OCHRONA DANYCH OSOBOWYCH W FIRMIE

1. Podstawowe zasady ochrony danych osobowych

Każdy przedsiębiorca w zakresie swojej działalności styka się z danymi osobowymi innych ludzi, swoich pracowników, klientów czy też kontrahentów. To, w jakim zakresie i na jakich zasadach może przetwarzać te dane zależy od ich charakteru. Podstawowym obowiązkiem przedsiębiorcy, który przetwarza dane osobowe jest ich ochrona i właściwe zabezpieczenie. Obowiązek ten może realizować samodzielnie lub przy pomocy powołanego administratora bezpieczeństwa informacji.

Kto odpowiada za ochronę danych w firmie?

Administratorem danych osobowych odpowiedzialnym za to, aby były one prawidłowo zabezpieczone i przetwarzane, jest podmiot, który dane przetwarza. W przypadku przedsiębiorców będących spółkami prawa handlowego administratorem danych osobowych jest sama spółka (np. sp. z o.o., akcyjna). W przypadku przedsiębiorców będących osobami fizycznymi administratorem danych osobowych jest osoba fizyczna.

Administrator danych osobowych może wyznaczyć osobę, która będzie pełniła funkcję administratora bezpieczeństwa informacji (ABI). ABI zajmuje się przede wszystkim nadzorowaniem zasad przetwarzania danych osobowych. Jeśli ABI nie został wyznaczony, to jego zadania wykonuje sam administrator danych osobowych. Powołanego ABI należy zgłosić Generalnemu Inspektorowi Ochrony Danych Osobowych, który prowadzi ogólnokrajowy, jawny rejestr administratorów bezpieczeństwa informacji. Jest na to 30 dni od dnia powołania ABI. Powołanie ABI jest prawem, ale nie obowiązkiem każdego administratora danych.

Te firmy, które zdecydują się na powołanie ABI i zgłoszenie go do rejestracji u Generalnego Inspektora Ochrony Danych Osobowych, nie muszą rejestrować w GIODO baz danych osobowych – ich rejestr prowadzi wtedy ABI.

Dzięki powołaniu w firmie ABI i zgłoszeniu go do rejestracji GIODO odpadają uciążliwe obowiązki związane z koniecznością zgłaszania do rejestracji GIODO baz danych osobowych. Zamiast zgłoszenia GIODO zbioru danych, ABI prowadzi jawny rejestr zbiorów danych przetwarzanych przez administratora danych.

Przetwarzanie danych osobowych jest dopuszczalne wtedy, gdy spełniona jest jedna z przesłanek wymienionych w art. 23 ust. 1 ustawy o ochronie danych osobowych. Jedną z nich jest zgoda osoby, której dane dotyczą. W ocenie Generalnego Inspektora Ochrony Danych Osobowych z treści zgody na przetwarzanie danych powinno w sposób niebudzący wątpliwości wynikać, w jakim celu, w jakim zakresie i przez kogo dane osobowe będą przetwarzane. Wyrażający zgodę musi mieć pełną świadomość tego, na co się godzi. Zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści. Zgoda może być odwołana w każdym czasie.

Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych. Osoby, które zostały upoważnione do przetwarzania danych, są obowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia.

Administrator danych jest zobowiązany zapewnić kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane. W związku z tym administrator danych musi prowadzić ewidencję osób upoważnionych do ich przetwarzania.

Zbieranie danych

Jeśli administrator danych zbiera je bezpośrednio od osoby, której dane dotyczą, to ma obowiązek poinformować ją o:

1) adresie swojej siedziby i pełnej nazwie, a w przypadku gdy administratorem danych jest osoba fizyczna – o miejscu swojego zamieszkania oraz imieniu i nazwisku,
2) celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych,
3) prawie dostępu do treści swoich danych oraz ich poprawiania; przyjmuje się, że nie chodzi tu o prawo fizycznego wglądu w oryginalny nośnik, na którym dane są zapisane, lecz o prawo uzyskania informacji o treści posiadanych przez administratora danych,
4) dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.

Informacje te należy według GIODO przekazać w momencie zbierania danych.

Wskazanych obowiązków informacyjnych nie trzeba realizować tylko w dwóch przypadkach. Po pierwsze, gdy osoba, której dane dotyczą, ma już te informacje. Po drugie, gdy przepis innej ustawy zezwala na przetwarzanie danych bez ujawniania faktycznego celu ich zbierania.

Niedopełnienie obowiązku poinformowania osoby, której dane dotyczą, o jej prawach jest przestępstwem. Osobie administrującej zbiorem danych osobowych grozi w takim przypadku grzywna, kara ograniczenia wolności albo pozbawienia wolności do roku (art. 54 ustawy). Taka sama kara grozi w razie niedopełnienia obowiązku przekazania osobie, której dane dotyczą, informacji umożliwiających korzystanie z praw przyznanych jej w ustawie.

Wykorzystanie danych w celach marketingowych

Zgody na przetwarzanie danych osobowych nie trzeba uzyskiwać, jeśli zostaną one wykorzystane do marketingu bezpośredniego własnych produktów lub usług administratora danych (art. 23 ust. 1 pkt 5 w związku z art. 23 ust. 4 pkt 1 ustawy). Nie oznacza to, że zainteresowana osoba nie ma żadnego wpływu na przetwarzanie jej danych w celach marketingowych. Ma bowiem prawo wniesienia sprzeciwu wobec takiego przetwarzania jej danych, przy czym administrator powinien ją o tym prawie poinformować (art. 32 ust. 1 pkt 8 ustawy). Jeśli promowane mają być produkty i usługi innych firm, to konieczne jest uzyskanie zgody zainteresowanych osób, gdyż brak jest przepisów pozwalających na takie wykorzystanie danych bez ich zgody. W ocenie Generalnego Inspektora Danych Osobowych „nawet zawarcie przez oba podmioty umowy w sprawie wzajemnej promocji nie jest wystarczającą podstawą do uznania, że wysyłanie oferty marketingowej firmy współpracującej jest prawnie usprawiedliwionym celem administratora danych".

Brak konieczności uzyskania zgody na przetwarzanie danych nie zwalnia z konieczności dopełnienia innych obowiązków wynikających z ustawy.

Windykacja należności

Informacje na temat zadłużenia osób fizycznych są danymi osobowymi i podlegają ochronie. Podejmowanie wobec dłużnika czynności windykacyjnych wymagających przetwarzania jego danych osobowych, w tym wysyłanie do dłużnika wezwań do zapłaty, nie wymaga odrębnej zgody dłużnika na ich przetwarzanie. Przetwarzanie danych, bez konieczności uzyskiwania zgody osoby zainteresowanej, jest dopuszczalne m.in. wtedy, gdy jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą. Za prawnie usprawiedliwiony cel w rozumieniu tego przepisu uważa się m.in. dochodzenie roszczeń z tytułu prowadzonej działalności gospodarczej (art. 23 ust. 1 pkt 5 w związku z art. 23 ust. 4 pkt 2 ustawy o ochronie danych osobowych).

Jeśli czynności windykacyjne są podejmowane w imieniu wierzyciela przez podmiot zewnętrzny, np. firmę windykacyjną, i w związku z tym następuje przekazanie danych osobowych dłużników temu podmiotowi, należy z nim zawrzeć umowę o powierzenie przetwarzania danych.

Podstawowe definicje

- ✓ zbiór danych – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie
- ✓ przetwarzanie danych – jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych
- ✓ administrator danych – organ, jednostka organizacyjna, podmiot lub osoba decydujące o celach i środkach przetwarzania danych osobowych

2. Powołanie administratora bezpieczeństwa informacji

Na mocy art. 36a ustawy o ochronie danych osobowych, administrator danych może powołać administratora bezpieczeństwa informacji, do którego zadań 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 danych osobowych. Taki wewnętrzny rejestr zbiorów danych przetwarzanych przez administratora danych prowadzi bowiem powołany przez niego ABI.

Kto może zostać ABI?

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

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. Ustawodawca planował zawrzeć w ustawie o ochronie danych osobowych wymóg posiadania przez ABI wyższego wykształcenia, ostatecznie jednak w obowiązujących przepisach takiej przesłanki nie ma. 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.

Stosunek pracy ABI

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 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, który dotychczas zajmował inne stanowisko. 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 zapewnić 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 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 swojemu kierownikowi 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 poprzez zmianę dotychczasowej umowy o pracę. Zmiana umowy o pracę może być przeprowadzona poprzez zawarcie porozumienia stron (tzw. aneksu do umowy) lub w drodze wypowiedzenia zmieniającego.

Łączenie funkcji ABI z innymi obowiązkami

Spore różnice zdań dotyczą kwestii tego, czy możliwe jest łączenie takich funkcji jak administrator systemów informatycznych 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 (ASI). 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 swoich 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.

Zgodnie z odmiennym poglądem powołany już wcześniej przepis, który umożliwia wykonywanie przez ABI innych obowiązków u tego samego administratora danych, umożliwia m.in. łączenie takich funkcji, a ocena czy wykonywanie obowiązków w zakresie funkcji administratora systemów informatycznych uniemożliwi tej samej osobie wykonywanie zadań jako administrator bezpieczeństwa informacji powinna być dokonywana w odniesieniu do konkretnego przypadku.

Zgłoszenia powołania ABI dokonuje się na podstawie wzoru stanowiącego załącznik do rozporządzenia Ministra Administracji i Cyfryzacji (Dz. U. z 2014 r. poz. 1934).

„Administrator danych nie powinien obarczać osoby pełniącej funkcję ABI obowiązkami, które utrudniałyby właściwe wykonywania zapewniania przestrzegania przepisów o ochronie danych osobowych (co może być oceniane w toku kontroli GIODO). Oznacza to konieczność dostosowania zakresu obowiązków do skutecznego wykonywania funkcji ABI".

Opina GIODO na zapytanie naszego Wydawnictwa w zakresie możliwości łączenia obowiązków pracownika ze stanowiskiem ABI

3. Zasady działania ABI w firmie

Administrator danych (przedsiębiorca będący osobą fizyczną, spółka prawa handlowego, jednostka samorządu terytorialnego, szkoła), może zdecydować się na powołanie administratora bezpieczeństwa informacji (ABI). Ustanowienie takiej osoby zdejmuje z administratora danych szereg ciążących na nim obowiązków w zakresie ochrony danych osobowych. Przede wszystkim nie musi zgłaszać do rejestracji u Generalnego Inspektora Ochrony Danych Osobowych rejestru przetwarzanych przez niego danych osobowych. Taki wewnętrzny rejestr prowadzi bowiem powołany ABI. Jednym z jego obowiązków jest sporządzanie dla administratora danych, dla którego pracuje, sprawozdania.

Obowiązki ABI

Podstawowym zadaniem ABI jest zapewnianie przestrzegania przepisów o ochronie danych osobowych. W tym celu sprawdza on w danej jednostce 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.

Rodzaje sprawdzeń

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 przez ABI wiadomości 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.

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 ABI

Po zakończeniu sprawdzenia ABI przygotowuje sprawozdanie. Może być ono sporządzane w postaci elektronicznej albo papierowej. ABI przekazuje administratorowi danych sprawozdanie ze sprawdzenia:
- planowego – nie później niż w terminie 30 dni od zakończenia sprawdzenia,
- doraźnego – niezwłocznie po jego zakończeniu,
- 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).

Sprawozdanie ABI powinno zawierać:
- ✓ 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. Obowiązki przedsiębiorcy, gdy w firmie nie ma ABI

Jeżeli administrator danych nie powołał w swojej firmie ABI, to przetwarzanie danych może rozpocząć dopiero po zgłoszeniu zbioru danych do rejestracji Generalnemu Inspektorowi, chyba że ustawa zwalnia go z tego obowiązku. Jeżeli zaś chodzi o tzw. dane wrażliwe, np. o stanie zdrowia, czy poglądach politycznych, to administrator danych może rozpocząć ich przetwarzanie w zbiorze danych po zarejestrowaniu zbioru przez GIODO (nie w momencie dokonania zgłoszenia do GIODO). Trzeba zauważyć, że nie wszyscy administratorzy danych mają obowiązek zgłaszania zbiorów przetwarzanych danych do rejestracji u GIODO. Katalog administratorów danych, którzy podlegają takiemu zwolnieniu, i którzy nawet jeśli nie powołają ABI nie muszą dokonywać wspomnianych zgłoszeń, zawiera art. 43 ust. 1 i 1a ustawy o ochronie danych osobowych (patrz ramka).

Obowiązki administratora danych

Administrator danych zobowiązany jest zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną. Przede wszystkim powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Administrator danych prowadzi dokumentację opisującą sposób przetwarzania danych oraz środki, które stosuje w celu zabezpieczania danych.

Przedsiębiorca, który zdecyduje się nie powoływać w swojej firmie ABI, zobowiązany jest wykonywać wszystkie te obowiązki, które obciążają ABI, z wyłączeniem obowiązku sporządzania sprawozdania. W związku z tym zapewnia przestrzeganie przepisów o ochronie danych osobowych, w szczególności przez:

- sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych,
- nadzorowanie opracowania i aktualizowania dokumentacji opisującej sposób przetwarzania danych oraz środki, które stosuje w celu zabezpieczania danych, a także przestrzegania zasad w niej określonych,
- zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych.

Zgłoszenie zbiorów danych

Administrator danych jest zobowiązany zgłosić zbiór danych do rejestracji Generalnemu Inspektorowi, z wyjątkiem przypadków, o których mowa w art. 43 ust. 1 i 1a ustawy o ochronie danych osobowych.

Takie zgłoszenie 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, a w przypadku powierzenia przetwarzania danych innemu podmiotowi lub wyznaczenia takiego podmiotu, oznaczenie tego podmiotu i adres jego siedziby lub miejsca zamieszkania,
- 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 środków technicznych i organizacyjnych zastosowanych w celu ochrony tych danych,
- informację o sposobie wypełnienia warunków technicznych i organizacyjnych,
- informację dotyczącą ewentualnego przekazywania danych do państwa trzeciego.

Zgłoszenia można dokonać także drogą elektroniczną, z użyciem bezpiecznego podpisu elektronicznego. Wzór takiego zgłoszenia zawiera rozporządzenie Ministra Administracji i Cyfryzacji w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz. U. z 2008 r. nr 229, poz. 1536).

Administrator danych jest zobowiązany zgłaszać Generalnemu Inspektorowi każdą zmianę informacji dotyczących danego zbioru, w terminie 30 dni od dnia dokonania modyfikacji w zbiorze danych. Wykreślenie z rejestru zbiorów danych osobowych jest dokonywane, w drodze decyzji administracyjnej, jeżeli:

- zaprzestano przetwarzania danych w zarejestrowanym zbiorze,
- rejestracji dokonano z naruszeniem prawa.

Dokumentacja dotycząca ochrony danych

Zakres dokumentacji, jaki powinien opracować administrator danych w związku z obowiązkiem zapewnienia prawidłowej ochrony danych osobowych, określa rozporządzenie Ministra Spraw Wewnętrznych i Administracji w sprawie dokumentacji przetwarzania danych osobowych (...) (Dz. U. z 2004 r. nr 100, poz. 1024). Na tę dokumentację składa się polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych (patrz tabela). Dokumenty te powinny być prowadzone w formie pisemnej.

Z obowiązku rejestracji zbioru danych zwolnieni są m.in. 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,
- dotyczących osób korzystających z ich usług medycznych, obsługi notarialnej, adwokackiej, radcy prawnego, rzecznika patentowego, doradcy podatkowego lub biegłego rewidenta,
- przetwarzanych wyłącznie w celu wystawienia faktury, rachunku lub prowadzenia sprawozdawczości finansowej,
- powszechnie dostępnych,
- przetwarzanych w zakresie drobnych bieżących spraw życia codziennego,
- w zbiorach, które nie są prowadzone z wykorzystaniem systemów informatycznych, z wyjątkiem zbiorów zawierających dane wrażliwe.

Dokumentacja w zakresie ochrony danych osobowych

Polityka bezpieczeństwa

- wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe,
- wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych,
- opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi, sposób przepływu danych pomiędzy poszczególnymi systemami,
- określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

Instrukcja zarządzania systemem informatycznym

- procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności,
- stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem,
- procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników,
- procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania,
- sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych,
- sposób zabezpieczenia systemu informatycznego,
- procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

5. Kiedy można przetwarzać dane osobowe?

Jak wynika z art. 23 ust. 1 ustawy o ochronie danych osobowych, przetwarzanie danych jest dopuszczalne tylko wtedy, gdy:

- osoba, której dane dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych,
- jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa,
- jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą,
- jest to niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego,
- jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.

Podstawową przesłanką umożliwiającą przetwarzanie danych osobowych jest zgoda osoby, której dane dotyczą. Zgodnie z definicją zawartą w ustawie o ochronie danych osobowych, taka zgoda musi mieć charakter oświadczenia woli. Może mieć ono charakter samodzielny (niepowiązany z innymi oświadczeniami), może też być elementem składanego aktu woli, np. w przypadku wyrażenia zgody przy przystępowaniu do organizacji.

Zgoda na przetwarzanie danych

Zgoda nie może być domniemana ani dorozumiana z oświadczenia woli o innej treści. To oznacza, że nie jest wystarczające powiadomienie danej osoby przez inny podmiot o zamiarze przetwarzania jej danych osobowych i brak sprzeciwu od osoby, której dane dotyczą.

Z definicji zgody osoby, której dane dotyczą, nie wynikają szczegółowe zasady jej formułowania. Powinno jednak z niej wynikać, w jakim celu, w jakim zakresie i przez kogo dane osobowe będą przetwarzane. Wyrażający zgodę musi mieć pełną świadomość tego, na co się godzi. Stanowisko takie wyraził także NSA w wyroku z dnia 4 kwietnia 2003 r., sygn. akt II SA 2135/02. Sąd stwierdził w nim, że: „Zgoda na przetwarzanie danych musi mieć charakter wyraźny, a jej wszystkie aspekty muszą być jasne dla podpisującego w momencie jej wyrażania. Czynności takiej nie konwaliduje późniejsze poinformowanie o treści regulaminu, ani możliwość zgłoszenia zastrzeżeń wobec pewnych form przetwarzania danych".

Nieważna jest zgoda udzielona przez osobę znajdującą się w stanie wyłączającym swobodne powzięcie decyzji, np. w przypadku osoby znajdującej się pod wpływem alkoholu, środków odurzających. Podobnie należy ocenić zgodę uzyskaną w wyniku:

- istotnego błędu,
- podstępu,
- posłużenia się bezprawną groźbą.

Zgoda wymuszona

Z informacji GIODO wynika, że zwracają się do niego osoby, które czują się zmuszane do wyrażania zgody na przetwarzanie ich danych osobowych. Dochodzi do tego najczęściej przy okazji zawierania różnego rodzaju umów. Sprzedawcy lub świadczeniodawcy usług sporządzają kwestionariusze, formularze zawierające w ich treści klauzulę zgody na przetwarzanie danych osobowych. Takie klauzule obejmują zgodę na przetwarzanie danych w celu wykonania zawieranej umowy, a dodatkowo zgodę na wykonywanie innych operacji na danych osobowych (np. ich przekazywanie innym podmiotom, udostępnianie, przekazywanie za granicę lub wykorzystywanie w celach marketingowych). Taka konstrukcja klauzuli zgody jest niedopuszczalna. Wynika bowiem z niej, że zawarcie umowy uzależnione jest od wcześniejszego wyrażenia przez daną osobę zgody na przetwarzanie jej danych osobowych.

Jak stwierdza GIODO: „Tym samym, klienci, przy okazji wypełniania przygotowanych przez różne firmy formularzy czy druków, są niejako zmuszani do wyrażania zgody na wykorzystywanie ich danych osobowych do określonych w klauzuli zgody celów, pozostając w przekonaniu, że bez wyrażenia tej zgody nie będą mogli skorzystać z produktów lub usług świadczonych przez firmę, czyli nie będą mogli zrealizować umowy". Trzeba w tym miejscu zwrócić uwagę, że zgodnie z ustawą o ochronie danych osobowych, na wykorzystywanie danych w celu zawarcia lub wykonania umowy zgoda w ogóle nie jest potrzebna. Jak bowiem wynika z art. 23 ust. 1 pkt 3 ustawy, przetwarzanie danych jest dopuszczalne, gdy jest to konieczne do realizacji umowy, a osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą.

GIODO stoi na stanowisku, że jeśli firma gromadzi dane swojego przyszłego klienta i ma zamiar wykorzystywać je jedynie do celu realizacji umowy, którą z nim zawiera, nie powinna zwracać się w ogóle o zgodę na przetwarzanie danych. Natomiast gdyby firma zamierzała wykorzystać dane swoich klientów w innym celu niż do realizacji lub wykonania umowy zawartej z klientem, nie spełniając przy tym żadnego z warunków określonych w art. 23 ust. 1 pkt 2–5 ustawy o ochronie danych osobowych, o taką zgodę powinna się zwrócić.

Jeżeli więc podmiot planuje wykorzystywać dane swoich klientów czy kontrahentów w innym celu niż realizacja umowy, to powinien wyodrębnić oświadczenia, które musi złożyć taka osoba od oświadczenia związanego z zawieraną umową.

Należy więc przypomnieć, że zgoda osoby, której dane dotyczą, to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie. Zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści.

Zgoda na przetwarzanie danych osobowych może być odwołana w każdym czasie, przy czym odwołanie wywołuje jedynie skutki na przyszłość.

6. Dokument poświadczający zgłoszenie ABI

Prowadzę własną działalność gospodarczą. Postanowiłem powołać w mojej firmie administratora bezpieczeństwa informacji. W jaki sposób mogę sprawdzić, czy został on prawidłowo zarejestrowany?

Przede wszystkim Czytelnik może wystąpić do Generalnego Inspektora Ochrony Danych Osobowych o wydanie zaświadczenia potwierdzającego zarejestrowanie administratora bezpieczeństwa informacji (ABI). Taka możliwość wynika wprost z art. 46b ust. 4 ustawy o ochronie danych osobowych. Za wydanie takiego zaświadczenia należy uiścić opłatę skarbową w wysokości 17 zł.

Administratorzy bezpieczeństwa informacji wpisywani są do rejestru prowadzonego przez Generalnego Inspektora, który jest jawny i publicznie dostępny. Tam również Czytelnik może sprawdzić, czy powołany w jego firmie ABI figuruje we właściwym rejestrze. Aplikacja Rejestr Administratorów Bezpieczeństwa Informacji dostępna jest pod adresem https://egiodo.giodo.gov.pl. Wyszukiwanie ABI możliwe jest według następujących kryteriów: nazwa administratora danych, REGON oraz dane adresowe, takie jak: nazwa miejscowości będącej siedzibą administratora danych, kod pocztowy i nazwa ulicy.

7. Powierzenie danych osobowych zewnętrznej firmie

Biuro zajmuje się obsługą kadrową firm, na ich zlecenie. Czy do umów z klientami należy wprowadzić postanowienia dotyczące przekazywanych nam danych osobowych pracowników tych firm i ich klientów?

TAK. Mamy tu do czynienia z powierzeniem przez klientów firmie Czytelników przetwarzania danych osobowych. Administrator danych może powierzyć innemu podmiotowi przetwarzanie danych, w drodze umowy zawartej na piśmie – pozwala na to art. 31 ustawy o ochronie danych osobowych. Konieczne jest zatem zawarcie umowy o powierzenie przetwarzania danych osobowych – może to być odrębny dokument lub dodatkowe postanowienia do umowy zawieranej z klientem, np. o świadczenie usług. Należy w niej wskazać zakres danych (ich rodzaj) i cel przetwarzania danych (do czego są przeznaczone). Podmiot, któremu powierzono przetwarzanie danych, może je wykorzystywać tylko i wyłącznie w zakresie i celu wskazanym w umowie.

Podmiot, któremu w tym trybie przekazano dane osobowe do przetwarzania (np. przygotowywania list płac) ma szereg obowiązków, mimo że nie jest on administratorem tych danych. Musi on przetwarzać dane zgodnie z umową powierzenia. Ma obowiązki związane z zabezpieczeniem danych i prowadzeniem dokumentacji. Przed rozpoczęciem przetwarzania danych musi zastosować środki zabezpieczające zbiór danych, o których mowa w ustawie o ochronie danych osobowych. W szczególności zobowiązany jest do wprowadzenia dokumentacji (polityki bezpieczeństwa oraz instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych), dopuszczenia do przetwarzania danych wyłącznie osób posiadających upoważnienie nadane przez administratora danych, prowadzenia ewidencji osób upoważnionych do przetwarzania danych. Może również powołać administratora bezpieczeństwa informacji.

8. Przetwarzanie danych przez biura rachunkowe

W ramach prowadzenia spraw kadrowych biuro rachunkowe przetwarza dane osobowe pracowników firm, z którymi ma podpisane umowy o obsługę kadrową. Jakie dokumenty (upoważnienia) powinni posiadać pracownicy biura, mający dostęp do danych osobowych? Czy każdy pracodawca musi powołać administratora bezpieczeństwa informacji i zgłosić go do GIODO?

Pracownicy, którzy z racji pełnionych obowiązków służbowych mają dostęp do danych osobowych, powinni posiadać pisemne upoważnienie do przetwarzania danych osobowych wystawione przez administratora danych. Administratorem danych jest m.in. pracodawca, który gromadzi dane o kandydatach do zatrudnienia, pracownikach i byłych pracownikach. Zgodnie z art. 37 ustawy o ochronie danych osobowych, musi on wystawić pisemne upoważnienie dla osób, które nie mają statusu administratora danych, ale mają do nich dostęp. W związku z tym, jeżeli pracodawcą jest biuro rachunkowe i zatrudnia pracowników prowadzących sprawy kadrowe, wówczas musi udzielić im upoważnienia do takich czynności. Natomiast przekazanie upoważnienia do przetwarzania danych biuru rachunkowemu jako podmiotowi realizującemu określone usługi, następuje na mocy umowy zawartej między daną firmą a biurem (art. 31 ustawy o ochronie danych osobowych).

Odnośnie powołania administratora bezpieczeństwa informacji (ABI), to obecnie pracodawca może to uczynić, ale nie musi. Przy czym, jeżeli pracodawca nie wyznaczy ABI, to musi sam wykonywać jego zadania, z wyłączeniem obowiązku sporządzania sprawozdania i prowadzenia wewnętrznego rejestru zbiorów danych przetwarzanych przez administratora danych.

9. Sprzedaż w internecie a obowiązki wobec GIODO

Prowadzę działalność gospodarczą, w ramach której sprzedaję towary za pośrednictwem serwisu aukcyjnego. Zbieram dane klientów potrzebne mi tylko do zawarcia umowy i wystawienia faktury. Czy jestem zobowiązany rejestrować zbiory danych osobowych moich klientów u GIODO?

Regulacjom ustawy o ochronnie danych osobowych podlegają osoby fizyczne i osoby prawne oraz jednostki organizacyjne niebędące osobami prawnymi, jeżeli przetwarzają dane osobowe w związku z działalnością zarobkową, zawodową lub dla realizacji celów statutowych.

Niewątpliwie osoba fizyczna prowadząca działalność gospodarczą polegającą na sprzedaży towarów poprzez serwisy aukcyjne przetwarza dane osobowe swoich klientów, które są jej niezbędne do zawarcia umowy sprzedaży, wysłania towaru i wystawienia faktury. Przedsiębiorca posiada w takim przypadku status administratora danych i jeżeli nie powołuje w swojej firmie administratora bezpieczeństwa informacji (ABI), na podstawie art. 43 ust. 1a ustawy o ochronie danych osobowych, zobowiązany jest zgłosić zbiór danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych.

Z obowiązku rejestracji zbioru danych u Generalnego Inspektora Ochrony Danych Osobowych zwolnieni są administratorzy danych przetwarzanych wyłącznie w celu wystawienia faktury, rachunku lub prowadzenia sprawozdawczości finansowej. Tak wynika z art. 43 ust. 1 pkt 8 ustawy.

Jednak w praktyce sklepy internetowe oraz przedsiębiorcy dokonujący sprzedaży za pośrednictwem portali aukcyjnych zbierają dane osobowe swoich klientów również w innych celach, np. w momencie, gdy klienci dokonują rejestracji w bazie sklepu (bazie przedsiębiorcy), przetwarzają je w celach marketingowych, do rozsyłania newsletterów, informacji handlowych itp. W takich przypadkach zgłoszenie zbioru danych do GIODO jest konieczne.

Jeśli administrator danych powoła ABI i zgłosi go do rejestracji GIODO, zwolniony jest z obowiązku rejestracji zbiorów danych u Generalnego Inspektora (z wyjątkiem zbiorów zawierających dane szczególnie chronione).

Zgłoszenia zbioru do rejestracji należy dokonać przed rozpoczęciem przetwarzania danych, czyli przed pierwszą czynnością, jaką administrator może wykonać na danych, tj. przed pozyskaniem pierwszych danych do zbioru. Zgodnie bowiem z art. 46 ust. 1 ustawy, administrator danych może rozpocząć ich przetwarzanie w zbiorze po jego zgłoszeniu do rejestracji Generalnemu Inspektorowi.

Podstawa prawna
Ustawa z dnia 29.08.1997 r. o ochronie danych osobowych (Dz. U. z 2015 r. poz. 2135 ze zm.)

10. Czy dane pracowników i ich rodzin trzeba zgłaszać do GIODO?

Spółka planuje zatrudnić na podstawie umowy o pracę dwie osoby. Czy będzie zobowiązana zarejestrować u Generalnego Inspektora Ochrony Danych Osobowych zbiory danych zawierające podania o pracę? Czy w związku z tym, że w zbiorach danych przyjętych pracowników będą znajdować się również dane ich rodzin, m.in. małżonków i ich dzieci, powinny one podlegać zgłoszeniu?

Ustawa o ochronie danych osobowych przewiduje zwolnienie z obowiązku rejestracji tego rodzaju zbiorów.

Administrator danych (np. osoba fizyczna prowadząca działalność gospodarczą), co do zasady, zobowiązany jest zgłosić zbiór danych osobowych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych. Z obowiązku rejestracji zwolnieni są administratorzy danych wymienieni w art. 43 ust. 1 i 1a ustawy oraz ci administratorzy, którzy powołają administratorów bezpieczeństwa informacji, jednocześnie nie przetwarzając danych wrażliwych, jak np. informacji o stanie zdrowia. Wspomniana ustawa zwalnia z obowiązku rejestracji u GIODO administratorów danych przetwarzanych np. w związku z zatrudnieniem u nich (art. 43 ust. 1 pkt 4 ustawy). Dotyczy to zbiorów aktualnych i byłych pracowników, a także kandydatów do pracy.

Warto natomiast pamiętać, że zwolnienie z wymogu rejestracyjnego u GIODO nie oznacza, że administrator danych nie ma obowiązku przestrzegania zasad związanych z przetwarzaniem danych osobowych i poszanowania praw osób, których dane dotyczą.

Odpowiadając na drugie pytanie należy stwierdzić, że na mocy art. 22^1 § 1 Kodeksu pracy (Dz. U. z 2014 r. poz. 1502 ze zm.) pracodawca ma prawo żądać od osoby ubiegającej się o zatrudnienie podania danych osobowych obejmujących: imię (imiona) i nazwisko, imiona rodziców, datę urodzenia, miejsce zamieszkania (adres do korespondencji), wykształcenie, przebieg dotychczasowego zatrudnienia. Ponadto na mocy art. 22^1 § 2 tej ustawy pracodawca może też żądać innych danych osobowych pracownika, a także imion i nazwisk oraz dat urodzenia dzieci pracownika, jeżeli podanie takich danych jest konieczne ze względu na korzystanie przez pracownika ze szczególnych uprawnień przewidzianych w prawie pracy.

Jak informuje GIODO na swojej stronie internetowej, tj. www.giodo.gov.pl, „Dane osobowe członków rodzin pracownika należą w istocie do danych pracownika. Ich przetwarzanie związane jest z zatrudnieniem pracownika i wynika z konieczności wywiązywania się przez pracodawców z obowiązków, jakie względem pracowników ciążą na nich na mocy przepisu prawa pracy (...). Przetwarzanie danych członków rodzin pracowników nie jest zatem celem samym w sobie, lecz dane te są ściśle związane z danymi pracownika". Pracodawcy zwolnieni są więc z obowiązku rejestrowania zbioru danych zawierającego dane osobowe członków rodzin osób u nich zatrudnionych.

11. Upoważnienie pracowników do dostępu do danych klientów

Prowadzę sklep internetowy. Oprócz mnie obsługą zamówień zajmują się jeszcze dwie osoby. Czy każda z nich powinna się logować do panelu sklepu własnym hasłem? Czy w związku z tym, że osoby te mają dostęp do danych osobowych klientów, muszę dopełnić jakiś formalności?

Administrator danych osobowych ma obowiązek prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych. Wynika on z art. 39 ust. 1 ustawy o ochronie danych osobowych. Ewidencja ta powinna zawierać:
- imię i nazwisko osoby upoważnionej,
- datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych,
- identyfikator, jeżeli dane są przetwarzane w systemie informatycznym.

Zatem dostęp do danych osobowych musi być kontrolowany, a osoby, które z danymi pracują, muszą dysponować stosownym upoważnieniem i być wpisane do ewidencji osób upoważnionych do przetwarzania danych. Taka ewidencja powinna stanowić wyodrębniony dokument administratora danych. Można w niej odnotowywać również inne informacje, np. o stanowiskach zajmowanych przez osoby upoważnione do przetwarzania danych, co pozwala ocenić, czy prawidłowo został określony zakres upoważnienia do dostępu do poszczególnych danych. Dostęp do danych przyznany pracownikom może być różny. Konkretny pracownik może mieć dostęp do takich danych, które mają związek z jego obowiązkami, a nie do wszystkich danych w systemie.

W przypadku danych przetwarzanych w systemie informatycznym (np. przy obsłudze sklepu internetowego) osoba upoważniona powinna logować się swoim identyfikatorem (loginem) i hasłem. Niedopuszczalna jest sytuacja, w której kilka osób korzysta ze wspólnego loginu i hasła.

Jednym z podstawowych obowiązków spoczywających na administratorze, wynikającym z art. 36 ust. 1 ustawy o ochronie danych osobowych, jest obowiązek zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, a w szczególności zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym. Stosownie zaś do treści art. 37 ustawy do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych.