Ochrona danych osobowych

Katarzyna Łotowska

Sokółka, 14 marca 2017

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych

Za **dane osobowe** uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne.

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych

Zbiór danych – rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych

System informatyczny – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;

Usuwanie danych – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą.

Kiedy przetwarzamy dane osobowe:

- osoba, której dane dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych;
- jest to niezbędne dla zrealizowania usprawnienia 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
- 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.

Polityka bezpieczeństwa ochrony danych osobowych zawiera przede wszystkim:

- 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.

Polityka bezpieczeństwa ochrony danych osobowych

Polityka powinna zostać przyjęta uchwałą.

Administratorem Danych Osobowych (ADO) jest organizacja.

Zadania Administratora Danych Osobowych:

- obowiązek informacyjny wypełniany przy zbieraniu danych osobowych (art. 24 i 25 ustawy)
- szczególna staranność przy przetwarzaniu danych osobowych w celu ochrony interesów osób, których dane przetwarza (art. 26 ustawy)
- udzielanie informacji o zakresie przetwarzanych danych osobowych (art. 33 ustawy)
- obowiązek uzupełniania, uaktualnienia, sprostowania danych, czasowego lub stałego wstrzymania przetwarzania kwestionowanych danych lub ich usunięcia ze zbioru, gdy zażąda tego osoba, której dane są przetwarzane przez administratora (art. 35 ustawy)

Zadania Administratora Danych Osobowych:

- obowiązek stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną (art. 36 ustawy)
- kontroluje, jakie dane, kiedy i przez kogo zostały wprowadzone do zbioru i komu są przekazywane (art. 38 ustawy)
- prowadzi ewidencje osób upoważnionych do przetwarzania danych osobowych (art. 39 ustawy)
- zgłasza zbiór do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych w przypadkach przewidzianych prawem (art. 40 ustawy)

Zbiór danych osobowych

- Obowiązkowa rejestracja zbiorów, o ile nie zawierają one danych wrażliwych, nie podlega ADO, który powołał i zgłosił do GIODO administratora bezpieczeństwa informacji (ABI)
- Oznacza to, że przetwarzająca dane zwykłe organizacja, która wyznaczyła w swojej organizacji ABI oraz wypełniła odpowiednie zgłoszenie i przesłał je do biura GIODO, w ogóle nie musi zgłaszać zbiorów danych do GIODO.
- Organizacja, która nie powołuje ABI – musi zgłosić zbiór do GIODO

Dane wrażliwe:

- ujawniających pochodzenie rasowe lub etniczne,
- poglądy polityczne,
- przekonania religijne lub filozoficzne,
- przynależność wyznaniową, partyjną lub związkową,
- o stanie zdrowia,
- kodzie genetycznym,
- nałogach,
- życiu seksualnym
- dotyczących skazań, mandatów karnych, orzeczeń wydanych w postepowaniu sądowym lub administracyjnym

Wyjątki - nie rejestruje się zbiorów:

- zawierających informacje niejawne;
- które zostały uzyskane w wyniku czynności operacyjno-rozpoznawczych przez funkcjonariuszy organów uprawnionych do tych czynności;
- przetwarzanych przez właściwe organy dla potrzeb postępowania sądowego oraz na podstawie przepisów o Krajowym Rejestrze Karnym;
- przetwarzanych przez Generalnego Inspektora Informacji Finansowej;
- przetwarzanych przez właściwe organy na potrzeby udziału Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym;

Wyjątki - nie rejestruje się zbiorów:

- przetwarzanych przez właściwe organy na podstawie przepisów o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej;
- dotyczących osób należących do kościoła lub innego związku wyznaniowego, o uregulowanej sytuacji prawnej, przetwarzanych na potrzeby tego kościoła lub związku wyznaniowego;
- 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;

Wyjątki - nie rejestruje się zbiorów:

- tworzonych na podstawie przepisów dotyczących wyborów do Sejmu, Senatu, Parlamentu Europejskiego, rad gmin, rad powiatów i sejmików województw, wyborów na urząd Prezydenta Rzeczypospolitej Polskiej, na wójta, burmistrza, prezydenta miasta oraz dotyczących referendum ogólnokrajowego i referendum lokalnego;
- dotyczących osób pozbawionych wolności na podstawie ustawy, w zakresie niezbędnym do wykonania tymczasowego aresztowania lub kary pozbawienia wolności;
- przetwarzanych wyłącznie w celu wystawienia faktury, rachunku lub prowadzenia sprawozdawczości finansowej;
- powszechnie dostępnych;

Administrator Bezpieczeństwa Informacji

Wyznaczenie

Administratora Bezpieczeństwa Informacji (ABI) nie jest obowiązkiem

jest to osoba wyznaczona w organizacji, która odpowiada za ochronę wszystkich danych osobowych w organizacji.

Nie może to być członek zarządu.

Administrator Bezpieczeństwa Informacji

Zgłoszenie ABI:

- oznaczenie organizacji (czyli ADO),
- dane administratora bezpieczeństwa informacji (imię i nazwisko, numer PESEL, adres do korespondencji, jeśli jest inny niż adres siedziby ADO),
- datę powołania,
- oświadczenie, że powołany przez niego ABI spełnia warunki określone w art. 36a ust. 5 i 7.

Termin na zgłoszenie: 30 dni.

(Formularz ze strony GIODO)

Administrator Bezpieczeństwa Informacji

Kto może być ABI? 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.**

ABI musi mieć wiedzę, (więc nikt przypadkowy nie powinien być.

Nie ma wytycznych jak weryfikować wiedzę!

Co zawiera rejestr zbiorów danych osobowych ABI:

- Pozycja
- Nazwa zbioru danych
- Oznaczenie administratora danych
- Oznaczenie przedstawiciela – art.31a ustawy
- Powierzenie przetwarzania danych
- Podstawa prawna prowadzenia zbioru danych
- Cel przetwarzania danych
- Kategorie osób, których dane dotyczą
- Zakres przetwarzanych danych

Co zawiera rejestr zbiorów danych osobowych ABI:

- Sposób zbierania danych
- Sposób udostępniania danych
- Oznaczenie odbiorcy danych
- Przekazywanie danych do państwa trzeciego
- Data wpisu do rejestru
- Data aktualizacji

Rejestr jest jawny.

Rejestr zbiorów danych osobowych ABI:

Administrator bezpieczeństwa informacji odnotowuje historię zmian w rejestrze (ale nie w danych!) zawierającą:

- informację o rodzaju zmiany (nowy wpis, aktualizacja, wykreślenie);
- datę dokonania zmiany;
- informację o zakresie zmiany.

Sprawdzenie:

Sprawdzenie jest dokonywane:

- dla administratora danych
- dla Generalnego Inspektora Ochrony Danych Osobowych

Sprawdzenie:

Sprawdzenie jest przeprowadzane w trybie:

- sprawdzenia planowego – według planu sprawdzeń,
- sprawdzenia doraźnego – w przypadku naruszeniu ochrony danych osobowych lub uzasadnionego podejrzenia wystąpienia takiego naruszenia;
- w przypadku zwrócenia się o dokonanie sprawdzenia przez GIODO.

Sprawdzenie:

- Plan sprawdzeń jest przygotowywany przez ABI/ADO na okres nie krótszy niż kwartał i nie dłuższy niż rok.
- Plan sprawdzeń jest przedstawiany ADO nie później niż na dwa tygodnie przed dniem rozpoczęcia okresu objętego planem.
- 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.

Sprawdzenie:

I. ABI - sprawozdanie.

Sprawozdanie jest sporządzane w postaci elektronicznej albo w postaci papierowej.

Administrator bezpieczeństwa informacji przekazuje administratorowi danych sprawozdanie:

- ze sprawdzenia planowego – nie później niż w terminie 30 dni od zakończenia sprawdzenia;
- ze sprawdzenia doraźnego – niezwłocznie po zakończeniu sprawdzenia;
- ze sprawdzenia, o którego dokonanie zwrócił się Generalny Inspektor – zachowując termin wskazany przez GIODO.

II. ADO – protokół ze sprawdzenia

Upoważnienie:

- podstawa prawna (art. 37),
- imię i nazwisko osoby upoważnionej,
- nazwę zbioru danych osobowych,
- zakres upoważnienia,
- zobowiązanie do zachowania tajemnicy,
- termin ważności,
- możliwość wygaśnięcia upoważnienia,
- nakaz zwrotu oryginału,

Ewidencja:

- imię i nazwisko osoby upoważnionej,
- datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych,
- identyfikator, jeżeli dane są przetwarzane w systemie informatycznym.

Oświadczenie:

- podstawa prawna (art. 23 ust. 1),
- imię i nazwisko osoby, od której dane są zbierane,
- wyrażenie zgody,
- nazwę, adres administratora danych osobowych,
- nazwę zbioru danych osobowych,
- cel przetwarzania,
- informacja o możliwości zmiany i odwołania zgodny na przetwarzanie.

Przechowywanie danych osobowych

- W systemach informatycznych - musza być w szczególny sposób zabezpieczone.
- Pomieszczenie powinno umożliwiać swobodne przeglądanie danych osobowych.
- Dane osobowe powinny być przechowywane w sposób uniemożliwiający dostęp osób trzecich.
- Dane osobowe w wersji papierowej powinny być przechowywane w „teczkach”, by przeglądając kartotekę nie można było widzieć wszystkich informacji.

Prawa osoby, której dane dotyczą

Każdej osobie przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych, a zwłaszcza prawo do:

1) uzyskania wyczerpującej informacji, czy taki zbiór istnieje, oraz do ustalenia administratora danych, adresu jego siedziby i pełnej nazwy, a w przypadku gdy administratorem danych jest osoba fizyczna – jej miejsca zamieszkania oraz imienia i nazwiska;

2) uzyskania informacji o celu, zakresie i sposobie przetwarzania danych zawartych w takim zbiorze;

3) uzyskania informacji, od kiedy przetwarza się w zbiorze dane jej dotyczące, oraz podania w powszechnie zrozumiałej formie treści tych danych;

Prawa osoby, której dane dotyczą

4) uzyskania informacji o źródle, z którego pochodzą dane jej dotyczące, chyba że administrator danych jest zobowiązany do zachowania w tym zakresie w tajemnicy informacji niejawnych lub zachowania tajemnicy zawodowej;

5) uzyskania informacji o sposobie udostępniania danych, a w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym dane te są udostępniane;

6) uzyskania informacji o przesłankach podjęcia rozstrzygnięcia sprawy,

7) żądania uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego wstrzymania ich przetwarzania lub ich usunięcia, jeżeli są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są już zbędne do realizacji celu, dla którego zostały zebrane;

7) wniesienia, w przypadkach wymienionych w art. 23 ust. 1 pkt 4 i 5, pisemnego, umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację;

8) wniesienia sprzeciwu wobec przetwarzania jej danych w przypadkach, wymienionych w art. 23 ust. 1 pkt 4 i 5, gdy administrator danych zamierza je

Prawa osoby, której dane dotyczą

W razie wniesienia sprzeciwu, dalsze przetwarzanie kwestionowanych danych jest niedopuszczalne. Administrator danych może jednak pozostawić w zbiorze imię lub imiona i nazwisko osoby oraz numer PESEL lub adres wyłącznie w celu uniknięcia ponownego wykorzystania danych tej osoby w celach objętych sprzeciwem.

Jeżeli dane są przetwarzane dla celów naukowych, dydaktycznych, historycznych, statystycznych lub archiwalnych, administrator danych może odstąpić od informowania osób o przetwarzaniu ich danych w przypadkach, gdy pociągałoby to za sobą nakłady niewspółmierne z zamierzonym celem.

www.giodo.gov.pl

Katarzyna Łotowska