

Ponadto, RODO daje możliwość wyznaczenia wspólnego IOD dla kilku organów lub podmiotów publicznych, jednak z uwzględnieniem ich struktury organizacyjnej i wielkości. Doświadczenie audytowe w sektorze publicznym wskazuje jednak, iż takie podmioty mają problemy z zabezpieczeniem organizacyjnym i technicznym danych osobowych. Dlatego też należy bardzo ostrożnie podchodzić do wyznaczenia jednego Inspektora Ochrony Danych dla kilku podmiotów publicznych, gdyż może to powodować fikcyjny nadzór nad systemem ochrony danych w tych podmiotach[8].

Zadania ABI/IOD

Jeżeli chodzi o zadania ABI, to na podstawie obowiązującej ustawy należy do niego:

1. prowadzenie rejestru zbiorów danych, przetwarzanych przez administratora danych, z wyjątkiem zbiorów zawierających dane wrażliwe,
2. zapewnianie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez:

8. Op. cit., Unijna reforma….
9. Op., cit., Unijna reforma….

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 z zakresu ochrony danych osobowych oraz przestrzegania zasad w niej określonych,
c. zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych.

Z kolei zadania IOD, wynikające z RODO, zostały znacznie rozbudowane w stosunku do zadań ABI. I tak do IOD należy:

1. informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;
2. monitorowanie przestrzegania rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
3. udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania;
4. współpraca z organem nadzorczym;
5. pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem danych.

FOTOLIA

Obowiązki IOD

Administrator oraz podmiot przetwarzający muszą zapewnić Inspektorowi Ochrony Danych właściwe i niezwłoczne włączanie we wszystkie sprawy dotyczące ochrony danych osobowych.

Z powyższego wynika, że jednym z głównych obowiązków IOD będzie współpraca z organem nadzorczym oraz pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem danych. Taka regulacja z jednej strony precyzuje rolę i niezależność Inspektora w jednostce, a z drugiej definiuje jego podległość względem organu nadzorczego.

Pełnienie funkcji punktu kontaktowego wiązać się będzie z koniecznością udzielania niezbędnych informacji i wyjaśnień osobom, których zbierane i przetwarzane dane dotyczą oraz z wykonywaniem praw przysługujących im na mocy niniejszego rozporządzenia. Podkreślić należy, że dane kontaktowe Inspektora, jako jeden z elementów spełnienia obowiązku informacyjnego, będą musiały zostać ujawnione w trakcie zbierania danych.

W przypadku działań zapewniających obowiązki Inspektora Ochrony Danych zostały znacznie rozbudowane. Musi on prowadzić szkolenia personelu i podejmować działania zwiększające jego świadomość potrzeby ochrony danych. Obowiązany jest do udzielania zaleceń, informowania osób przetwarzających dane osobowe o obowiązkach spoczywających na nich na mocy Rozporządzenia o ochronie danych osobowych oraz innych, unijnych i lokalnych, przepisów o ochronie danych oraz doradzanie im w tej sprawie.

Zamiast sprawdzeń monitorowanie i audyt

W miejsce prowadzenia sprawdzeń pojawił się obowiązek monitorowania przestrzegania RODO i innych przepisów Unii lub państw członkowskich oraz polityk administratora lub podmiotu przetwarzającego i prowadzenia powiązanych z tym audytów. Wszystkie te zadania muszą uwzględniać analizę ryzyka związanego z operacjami przetwarzania. Analiza ryzyka musi z kolei uwzględniać charakter, zakres, kontekst i cele przetwarzania danych.

Przepisy RODO wskazują także, iż Inspektor Ochrony Danych może przeprowadzać audyty przestrzegania wytycznych ustanowionych w przepisach.

W RODO nie sprecyzowano terminów przeprowadzania ewentualnych audytów. Wydaje się jednak, że powinny być nie rzadsze niż raz w roku. Okres ten pozwala Inspektorowi na ocenę zmian, jakie zachodzą w funkcjonującym w organizacji systemie przetwarzania danych, jak i na wprowadzenie rekomendacji wydanych przy poprzednim audycie[9].

Zasady przeprowadzania audytu przez IOD

Warto, aby przyszły IOD zapoznał się z normą PN-EN ISO 19011, zawierającą wytyczne dotyczące audytowania systemów zarządzania jakością i/lub zarządzania środowiskowego. Opisuje ona m.in. zasady przeprowadzania audytu. Zadaniem Inspektora jest przedstawienie najwyższemu kierownictwu organizacji wiarygodnych informacji dotyczących przetwarzania i ochrony danych osobowych. Aby IOD posiadł takie informacje, musi systematycznie przeprowadzać audyty. Aby audyt był wiarygodnym i efektywnym narzędziem do dostarczania niezbędnych informacji dla kierownictwa organizacji, powinien opierać się na kilku zasadach przedstawionych w przedmiotowej normie ISO.

Wnioski

W tym miejscu mocno należy podkreślić rolę IOD, jako audytora, ponieważ realizacja zadań w zakresie audytu dotyczyć będzie przede wszystkim podmiotów publicznych. Audyt w tym znaczeniu rozumiany jest, jako profesjonalna działalność zapewniająca, skuteczny instrument wspomagający władze organizacji/instytucji w procesach właściwego zarządzania. Jest niezależny i obiektywny, a jego celem jest wspieranie kierownika jednostki w realizacji celów i zadań przez systematyczną ocenę kontroli zarządczej, w tym wypadku ochrony zasobów oraz czynności doradcze.

Mając powyższe na uwadze oraz zadania w zakresie analizy ryzyka wynikające z RODO, prawidłowa realizacja zadań przez IOD będzie wymagała posiadania niezbędnej wiedzy i kwalifikacji w przedmiotowym zakresie, co powinno zostać wyraźnie określone w projektowanej ustawie o ochronie danych osobowych.

Jeśli IOD ma służyć radą i pomocą najwyższemu kierownictwu w podejmowaniu decyzji, jak najszybciej zmienić się musi podejście do osoby, która pełni tę funkcję. Kierownictwo musi do takiej osoby mieć zaufanie, dlatego w RODO wskazano, iż piastujący to

10. Op. cit., Unijna reforma, …

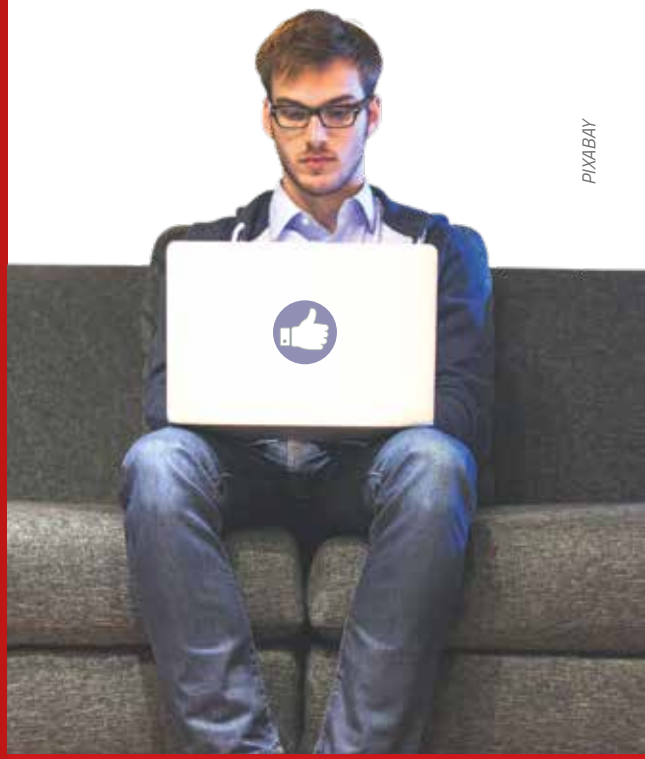
stanowisko zobowiązany jest do zachowania tajemnicy lub poufności co do wykonywania swoich zadań – zgodnie z prawem Unii lub prawem państwa członkowskiego[10].

Należy również dodać, że projekt zmian ustawy o ochronie danych osobowych i dostosowania jej do przepisów Rozporządzenia jest na razie w początkowym stadium realizacji i nie zawiera żadnych szczegółów, co do przyszłego IOD. Jedyna wzmianka dotyczy konieczności zgłoszenie Inspektora Ochrony Danych do Urzędu w ciągu 14 dni od jego wyznaczenia, a w przypadku osób obecnie pełniących funkcję ABI, będą oni mieli czas do 01.09.2018 r. na podjęcie decyzji w sprawie rezygnacji z funkcji lub pozostania na stanowisku, jako IOD[11].

BIBLIOGRAFIA

1. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE
2. Dz. U. z 2014 r., poz. 1182 z późn. zm.
3. Więcej: Stanisław Hady-Głowiak Administrator bezpieczeństwa informacji (ABI), jako urzędnik do spraw ochrony danych osobowych [w] KontrolerINFO Nr 5 2016
4. Dz. U z 2016 r., poz. 1182
5. red. Anna Dmochowska, Marcin Zadrożny Unijna reforma ochrony danych osobowych. Analiza zmian, https://sip.legalis.pl/document-full.seam?documentId=mjxw62zogi3damjuheydgnq

11. Projekt ochrony danych osobowych, Tomasz Osiej 28.04.2017 r., https://sip.legalis.pl/document-full.seam?documentId=nzsxo4zogi3damjwga3tmmi



PIXABAY

Konkurs „SUPER KONTROLER 2017”

Zakończył się pierwszy etap zorganizowanego przez Polski Instytut Kontroli Wewnętrznej konkursu.

Dziękujemy za nadesłane prace. W tej chwili pochyla się nad nimi Komisja Konkursowa.

O rozstrzygnięciu konkursu poinformujemy na naszym portalu, a od następnego numeru magazynu „KontrolerINFO” rozpoczniemy publikację trzech najlepszych opracowań. Wystąpienia zwycięzcy konkursu będzie można wysłuchać na 16 Międzynarodowym Kongresie Kontroli Wewnętrznej Audytu Wewnętrznego i Zwalczania Oszustw.