ADMINISTRATOR DANYCH OSOBOWYCH JAKO PODMIOT SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI W ORGANIZACJI

PERSONAL DATA ADMINISTRATOR AS A SUBJECT OF THE INFORMATION SECURITY MANAGEMENT SYSTEM IN THE ORGANISATION

Anna LASOTA-KAPCZUK
a.lasota91@gmail.com

Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach
Wydział Humanistyczny
Instytut Nauk Społecznych i Bezpieczeństwa

Streszczenie: Administrator danych osobowych to każdy podmiot decydujący o celach i środkach przetwarzania danych osobowych. Głównym obowiązkiem administratora jest zapewnienie przestrzegania zapisów ustawy o ochronie danych osobowych w organizacji. Regulacje prawne w zakresie ochrony prywatności oraz rosnąca liczba zagrożeń dla bezpieczeństwa informacji sprawiają, że administrator staje się również podmiotem kluczowym w procesie zarządzania informacjami w celu zapewnienia ich bezpieczeństwa. Celem artykułu jest zaprezentowanie roli administratora danych w systemie zarządzania bezpieczeństwem informacji w organizacji oraz głównych jego zadań w tym zakresie.
Abstract: The personal data administrator is every subject, who decides about the purposes and means of processing personal data. His main responsibility is to ensure keeping rules of the Personal Data Protection Act in organization. Legally enforced privacy requirements and the growing number of information security threats make the administrator a main player in the process of management of the information. The aim of the article is to present a role of personal data administrator in the information security management system in organization and his main tasks in this area.
Słowa kluczowe: dane osobowe, administrator danych osobowych, ochrona, bezpieczeństwo, informacja
Key words: personal data, personal data administrator, protection, security, information

WSTĘP

Zgodnie z zapisami art. 7 pkt 4 ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych (u.o.d.o.), pod pojęciem administratora danych należy rozumieć organ, jednostkę organizacyjną, podmiot lub osobę decyzyjną w kwestii celów i środków przetwarzania danych osobowych (Ustawa o ochronie danych osobowych, 1997). Administrator posiada wobec danych osobowych władztwo decyzyjne, co oznacza, że może decydować o rodzaju gromadzonych i przetwarzanych w organizacji danych, o podmiotach, którym je udostępnia, a także o środkach bezpieczeństwa stosowanych w celu ochrony danych (Serzycki, 2010). Administrator zapewnia bezpieczeństwo przetwarzania danych oraz realizację organizacyjnych i technicznych przedsięwzięć na rzecz ochrony danych przetwarzanych w organizacji. Wszelkie zadania przez niego wykonywane muszą pozostawać w zgodności z przepisami ustawy o ochronie danych osobowych oraz stosownych przepisów wykonawczych. Przegląd obowiązujących regulacji prawnych w zakresie ochrony danych osobowych, krajowego piśmiennictwa oraz raportów i analiz Generalnego Inspektora Ochrony Danych Osobowych pozwala jednoznacznie stwierdzić, iż administrator danych osobowych jest osobą kluczową w procesie zapewniania bezpieczeństwa i ochrony danych osobowych. Na potrzeby niniejszego artykułu wykorzystano charakterystyczny dla obszaru

nauk prawnych opisowo-analityczny model badań. Krytyczna analiza aktów prawa krajowego oraz opracowań naukowych z zakresu ochrony danych osobowych umożliwia przybliżenie roli, jaką administrator danych odgrywa w systemie zarządzania bezpieczeństwem informacji w organizacji oraz głównych zadań, jakie realizuje on w tym zakresie.

1. ZADANIA ADMINISTRATORA DANYCH OSOBOWYCH W ŚWIETLE PRAWODAWSTWA KRAJOWEGO

Odpowiedzialność administratora danych osobowych ponosi zarząd przedsiębiorstwa lub osoba stojąca na najwyższym stopniu w hierarchii organizacji (np. właściciel firmy), jednak z formalnego punktu widzenia administratorem danych nie jest konkretna osoba fizyczna, ale podmiot, czyli organizacja. Możliwe jest powołanie przez właściciela przedsiębiorstwa odrębnego administratora danych osobowych (poza zarządem), który wypełnia obowiązki związane z ochroną danych osobowych. Należy jednak zauważyć, że funkcjonujący w ten sposób administrator nie ponosi w tym zakresie odpowiedzialności na zewnątrz organizacji - odpowiedzialność tę zawsze ponosi zarząd przedsiębiorstwa.

Administratorem danych mogą być zarówno podmioty prywatne (osoby fizyczne, osoby prawne, podmioty niepubliczne realizujące zadania publiczne, a także jednostki organizacyjne nieposiadające osobowości prawnej, jeżeli przetwarzają dane w związku z działalnością zawodową, zarobkową lub realizując cele statusowe), jak i publiczne (organy państwowe, organy samorządu terytorialnego oraz organy państwowych i samorządowych jednostek organizacyjnych). W przypadku podmiotów prywatnych administratorem danych osobowych jest organizacja, a nie osoba nią kierująca czy pracownik realizujący faktyczne czynności związane z ochroną tych danych w przedsiębiorstwie. Podmioty publiczne działają na podstawie przepisów ustawowych lub wykonawczych określających cele i środki przetwarzania danych, zatem rzadko mogą samodzielnie podejmować decyzje w tym zakresie. Fakt ten może powodować trudności z ustaleniem, kto jest faktycznym administratorem zbioru danych osobowych. Możliwym rozwiązaniem jest wskazanie podmiotu odpowiedzialnego za utworzenie i prowadzenie zbioru danych osobowych (wraz z zasadami realizacji tego obowiązku) w przepisach prawa, stanowiących podstawę utworzenia zbioru, w którym przetwarzane są wskazane dane. Przykładem zastosowania takiego zabiegu jest ustawa z dnia 24 maja 2000 r. o Krajowym Rejestrze Karnym, w myśl art. 4 ust 2 której, administratorem danych osobowych zgromadzonych w Rejestrze jest Biuro informacyjne (ustawa o Krajowym Rejestrze Karnym, 2000). Administratorem danych jest zawsze organ administracji publicznej, np. prezydent miasta, nie zaś urząd go obsługujący lub wyspecjalizowana komórka organizacyjna.

Ustawa z 1997 r. nakłada na administratora danych osobowych szereg obowiązków, których spełnienie warunkuje legalność pozyskiwania, przechowywania i przetwarzania danych osobowych przez organizację. Fundamentalnym obowiązkiem administratora danych jest wskazanie podstawy prawnej do legalnego przetwarzania danych. Podstawy te zostały określone w przedmiotowej ustawie i są zależne od kategorii danych osobowych: katalog przesłanek zezwalających na przetwarzanie zwykłych danych wskazuje art. 23 u.o.d.o., natomiast do okoliczności przetwarzania danych sensytywnych (szczególnie chronionych, tj. ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, dane o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz dane dotyczące skazań, orzeczeń o ukaraniu i mandatów karnych, a także o innych orzeczeniach wydanych w postępowaniu sądowym lub administracyjnym) odnosi się art. 27. Jeżeli administrator spełnia co najmniej jeden warunek wymieniony w ustawie, dane osobowe w organizacji przetwarzane są zgodnie z prawem (Serzycki, 2010).

Ustawową powinnością administratora danych osobowych jest także obowiązek informacyjny, wskazany w art. 24 i 25 u.o.d.o. Jeżeli przetwarzane w organizacji dane osobowe pozyskiwane są bezpośrednio od osoby, której dotyczą, administrator jest zobowiązany poinformować tę osobę o: pełnej nazwie organizacji oraz adresie jej siedziby (jeśli administratorem jest osoba fizyczna, powinna przedstawić podmiotowi również swoje imię, nazwisko i adres zamieszkania), celu zbierania danych oraz ich odbiorcach (lub kategoriach odbiorców), prawie podmiotu do dostępu do treści swoich danych i możliwości ich aktualizacji, a także dobrowolności lub obowiązku podania danych osobowych przez podmiot. Jeżeli taki obowiązek istnieje, administrator wskazuje również jego podstawę prawną (ustawa o ochronie danych osobowych, 1997). W sytuacji, gdy podmiot przetwarzania danych osobowych posiada powyższe informacje lub przepis odrębnej ustawy pozwala na przetwarzanie danych bez ujawniania faktycznego celu ich gromadzenia, administrator jest zwolniony z obowiązku informacyjnego. Jeżeli dane osobowe nie są pozyskiwane bezpośrednio od podmiotu, którego dotyczą, administrator ma obowiązek poinformować go dodatkowo o źródle danych oraz prawach wynikających z art. 32 u.o.d.o., tj. o prawie do zgłoszenia sprzeciwu wobec dalszego ich przetwarzania oraz wniesienia umotywowanego, pisemnego żądania zaprzestania tego działania. W sytuacji, gdy udzielenie powyższych informacji mogłoby spowodować: ujawnienie wiadomości zawierających informacje niejawne, zagrożenie dla obronności lub bezpieczeństwa państwa, życia i zdrowia ludzi lub bezpieczeństwa i porządku publicznego, zagrożenie dla podstawowego interesu

gospodarczego lub finansowego państwa lub istotne naruszenie dóbr osobistych osób, których dane dotyczą, lub innych osób - na mocy art. 34 administrator danych może odmówić udzielenia wskazanych informacji osobie, której dane te dotyczą.

Artykuł 26 u.o.d.o. nakłada na administratora obowiązek szczególnej staranności w kwestii ochrony interesów osób, których przetwarzane dane dotyczą. W tym celu administrator musi zapewnić dopełnienie czterech ustawowych warunków: legalności przetwarzania danych, gromadzenia ich jedynie dla oznaczonych, zgodnych z prawem celów, zachowania ich merytorycznej poprawności i adekwatności w stosunku do celów, a także przechowywania ich w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż wymaga tego cel ich przetwarzania (ustawa o ochronie danych osobowych, 1997).

Kolejny obowiązek administratora został określony w art. 36 u.o.d.o., na mocy zapisów którego organ ten zobowiązany jest do stosowania środków technicznych i organizacyjnych, zapewniających ochronę przetwarzanych danych, adekwatną zarówno do ich kategorii, jak i potencjalnych dla nich zagrożeń. Zadaniem administratora jest wybór odpowiednich środków zabezpieczających, za pomocą których zminimalizuje ryzyko zniszczenia, zmiany lub utraty danych. Ten sam artykuł nakłada na administratora obowiązek prowadzenia dokumentacji opisującej zarówno sposób przetwarzania danych, jak i stosowane w celu ich zabezpieczenia środki.

Zgodnie z art. 37 u.o.d.o., do przetwarzania danych dopuszczone mogą być osoby posiadające stosowne upoważnienie, nadane przez administratora. Podmiot ten ma zatem obowiązek dołożenia starań, by każda osoba wykonująca czynności związane z przetwarzaniem danych dysponowała wskazanym upoważnieniem. Administrator jest również zobowiązany do prowadzenia ewidencji osób upoważnionych do przetwarzania danych, zawierającej imię i nazwisko osoby, datę nadania i ustania upoważnienia oraz jego zakres. W sytuacji, gdy dane są przetwarzane w systemie informatycznym, dodatkowym elementem ewidencji staje się również indywidualny identyfikator użytkownika systemu (ustawa o ochronie danych osobowych, 1997). Z kolei art. 38. u.o.d.o. zobowiązuje administratora do zapewnienia kontroli nad tym, jakie dane osobowe zostały wprowadzone do zbioru danych, kto i kiedy je wprowadził, a także komu są one przekazywane.

Ustawowym obowiązkiem administratora danych jest również zgłoszenie zbioru danych osobowych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych. Kategorie administratorów zwolnionych z jego realizacji wskazuje art. 43 ust. 1 u.o.d.o., toteż przed zgłoszeniem każdy administrator danych powinien sprawdzić, czy administrowany przez niego zbiór nie podlega zwolnieniu z rejestracji. Po nowelizacji ustawy o ochronie

danych osobowych, tj. od 1 stycznia 2015 r., z obowiązku zgłoszenia zbioru danych do GIODO zwolnieni są również administratorzy danych, którzy powołali administratora bezpieczeństwa informacji i zgłosili go do rejestru ABI, prowadzonego przez GIODO. Zgłoszenia zbioru do GIODO dokonuje się poprzez wypełnienie formularza, stanowiącego załącznik do rozporządzenia MSWiA z 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji GIODO lub przez elektroniczną platformę e-GIODO. Administrator, jako strona postępowania administracyjnego prowadzonego w celu rejestracji zbioru, może zostać również wezwany do przedstawienia innych dokumentów, mogących mieć istotne znaczenie w tym procesie (Serzycki, 2010).

Należy zauważyć, że przetwarzanie danych w ramach zbioru zawierającego zwykłe dane osobowe, administrator może rozpocząć już w momencie zgłoszenia tego zbioru do GIODO, przy czym zaświadczenie o jego rejestracji jest wydawane przez Inspektorat na wniosek administratora. W przypadku zbioru zawierającego dane wrażliwe, przetwarzanie tych danych administrator może rozpocząć dopiero po zarejestrowaniu zbioru, przy czym zaświadczenie o rejestracji wydawane jest przez GIODO obligatoryjnie (Serzycki, 2010).

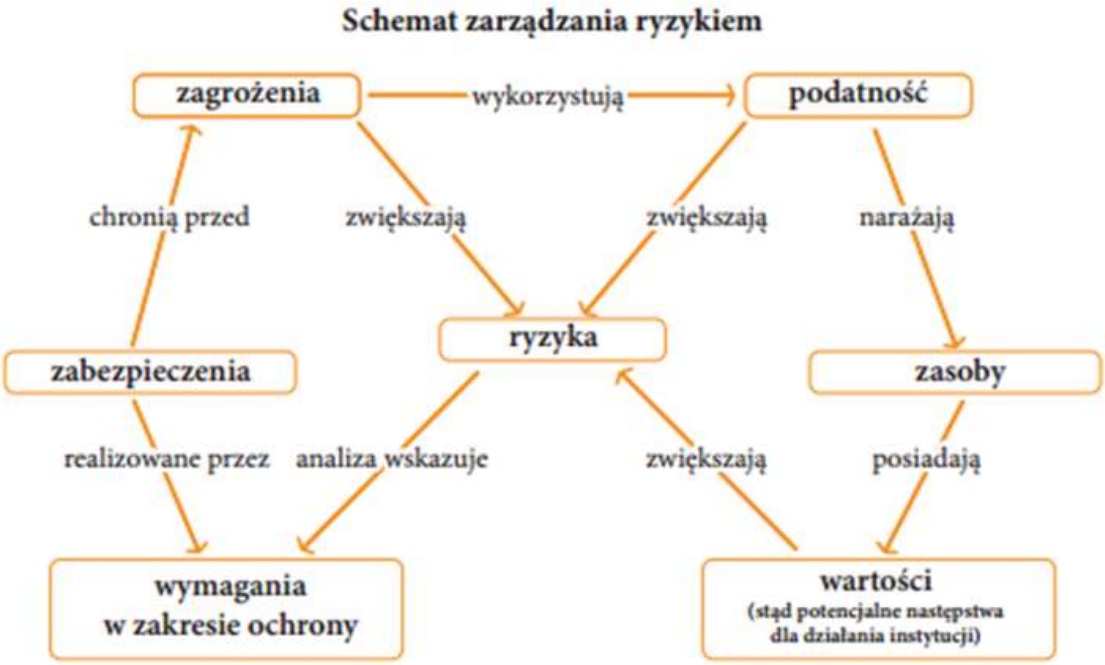
2. ROLA ADMINISTRATORA DANYCH W SYSTEMIE ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI

Uregulowane prawnie wymogi ochrony prywatności w połączeniu z nieustannie zwiększającą się liczbą zagrożeń dla bezpieczeństwa informacji przetwarzanych z wykorzystaniem systemów teleinformatycznych sprawiają, że stosowanie nowoczesnych narzędzi informatycznych wymaga profesjonalnego podejścia do organizowania ich bezpieczeństwa. W toku działań na rzecz budowy systemu zarządzania bezpieczeństwem informacji, administrator danych powinien zapewnić realizację pięciu jego podstawowych elementów, tj.:

- przeprowadzić analizę ryzyka bezpieczeństwa informacji w obszarze utraty, zniszczenia, nieuprawnionej modyfikacji lub utraty poufności przetwarzanych danych; analiza ta powinna uwzględniać takie etapy jak: identyfikacja i ocena posiadanych zasobów, identyfikacja zagrożeń, identyfikacja istniejących zabezpieczeń, identyfikacja podatności, szacowanie ryzyka, opracowanie rekomendacji;
- ustanowić politykę bezpieczeństwa, stosowną do zakresu i celów przetwarzania posiadanych danych;
- wdrożyć i zapewnić stosowanie środków bezpieczeństwa przewidzianych w przyjętej polityce;

- przeszkolić pracowników w zakresie legalnego przetwarzania danych osobowych, kładąc szczególny nacisk na odpowiedzialność za jego naruszenia;
- zapewnić odpowiednie relacje pomiędzy administratorem danych a podmiotem, któremu powierzono przetwarzanie danych (Kaczmarek, 2009).

Analiza ryzyka stanowi kluczowy element procesu zarządzania ryzykiem bezpieczeństwa informacji. Zgodnie z § 20 ust. 2 pkt 3 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, zarządzanie bezpieczeństwem informacji realizuje się w szczególności poprzez prowadzenie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji, a także poprzez podejmowanie działań minimalizujących wskazane ryzyko, stosownie do wyników przeprowadzonej analizy (Dz. U. 2012, poz. 526). Polska Norma ISO/IEC 27001 definiuje ryzyko jako kombinację prawdopodobieństwa i skutku wystąpienia określonego negatywnego zdarzenia (Kaczmarek, 2009). Mianem ryzyka bezpieczeństwa informacji określa się natomiast prawdopodobieństwo wystąpienia zagrożenia dla systemu, a w konsekwencji - powstania zniszczeń w jego zasobach oraz zakłóceń utrudniających lub uniemożliwiających prawidłowe jego funkcjonowanie (Kaczmarek, 2009). W omawianym kontekście należy zwrócić uwagę na niuanse definicyjne, które można odnaleźć w przyjętych normach dotyczących systemów zarządzania bezpieczeństwem informacji. Często szacowanie i analiza ryzyka stosowane są jako pojęcia tożsame, podczas gdy przywołana wcześniej norma 27001 definiuje pierwsze z nich jako całościowy proces analizy i oceny ryzyka, zaś samą analizę ryzyka - jako systematyczne korzystanie z dostępnych informacji celem zidentyfikowania źródeł i skali ryzyka (Stróżyk, b.r.). Szacując ryzyko należy uwzględnić takie aspekty jak: rodzaj zagrożeń, prawdopodobieństwo ich wystąpienia, potencjalne konsekwencje oraz przypuszczalny okres bądź częstotliwość ich pojawienia się (Janus, b.r.). Identyfikację potencjalnych i realnych zagrożeń i podatności na nie systemu, szacowanie ryzyka, a także rekomendowanie zastosowania dodatkowych środków ochrony nazywa się zarządzaniem ryzykiem (Piotrowski, b.r.). Zgodnie z Polską Normą PN-I-13335-1, zarządzanie ryzykiem stanowi jeden z kluczowych elementów zarządzania bezpieczeństwem systemów informatycznych. Wskazana norma określa również związki występujące pomiędzy poszczególnymi elementami tego procesu (rys.1).



Rys. 1. Zależności pomiędzy elementami systemu zarządzania ryzykiem przy ocenie ryzyka według normy PN-I-13335-1.
Źródło: Kaczmarek, A. (2009). *ABC zagrożeń bezpieczeństwa danych osobowych w systemach informatycznych*. Warszawa: Generalny Inspektor Ochrony Danych Osobowych. s. 68.

Iga Stróżyk wyróżnia w procesie zarządzania ryzykiem kilka podstawowych etapów, tworzących zamkniętą pętlę:

1. wyznaczenie kontekstu strategicznego, organizacyjnego i związanego z zarządzaniem ryzykiem (opracowanie metodyki zarządzania ryzykiem) oraz określenie odpowiedzialności w tym zakresie;
2. identyfikację ryzyk - określenie potencjalnych przyczyn i sposobu materializacji zagrożeń poprzez inwentaryzację wszystkich aktywów organizacji (pracowników, oprogramowania, sprzętu, technologii i lokalizacji), zagrożeń, podatności i ewentualnych konsekwencji wystąpienia niepożądanych incydentów;
3. określenie zagrożeń dla zidentyfikowanych aktywów; zagrożenia te mogą być wynikiem przypadkowych i celowych działań lub okoliczności środowiskowych - wśród zagrożeń uwzględnianych w procesie szacowania ryzyka najczęściej wymienia się pożary, zalania, zanieczyszczenia, wypadki, kradzieże, zniszczenia urządzeń, przeciążenia systemu oraz awarie zasilania;
4. właściwą analizę ryzyka, podejmowaną na podstawie istniejących zabezpieczeń, prawdopodobieństwa wystąpienia incydentu naruszenia bezpieczeństwa oraz jego konsekwencji; szacując prawdopodobieństwo materializacji zagrożenia należy zatem uwzględnić następujące czynniki: statystykę prawdopodobieństwa zagrożeń, podatności, możliwości oraz motywy wystąpienia zagrożeń spowodowanych celowym działaniem,

czynniki środowiskowe, czynniki generujące możliwość wystąpienia błędów ludzkich, nieprawidłowe funkcjonowanie urządzeń oraz stan i skuteczność posiadanych zabezpieczeń;

5. analizę skutków wystąpienia ryzyka, z uwzględnieniem konsekwencji bezpośrednich (np. kosztu naprawy uszkodzonych lub utraconych aktywów) oraz pośrednich (za które uznać można koszty utraconych możliwości lub utratę wizerunku organizacji);
6. ocenę ryzyka, dokonywaną poprzez porównanie oszacowanych poziomów ryzyka z obowiązującymi kryteriami oraz nadanie tym ryzykom priorytetów poprzez zakwalifikowanie szansy ich wystąpienia jako niskiej, średniej lub wysokiej. Pożądanym efektem tego etapu jest utworzenie listy ryzyk, wobec których konieczne jest podjęcie działań redukujących ich faktyczną wartość do akceptowalnego poziomu (Stróżyk, b.r.).

Analiza powyższych elementów procesu zarządzania ryzykiem pozwala zauważyć, że podstawowym zadaniem analizy ryzyka jest zatem identyfikacja zasobów dostępnych w systemie, ich podatności na określone rodzaje zagrożeń, wskazanie owych zagrożeń, oszacowanie prawdopodobieństwa ich zaistnienia oraz poznanie skali potencjalnych strat. Głównym celem tego procesu jest obniżenie ryzyka do akceptowalnego poziomu, czyli takiego, przy którym organizacja będzie w stanie udźwignąć ciężar strat spowodowanych zagrożeniem w postaci nieuprawnionej modyfikacji lub utraty danych. Dlatego też analiza ryzyka powinna być wykonywana w każdej organizacji wdrażającej system bezpieczeństwa informacji. Procedura ta powinna być uruchamiana nie tylko podczas zaplanowanych terminów przeglądu ryzyk, ale również każdorazowo w sytuacji wystąpienia w organizacji istotnych zmian, mogących mieć wspływ na bezpieczeństwo informacji. Jednocześnie należy zauważyć, że pomimo stosowania organizacyjnych, fizycznych i technicznych środków ochrony, organizacja nie jest w stanie całkowicie wyeliminować ryzyka. Wynikiem przeprowadzenia analizy ryzyka nie jest jednak całkowita jego redukcja, ale zastosowanie przez administratora danych osobowych odpowiednich zabezpieczeń dla przetwarzanych danych oraz opracowanie odpowiedniej dokumentacji określającej właściwe ich stosowanie (Byczkowski i Zawiła-Niedźwiedzki, 2014).

Zgodnie z § 3 rozporządzenia 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, administrator danych zobowiązany jest do wdrożenia w organizacji dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę tych danych

(Dz. U. 2004, nr 100, poz. 1024). Wskazaną dokumentację tworzą polityka bezpieczeństwa oraz instrukcja zarządzania systemem informatycznym. Polityka bezpieczeństwa jest dokumentem zawierającym katalog praw, reguł oraz praktycznych rozwiązań w zakresie sposobu zarządzania, ochrony i rozpowszechniania danych osobowych w organizacji (Polski Komitet Normalizacyjny, 2002). Jej celem jest określenie i wdrożenie zasad bezpieczeństwa przetwarzania i ochrony danych osobowych ze szczególnym uwzględnieniem zabezpieczenia przed udostępnieniem osobom nieupoważnionym i przetwarzaniem naruszającym przyjęte normy prawne, a także ochrony przed nieautoryzowaną zmianą, uszkodzeniem lub zniszczeniem. Cel ten administrator danych osobowych realizuje poprzez zapewnienie danym trzech właściwości: poufności, integralności i rozliczalności przetwarzania danych.

Można zatem stwierdzić, że polityka bezpieczeństwa wskazuje działania jakie należy podjąć w celu właściwego zabezpieczenia danych osobowych oraz określa zasady i normy postępowania, których w tym celu należy przestrzegać. Zgodnie z zapisami Polskiej Normy ISO/IEC 17799:2005, politykę bezpieczeństwa instytucji tworzy się w celu zapewnienia kierunków działania i wsparcia kadry kierowniczej w kwestiach związanych z bezpieczeństwem informacji. Dokument ten powinien bowiem wyznaczać podejście organizacji do zarządzania bezpieczeństwem informacji oraz stanowić wyraz zaangażowania kierownictwa w ten obszar funkcjonowania przedsiębiorstwa (Kaczmarek, 2009). Zgodnie z art. 36a. ust. 1 pkt 2 lit. b ustawy o ochronie danych osobowych, w sytuacji gdy administrator danych powołał administratora bezpieczeństwa informacji (ABI), to ten podmiot staje się odpowiedzialny za nadzorowanie opracowania i aktualizacji polityki bezpieczeństwa oraz przestrzegania określonych w niej zasad.

Dokument określający politykę bezpieczeństwa informacji powinien nie tylko uwzględniać wymagania wywodzące się z obowiązującego prawa oraz strategii biznesowej organizacji, ale również brać pod uwagę charakter zagrożeń występujących w środowisku przetwarzania danych. Administrator danych osobowych jest odpowiedzialny za dostosowanie treści polityki do zmian zachodzących w przepisach dotyczących ochrony danych oraz do polskich norm, ustanawiających wytyczne w dziedzinie zarządzania bezpieczeństwem teleinformatycznym. Powinien również monitorować strukturalne i organizacyjne zmiany zachodzące zarówno wewnątrz organizacji, jak i poza nią, ponieważ mogą one stać się przyczyną dezaktualizacji zasad określonych w polityce bezpieczeństwa. Podczas tworzenia polityki bezpieczeństwa należy postarać się by dokument ten nie był zbyt abstrakcyjny - zasady postępowania w nim określone powinny być uzasadnione i wyjaśnione, ponieważ wpływa to pozytywnie na poziom ich respektowania.

Fundamentalne elementy, które powinna zawierać polityka bezpieczeństwa, wskazuje § 4 rozporządzenia MSWiA z 29 kwietnia 2004 r.:

- wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszary przetwarzania danych osobowych;
- wykaz zbiorów danych osobowych wraz ze wskazaniem programów stosowanych do przetwarzania danych w ich zakresie;
- opis struktury zbiorów danych, wskazujący zawartość poszczególnych pól informacyjnych i ich wzajemnych powiązań;
- sposób przepływu danych pomiędzy poszczególnymi systemami;
- określenie środków technicznych i organizacyjnych, niezbędnych dla zapewnienia integralności i rozliczalności przetwarzanych danych (Dz. U. 2004, nr 100, poz. 1024.).

Polska Norma PN-ISO/IEC 17799:2005 wskazuje dodatkowe składniki, które powinien zawierać dokument określający politykę bezpieczeństwa instytucji. Wśród nich wymieniono takie elementy, jak:

- określenie mechanizmów umożliwiających współkorzystanie z informacji (mechanizmy specyfikacji zakresu dostępu do danych oraz uprawnień do ich przetwarzania);
- oświadczenie o intencjach kadry kierowniczej, zbieżnych z celami i zasadami bezpieczeństwa informacji w kontekście strategii i wymagań biznesowych;
- struktura wyznaczania celów stosowania zabezpieczeń z uwzględnieniem struktury szacowania i zarządzania ryzykiem;
- wyjaśnienie polityki bezpieczeństwa w zakresie: zgodności z prawem, wewnętrznymi regulacjami organizacji oraz wymogami wynikającymi z zawieranych umów; wymagań dotyczących kształcenia w dziedzinie zapewniania bezpieczeństwa; zarządzania ciągłością działania przedsiębiorstwa; konsekwencji naruszeń postanowień polityki bezpieczeństwa;
- definicje obowiązków pracowników w zakresie zarządzania bezpieczeństwem informacji, w tym także zgłaszanie incydentów związanych z naruszeniem tego bezpieczeństwa;
- odsyłacze do dokumentacji uzupełniającej politykę bezpieczeństwa (np. szczegółowych polityk i procedur odnoszących się do poszczególnych systemów informatycznych) (Bednarczyk, 2012).

Polityka bezpieczeństwa powinna zawierać w sobie szczegółową inwentaryzację posiadanych przez instytucję zasobów oraz ich charakterystykę. Element ten, opisujący realny stan posiadanych zasobów informacyjnych, w tym także przepływy danych pomiędzy poszczególnymi systemami informatycznymi oraz bazami danych, jest szczególnie ważny w kontekście oceny ryzyka, na jakie dane te mogą być narażone w procesie przetwarzania,

a także odgrywa istotną rolę przy wyborze adekwatnych środków bezpieczeństwa. Środki te powinny być dobrane tak, by zapewnić redukcję zidentyfikowanego ryzyka do akceptowalnego poziomu. Zadaniem administratora danych jest wybór konkretnych środków technicznych i organizacyjnych, przy czym jest on zobowiązany do zastosowania przynajmniej minimalnych środków bezpieczeństwa wskazanych w rozporządzeniu MSWiA z dn. 29 kwietnia 2004 r. Środki te zależne są od kategorii przetwarzanych danych oraz rodzaju potencjalnych zagrożeń. Przytoczone rozporządzenie wprowadza trzy poziomy bezpieczeństwa:

1. poziom podstawowy - w systemie nie są przetwarzane dane wrażliwe, zaś sam system nie jest połączony z publiczną siecią komunikacyjną;
2. poziom podwyższony - w systemie przetwarza się dane wrażliwe, ale system nie jest połączony z publiczną siecią komunikacyjną;
3. poziom wysoki - system jest połączony z publiczną siecią komunikacyjną, co naraża przetwarzane w nim dane na zagrożenia pochodzące z sieci zewnętrznej.

3. ADMINISTRATOR DANYCH OSOBOWYCH A ADMINISTRATOR BEZPIECZEŃSTWA INFORMACJI

Zgodnie z art. 36a ust. 1 u.o.d.o., administrator danych może powołać administratora bezpieczeństwa informacji (ABI). Podejmując decyzję o powołaniu ABI, administrator danych pozyskuje dla organizacji osobę, która ze względu na wiedzę w zakresie ochrony danych osobowych dba nie tylko o prawidłowe zabezpieczenie danych osobowych w przedsiębiorstwie, ale zapewnia również kompleksowe przestrzeganie przepisów o ochronie danych osobowych. Z tego też powodu powołanie administratora bezpieczeństwa informacji jest uzasadnione zarówno w przez administratorów danych przetwarzanych systemach informatycznych, ale również w organizacjach pracujących na tradycyjnych (zazwyczaj papierowych) zbiorach danych. Ogólny zakres obowiązków ABI został określony w art. 36a ust. 2 ustawy o ochronie danych osobowych jako:

1. zapewnianie przestrzegania przepisów o ochronie danych osobowych, w szczególności poprzez:
   - sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ich ochronie oraz opracowywanie w tym zakresie sprawozdania dla administratora danych;
   - nadzorowanie opracowania i aktualizacji dokumentacji opisującej sposób przetwarzania danych oraz przestrzegania zasad w niej określonych;
   - zapewnianie zapoznania osób upoważnionych do przetwarzania danych z przepisami o ich ochronie;

2. prowadzenie rejestru zbiorów danych przetwarzanych przez administratora, zawierającego następujące elementy: nazwę zbioru, oznaczenie administratora danych i adres jego siedziby, podstawę prawną upoważniającą do prowadzenia zbioru danych, informacje na temat powierzenia danych innemu podmiotowi, cel przetwarzania danych, zakres przetwarzanych danych, opis kategorii osób, których dane dotyczą, sposób pozyskiwania i udostępniania danych, informację o odbiorcach (lub kategoriach odbiorców), którym przetwarzane dane mogą być przekazywane, opis środków technicznych i organizacyjnych stosowanych w celu zabezpieczenia danych osobowych, informację o sposobie wypełnienia warunków technicznych i organizacyjnych którym powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych, a także informację dotyczącą ewentualnego przekazywania danych do państwa trzeciego (ustawa o ochronie danych osobowych, 1997).

Realizując zaprezentowany powyżej zakres obowiązków, ABI może przede wszystkim:

- kontrolować realizację przedsięwzięć określonych w art. 36 ust. 1 u.o.d.o. oraz przepisów wykonawczych wydanych na podstawie jej art. 39a;
- nadzorować i kontrolować stosowania środków technicznych oraz przedsięwzięć organizacyjnych zapewniających ochronę przetwarzanych danych, adekwatną do zagrożeń oraz kategorii tych danych, a także zabezpieczających dane przed utratą, nieuprawnioną zmianą, uszkodzeniem, zniszczeniem, przywłaszczeniem lub udostępnieniem osobom nieuprawnionym;
- nadzorować i kontrolować czynności związane z ochroną danych osobowych, tj.:
  - przebieg procesu nadawania upoważnień do przetwarzania danych osobowych oraz stosownych uprawnień w systemach informatycznych;
  - wykonywanie zadań w przedmiotowym zakresie przez użytkowników, przełożonych oraz administrujących zbiorami danych;
  - realizację zadań przez komórki organizacyjne zobligowane do zapewniania właściwych środków zabezpieczających dane osobowe;
  - prowadzenie wymaganej przez przepisy prawa dokumentacji dotyczącej przetwarzania danych osobowych;
  - stosowanie środków fizycznych związanych z ochroną danych, w szczególności zaś nadzorowanie adekwatności stosowanych zabezpieczeń do kategorii danych oraz możliwości wystąpienia zagrożeń;
- wykonywać inne zadania związane z ochroną danych osobowych, w szczególności:

- współuczestniczyć w rozpatrywaniu skarg i wniosków związanych z przetwarzaniem i ochroną danych w organizacji;
- występować do GIODO z wnioskiem o rejestrację zbiorów danych osobowych w prowadzonym przez niego rejestrze (z wyjątkiem zbiorów zwolnionych z obowiązku rejestracyjnego) oraz zgłaszać zmiany w zarejestrowanych zbiorach;
- koordynować czynności związanych z postępowaniami administracyjnymi prowadzonymi przez GIODO z udziałem administratora danych;
- inicjować zmiany w procesie przetwarzania danych osobowych w organizacji;
- sprawować nadzór nad wyjaśnianiem i dokumentowaniem incydentów naruszenia zasad bezpieczeństwa i ochrony danych osobowych w organizacji;
- organizować szkolenia z zakresu przetwarzania i ochrony danych osobowych;
- dokonywać oceny analiz zagrożeń bezpieczeństwa oraz ocen stanu ochrony danych osobowych przetwarzanych w organizacji.

Zgodnie z obowiązującymi przepisami, administrator bezpieczeństwa informacji musi podlegać bezpośrednio kierownikowi jednostki, zaś administrator danych osobowych jest zobowiązany do zapewnienia mu adekwatnych środków oraz organizacyjnej odrębności. Przedsięwzięcia te mają umożliwić ABI niezależność w realizacji powierzonych mu zadań, jednak mogą one oznaczać konieczność zmian w strukturze organizacyjnej przedsiębiorstwa, np. reorganizację dotychczasowego zakresu zadań pracownika wyznaczonego do realizowania funkcji ABI, utworzenie nowego etatu lub poniesienie kosztów związanych z wyznaczeniem zewnętrznego administratora, w ramach tzw. outsourcingu funkcji ABI (Zegarek, b.r.). Powołanie ABI jest jednocześnie równoważne z poszerzeniem kręgu osób mających dostęp do informacji o znaczeniu strategicznym dla organizacji, co zwiększa ryzyko wycieku tych informacji poza przedsiębiorstwo. Aby administrator bezpieczeństwa mógł prawidłowo realizować swoje zadania, musi bowiem posiadać wiedzę w zakresie procesów przetwarzania danych w organizacji, m.in. w zakresie umów zawieranych przez administratora danych.

Ustawowe obowiązki w zakresie ochrony danych osobowych muszą być przez organizację realizowane, niezależnie od tego, kto będzie odpowiedzialny za ich faktyczną realizację. Niepowoływanie administratora bezpieczeństwa informacji wydaje się być racjonalne jedynie w niewielkich, maksymalnie kilkunastoosobowych przedsiębiorstwach, gdzie zadania z zakresu ochrony danych mogą realizować ich właściciele. W przypadku większych organizacji ciężko jest wyobrazić sobie, by osoba fizyczna reprezentująca administratora danych (np. burmistrz miasta czy prezes przedsiębiorstwa) osobiście

wypełniała wszelkie zadania związane z ochroną danych, takie jak przygotowywanie zapisów polityki bezpieczeństwa organizacji, nadawanie upoważnień do przetwarzania danych czy prowadzenie szkoleń pracowników. Z perspektywy administratora danych, powołanie ABI pozwala w sposób efektywny rozdzielić obowiązki nałożone na pracowników oraz zapewnić właściwą delegację zadań w obszarze ochrony danych. Pozwala bowiem przenieść odpowiedzialność z tego zakresu ze wszystkich pracowników na osobę merytoryczną w tej kwestii, co przekłada się na skupienie uwagi pozostałych członków organizacji na swoich zadaniach. Funkcjonowanie administratora bezpieczeństwa informacji w ramach organizacji stanowi również dla jej otoczenia, zarówno wewnętrznego, jak i zewnętrznego, wyraźny sygnał, że przedsiębiorstwo poważnie podchodzi do kwestii ochrony danych, co pozytywnie wpływa na jej wizerunek.

Niewątpliwą zaletą powołania administratora bezpieczeństwa informacji jest również zwolnienie z obowiązku rejestracji w GIODO zbiorów niezawierających danych sensytywnych. ABI niejako przejmuje funkcje GIODO, ewidencjonując wskazane zbiory we własnym rejestrze wewnętrznym. Wyznaczenie ABI wskazuje się również jako czynnik mogący zminimalizować ryzyko skontrolowania administratora danych przez GIODO. W przypadku kontroli zgodności przetwarzania danych osobowych z obowiązującymi przepisami, Inspektorat w pierwszej kolejności wzywa do złożenia wyjaśnień, których w takiej sytuacji udziela ABI. Dodatkowo, od momentu nowelizacji u.o.d.o., ABI wpisany do rejestru może, na wniosek Inspektoratu, sam skontrolować poprawność procesu przetwarzania danych u administratora danych, u którego realizuje on swoje obowiązki. Kontrola prowadzona przez „własnego" administratora bezpieczeństwa informacji jest przez to mniej ryzykowna dla organizacji (Zegarek, b.r.). Należy pamiętać, że powołanie administratora bezpieczeństwa informacji jest uprawnieniem, a nie obowiązkiem administratora danych. W przypadku jego niepowołania, zakres jego obowiązków realizuje sam administrator, z wyłączeniem obowiązku prowadzenia wewnętrznego rejestru zbiorów danych przetwarzanych przez administratora oraz sporządzania sprawozdania z przeprowadzonej kontroli zgodności przetwarzania danych osobowych z zasadami, o których mowa w art. 23-27 oraz 31-35 u.o.d.o., z zasadami dotyczącymi zabezpieczenia danych osobowych, o których mowa w art. 36, art. 37-39 u.o.d.o. oraz w przepisach wykonawczych wydanych na podstawie art. 39a do ustawy (GIODO, b.r.). Administrator danych pozostaje odpowiedzialny za legalne i zgodne z przepisami prawa zorganizowanie procesu przetwarzania danych w organizacji.

PODSUMOWANIE

Reasumując, administrator danych osobowych odgrywa kluczową rolę w procesie budowy systemu zarządzania bezpieczeństwem informacji w organizacji. Oprócz realizacji obowiązków, które nakłada na niego ustawa o ochronie danych osobowych, jest również podmiotem ponoszącym w największym stopniu odpowiedzialność za realizację podstawowych elementów budowy systemu zarządzania bezpieczeństwem informacji w organizacji. Do jego obowiązków w tym zakresie należy przeprowadzenie analizy ryzyka bezpieczeństwa informacji, ustanowienie kluczowych dokumentów w zakresie ochrony danych (tj. polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym), wdrożenie i zapewnienie faktycznego stosowania środków bezpieczeństwa przyjętych w polityce, przeszkolenie pracowników w zakresie legalnego przetwarzania danych osobowych oraz zapewnienie odpowiednich, kontrolowanych relacji z podmiotami, którym powierzono przetwarzanie danych. Aby zapewnić kompleksową ochronę danych w organizacji, administrator danych może powołać administratora bezpieczeństwa informacji, który przejmuje odpowiedzialność związaną z prawidłowym zabezpieczeniem danych, a także zapewnia przestrzeganie przepisów o ochronie danych osobowych w przedsiębiorstwie. W sytuacji, gdy administrator danych nie zdecyduje się na powołanie administratora bezpieczeństwa informacji, pozostaje odpowiedzialny za legalne i zgodne z przepisami prawa zorganizowanie procesu przetwarzania danych w organizacji.

LITERATURA

Akty prawne:

1. 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. 2004, nr 100, poz. 1024.
2. Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych. Dz. U. 2012, poz. 526.
3. Ustawa z 29 sierpnia 1997 r. o ochronie danych osobowych. Dz. U. 2016, poz. 922.
4. Ustawa z dnia 24 maja 2000 r. o Krajowym Rejestrze Karnym. Dz. U. 2008, nr 50, poz. 292.

5. Zarządzenie nr 700/2015 Prezydenta m.st. Warszawy z dnia 27 maja 2015 r. w sprawie wyznaczenia administratora bezpieczeństwa informacji i jego zastępcy w Urzędzie m.st. Warszawy oraz określenia ich zadań. GP-OR.0050.700.2015.

Publikacje książkowe jednego autora:

1. Kaczmarek, A. (2009). *ABC zagrożeń bezpieczeństwa danych osobowych w systemach informatycznych*. Warszawa: Generalny Inspektor Ochrony Danych Osobowych.

Rozdziały w publikacjach książkowych zbiorowych:

1. Bednarczyk, A. (2012). *Publicznoprawne aspekty bezpieczeństwa danych osobowych w szkołach wyższych w Polsce*. W: W. Chmielowski, D. Wilk-Kołodziejczyk (red.), *Metody analizy i oceny bezpieczeństwa oraz jakości informacji*. Kraków: Oficyna Wydawnicza AFM.

Artykuły w czasopiśmie:

1. Byczkowski, M., Zawiła-Niedźwiedzki, J. (2014). Analiza ryzyka w zarządzaniu bezpieczeństwem danych osobowych. Zarządzanie ryzykiem w kontekście ochrony informacji. *Monitor Prawniczy*, nr 9, 45-49.
2. Serzycki M. (2010). Administrator danych - kto to taki? *Przegląd Komunalny,* nr 2(221), 52.

Raporty instytucji:

1. Polski Komitet Normalizacyjny. (2002). *Polska Norma PN-I-0200: Technika informatyczna. Zabezpieczenia w systemach informatycznych. Terminologia.* Warszawa: Polski Komitet Normalizacyjny.
2. Polski Komitet Normalizacyjny. (2005). *Polska Norma PN-I-07799-2:2005. Systemy zarządzania bezpieczeństwem informacji. Część 2: Specyfikacja i wytyczne do stosowania.* Warszawa: Polski Komitet Normalizacyjny.

Źródła internetowe:

1. Janus R. *Zarządzanie ryzykiem a bezpieczeństwo informacji – definicje*. http://itfocus.pl/dzial-it/bezpieczenstwo/zarzadzanie-ryzykiem-a-bezpieczenstwo-informacji-definicje/ (27.12.2016).
2. Generalny Inspektor Ochrony Danych Osobowych. *Czy powołanie administratora danych jest obowiązkowe?* http://www.giodo.gov.pl/1520223/id_art/8344/j/pl/ (10.05.2017).
3. Kaczmarek A. *Wytyczne w zakresie opracowania i wdrożenia polityki bezpieczeństwa*. www.giodo.gov.pl/plik/id_p/10212/j/pl/ (29.12.2016).
4. Piotrowski M. *Zarządzanie ryzykiem bezpieczeństwa informacji w systemach IT*.

http://www.computerworld.pl/news/318160/Zarzadzanie.ryzykiem.bezpieczenstwa.informacji.w.systemach.TI.html (27.12.2016).

5. Stróżyk I. *Zarządzanie ryzykiem w bezpieczeństwie informacji*. http://iso27000.pl/webroot/uploads/Zarzadzanie_ryzykiem_w_bezpieczeństwie_informacji.pdf (27.12.2016).
6. Zegarek P. Plusy i minusy powołania ABI (cz. III). http://blog-daneosobowe.pl/plusy-i-minusy-powolania-abi-cz-iii/ (16.05.2017).