Odpowiedzi na 30 najważniejszych pytań

o administratora bezpieczeństwa informacji

experto24.pl

Spis treści

Administrator bezpieczeństwa informacji (w skrócie ABI) jest kluczową postacią w procesie ochrony danych osobowych i powinien zostać odpowiednio usytuowany w strukturze organizacyjnej urzędu czy firmy. Jest to specjalista, który w danym podmiocie zajmuje się kwestiami ochrony danych osobowych.

Administratora bezpieczeństwa informacji powołuje administrator danych osobowych, czyli na przykład wójt (burmistrz, prezydent miasta). Zawsze jednak ABI powinien zostać tak uplasowany w strukturze organizacyjnej danego podmiotu, aby podlegał bezpośrednio kierownikowi tej jednostki. Regulując kwestie powołania ABI, należy zagwarantować, że administrator danych będzie decydował wyłączne o wyznaczeniu konkretnej osoby na to stanowisko.

Decyzja o powołaniu ABI należy do administratora danych osobowych. Jeżeli stwierdzi, że potrafi samodzielnie zapewnić prawidłowe przetwarzanie danych osobowych, to nie musi wyznaczać ABI.

Administrator bezpieczeństwa informacji może być zarówno pracownikiem, jak i zleceniobiorcą administratora danych osobowych. Bardzo często funkcję ABI powierza się, w ramach powiększonego zakresu obowiązków, pracownikowi działu IT lub działu prawnego. Właściwszy wybór to osoba z przygotowaniem prawnym/administracyjnym, wykształcenie informatyczne przyda się zaś bardziej administratorowi systemów informatycznych.

Kto może być administratorem bezpieczeństwa informacji?

Na administratora bezpieczeństwa informacji można wyznaczyć jedynie osobę fizyczną. Nie można więc wskazać w wewnętrznych aktach normatywnych, że funkcje ABI wykonuje jakaś jednostka organizacyjna lub zespół osób. Wynika to z faktu, że wykonywanie nadzoru nad przestrzeganiem zasad ochrony przetwarzania danych osobowych wymaga dostępu do tych danych.

Zgodnie zaś z art. 37 ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie od administratora danych. Naczelny Sąd Administracyjny w wyroku z 21 lutego 2014 r. (I OSK 2445/12) potwierdził, że chodzi tu o osoby fizyczne, odnotowane w ewidencji osób upoważnionych do przetwarzania danych.

Kandydat na administratora bezpieczeństwa informacji powinien mieć pełną zdolność do czynności prawnych oraz korzystać z pełni praw publicznych. Musi także posiadać odpowiednią wiedzę w zakresie ochrony danych osobowych oraz nie może być karany za umyślne przestępstwo.

Czy trzeba mieć ukończone szkolenie albo studia, żeby zostać ABI?

Tak naprawdę administrator bezpieczeństwa informacji nie musi się legitymować żadnym konkretnym poziomem ani kierunkiem wykształcenia. W zakresie wymogu przygotowania merytorycznego ustawa o ochronie danych osobowych przewiduje jedynie, że ABI powinien „posiadać odpowiednią wiedzę w zakresie ochrony danych osobowych". Przepisy nie precyzują, czy i jaki poziom wykształcenia gwarantuje taką „odpowiednią wiedzę". Nie mają też znaczenia certyfikaty, kursy czy szkolenia z dziedziny ochrony dany osobowych.

Ta „odpowiednia wiedza" powinna być weryfikowana przez administratora danych osobowych, ponieważ to ostatecznie on może zostać w wyniku kontroli obciążony przez Generalnego Inspektora Ochrony Danych Osobowych zarzutem naruszenia przepisów ustawy przez powołanie na stanowisko ABI osoby niespełniającej niezbędnych wymagań.

Wyznaczenie inspektora powinno się odbyć na podstawie kwalifikacji zawodowych. Chodzi tu o wiedzę fachową na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętność wypełnienia zadań inspektora. ABI zawsze powinien być specjalistą w zakresie ochrony danych osobowych, niezależnie czy i jak jest w stanie tego dowieść, powołując się na swoje wykształcenie.

Czy administrator bezpieczeństwa informacji może pełnić funkcje niezwiązane z ochroną danych osobowych?

Nie ma żadnych przeszkód formalnoprawnych, aby administrator bezpieczeństwa informacji łączył swoje obowiązki z innymi. W szczególności może być jednocześnie administratorem systemów informatycznych czy głównym informatykiem w firmie. Może być zatrudniony jako prawnik albo specjalista od ochrony informacji niejawnych. Takie łączenie obowiązków nie zawsze jednak musi się sprawdzić.

Zwłaszcza w rozbudowanych podmiotach o skomplikowanych zależnościach wewnętrznych i strukturze organizacyjnej obowiązków ABI wystarczy na pełne obciążenie całego etatu. Zlecanie dodatkowych zadań ABI może niekorzystnie odbić się na jakości jego pracy w zakresie obowiązków dotyczących ochrony danych osobowych, a to w konsekwencji przyniesie więcej strat niż korzyści z pozornych oszczędności.

Złotą zasadą jest unikanie nakładania takich dodatkowych obowiązków na administratora bezpieczeństwa informacji, które mogą powodować konflikt interesów. Chodzi tu np. o pokusę wykorzystywania danych osobowych, do których ma dostęp jako administrator, na cele związane z innymi funkcjami przez niego pełnionymi (np. kadrowymi).

Czy każdy podmiot jest zobowiązany do wyznaczenia administratora bezpieczeństwa informacji?

Obecnie nie ma obowiązku ustanowienia administratora bezpieczeństwa informacji. Decyzja o jego wyznaczeniu została więc oddana samemu administratorowi danych osobowych. Powinien on ocenić potrzebę powołania ABI w swojej organizacji, kierując się zakresem przetwarzanych danych osobowych, ich rodzajem oraz wymaganym poziomem ochrony przetwarzania tych danych.

Sytuacja zmieni się wskutek tzw. GDPR, czyli rozporządzenia Parlamentu Europejskiego i Rady 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. Będzie ono bezpośrednio stosowane w państwach członkowskich od 25 maja 2018 r. Od tej daty też ABI zostanie zastąpiony tzw. inspektorem ochrony danych, którego ustanowienie będzie obowiązkowe, gdy:

1) przetwarzania dokonują organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości,
2) główna działalność administratora polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę,
3) główna działalność administratora polega na przetwarzaniu na dużą skalę danych osobowych wrażliwych oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa.

Czy należy zgłosić administratora bezpieczeństwa informacji do rejestracji?

W obecnym stanie prawnym zgłoszenie administratora bezpieczeństwa informacji jest obowiązkowe. Oznacza to, że o ile samo powołanie ABI jest możliwością, ale nie obowiązkiem, o tyle gdy zostanie on

już powołany, to musi zostać zgłoszony do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych.

Taki sam obowiązek administratora danych osobowych powstaje w przypadku odwołania administratora bezpieczeństwa informacji. Natomiast nie ma żadnego obowiązku zgłaszania do rejestru faktu powołania lub odwołania przez administratora danych osobowych zastępcy administratora bezpieczeństwa informacji.

Po wejściu w życie rozporządzenia Parlamentu Europejskiego i Rady 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, tj. po 25 maja 2018 r., obowiązek rejestrowania ABI w krajowym organie nadzorczym (w Polsce jest nim GIODO) zostanie utrzymany.

W jaki sposób należy dokonać zgłoszenia ABI?

Obowiązek zgłoszenia ciąży na administratorze danych i obejmuje zarówno powołanie, jak i odwołanie administratora bezpieczeństwa informacji. Zgłoszenie powinno nastąpić w terminie 30 dni od dnia takiego powołania lub odwołania.

Zgłoszenie powołania administratora bezpieczeństwa informacji do rejestracji powinno zawierać:

1) oznaczenie administratora danych i adres jego siedziby lub miejsca zamieszkania, w tym numer identyfikacyjny rejestru podmiotów gospodarki narodowej, jeżeli został mu nadany;
2) dane administratora bezpieczeństwa informacji:
    a) imię i nazwisko,
    b) numer PESEL lub, gdy ten numer nie został nadany, nazwę i numer dokumentu stwierdzającego tożsamość,
    c) adres do korespondencji;
3) datę powołania;
4) oświadczenie administratora danych o spełnianiu przez administratora bezpieczeństwa informacji warunków jego ustanowienia (m.in. niekaralność).

Administrator danych osobowych powinien też zgłaszać do Generalnego Inspektora Ochrony Danych Osobowych wszelkie zmiany informacji objętych zgłoszeniem w terminie 14 dni od dnia zmiany.

Generalny inspektor wydaje też zaświadczenia o zarejestrowaniu administratora bezpieczeństwa informacji – na żądanie ABI lub ADO.

Gdzie znajduje się rejestr administratorów bezpieczeństwa informacji?

Rejestr administratorów bezpieczeństwa informacji jest prowadzony przez Generalnego Inspektora Ochrony Danych Osobowych. Od 26 stycznia 2015 r. został uruchomiony system informatyczny zapewniający publiczny dostęp do rejestru administratorów bezpieczeństwa informacji.
Dostęp do rejestru jest zapewniany z wykorzystaniem elektronicznej platformy komunikacji z Generalnym Inspektorem Ochrony Danych Osobowych, tzw. e-GIODO. Strona e-GIODO jest dostępna pod adresem: http://egiodo.giodo.gov.pl. Platforma nie tylko zapewnia dostęp do informacji zawartych w rejestrze ABI, ale także pozwala na przesyłanie drogą elektroniczną wniosków do Generalnego Inspektora Ochrony Danych Osobowych o wpis lub aktualizację zawartych w nich informacji.

Aby skorzystać z interaktywnych funkcjonalności platformy (tj. składania wniosków), konieczna jest uprzednia rejestracja konta pod adresem https://konto.biznes.gov.pl/rejestracja. Od pewnego czasu zostało jednak także umożliwione składanie wniosków o wpis, aktualizację lub wykreślenie ABI drogą elektroniczną z wykorzystaniem platformy ePUAP. Wówczas wystarcza posiadanie konta w ePUAP.

Czy można powołać zastępców ABI?

Zgodnie z art. 36a ust. 6 ustawy o ochronie danych osobowych administrator danych może powołać zastępców administratora bezpieczeństwa informacji. Może to być jedna lub kilka osób. Osoby te, podobnie jak ABI, muszą spełniać następujące kryteria określone w art. 36a ust. 5 uodo:

- mieć pełną zdolność do czynności prawnych oraz korzystać z pełni praw publicznych,
- posiadać odpowiednią wiedzę,
- nie być karane za umyślne przestępstwo.

Zastępcy ABI mają zastępować go podczas jego nieobecności w realizacji następujących obowiązków:

- przeprowadzania sprawdzenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowywania w tym zakresie sprawozdania,
- nadzorowania opracowania i aktualizowania dokumentacji, o której mowa w art. 36 ust. 2 uodo, oraz przestrzeganiu zasad w niej określonych,
- zapewniania zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych,
- prowadzenia rejestru zbiorów danych.

Nie ma w ustawie zapisanych innych wymogów, które wprost odnoszą się do zastępców ABI. Ich powołania nie trzeba zgłaszać do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych. Nie będzie mógł on też zlecać sprawdzenia w trybie art. 19b uodo zastępcom ABI.

Kto może być zastępcą ABI?

Decyzja o tym, kogo należy powołać na zastępców ABI, zależy wyłącznie od administratora danych. Może być to pracownik zatrudniony na innym stanowisku, który w razie konieczności przejmie wykonywanie obowiązków powołanego administratora bezpieczeństwa informacji.

Można również wyznaczyć na zastępców kilka osób, które będą zastępować ABI przy wykonywaniu konkretnych zadań określonych w art. 36a ust. 2 uodo. Jeden zastępca będzie np. wykonywał sprawdzenia (jeżeli ich termin został zaplanowany lub w sytuacji wystąpienia incydentu związanego z naruszeniem bezpieczeństwa danych), inny będzie sprawował nadzór nad dokumentacją przetwarzania danych, a jeszcze inny zapewniał zapoznanie osób upoważnionych z przepisami itp. W takim wypadku należy ustalić konkretny zakres zadań dla takich osób.

Jakie zadania ma administrator bezpieczeństwa informacji?

Do 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 opisującej środki przetwarzania danych 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 osobowych, z wyjątkiem zbiorów, z obowiązku rejestracji których ADO są zwolnieni; przy czym taki rejestr zbiorów danych przetwarzanych przez administratora danych osobowych, a prowadzony przez administratora bezpieczeństwa informacji jest jawny.

Obowiązek dokonywania sprawdzeń, o których mowa w pkt 1 dotyczy dwóch rodzajów sprawdzeń prowadzonych:

1) na zlecenie Generalnego Inspektora Ochrony Danych Osobowych, który wskazuje zakres i termin sprawdzenia, a administrator bezpieczeństwa informacji dokonuje sprawdzenia zgodnie z wytycznymi GIODO, po czym za pośrednictwem administratora danych przekazuje do tego organu sprawozdanie z przeprowadzonych czynności,
2) z inicjatywy samego administratora bezpieczeństwa informacji – może to być sprawdzenie planowane, ale także i doraźne (np. w wyniku zaistnienia incydentów naruszenia bezpieczeństwa ochrony danych osobowych); sprawozdania z tych sprawdzeń ABI przekazuje tylko do swojego administratora danych osobowych.

Czym jest plan sprawdzeń?

Jednym z rodzajów sprawdzeń, jakie administrator bezpieczeństwa informacji wykonuje dla administratora danych osobowych, jest sprawdzenie okresowe. Nie jest ono dokonywane w wyniku jakiegoś zaistniałego incydentu, ale na potrzeby okresowej weryfikacji poziomu ochrony danych osobowych w organizacji.

Dokonywanie takich sprawdzeń wynika z uprzedniego planu sprawdzeń przygotowanego przez administratora bezpieczeństwa informacji i przedstawionego administratorowi danych osobowych. Plan sprawdzeń określa przedmiot, zakres oraz termin przeprowadzenia poszczególnych sprawdzeń oraz sposób i zakres ich dokumentowania. Plan powinien obejmować okres nie krótszy niż kwartał i nie dłuższy niż rok. Po sporządzeniu planu przez ABI jego przedstawienie ADO następuje nie później niż na dwa tygodnie przed dniem rozpoczęcia okresu objętego planem. Każdy plan sprawdzeń obejmuje co najmniej jedno sprawdzenie.

Zbiory danych oraz systemy informatyczne służące do przetwarzania lub zabezpieczania danych osobowych powinny być objęte sprawdzeniem co najmniej raz na pięć lat.

Jak powinno wyglądać sprawdzenie planowe?

Administrator bezpieczeństwa informacji, którego obowiązkiem jest zapewnienie przestrzegania zasad ochrony danych osobowych, realizuje to zadanie m.in. przez wykonywanie sprawdzenia na podstawie planu.

Sprawdzenie planowe musi być przeprowadzone zgodnie z ustalonym wcześniej planem sprawdzeń, określającym termin, przedmiot i zakres każdego sprawdzenia objętego planem. Przed rozpoczęciem samego sprawdzenia warto sporządzić jego program, który będzie stanowił rozkład poszczególnych czynności dokonywanych w ramach sprawdzenia. Dzięki temu ABI będzie miał pewność, że wykonując wszystkie czynności wyszczególnione w programie, zdobędzie informacje pozwalające na

sporządzenie wyczerpującego sprawozdania dla ADO. Jest to jakby plan, ale dla konkretnego sprawdzenia.

ABI ma obowiązek zawiadomić kierownika jednostki organizacyjnej objętej sprawdzeniem o zakresie planowanych czynności w terminie co najmniej 7 dni przed dniem przeprowadzenia czynności. W czynnościach sprawdzenia ma prawo brać udział osoba odpowiedzialna za przetwarzanie danych osobowych, której dotyczy sprawdzenie. Ma ona także obowiązek umożliwienia ABI przeprowadzenie czynności w toku sprawdzenia (np. otwierania pomieszczeń, udostępniania danych uwierzytelniających w systemach informatycznych).

Jak często trzeba wykonywać sprawdzenie planowe?

Częstotliwość sprawdzeń planowych określa sam plan sprawdzeń. To na etapie ustalania planu ABI decyduje o tym, jaki aspekt przetwarzania danych osobowych będzie sprawdzany i czy tylko jeden raz w planowanym okresie, czy też częściej. To w planie też określone są jednostki organizacyjne w danym podmiocie podlegające sprawdzeniu.

Planując częstotliwość sprawdzeń, trzeba pamiętać o dwóch wymogach prawa:

1) zbiory danych oraz systemy informatyczne służące do przetwarzania lub zabezpieczania danych osobowych powinny być objęte sprawdzeniem co najmniej raz na pięć lat,
2) plan powinien obejmować okres nie krótszy niż kwartał i nie dłuższy niż rok.

Pracując nad sporządzeniem nowego planu, należy więc przeanalizować w pierwszym rzędzie, jakie zbiory danych oraz systemy nie były sprawdzane w ostatnich kilku latach i powinny być sprawdzone w najbliższym planowanym okresie. Administrator bezpieczeństwa informacji może naturalnie częściej dokonywać sprawdzenia konkretnych zbiorów danych lub systemów, jeżeli uzna je za newralgiczne dla funkcjonowania ochrony danych osobowych w danym podmiocie.

W jakich sytuacjach należy przeprowadzić sprawdzenie doraźne?

Sprawdzenia doraźne powinny być dokonywane przez administratora bezpieczeństwa informacji w przypadku nieprzewidzianym w planie sprawdzeń. Należy je przeprowadzić, w sytuacji gdy administrator bezpieczeństwa informacji dowie się o naruszeniu ochrony danych osobowych lub będzie miał uzasadnione podejrzenie, że takie naruszenie wystąpiło.

Sprawdzenie doraźne jest przeprowadzane niezwłocznie po tym, jak administrator bezpieczeństwa informacji dowie się o naruszeniu ochrony danych osobowych lub pojawi się uzasadnione podejrzenie takiego naruszenia. Administrator bezpieczeństwa informacji powinien zawiadomić:

1) administratora danych osobowych – o rozpoczęciu sprawdzenia doraźnego przed podjęciem pierwszej czynności w toku sprawdzenia,
2) kierownika jednostki organizacyjnej objętej sprawdzeniem – o zakresie planowanych czynności w terminie co najmniej 7 dni przed dniem przeprowadzenia czynności, chyba że niezwłoczne rozpoczęcie sprawdzenia jest niezbędne do przywrócenia stanu zgodnego z prawem lub weryfikacji, czy naruszenie nastąpiło.

Czy należy przygotować sprawozdanie ze sprawdzeń?

Administrator bezpieczeństwa informacji powinien sporządzić sprawozdanie po każdym ze sprawdzeń, niezależnie od jego rodzaju. Z tego powodu w toku sprawdzenia ABI powinien dokumentować czynności sprawdzające przeprowadzane w toku sprawdzenia, w zakresie niezbędnym nie tylko do oceny zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych, ale i w zakresie potrzebnym do opracowania sprawozdania.

Sprawozdanie jest sporządzane w postaci elektronicznej albo w postaci papierowej. Administrator bezpieczeństwa informacji powinien przekazać administratorowi danych sprawozdanie:

1) ze sprawdzenia planowego – nie później niż w terminie 30 dni od zakończenia sprawdzenia,
2) ze sprawdzenia doraźnego – niezwłocznie po zakończeniu sprawdzenia,
3) ze sprawdzenia, o którego dokonanie zwrócił się Generalny Inspektor Ochrony Danych Osobowych – zachowując termin wskazany przez GIODO.

W sprawozdaniu administrator bezpieczeństwa informacji może też zawrzeć zawiadomienie dla administratora danych o osobach odpowiedzialnych za naruszenie zasad określonych w dokumentacji przetwarzania danych oraz o zakresie tego naruszenia.

Czy ABI musi szkolić pracowników z zasad ochrony danych osobowych?

Jeszcze nie tak dawno administrator bezpieczeństwa informacji nie miał obowiązku szkolenia pracowników z zasad ochrony danych osobowych. Obecnie ustawa wyraźnie wskazuje, że do jego

zadań należy m.in. „zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych”.
Trudno mówić o zachowaniu wymaganego prawem poziomu ochrony danych osobowych bez zapewnienia pewnego poziomu świadomości zasad ochrony tych danych wśród pracowników. Chodzi także o możliwość pociągnięcia pracownika do odpowiedzialności w razie naruszenia zasad ochrony danych osobowych – bez uprzedniego przeszkolenia go może on posłużyć się zarzutem, iż pracodawca nie poinformował go o aktualnie obowiązujących regulacjach (w tym wewnętrznych).

Pisząc o pracownikach, mamy na myśli zarówno pracowników podległych ABI, jak i wszystkich innych pracowników danej organizacji, uczestniczących w przetwarzaniu danych osobowych.

Jak często powinno odbywać się takie szkolenie?

Szkolenia powinny być organizowane cyklicznie, gdyż ewoluują nie tylko same przepisy prawne (vide nowe rozporządzenie ogólne o ochronie danych osobowych obowiązujące od 2018 roku), ale i rzeczywistość wokół nas (np. przetwarzanie danych w chmurze, geotagowanie). Z tego też powodu w swoim obowiązku szkoleniowym administrator bezpieczeństwa informacji nie powinien ograniczać się do przedstawienia samych tylko przepisów.

Warte rozważenia jest wprowadzenie przez administratora bezpieczeństwa informacji planu szkoleń. Taki np. roczny plan szkoleń precyzowałby, jakie jednostki organizacyjne w danym podmiocie wymagają przeprowadzenia szkolenia z zakresu ochrony danych osobowych i w jakim terminie takie szkolenie byłoby możliwe.

Pozwoli to także na dostosowanie treści konkretnego szkolenia do zakresu niezbędnego w zwyczajnym toku pracy danej jednostki. Specjalizacja wkracza bowiem także w świat ochrony danych osobowych i np. pracownikowi sprzedaży będą bardziej potrzebne informacje dotyczące tworzenia bazy danych klientów, a pracownikowi marketingu zakres, w jakim może wykorzystywać przetwarzane dane osobowe na tzw. marketing usług własnych.

Na czym polega obowiązek nadzorowania tworzenia i aktualizowania dokumentacji ochrony danych osobowych?

Jednym z zadań administratora bezpieczeństwa informacji jest nadzorowanie opracowania i aktualizowania dokumentacji opisującej sposób przetwarzania danych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną.

W zakresie nadzorowania opracowania oznacza to obowiązek ABI samodzielnego stworzenia dokumentacji albo też sprawowania kontroli nad podmiotem zewnętrznym, który tę dokumentację przygotowuje. Dlatego w umowie zlecającej stworzenie dokumentacji warto wskazać administratora bezpieczeństwa informacji jako osobę do bieżącego kontaktu, zgłaszania uwag i podpisania protokołu odbioru.

Z kolei obowiązek aktualizacji wymusza na ABI okresowe przeglądy dokumentacji. Chodzi tu o zwracanie uwagi na zmiany otoczenia prawnego w zakresie ochrony danych osobowych i związaną z tym konieczność dostosowania dokumentacji do nowych zasad prawnych. Administrator bezpieczeństwa informacji powinien w tym celu wykorzystywać także swoją wiedzę dotyczącą rzeczywistego stanu procesów przetwarzania danych osobowych pozyskaną np. ze sprawdzeń.

Czy ABI upoważnia do przetwarzania danych osobowych i prowadzi ewidencję osób upoważnionych?

Nadawanie upoważnień do przetwarzania danych osobowych zgodnie art. 37 ustawy o ochronie danych osobowych jest obowiązkiem administratora danych osobowych. Artykuł 39 ustawy wskazuje zaś, że to administrator danych osobowych prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych. Wśród zadań administratora bezpieczeństwa informacji nie ma obowiązku nadawania upoważnień do przetwarzania danych osobowych ani prowadzenia ewidencji. Nie jest to więc zadanie ABI wynikające z ustawy.

Administrator danych osobowych może jednak powierzyć administratorowi bezpieczeństwa informacji (na podstawie art. 36a ust. 4 ustawy o ochronie danych osobowych) obowiązek nadawania upoważnień do przetwarzania danych osobowych i prowadzenia ewidencji osób upoważnionych. Można to zrobić za pomocą odrębnego dokumentu albo wpisując te zadania w zakresie obowiązków ABI zawartym w akcie jego powołania.

W niektórych organizacjach kwestią nadawania upoważnień do przetwarzania danych zajmuje się dział kadr – upoważnienia nadaje szef działu kadr, wyznaczony pracownik działu kadr prowadzi ewidencję osób upoważnionych, a ABI nadzoruje wykonywanie tych obowiązków.

Czy ABI powinien prowadzić rejestr zbiorów danych osobowych?

Co do zasady administrator danych jest obowiązany zgłosić zbiór danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych. Jest jednak zwolniony z obowiązku rejestracji zbiorów danych osobowych, z wyjątkiem zbiorów zawierających dane wrażliwe, jeżeli powołał administratora bezpieczeństwa informacji i zgłosił go Generalnemu Inspektorowi Ochrony Danych Osobowych do rejestracji.

Nie oznacza to jednak, że powołanie administratora bezpieczeństwa informacji w ogóle pozbawia konieczności prowadzenia rejestru zbiorów danych osobowych. Administrator bezpieczeństwa informacji prowadzi bowiem lokalny rejestr zbiorów danych osobowych w celu zapewnienia transparentności działań danego ADO w zakresie przetwarzania danych osobowych. Rejestr lokalny umożliwia zapanowanie nad rodzajami danych osobowych przetwarzanych w danym podmiocie i na szybkie pozyskanie takich informacji, jak sam fakt przetwarzania przez ADO danych określonego rodzaju albo czy dane osobowe konkretnej osoby są przetwarzane i w jakiego rodzaju zbiorach. Skuteczna ochrona danych osobowych jest niemożliwa bez zidentyfikowania i zarejestrowania zasobów, w jakich te dane są przetwarzane.

Jak powinien wyglądać rejestr zbiorów danych osobowych prowadzony przez ABI?

W lokalnym rejestrze zbiorów danych osobowych należy zawrzeć wszelkie zbiory danych osobowych (w tym ich części i podzbiory, jeśli ze względów technicznych dany zbiór został podzielony) przetwarzanych przez administratora danych osobowych. W polityce bezpieczeństwa administrator bezpieczeństwa informacji powinien zamieścić wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych. W dokumencie tym powinien zostać także określony opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi.

Prawidłowo prowadzony rejestr powinien zawierać:

1) nazwę zbioru danych,
2) oznaczenie administratora danych i adres jego siedziby lub miejsca zamieszkania oraz numer identyfikacyjny rejestru podmiotów gospodarki narodowej, jeżeli został mu nadany,
3) oznaczenie przedstawiciela ADO i adres jego siedziby lub miejsca zamieszkania – w przypadku wyznaczenia takiego podmiotu,

4) oznaczenie podmiotu, któremu powierzono przetwarzanie danych ze zbioru i adres jego siedziby lub miejsca zamieszkania – w przypadku powierzenia przetwarzania danych temu podmiotowi,
5) podstawę prawną upoważniającą do prowadzenia zbioru danych,
6) cel przetwarzania danych w zbiorze,
7) opis kategorii osób, których dane są przetwarzane w zbiorze,
8) zakres danych przetwarzanych w zbiorze,
9) sposób zbierania danych do zbioru, w szczególności informację, czy dane do zbioru są zbierane od osób, których dotyczą, czy z innych źródeł niż osoba, której dane dotyczą,
10) sposób udostępniania danych ze zbioru, w szczególności informację, czy dane ze zbioru są udostępniane innym podmiotom niż upoważnione na podstawie przepisów prawa,
11) oznaczenie odbiorcy danych lub kategorii odbiorców, którym dane mogą być przekazywane,
12) informację dotyczącą ewentualnego przekazywania danych do państwa trzeciego.

Jak wygląda zgłaszanie zbiorów danych osobowych, gdy administrator danych nie powoła ABI?

Ustawodawca postanowił zmobilizować administratorów danych do ustanawiania administratorów bezpieczeństwa informacji i w tym celu ustanowił swoistą zachętę. Jeżeli dany administrator danych powoła administratora bezpieczeństwa informacji, to ten administrator danych nie podlega już obowiązkowi rejestracji zbiorów danych osobowych.

Jest jednak pewien wyjątek. Obowiązkowi rejestracji u Generalnego Inspektora Ochrony Danych Osobowych podlegają nadal zbiory danych wrażliwych, tj. danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

Należy też pamiętać, że na administratorze bezpieczeństwa informacji spoczywa wówczas obowiązek utworzenia i aktualizowania tzw. lokalnego rejestru zbiorów danych osobowych.

Co się stanie, jeśli administrator danych nie zgłosi administratora bezpieczeństwa informacji do rejestracji GIODO?

Dnia 1 stycznia 2015 r. weszła w życie nowelizacja ustawy o ochronie danych osobowych, która nakazywała tym administratorom danych osobowych, którzy mieli do tej pory powołanego administratora bezpieczeństwa informacji, zdecydować się do 30 czerwca 2015 r., czy nadal będą posiadali ABI w swojej organizacji.

Jeżeli administrator danych osobowych nic by nie zrobił do tego czasu, to z mocy prawa dotychczasowy ABI przestawał nim być. Aby zachować „starego" administratora bezpieczeństwa informacji, ADO powinien był go zgłosić do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych. Można więc uznać, że za tamto niezgłoszenie nie było żadnej sankcji z wyjątkiem wygaśnięcia pełnienia funkcji przez starego ABI.

Obecnie zaś administrator danych jest obowiązany zgłosić do rejestracji GIODO powołanie i odwołanie administratora bezpieczeństwa informacji w terminie 30 dni od dnia jego powołania lub odwołania. Zgłoszenie powołania administratora bezpieczeństwa informacji do rejestracji GIODO oraz zgłoszenie odwołania ABI dokonuje się z użyciem specjalnego wzoru zgłoszenia powołania i odwołania ABI. Także w tym przypadku brak jest wyraźnie zarysowanej sankcji. Należy stwierdzić, że niezarejestrowanie administratora bezpieczeństwa informacji prowadzi do sytuacji, w której u danego administratora danych osobowych w ogóle nie ma ABI (nie istnieje coś takiego jak ABI niezarejestrowany w GIODO), ze wszystkimi tego konsekwencjami. Podstawową z tych konsekwencji jest zaś obowiązek zarejestrowania w rejestrze Generalnego Inspektora Ochrony Danych Osobowych zbiorów danych osobowych przetwarzanych u danego ADO.

Czy jeśli ADO nie zgłosi ABI do GIODO, sam prowadzi sprawdzenia?

Jeśli administrator danych osobowych nie powoła administratora bezpieczeństwa informacji, sam musi realizować jego obowiązki wynikające z ustawy o ochronie danych osobowych. Wyjątek stanowi:

- prowadzenie jawnego rejestru zbiorów danych osobowych,
- przeprowadzenie sprawdzenia zgodności przetwarzania danych osobowych z przepisami oraz
- przygotowanie sprawozdania z takiego sprawdzenia.

Dodatkowo administrator danych, który nie powoła ABI, nie zostanie wezwany przez Generalnego Inspektora Ochrony Danych Osobowych do przeprowadzenia sprawdzenia i złożenia z niego sprawozdania.

Ustawa nie daje administratorowi danych osobowych wskazówek, co powinien robić w przypadku niewyznaczenia administratora bezpieczeństwa informacji. Część z podmiotów, które nie posiadają administratora bezpieczeństwa informacji, decyduje się, aby jego obowiązki przypisać jednemu z pracowników.

Taka osoba, która nie jest administratorem bezpieczeństwa informacji w rozumieniu ustawy o ochronie danych osobowych, jest odpowiedzialna umownie za ochronę danych osobowych i wykonuje obowiązki ABI, zgodnie z zawartą umową i przepisami w tym zakresie.

W praktyce taka osoba planuje i na podstawie planu przeprowadza sprawdzenie zgodności przetwarzania danych osobowych z przepisami. Celem tak dokonanego sprawdzenia jest kontrola legalności przetwarzania danych osobowych. Administrator danych osobowych może w ten sposób zobaczyć, jakie ewentualne zagrożenia i ryzyko występują w jego podmiocie.

Jeśli ABI nie jest powołany, ADO sam szkoli pracowników z ochrony danych?

Administrator ochrony danych nie musi wyznaczać administratora bezpieczeństwa informacji. Ustanowienie ABI jest bowiem fakultatywne. Nie oznacza to jednak, że obowiązki, które normalnie ciążyłyby na ABI, w przypadku jego nieustanowienia nie obciążają nikogo. Ustanowienie administratora bezpieczeństwa informacji ma bowiem na celu jedynie odciążenie administratora danych osobowych od części jego zadań, które ustawa pozwala scedować na ABI.

Wśród tych zadań, które normalnie są przypisane ABI, znajduje się m.in. „zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych". W przypadku braku administratora bezpieczeństwa informacji w danej organizacji, to na administratorze danych ciąży obowiązek dbania o właściwy poziom merytoryczny pracowników, pozwalający przetwarzać dane osobowe z poszanowaniem zasad ich ochrony.

Czy jeśli ABI nie jest powołany, ADO sam nadzoruje opracowanie i aktualizowanie dokumentacji?

Podobnie jak w przypadku innych obowiązków administratora bezpieczeństwa informacji, w przypadku nieustanowienia administratora bezpieczeństwa informacji w danym podmiocie, jego obowiązki wykonuje administrator danych osobowych.

Dotyczy to także nadzorowania opracowania i aktualizowania dokumentacji opisującej sposób przetwarzania danych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną. Ponadto w przypadku niepowołania administratora bezpieczeństwa informacji to administrator danych osobowych musi np. sprawdzać zgodność przetwarzania danych osobowych z przepisami o ochronie danych, czyli przeprowadzać wewnętrzne kontrole w organizacji.

Nawet wówczas administrator danych może jednak powierzyć wykonywanie części swoich zadań określonej osobie (pracownikowi), bez powoływania go na ABI. Niesie to z sobą jednak tą wadę, że administrator danych ponosi w pewnym sensie koszty zatrudniania pracownika zajmującego się (wyłącznie lub pobocznie) ochroną danych osobowych, a nadal nie posiada ABI, pozostając z obowiązkiem rejestracji zbiorów danych osobowych.

Czy można odwołać administratora bezpieczeństwa informacji?

To administrator danych osobowych powołuje i odwołuje administratora bezpieczeństwa informacji oraz jego zastępców. Administrator bezpieczeństwa informacji podlega bezpośrednio kierownikowi jednostki organizacyjnej lub osobie fizycznej będącej administratorem danych. Mamy więc bezpośrednią podległość ABI wobec ADO.

Administrator danych osobowych jest obowiązany zgłosić do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych odwołanie administratora bezpieczeństwa informacji w terminie 30 dni od dnia tego odwołania. Zgłoszenie odwołania, poza danymi przesyłanymi do GIODO przy powołaniu, powinno także wskazywać na datę i przyczynę odwołania. Jeżeli administrator danych jednocześnie rozwiązuje z administratorem bezpieczeństwa informacji umowę o pracę, wskazując w wypowiedzeniu przyczynę tego rozwiązania, warto zadbać o to, aby przyczyna odwołania była spójna z przyczyną rozwiązania umowy o pracę.

Nie chodzi tu tyle o skuteczność zgłoszenia odwołania do Generalnego Inspektora Ochrony Danych Osobowych, co przede wszystkim o niedawanie byłemu pracownikowi argumentów dotyczących samej przyczyny zwolnienia z pracy (np. pozorności tej przyczyny).

Jak będzie wyglądała pozycja administratora bezpieczeństwa w ogólnym rozporządzeniu o ochronie danych osobowych?

W ogólnym rozporządzeniu o ochronie danych osobowych próżno szukać określenia „administrator bezpieczeństwa informacji". Zamiast tego w systemie ochrony danych osobowych pojawi się tzw. inspektor ochrony danych. Przejmie on prawa i obowiązki ABI.
Administrator danych powinien:

- zapewnić, aby inspektor był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych,
- wspierać inspektora w wypełnianiu przez niego jego zadań, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej,
- zagwarantować, aby inspektor nie otrzymywał instrukcji dotyczących wykonywania jego zadań.

Administrator nie może odwołać ani ukarać inspektora za wykonywanie przez niego zadań, ale tylko tak długo, jak długo inspektor działa w granicach i na podstawie rozporządzenia. Inspektor powinien być usytuowany w strukturze firmy lub urzędu bezpośrednio pod zarządzającym tą jednostką. Administrator nie może także zabronić osobom, których dane dotyczą, kontaktu bezpośrednio z inspektorem we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących tym osobom. Nie ogranicza to jednak prawa administratora do zlecania inspektorowi także innych zadań i obowiązków, jeżeli tylko nie powodują konfliktu interesów. Inspektor powinien zachować w tajemnicy informacje uzyskiwane w toku wykonywania swoich zadań.

Czy powołanie inspektora ochrony danych będzie obowiązkowe?

Administrator danych osobowych, zgodnie z przepisami rozporządzenia, będzie miał obowiązek wyznaczyć inspektora ochrony danych, gdy:

- przetwarzanie prowadzi organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości,
- główna działalność administratora polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę,
- główna działalność administratora polega na przetwarzaniu na dużą skalę danych osobowych wrażliwych oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa.

Czy RODO wprowadzi nowe obowiązki dla ABI?

Do zadań inspektora ochrony danych (obecnego ABI) będzie należało:

1) informowanie administratora oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy rozporządzenia oraz innych przepisów o ochronie danych obowiązujących w Unii lub w państwach członkowskich i doradzanie im w tej sprawie,
2) monitorowanie przestrzegania przepisów o ochronie danych oraz polityk administratora, 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 (chodzi o Generalnego Inspektora Ochrony Danych Osobowych),
5) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem danych osobowych.

Zadania te powinny być wypełniane z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania. Zadania inspektora muszą być także określone w wiążących regułach korporacyjnych, jeżeli w danej organizacji zostaną przyjęte.

Autor:
Marcin Sarna

Stopka redakcyjna

Redaktor:	Wioleta Szczygielska
ISBN:	978-83-269-5592-1
E-book nr:	2HH0501
Wydawnictwo:	Wydawnictwo Wiedza i Praktyka sp. z o.o.
Adres:	03-918 Warszawa, ul. Łotewska 9a
Kontakt:	Telefon 22 518 29 29, faks 22 617 60 10, e-mail: *cok@wip.pl*
NIP:	526-19-92-256
Numer KRS:	0000098264 – Sąd Rejonowy dla m.st. Warszawy, Sąd Gospodarczy XIII Wydział Gospodarczy Rejestrowy. Wysokość kapitału zakładowego: 200.000 zł