OBOWIĄZKI I UPRAWNIENIA ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI (ABI)

1. Zasady ochrony danych osobowych str. 1
2. Kto może zostać powołany na stanowisko ABI? str. 2
3. Sprawozdania przygotowywane przez ABI str. 2
4. Rejestr zbiorów przetwarzanych danych prowadzony przez ABI str. 3
5. Kto przejmuje obowiązki ABI po jego odwołaniu? str. 3
6. Obcokrajowiec na stanowisku ABI str. 3
7. Podległość ABI w spółce str. 3
8. ABI w spółce komandytowej str. 4
9. Zmiana na stanowisku ABI str. 4
10. Przekazanie obowiązków ABI str. 4
11. Czy stowarzyszenie musi powołać swojego ABI? str. 4
12. Jeden ABI dla kilku firm str. 4

1. Zasady ochrony danych osobowych

Zasady przetwarzania danych osobowych przez podmioty prywatne i publiczne oraz ochronę jaką należy tym danym zapewnić określa ustawa o ochronie danych osobowych i wydane na jej podstawie przepisy wykonawcze.

Odpowiedzialność w zakresie ochrony przetwarzanych danych osobowych ponosi administrator danych (ADO). Administratorem w sferze niepublicznej jest, co do zasady, podmiot (np. spółka prawa handlowego, spółdzielnia, przedsiębiorca prowadzący jednoosobowo działalność gospodarczą, stowarzyszenie, fundacja). Administratorem danych nie jest więc osoba lub osoby zarządzające tym podmiotem (np. dyrektor przedsiębiorstwa, prezes spółdzielni, zarząd spółki) lub też pracownik wykonujący czynności związane z ochroną danych osobowych (np. pełnomocnik zarządu ds. ochrony danych osobowych, administrator bezpieczeństwa informacji). GIODO wielokrotnie zwracał uwagę, że administratorem danych przetwarzanych w jednostce organizacyjnej osoby prawnej (np. oddziale spółki) jest, co do zasady, dana osoba prawna, a nie jej jednostka organizacyjna (oddział spółki).

Przetwarzaniem danych są wszelkie operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych. Dane osobowe mogą być przetwarzane w kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych, a także w systemach informatycznych, również w przypadku przetwarzania danych poza zbiorem danych.

Administrator danych w stosunku do zbiorów danych osobowych może być zobowiązany do zgłoszenia ich do rejestracji u GIODO. Aby uznać, że mamy do czynienia ze zbiorem danych, trzeba przyjrzeć się jego strukturze. Jeżeli jest tak uporządkowany, że daje możliwość wyszukania konkretnych danych według określonego kryterium, takiego jak np. imię, nazwisko, data urodzenia, PESEL, data zamieszczenia danych w zbiorze, to mamy do czynienia ze zbiorem danych. Jak informuje GIODO na swojej stronie internetowej www.giodo.gov.pl: „Tylko usystematyzowany zestaw danych, będący zbiorem danych osobowych, powinien być zgłoszony do rejestracji Generalnemu Inspektorowi przez administratora danych, na którym ciąży ten obowiązek".

Rejestracja zbiorów u GIODO

Zgłoszenia zbioru do rejestracji należy dokonać przed rozpoczęciem przetwarzania danych, czyli przed pierwszą czynnością, jaką administrator może wykonać na tych danych, tj. przed pozyskaniem pierwszych danych do zbioru. Do przetwarzania danych w zgłoszonym zbiorze można przystąpić po złożeniu wniosku o rejestrację zbioru u GIODO. Zasada ta dotyczy większości przetwarzanych danych. Natomiast jeżeli administrator danych przetwarza dane wrażliwe, to zbieranie tego typu danych może rozpocząć dopiero po zarejestrowaniu zbioru przez GIODO.

Obecnie rejestracji w rejestrze prowadzonym przez GIODO podlegają tylko zbiory prowadzone z wykorzystaniem systemów informatycznych. Zbiory prowadzone w formie papierowej takiej rejestracji nie podlegają, chyba że zawierają tzw. dane wrażliwe, wtedy też trzeba je zgłosić do rejestracji.

Nie oznacza to, że rejestracji podlega każdy zbiór danych prowadzony w systemie informatycznym. Art. 43 ust. 1 i ust. 1a ustawy o ochronie danych osobowych określa, jakie zbiory danych podlegają wyłączeniu z tego obowiązku.

Przykładem jest zwolnienie w przypadku przetwarzania danych w zbiorze wyłącznie w celu wystawienia faktury, rachunku lub prowadzenia sprawozdawczości finansowej. Jeśli jednak zgromadzone w zbiorze dane są przetwarzane również w innych celach, np. oprócz celów stricte finansowo-księgowych dane są wykorzystywane do realizacji umów, dochodzenia roszczeń, celów marketingowych, utrzymywania kontaktu z klientem, to taki zbiór administrator danych będzie musiał zarejestrować u GIODO.

GIODO prowadzi ogólnokrajowy, jawny rejestr zbiorów danych osobowych.

Zgłoszenie zbioru danych do rejestracji powinno zawierać:
- wniosek o wpisanie zbioru do rejestru zbiorów danych osobowych,
- oznaczenie administratora danych i adres jego siedziby lub miejsca zamieszkania, w tym numer REGON, jeżeli został mu nadany, oraz podstawę prawną upoważniającą do prowadzenia zbioru,
- cel przetwarzania danych,
- opis kategorii osób, których dane dotyczą, oraz zakres przetwarzanych danych,
- sposób zbierania oraz udostępniania danych,
- informację o odbiorcach lub kategoriach odbiorców, którym dane mogą być przekazywane,
- opis zastosowanych środków technicznych i organizacyjnych,
- informację o sposobie wypełnienia warunków technicznych i organizacyjnych, określonych w przepisach,
- informację dotyczącą ewentualnego przekazywania danych do państwa trzeciego.

Powołanie ABI

Od stycznia 2015 r. administratorzy danych zwykłych mogą nie rejestrować przetwarzanych zbiorów danych, jeżeli powołają administratora bezpieczeństwa informacji. Podstawowym zadaniem ABI jest zapewnianie przestrzegania przepisów o ochronie danych osobowych w firmie. W tym celu kontroluje on zgodność przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowuje w tym zakresie sprawozdanie dla administratora danych. Ponadto nadzoruje opracowanie i aktualizowanie dokumentacji opisującej sposób przetwarzania danych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych. Nadzoruje również przestrzeganie zasad określonych w tych dokumentach. Do obowiązków ABI należy zapoznawanie osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych. Oprócz tego prowadzi on rejestr zbiorów danych przetwarzanych przez administratora danych.

Obowiązki administratora danych

Administratorzy danych podlegają kontroli Generalnego Inspektora Ochrony Danych Osobowych. Dla GIODO najważniejsze jest czy administrator, przetwarzając dane osobowe, przestrzega zasad ochrony danych osobowych określonych przepisami ustawy i czy prawidłowo zabezpieczył dane w zbiorze, zgodnie z przepisami prawa regulującymi kwestie zabezpieczeń.

Jeżeli zbiory przetwarzanych przez administratora danych nie podlegają rejestracji, nie zwalnia go to automatycznie z innych obowiązków określonych w ustawie o ochronie danych osobowych, tzn. z obowiązku legitymowania się jedną z przesłanek umożliwiających przetwarzanie danych, obowiązków informacyjnych w stosunku do osób, od których pobiera dane, a także obowiązku zapewnienia, aby dane były przetwarzane zgodnie z prawem.

Każdy administrator danych, bez względu na to, czy zbiory przetwarzanych przez niego danych podlegają rejestracji u GIODO, ma obowiązek stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, odpowiednią do zagrożeń oraz kategorii danych objętych ochroną.

Natomiast w przypadku przetwarzania danych w systemie informatycznym musi stosować się do przepisów rozporządzenia Ministra Spraw Wewnętrznych i Administracji 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. z 2004 r. nr 100, poz. 1024).

Danymi osobowymi są zarówno takie dane, które pozwalają na określenie tożsamości konkretnej osoby, jak i takie, które nie pozwalają na jej natychmiastową identyfikację, ale są, przy pewnym nakładzie kosztów, czasu i działań, wystarczające do jej ustalenia. Pojedynczą daną osobową umożliwiającą identyfikację jest numer PESEL.

2. Kto może zostać powołany na stanowisko ABI?

Jak wynika z informacji Generalnego Inspektora Ochrony Danych Osobowych, w ostatnim czasie przybywa podmiotów, które powołują administratorów bezpieczeństwa informacji. GIODO zachęca do powoływania ABI, gdyż czekająca nas unijna reforma prawa ochrony danych osobowych, która zacznie obowiązywać w Polsce od 25 maja 2018 r. wprowadzi do naszego porządku prawnego instytucję inspektorów ochrony danych. Prawdopodobnie staną się nimi z mocy prawa obecnie funkcjonujący ABI. To właśnie oni powinni przygotować podmiot, w którym są administratorami bezpieczeństwa informacji do unijnej reformy prawa.

Powołanie ABI jest fakultatywne

Obecnie na mocy art. 36a ustawy o ochronie danych osobowych, administrator danych może powołać administratora bezpieczeństwa informacji, do którego należy m.in. sprawdzanie zgodności przetwarzania danych osobowych w firmie z przepisami o ochronie danych osobowych. Przy czym powołanie administratora bezpieczeństwa informacji jest uprawnieniem, a nie obowiązkiem administratora danych (przedsiębiorcy będącego osobą fizyczną, spółki, stowarzyszenia). Ustanowienie ABI zwalnia administratora danych z obowiązku rejestrowania u GIODO zbiorów przetwarzanych przez niego zwykłych danych osobowych. Taki wewnętrzny rejestr zbiorów danych przetwarzanych przez administratora danych prowadzi bowiem powołany przez niego ABI.

Obowiązujące przepisy w zakresie tego, kto może zostać powołany na stanowisko ABI, są bardzo lakoniczne. Określają tylko trzy podstawowe wymogi dla kandydata na ABI, tj.:
- pełna zdolność do czynności prawnych oraz korzystanie z pełni praw publicznych,
- niekaralność za umyślne przestępstwo,
- odpowiednia wiedza w zakresie ochrony danych osobowych.

Dwie pierwsze przesłanki mają charakter obiektywny. Zdolność do czynności prawnych ocenia się z uwzględnieniem przepisów prawa cywilnego. Natomiast kwestia niekaralności oceniana jest na podstawie informacji z Krajowego Rejestru Karnego. Do złożenia takiego zaświadczenia administrator danych może zobowiązać kandydata na ABI. Można jednak spotkać się ze stanowiskiem, że administrator danych może oprzeć się jedynie na oświadczeniu kandydata na ABI na temat jego niekaralności.

Ostatnia z przytoczonych przesłanek ma charakter subiektywny. Ocena czy kandydat na ABI spełnia wymóg posiadania odpowiedniej wiedzy w zakresie ochrony danych osobowych należy bowiem do administratora danych. W pierwotnej wersji projektu zmian w ustawie o ochronie danych osobowych pojawił się wymóg posiadania przez ABI wyższego wykształcenia, został jednak on z ostatecznej wersji ustawy usunięty. Przy dokonywaniu oceny spełniania przez kandydata na ABI wymogu odpowiedniej wiedzy administrator danych może oczywiście uwzględnić, np. ukończone przez niego kursy, szkolenia czy też posiadane doświadczenie zawodowe.

Administrator danych zgłasza do rejestracji GIODO powołanie i odwołanie ABI w terminie 30 dni od dnia jego powołania lub odwołania.

Łączenie funkcji

Przedsiębiorcy rozważający ustanowienie w swojej firmie ABI zastanawiają się nad możliwością powierzenia takiej funkcji etatowemu pracownikowi i połączenia dotychczasowych jego obowiązków z nowymi. Takie połączenie jest możliwe na mocy art. 36a ust. 4 ustawy o ochronie danych osobowych. Stanowi on, że administrator danych może powierzyć administratorowi bezpieczeństwa informacji wykonywanie innych obowiązków, jeżeli nie naruszy to prawidłowego wykonywania przez niego zadań, do których jest zobowiązany jako ABI. W praktyce oznacza to, że możliwe jest wyznaczenie przez administratora danych na funkcję ABI pracownika spółki, który dotychczas zajmował inne stanowisko. Jednak co istotne, może on łączyć wykonywanie dotychczasowych obowiązków z obowiązkami ABI, tylko jeżeli łączenie takie nie uniemożliwi mu pełnienia funkcji ABI. Trzeba też pamiętać, że administrator danych ma obowiązek zapewniać środki i organizacyjną odrębność administratora bezpieczeństwa informacji niezbędne do niezależnego wykonywania przez niego zadań. Chodzi tu o środki techniczne, organizacyjne i finansowe. W praktyce konieczne jest więc wydzielenie ABI ze struktur organizacyjnych jednostki i stworzenie samodzielnego stanowiska lub nawet odrębnego działu ABI.

ABI podlega bezpośrednio kierownikowi jednostki organizacyjnej lub osobie fizycznej będącej administratorem danych. Taka bezpośrednia podległość ma umożliwić mu skuteczne wypełnianie nałożonych na niego zadań, szczególnie w zakresie nadzoru nad przestrzeganiem przepisów obwiązujących w zakresie ochrony danych osobowych. Gdyby bowiem ABI podlegał tylko np. bezpośrednio pod swojego kierownika działu, to mógłby mieć problemy ze sprawowaniem takiej kontroli i stosowaniem ewentualnych środków władczych.

W zakresie dopuszczalności powierzenia pracownikowi zatrudnionemu u pracodawcy w ramach stosunku pracy dodatkowo obowiązków administratora bezpieczeństwa informacji przepisy prawa pracy oraz ustawy o ochronie danych osobowych nie wykluczają takiej możliwości. Powierzenie obowiązków ABI może nastąpić w ramach zmiany dotychczasowej umowy o pracę. Zmiana umowy o pracę może być przeprowadzona poprzez zawarcie porozumienia stron (tzw. aneksu do umowy) lub w drodze wypowiedzenia zmieniającego.

Spore różnice zdań dotyczą kwestii, czy możliwe jest łączenie takich funkcji jak administrator systemów informatycznych (ASI) czy też pełnomocników ds. niejawnych z wykonywaniem funkcji administratora bezpieczeństwa informacji. Otóż z żadnego z przepisów ustawy o ochronie danych osobowych nie wynika zakaz łączenia takich funkcji. Co więcej, w żadnym z przepisów nie ma mowy o funkcji administratora systemów informatycznych. Administrator danych ma możliwość dowolnego tworzenia wewnętrznej struktury organizacyjnej, a powoływanie ASI lub np. pełnomocników ds. niejawnych jest w polskich firmach bardzo popularne. Zdarza się więc, że na funkcję ABI powoływane są właśnie takie osoby. Przyjęcie takiego rozwiązania może prowadzić do sytuacji, w której ABI będzie nadzorował w ramach przyznanych mu kompetencji swoje własne czynności wykonywane jako administrator systemów informatycznych. Z tego względu lepszym rozwiązaniem jest wyznaczanie ABI spośród pracowników, którzy nie są zatrudnieni przy przetwarzaniu danych osobowych. Postuluje się, aby ABI miał funkcję zupełnie niezależną od pionu informatycznego.

3. Sprawozdania przygotowywane przez ABI

Rodzaje sprawdzeń ABI

Jednym z obowiązków ABI jest sporządzanie dla administratora danych, dla którego pracuje, sprawozdania. Sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przez ABI dokonywane jest dla administratora danych, oraz dla Generalnego Inspektora Ochrony Danych Osobowych, w przypadku gdy zwróci się on do administratora danych o dokonanie takiego sprawdzenia.

Sprawdzenie jest przeprowadzane w trybie:
- sprawdzenia planowego – według planu sprawdzeń,
- sprawdzenia doraźnego – w przypadku nieprzewidzianym w planie sprawdzeń, w sytuacji powzięcia przez ABI wiadomości o naruszeniu ochrony danych osobowych lub uzasadnionego podejrzenia wystąpienia takiego naruszenia.

Plan sprawdzeń określa przedmiot, zakres, a także termin przeprowadzenia poszczególnych sprawdzeń oraz sposób i zakres ich dokumentowania. Przygotowuje go ABI na okres nie krótszy niż kwartał i nie dłuższy niż rok. Ma obowiązek przedstawić go administratorowi danych nie później niż na dwa tygodnie przed dniem rozpoczęcia okresu objętego tym planem. Zbiory danych oraz systemy informatyczne, które służą do przetwarzania lub zabezpieczania danych osobowych, muszą być objęte sprawdzeniem co najmniej raz na pięć lat.

Z kolei doraźne sprawdzenie powinno być przeprowadzone niezwłocznie po powzięciu wiadomości przez ABI o naruszeniu ochrony danych osobowych lub uzasadnionym podejrzeniu takiego naruszenia. Czynności podjęte w ramach sprawdzenia muszą być przez ABI udokumentowane poprzez utrwalenie danych z systemu informatycznego na nośniku danych lub przez ich wydruk. Ponadto ABI sporządza notatki z czynności, w szczególności z zebranych wyjaśnień, przeprowadzonych oględzin oraz z czynności związanych z dostępem do urządzeń, nośników, a także systemów informatycznych.

ABI zawiadamia administratora danych o stwierdzonych nieprawidłowościach.

Plan sprawdzeń

ABI w planie sprawdzeń musi uwzględnić w szczególności zbiory danych osobowych i systemy informatyczne służące do przetwarzania danych osobowych oraz konieczność weryfikacji zgodności przetwarzania tych danych z:
- zasadami przetwarzania danych osobowych, ich zbierania od osób, których dotyczą, i od innych podmiotów,
- zasadami dotyczącymi zabezpieczenia danych osobowych (chodzi tu o stosowane środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, oraz kontrolę nad właściwym upoważnieniem osób, które mają dostęp do danych),
- obowiązkiem zgłoszenia zbioru danych do rejestracji u GIODO i jego aktualizacji, jeżeli zbiór zawiera tzw. dane wrażliwe.

Sprawozdanie dla administratora danych

Po zakończeniu sprawdzenia ABI przygotowuje sprawozdanie. Może być ono sporządzane w postaci elektronicznej albo w postaci papierowej. ABI przekazuje administratorowi danych sprawozdanie ze:
- sprawdzenia planowego nie później niż w terminie 30 dni od zakończenia sprawdzenia,
- sprawdzenia doraźnego – niezwłocznie po zakończeniu sprawdzenia,
- sprawdzenia, o którego dokonanie zwrócił się Generalny Inspektor – zachowując termin wskazany przez GIODO.

To, jakie elementy powinno zawierać sprawozdanie, określa art. 36c ustawy o ochronie danych osobowych (patrz ramka).

Stanowisko GIODO

GIODO na swojej stronie internetowej wyjaśnia zasady przesyłania do niego sprawozdań ABI. „W ostatnim czasie do Biura Generalnego Inspektora Ochrony Danych Osobowych wpływają sprawozdania z przygotowywanych przez administratorów bezpieczeństwa informacji (ABI) sprawdzeń planowych i doraźnych. Ich opracowywanie jest jednym z ich zadań wynikającym z przepisów ustawy o ochronie danych osobowych (art. 36c w związku z art. 36a ust. 2 pkt 1 lit. a), lecz są one tworzone przede wszystkim na użytek danego podmiotu i nie powinny być przesyłane do GIODO. Obowiązek przedstawienia Generalnemu Inspektorowi Ochrony Danych Osobowych – za pośrednictwem administratora danych osobowych – sprawozdania ze sprawdzenia, dotyczy wyłącznie sprawdzeń realizowanych na wniosek GIODO (a więc przypadków określonych w art. 19b ustawy). W innych przypadkach, tj. dokonywania planowych lub doraźnych sprawdzeń dla administratora danych osobowych (wymienionych w § 3 ust. 2 pkt 1 i 2 rozporządzenia Ministra Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji), na administratorze bezpieczeństwa informacji nie ciąży obowiązek przedstawienia sprawozdania Generalnemu Inspektorowi Ochrony Danych Osobowych. Sprawozdania z dokonanych przez ABI planowych bądź doraźnych sprawdzeń nie podlegają zatem przekazaniu Generalnemu Inspektorowi Ochrony Danych Osobowych, lecz stanowią jedynie dokumentację wewnętrzną administratora danych osobowych. Niemniej może zajść konieczność przedstawienia takiego sprawozdania na żądanie inspektora GIODO, w sytuacji gdyby zostały podjęte czynności kontrolne mające na celu ustalenie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych".

Co musi zawierać sprawozdanie ABI:
- oznaczenie administratora danych i adres jego siedziby lub miejsca zamieszkania,
- imię i nazwisko ABI,
- wykaz czynności podjętych przez ABI w toku sprawdzenia oraz imiona, nazwiska i stanowiska osób biorących udział w tych czynnościach,
- datę rozpoczęcia i zakończenia sprawdzenia,
- określenie przedmiotu i zakresu sprawdzenia,
- opis stanu faktycznego stwierdzonego w toku sprawdzenia oraz inne informacje mające istotne znaczenie dla oceny zgodności przetwarzania danych z przepisami o ochronie danych osobowych,
- stwierdzone przypadki naruszenia przepisów o ochronie danych osobowych w zakresie objętym sprawdzeniem wraz z planowanymi lub podjętymi działaniami przywracającymi stan zgodny z prawem,
- wyszczególnienie załączników stanowiących składową część sprawozdania,
- podpis ABI, a w przypadku sprawozdania w postaci papierowej – dodatkowo parafy ABI na każdej stronie sprawozdania,
- datę i miejsce podpisania sprawozdania przez ABI.

4. Rejestr zbiorów przetwarzanych danych prowadzony przez ABI

Podstawową zaletą powołania ABI i zarejestrowania go u GIODO jest fakt, iż to on prowadzi jawny rejestr zbiorów danych osobowych przetwarzanych u danego podmiotu (czyli u administratora danych). To zaś oznacza, że nie trzeba tych zbiorów rejestrować u GIODO, chyba że zbiór zawiera tzw. dane wrażliwe.

Dane te określa art. 27 ustawy o ochronie danych osobowych. Są to dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również dane o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz dane dotyczące skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

Rejestr zbiorów danych składa się z wykazu zbiorów danych zawierającego szereg informacji zamieszczanych odrębnie dla każdego ze zbiorów danych wpisanych do tego rejestru (patrz ramka). W rejestrze tym nie są zamieszczane dane osobowe tworzące poszczególne zbiory, a jedynie informacje o tym, jakie zbiory danych posiada administrator danych osobowych (np. zbiór danych klientów).

ABI ma następujące obowiązki w związku z prowadzeniem tego rejestru:
- wpisuje zbiór danych do rejestru przed rozpoczęciem przetwarzania w zbiorze danych,
- niezwłocznie aktualizuje informacje dotyczące zbioru danych w rejestrze – w przypadku zmiany informacji objętych wpisem,
- niezwłocznie wykreśla zbiór danych z rejestru – w przypadku zaprzestania przetwarzania w nim danych osobowych,
- udostępnia rejestr do przeglądania.

Rejestr jest jawny

Rejestr może być prowadzony w postaci papierowej lub w postaci elektronicznej. Jest on jawny, co oznacza, że każdy ma prawo się z nim zapoznać. Obowiązujące przepisy określają w jaki sposób można przeglądać rejestr. W przypadku prowadzenia rejestru w postaci elektronicznej ABI udostępnia rejestr do przeglądania:
- na stronie internetowej administratora danych, przy czym na stronie głównej umieszcza się odwołanie umożliwiające bezpośredni dostęp do rejestru lub
- na stanowisku dostępowym w systemie informatycznym administratora danych znajdującym się w siedzibie lub miejscu zamieszkania tego administratora, lub
- przez sporządzenie wydruku rejestru z systemu informatycznego administratora danych.

W razie prowadzenia rejestru w postaci papierowej, ABI udostępnia każdemu zainteresowanemu treść rejestru do przeglądania w siedzibie lub miejscu zamieszkania administratora danych.

Wyjątek zrobiono dla zamieszczanych w rejestrze informacji o tym, że dane zostały powierzone do przetwarzania podmiotowi trzeciemu (np. biuru rachunkowemu). Jeśli rejestr jest prowadzony w formie elektronicznej, to można w postaci elektronicznej udostępnić informację o tym, że dane zostały powierzone do przetwarzania innemu podmiotowi, natomiast nazwę i adres tego podmiotu można udostępniać w siedzibie.

Zmiany w zbiorze

ABI ma obowiązek aktualizować rejestr. Musi więc odnotować w nim historię zmian, zawierającą:
- informację o rodzaju zmiany (nowy wpis, aktualizacja, wykreślenie),
- datę dokonania zmiany,
- informację o zakresie zmiany.

W przypadku wykreślenia zbioru danych z rejestru, w rejestrze pozostawia się nazwę zbioru danych, datę wpisania zbioru danych oraz datę ostatniej aktualizacji informacji dotyczących tego zbioru wraz z adnotacją, że jest to data wykreślenia zbioru z rejestru.

Szczególne zasady prowadzenia rejestru przez administratora bezpieczeństwa informacji określa rozporządzenie Ministra Administracji i Cyfryzacji w sprawie sposobu prowadzenia przez ABI rejestru zbiorów danych (Dz. U. z 2015 r. poz. 719).

W rejestrze zbiorów danych zamieszcza się następujące informacje dotyczące każdego zbioru:
- nazwę zbioru danych,
- oznaczenie administratora danych i adres jego siedziby lub miejsca zamieszkania oraz numer REGON, jeżeli został mu nadany,
- w przypadku przetwarzania danych osobowych przez podmioty mające siedzibę albo miejsce zamieszkania w państwie trzecim – oznaczenie przedstawiciela administratora danych i adres jego siedziby lub miejsca zamieszkania – w przypadku wyznaczenia takiego podmiotu,
- oznaczenie podmiotu, któremu powierzono przetwarzanie danych ze zbioru na podstawie art. 31 ustawy o ochronie danych osobowych, i adres jego siedziby lub miejsca zamieszkania – w przypadku powierzenia przetwarzania danych temu podmiotowi,
- podstawę prawną upoważniającą do prowadzenia zbioru danych,
- cel przetwarzania danych w zbiorze,
- opis kategorii osób, których dane są przetwarzane w zbiorze,
- zakres danych przetwarzanych w zbiorze,
- sposób zbierania danych do zbioru, w szczególności informacja, czy dane do zbioru są zbierane od osób, których dotyczą, czy z innych źródeł niż osoba, której dane dotyczą,
- o udostępnianiu danych ze zbioru, w szczególności informacje, czy dane ze zbioru są udostępniane innym podmiotom niż upoważnione na podstawie przepisów prawa,
- oznaczenie odbiorcy danych lub kategorii odbiorców, którym dane mogą być przekazywane,
- informację dotyczącą ewentualnego przekazywania danych do państwa trzeciego.

Ponadto w rejestrze podaje się datę wpisu każdego zbioru danych do rejestru, a także datę ostatniej aktualizacji informacji dotyczących każdego zbioru danych.

5. Kto przejmuje obowiązki ABI po jego odwołaniu?

Prowadzę firmę wpisaną do CEIDG. Parę miesięcy temu powołałam administratora bezpieczeństwa informacji. Nie jestem jednak zadowolona z takiego rozwiązania. W jaki sposób odwołać go ze stanowiska? Czy jako właścicielka firmy będę musiała przejąć jego obowiązki?

Czytelniczka powinna zgłosić Generalnemu Inspektorowi Ochrony Danych Osobowych odwołanie administratora bezpieczeństwa informacji w terminie 30 dni od dnia jego odwołania. Taki obowiązek wynika z art. 46b ust. 1 ustawy o ochronie danych osobowych. Wykreślenie ABI z rejestru administratorów bezpieczeństwa informacji następuje po powiadomieniu o jego odwołaniu.

GIODO z urzędu wydaje administratorowi danych decyzję o wykreśleniu administratora bezpieczeństwa informacji, jeżeli ABI:
- nie spełnia warunków do pełnienia tej funkcji,
- nie wykonuje zadań nałożonych na niego przez ustawę,
- administrator danych nie powiadomił o odwołaniu ABI.

Zarówno zgłoszenia powołania, jak i odwołania ABI należy dokonać przy użyciu wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji, które stanowią załączniki do rozporządzenia Ministra Administracji i Cyfryzacji w tej sprawie (Dz. U. z 2014 r. poz. 1934). W przypadku gdy w danym podmiocie nie ma powołanego administratora bezpieczeństwa informacji, to jego obowiązki (z wyjątkiem obowiązku sporządzania sprawozdania dla administratora danych) wykonuje sam administrator danych. Administratorem danych osobowych (ADO) wykorzystywanych w zakresie działalności prowadzonej przez przedsiębiorcę jest dany przedsiębiorca. Administratorem danych jest w szczególności spółka z ograniczoną odpowiedzialnością, spółka akcyjna, spółka jawna czy też spółka komandytowa. Przy czym ADO jest sama spółka prawa handlowego, nie zaś jej organy, osoby zasiadające w organach tej spółki lub pełniące w niej funkcje kierownicze. W przypadku jednoosobowego przedsiębiorcy będącego osobą fizyczną, administratorem danych jest właśnie ta osoba, w omawianym przypadku Czytelniczka.

Wspomniane obowiązki określa art. 36a ust. 2 ustawy o ochronie danych osobowych. Chodzi tu o zapewnianie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez:
- sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych,
- nadzorowanie opracowania i aktualizowania dokumentacji oraz przestrzegania zasad w niej określonych,
- zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych.

Ponadto Czytelniczka musi pamiętać, że w momencie, kiedy w jej firmie nie będzie już ustanowionego ABI, to będzie musiała zgłaszać do rejestracji u GIODO zbiory przetwarzanych przez nią danych, oczywiście z wyjątkiem tych określonych w art. 43 ust. 1 wspomnianej ustawy.

6. Obcokrajowiec na stanowisku ABI

Spółka planuje powołać administratora bezpieczeństwa informacji. Naszym kandydatem na to stanowisko jest obcokrajowiec. Czy można go powołać na taką funkcję?

Przepisy ustawy o ochronie danych osobowych w art. 36a ust. 5 określają ogólne przesłanki, jakie musi spełniać osoba powoływana na funkcję administratora bezpieczeństwa informacji. Zatem ABI może zostać osoba, która:
- ma pełną zdolność do czynności prawnych oraz korzysta z pełni praw publicznych,
- posiada odpowiednią wiedzę w zakresie ochrony danych osobowych,
- nie była karana za umyślne przestępstwo.

Ustawodawca nie uregulował natomiast kwestii obywatelstwa takiej osoby. Wobec tego obcokrajowiec, który będzie spełniał wykazane przesłanki, może zostać powołany jako ABI i zgłoszony do rejestracji u Generalnego Inspektora Ochrony Danych Osobowych.

Zgłoszenie powołania administratora bezpieczeństwa informacji do rejestracji powinno zawierać:
- oznaczenie administratora danych i adres jego siedziby lub miejsca zamieszkania, w tym numer identyfikacyjny rejestru podmiotów gospodarki narodowej, jeżeli został mu nadany,
- dane administratora bezpieczeństwa informacji:
  - imię i nazwisko,
  - numer PESEL lub nazwę i numer dokumentu stwierdzającego tożsamość,
  - adres do korespondencji, jeżeli jest inny niż adres administratora danych,
- datę powołania,
- oświadczenie administratora danych o spełnianiu przez administratora bezpieczeństwa informacji warunków określonych w art. 36a ust. 5 i 7 ustawy o ochronie danych osobowych.

Jak już wspomniano przy rejestracji ABI należy podać m.in. jego numer PESEL. W sytuacji gdy ABI nie posiada tego numeru, należy wskazać nazwę i numer dokumentu stwierdzającego tożsamość.

Bardzo ważne jest podanie daty powołania ABI, bowiem administrator danych zobowiązany jest zgłosić do rejestracji Generalnemu Inspektorowi powołanie i odwołanie administratora bezpieczeństwa informacji w terminie 30 dni. Powołany przez administratora danych i zgłoszony do GIODO administrator bezpieczeństwa informacji podlega wpisaniu do Rejestru Administratorów Bezpieczeństwa Informacji. Rejestr ten jest jawny i dostępny pod adresem http://egiodo.giodo.gov.pl.

7. Podległość ABI w spółce

Spółka z o.o. chce powołać w swoich strukturach administratora bezpieczeństwa informacji. Z przepisów wynika, że ABI ma podlegać kierownikowi jednostki organizacyjnej. Kogo należy rozumieć przez to pojęcie? W jaki sposób ABI ma być bezpośrednio podległy takiej osobie?

Rzeczywiście art. 36a ust. 7 ustawy o ochronie danych osobowych stanowi, że administrator bezpieczeństwa informacji (ABI) podlega bezpośrednio kierownikowi jednostki organizacyjnej lub osobie fizycznej będącej administratorem danych. Jeżeli np. administratorem danych zobowiązanym do przestrzegania przepisów ustawy o ochronie danych osobowych jest przedsiębiorca będący osobą fizyczną, wpisaną do CEIDG, to ABI podlega bezpośrednio jemu. Sprawa komplikuje się w przypadku gdy, administratorem danych jest np. spółka prawa handlowego lub inna jednostka. W takiej sytuacji przyjmuje się, że kierownikiem jednostki organizacyjnej jest osoba lub osoby (np. wchodzące w skład organu), które kierują jej pracami (np. ministrowie kierujący działami administracji rządowej, dyrektorzy szkół) lub prowadzą jej sprawy (np. zarząd spółki).

Oznacza to, że w przypadku opisanym w pytaniu kierownikiem organizacyjnym jednostki, której będzie podlegał ABI, będzie osoba lub osoby wchodzące w skład zarządu spółki. To zarządowi spółki (lub osobie reprezentującej zarząd) będzie bezpośrednio podlegał ABI. Administrator bezpieczeństwa informacji nie może podlegać innym osobom niż kierownik jednostki organizacyjnej. Zatem nie może on podlegać np. kierownikowi działu kadr, działu prawnego, prokurentowi spółki, dyrektorowi ds. informatycznych czy też dyrektorowi generalnemu (w przypadku urzędu publicznego).

8. ABI w spółce komandytowej

Rozpoczynamy działalność w ramach spółki komandytowej. Czy mamy obowiązek powołania ABI? Jeśli nie, to kto będzie odpowiedzialny za ochronę danych osobowych w firmie?

Jeżeli spółka będzie przetwarzać dane osobowe w związku z prowadzoną działalnością, to będą ją obciążać obowiązki dotyczące ochrony danych osobowych. Spółka komandytowa będzie w rozumieniu tych przepisów administratorem danych (ADO). Jej podstawowym obowiązkiem jako ADO będzie stosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych. W szczególności spółka będzie zobowiązana zabezpieczać dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Tak wynika z art. 36 ustawy o ochronie danych osobowych.

Spółka może zdecydować się na powołanie administratora bezpieczeństwa informacji, który będzie wykonywał obowiązki związane z ochroną danych osobowych w spółce. Przy czym od 1 stycznia 2015 r. powołanie ABI jest uprawnieniem, a nie obowiązkiem administratora danych. Spółka może zdecydować, że nie powoła ABI i w takim przypadku to ona, jako administrator danych, będzie wykonywać zadania określone w art. 36a ust. 2 pkt 1 powołanej ustawy. Chodzi tu przede wszystkim o zapewnianie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez:

- sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych,
- nadzorowanie opracowania i aktualizowania dokumentacji oraz przestrzegania zasad w niej określonych,
- zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych.

Trzeba również pamiętać, że w sytuacji, gdy w danym podmiocie nie został powołany ABI, to administrator danych ma obowiązek zgłaszania do rejestracji u GIODO zbiorów przetwarzanych danych osobowych. W przypadku powołania ABI takiego obowiązku nie ma (oprócz zbiorów danych wrażliwych).

Jeżeli więc Czytelnicy nie zdecydują się powołać ABI, to należy pamiętać, że to spółka, jako administrator danych, będzie odpowiedzialna za ochronę przetwarzanych przez nią danych osobowych. Spółka komandytowa jest osobową spółką handlową, gdzie uprawnieni do prowadzenia jej spraw są komplementariusze. Należy pamiętać, że do czynności związanych z zapewnieniem ochrony danych osobowych mogą zostać upoważnione konkretne osoby, np. pracownicy lub spółka może zlecić takie czynności firmie zewnętrznej.

Kto jest administratorem danych według GIODO?

Administratorem w sferze niepublicznej jest co do zasady podmiot (np. spółka prawa handlowego, spółdzielnia, przedsiębiorca prowadzący działalność gospodarczą jednoosobowo, stowarzyszenie, fundacja), a nie osoba lub osoby zarządzające tym podmiotem (np. dyrektor przedsiębiorstwa, prezes spółdzielni, zarząd spółki) lub też pracownik wykonujący czynności związane z ochroną danych osobowych (np. pełnomocnik zarządu ds. ochrony danych osobowych, administrator bezpieczeństwa informacji). Niemniej to osoby zarządzające danym podmiotem ponoszą odpowiedzialność za naruszenie przepisów o ochronie danych osobowych. Osoby te mogą być bowiem pociągnięte do odpowiedzialności karnej za przestępstwa określone w rozdziale ósmym ustawy o ochronie danych osobowych, jeżeli ich działaniom naruszającym przepisy ustawy, podejmowanym w związku z reprezentowaniem administratora danych, można przypisać winę.

(źródło: www.giodo.gov.pl)

9. Zmiana na stanowisku ABI

W zeszłym roku spółka powołała administratora bezpieczeństwa informacji. Osoba ta postanowiła rozwiązać z nami umowę o pracę. Planujemy powołać nowego ABI. W jaki sposób zgłosić taką zmianę GIODO?

Administrator danych jest zobowiązany zgłosić Generalnemu Inspektorowi Ochrony Danych Osobowych odwołanie administratora bezpieczeństwa informacji w terminie 30 dni od dnia jego odwołania. Tak wynika z art. 46b ust. 1 ustawy o ochronie danych osobowych. Również w terminie 30 dni od momentu powołania nowego ABI Czytelnicy powinni go zgłosić do rejestracji GIODO.

Zarówno zgłoszenia powołania, jak i odwołania ABI należy dokonać przy użyciu wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji, które stanowią załączniki do rozporządzenia Ministra Administracji i Cyfryzacji w tej sprawie.

Na wniosek administratora danych GIODO może wydać zaświadczenie o zarejestrowaniu ABI.

10. Przekazanie obowiązków ABI

Firma planuje powołać administratora bezpieczeństwa informacji. Na to stanowisko chcemy skierować osobę, która obecnie zatrudniona jest w dziale marketingu. W jaki sposób dokonać takiego powołania?

Ustawa o ochronie danych osobowych w żadnym z przepisów nie stanowi, w jakiej formie powinno nastąpić powołanie administratora bezpieczeństwa informacji przez administratora danych. Określa jedynie ogólne kwalifikacje, jakie powinien mieć ABI, tj.:

- pełną zdolność do czynności prawnych oraz pełnię praw publicznych,
- odpowiednią wiedzę w zakresie ochrony danych osobowych,
- niekaralność za umyślne przestępstwo.

Generalny Inspektor Ochrony Danych Osobowych w wyjaśnieniach zawartych na stronie www.abi.giodo.gov.pl stwierdza, że „W przypadku ewentualnej kontroli GIODO istotna będzie możliwość udowodnienia dokonania tej czynności i przyjęcia tej funkcji przez osobę powoływaną. Możliwe jest wprowadzenie nowych obowiązków np. aneksem do umowy o pracę albo zawarcie odrębnej umowy w przypadku innej podstawy zatrudnienia".

11. Czy stowarzyszenie musi powołać swojego ABI?

Jako stowarzyszenie zatrudniamy 10 pracowników i około 30 zleceniobiorców. Do naszego stowarzyszenia wstępują członkowie podając swoje podstawowe dane. Czy w związku z tym powinniśmy powołać administratora bezpieczeństwa informacji?

Stowarzyszenie na gruncie przepisów ustawy o ochronie danych osobowych może być administratorem przetwarzanych danych osobowych. Obowiązek zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych wynika z art. 40 ustawy o ochronie danych osobowych. Nie oznacza to, że wszystkie zbiory przetwarzanych danych osobowych podlegają zgłoszeniu do GIODO. Rodzaje zbiorów danych, które podlegają zwolnieniu z takiego obowiązku, zawiera art. 43 ust. 1 powołanej ustawy. Stanowi on m.in., że z obowiązku rejestracji zbioru danych zwolnieni są administratorzy danych przetwarzanych w związku z zatrudnieniem u nich, świadczeniem im usług na podstawie umów cywilnoprawnych, a także dotyczących osób u nich zrzeszonych lub uczących się. Przepis ten znajduje zastosowanie do stowarzyszenia Czytelników, którzy przetwarzają dane swoich pracowników, osób wykonujących w stowarzyszeniu zlecenia oraz zrzeszonych w nim członków.

Z kolei z art. 43 ust. 1 pkt 8 ustawy wynika, że z obowiązku zgłaszania zbiorów przetwarzanych danych do GIODO zwolnieni są też administratorzy danych przetwarzanych wyłącznie w celu wystawienia faktury, rachunku lub prowadzenia sprawozdawczości finansowej. Jedynie jeżeli zbiory danych tworzone w celach rozliczeniowych są jednocześnie wykorzystywane w innych celach, np. marketingowych, to muszą być zgłoszone do rejestracji.

Z wyjaśnień GIODO zawartych na stronie internetowej www.edugiodo.giodo.gov.pl wynika, że: „Zarówno fundacje, jak i stowarzyszenia są jednak zobowiązane do zgłoszenia do rejestracji zbiorów (innych niż zbiory danych osób zrzeszonych w stowarzyszeniu), takich, jak np.: zbiory danych darczyńców, osób, którym fundacja lub stowarzyszenie udziela pomocy lub wsparcia w związku z realizacją zadań statutowych, czy też osób utrzymujących kontakty z tymi instytucjami". W przypadku takich zbiorów danych Czytelnicy mogą mieć obowiązek ich zgłoszenia do GIODO, chyba że powołają w stowarzyszeniu ABI.

Obecnie administratorzy danych, którzy muszą zgłaszać zbiory danych do rejestracji do GIODO, mogą zdecydować się na powołanie administratora bezpieczeństwa informacji. Powołanie takiej osoby powoduje, że administrator danych nie musi zgłaszać przetwarzanych zbiorów danych do GIODO, bo taki wewnętrzny rejestr tych zbiorów prowadzi dla niego ABI. Jeśli taka osoba nie zostanie powołana, to zbiory danych, które nie podlegają zwolnieniu z obowiązku rejestracji na mocy art. 43 ust. 1, muszą zostać zgłoszone do GIODO. Warto też wspomnieć, iż obecnie administratorzy danych nie mają obowiązku rejestrowania tych zbiorów danych, które nie są prowadzone w formie elektronicznej.

12. Jeden ABI dla kilku firm

Ukończyłam szkolenie dla administratorów bezpieczeństwa informacji. Będę wykonywać funkcję ABI u swojego pracodawcy, obok dotychczasowych obowiązków. Chciałabym również ubiegać się stanowisko administratora bezpieczeństwa informacji w innych instytucjach. Czy mogę pełnić tę funkcję u kliku administratorów danych jednocześnie?

Ustawa o ochronie danych osobowych w art. 36a ust. 5 określa ogólne przesłanki, jakie musi spełniać osoba powoływana na funkcję administratora bezpieczeństwa informacji. ABI może być osoba, która:

- ma pełną zdolność do czynności prawnych oraz korzysta z pełni praw publicznych,
- posiada odpowiednią wiedzę w zakresie ochrony danych osobowych,
- nie była karana za umyślne przestępstwo.

Oprócz tego przepisy stanowią, że administrator danych zobowiązany jest zapewnić środki i organizacyjną odrębność administratora bezpieczeństwa informacji niezbędne do niezależnego wykonywania nałożonych na niego zadań. Z kolei łączenie obowiązków ABI z wykonywaniem innych zadań jest możliwe, o ile nie narusza prawidłowego wykonywania przez ABI jego głównych zadań.

Generalny Inspektor Ochrony Danych Osobowych poddaje w wątpliwość czy wykonywanie obowiązków administratora bezpieczeństwa informacji jednocześnie u różnych administratorów danych osobowych jest możliwe. Na stronie www.abi.giodo.gov.pl stwierdza, że: „ABI musi mieć zapewnione takie warunki funkcjonowania, które pozwolą mu na rzeczywiste i prawidłowe realizowanie obowiązków wynikających z przepisów prawa. Zarówno administrator danych, jak i powołany przez niego ABI odpowiedzialni są za rzetelne zapewnienie przestrzegania przepisów o ochronie danych osobowych w danej organizacji. Osiągnięcie tego celu, w sytuacji, gdy wybrana przez administratora danych osobowych osoba jednocześnie pełni tę funkcję u kilkunastu czy nawet kilkudziesięciu innych administratorów danych może okazać się niemożliwe. Wyboru określonej osoby do pełnienia funkcji ABI należy zatem dokonywać starannie, z dobrym rozeznaniem oraz ze świadomością ciążącej na administratorze danych odpowiedzialności za zgodne z prawem przetwarzanie danych osobowych. W przypadku powoływania na to stanowisko osoby z zewnątrz, warto sprawdzić w ogólnopolskim rejestrze administratorów bezpieczeństwa informacji, czy i jak wielu innych administratorów danych taka osoba już obsługuje (wystarczy wpisać w wyszukiwarce na platformie e-GIODO jej imię i nazwisko)".

GIODO wspomina o pełnieniu funkcji ABI u kilkunastu lub nawet kilkudziesięciu administratorów danych jednocześnie. Taka sytuacja oczywiście nie powinna mieć miejsca. Natomiast wykonywanie funkcji u dwóch różnych podmiotów, przy prawidłowym zorganizowaniu i rozplanowaniu zadań jest dopuszczalne. Warto też wspomnieć, że administrator danych może powołać zastępców ABI, którzy pomogą mu realizować nałożone na niego zadania.

25 maja 2018 r. zacznie obowiązywać w naszym kraju unijne ogólne rozporządzenie o ochronie danych osobowych, na mocy którego spora część administratorów danych będzie musiała powołać inspektorów ochrony danych (zastąpią oni ABI). Przepisy tego rozporządzenia stanowią, że grupa przedsiębiorstw będzie mogła wyznaczyć jednego inspektora ochrony danych, o ile można będzie łatwo nawiązać z nim kontakt z każdej jednostki organizacyjnej.

Podstawa prawna
Ustawa z dnia 29.08.1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922)