Ochrona danych osobowych w Polsce

Spis treści:

***

1. Ochrona danych osobowych w Polsce

Na poziomie europejskim, problematyka ochrony danych osobowych uregulowana została w (stanowiącej podstawę polskich regulacji) Dyrektywie 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych. Obowiązuje ona do dnia 25 maja 2018 r. - z którym to dniem jej postanowienia przestaną obowiązywać (zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady nr 2016/679 z dnia 27 kwietnia 2016 r.) i zostaną zastąpione przez zmodernizowaną regulację, dostosowaną do współczesnych realiów przetwarzania danych.

Od wejścia w życie Traktatu Lizbońskiego, zasada ochrony danych osobowych każdej osoby fizycznej zawarta jest także w regulacji o fundamentalnym znaczeniu dla Unii jakim jest Traktat o Funkcjonowaniu Unii Europejskiej - jego art. 16 stanowi, że „Każda osoba ma prawo do ochrony danych osobowych jej dotyczących".

Zagadnienia dotyczące ochrony danych osobowych zostały w prawie polskim uregulowane po raz pierwszy w roku 1997 - w art. 51 Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. oraz - w sposób kompleksowy - w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

Oprócz podstawowej ustawy o ochronie danych osobowych - w polskim porządku prawnym funkcjonują ponadto rozporządzenia (akty wykonawcze do ww. ustawy), z których najważniejsze z perspektywy przedsiębiorcy przetwarzającego dane osobowe to rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych oraz rozporządzenie Ministra Administracji i Cyfryzacji z dnia 10 grudnia 2014 r. w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji.

2. Podstawowe definicje i pojęcia związane z ochroną danych osobowych

Dane osobowe - to informacje o osobach fizycznych. Dotyczą one osoby zidentyfikowanej lub możliwej do zidentyfikowania bezpośrednio (np. na podstawie danych posiadanych przez administratora) lub pośrednio (na podstawie danych, do których administrator jest w stanie stosunkowo łatwo dotrzeć - bez nadmiernych kosztów, czasu lub działań).

Nie ma ustawowego katalogu danych osobowych, jednakże wskazuje się, że danymi osobowymi są w szczególności numer identyfikacyjny, czynniki określające cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Dane osobowe mogą mieć formę alfabetyczna, cyfrową, zdjęcia, video, dźwięku lub np. danych biometrycznych (odciski palców, obraz tęczówki). Np. adres e-mail może stanowić dane osobowe.

Dane osobowe wrażliwe - kategoria danych osobowych objętych szczególną ochroną, których przetwarzanie jest poddane zasadom bardziej rygorystycznym niż przetwarzanie innych kategorii danych osobowych. Ich przetwarzanie jest co do zasady zabronione, a dopuszczalne jedynie w szczególnych, ściśle określonych w ustawie okolicznościach.

Danymi osobowymi wrażliwymi są informacje (katalog zamknięty) - ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, dane o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz dane dotyczące skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

Osoba, której dane dotyczą - sformułowanie którym posługuje się polska ustawa o ochronie danych osobowych - każda osoba fizyczna, bez względu na jej obywatelstwo, wiek czy też zdolność do czynności prawnych. Ustawy nie stosuje się do danych dotyczących osób zmarłych oraz (w części) do jawnych danych i informacji udostępnianych w ramach Centralnej Ewidencji i Informacji o Działalności Gospodarczej.

Przetwarzanie danych osobowych - to jakiekolwiek operacje wykonywane na danych osobowych od ich zebrania do usunięcia, przykładowo: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie (niszczenie danych osobowych lub ich modyfikacja, która uniemożliwia ustalenie tożsamości osoby, której dane dotyczą). Przetwarzanie może się odbywać w systemie informatycznym lub metodami tradycyjnymi (w segregatorach, skorowidzach, księgach).

Administrator danych osobowych - może być podmiotem publicznym lub prywatnym. To podmiot (np. jednostka organizacyjna, organ władzy publicznej, osoba) decydująca o celach i środkach przetwarzania danych osobowych.

W przypadku spółki administratorem danych osobowych jest sama spółka, nie zaś jej organy, osoby zasiadające w organach tej spółki lub pełniące w niej funkcje kierownicze. W przypadku organów państwowych, organów samorządu terytorialnego oraz państwowych i komunalnych jednostek organizacyjnych, organy takie uznaje się za jednego administratora, jeżeli przetwarzanie danych służy temu samemu interesowi publicznemu.

Administrator decyduje o tym jakie dane zbiera, do czego je przetwarza i czy przetwarza je sam czy np. powierza dane do przetwarzania osobom trzecim (np. outsourcując te czynności).

Polską ustawę stosuje się do administratorów, którzy mają siedzibę albo miejsce zamieszkania na terytorium Rzeczypospolitej Polskiej, albo w państwie trzecim (nienależącym do Europejskiego Obszaru Gospodarczego), o ile przetwarzają dane osobowe przy wykorzystaniu środków technicznych znajdujących się na terytorium Rzeczypospolitej Polskiej. Stosowanie ustawy jest wyłączone, jeśli środki techniczne znajdujące się na terenie Polski służą wyłącznie do przekazywania danych (tranzytu).

Administrator bezpieczeństwa informacji - osoba, posiadająca pełną zdolność do czynności prawnych oraz pełnię praw publicznych, niekarana za przestępstwo umyślne i posiadająca odpowiednią wiedzę w zakresie ochrony danych osobowych. Może zostać powołana przez Administratora danych osobowych. Jego rolą jest zapewnienie przestrzegania przepisów o ochronie danych osobowych w organizacji. Administrator bezpieczeństwa informacji podlega bezpośrednio kierownikowi jednostki organizacyjnej lub osobie fizycznej będącej administratorem danych. Administrator danych może powołać zastępców administratora bezpieczeństwa informacji.

Zbiór danych osobowych - posiadający strukturę zestaw danych osobowych, dostępnych według określonych kryteriów (osobowych - takich jak imię, nazwisko, data urodzenia, lub też nieosobowych - np. data wprowadzenia danych do zbioru). Zestaw ten może być rozproszony lub podzielony funkcjonalnie. W przypadku danych osobowych przetwarzanych w systemach informatycznych, ustawę stosuje się zarówno do danych przetwarzanych w zbiorach, jak i poza nimi, jednakże w przypadku przetwarzania metodami tradycyjnymi, przetwarzanie danych w zbiorze jest warunkiem stosowania ustawy.

Przetwarzający dane osobowe - podmiot przetwarzający dane osobowe, którym może być sam administrator danych osobowych, osoba upoważniona przez administratora do przetwarzania (np. pracownik, do którego zadań należy przetwarzanie danych osobowych) lub podmiot zewnętrzny, któremu powierzono przetwarzanie danych osobowych w drodze umowy zawartej na piśmie. Z taką sytuacją mamy do czynienia np. przy outsourcowaniu usług. Należy pamiętać, że podmiot upoważniony ani przetwarzający dane osobowe na podstawie umowy powierzenia przetwarzania danych, nie staje się administratorem.

Pojęcie przetwarzającego nie musi być przypisane do jednego podmiotu w odniesieniu do jednego zbioru danych osobowych - możliwe jest częściowe przetwarzanie danych przez administratora, a częściowe ich powierzenie lub też powierzenie przetwarzania kilku podmiotom.

3. Obowiązki administratora danych osobowych

Administrator danych osobowych jest podmiotem odpowiedzialnym za przetwarzanie danych osobowych. Oznacza to, że z jednej strony przysługują mu ważne uprawnienia (decyduje on o celach i środkach przetwarzania danych), jednak z drugiej strony ciążą na nim liczne obowiązki i ponosi on konsekwencje przetwarzania danych niezgodnie z ustawą o ochronie danych osobowych.

Podstawowe obowiązki administratora danych to:

- spełnienie jednej ze wskazanych w ustawie przesłanek legalizujących przetwarzanie danych osobowych (przesłanki te opisano szerzej w części 4 niniejszego opracowania);
- obowiązek informacyjny związany z pozyskaniem danych;
- obowiązek dochowania szczególnej staranności przy przetwarzaniu danych, w celu ochrony interesów osób, których dane dotyczą;
- obowiązek zabezpieczenia danych;
- obowiązek zgłoszenia zbioru danych osobowych do rejestru zbiorów danych prowadzonego przez Generalnego Inspektora Ochrony Danych Osobowych, z wyłączeniem sytuacji przetwarzania danych w zbiorze zwolnionym z obowiązku rejestracji (zagadnienia związane z rejestracją zbiorów opisano szerzej w części 7 niniejszego opracowania);
- obowiązek prowadzenia dokumentacji związanej z przetwarzaniem danych osobowych (dokumentację, do której prowadzenia zobowiązany jest administrator danych osobowych, opisano szerzej w części 5 niniejszego opracowania).

Obowiązek informacyjny związany z pozyskaniem danych

Każdy administrator danych osobowych, bez względu na sposób, w jaki wszedł w posiadanie danych osobowych (czy pozyskał je od osoby, której dane dotyczą, czy tez od innego podmiotu - np. przez zakup bazy danych), ma obowiązek poinformowania osoby, której dane dotyczą o tym, że przetwarza jej dane.

W przypadku zbierania danych osobowych od osoby, której one dotyczą, administrator danych osobowych ma obowiązek poinformowania jej o:

- adresie swojej siedziby i pełnej nazwie (w przypadku gdy administratorem danych jest osoba fizyczna, informuje ona o swoim miejscu zamieszkania oraz imieniu i nazwisku);
- celu zbierania danych osobowych;
- przewidywanych odbiorcach lub kategoriach odbiorców danych;
- prawie dostępu do treści swoich danych oraz ich poprawiania;
- dobrowolności albo obowiązku podania danych (jeżeli taki obowiązek istnieje, o jego podstawie prawnej).

W przypadku zbierania danych osobowych nie od osoby, której one dotyczą, administrator danych osobowych ma obowiązek poinformowania tej osoby, bezpośrednio po utrwaleniu zebranych danych, o:

- adresie swojej siedziby i pełnej nazwie (w przypadku gdy administratorem danych jest osoba fizyczna, informuje ona o swoim miejscu zamieszkania oraz imieniu i nazwisku);
- celu zbierania danych;
- zakresie zbierania danych;
- odbiorcach lub kategoriach odbiorców danych;
- źródle danych;
- prawie dostępu do treści swoich danych oraz ich poprawiania;
- prawie wniesienia pisemnego, umotywowanego żądania zaprzestania przetwarzania danych osobowych ze względu na jej szczególną sytuację;
- prawie wniesienia sprzeciwu wobec przetwarzania danych osobowych, gdy administrator danych zamierza je przetwarzać w celach marketingowych lub wobec przekazywania jej danych osobowych innemu administratorowi danych.

Obowiązek dochowania szczególnej staranności przy przetwarzaniu danych w celu ochrony interesów osób, których dane dotyczą.

Administrator danych osobowych ma obowiązek zapewnienia, że przetwarzanie przez niego danych osobowych jest zgodne z następującymi zasadami:

- legalności - przetwarzanie opiera się na jednej z podstaw wskazanych w ustawie o ochronie danych osobowych, odbywa się na zasadach określonych w tej ustawie, a także jest zgodne z

postanowieniami innych ustaw (np. przetwarzanie danych osobowych pracowników musi być zgodne nie tylko z ustawą o ochronie danych osobowych, ale także z regulacjami zawartymi w Kodeksie pracy);
- celowości - prawidłowa realizacja tej zasady oznacza zbieranie danych osobowych dla wyraźnie oznaczonych, zgodnych z prawem celów;
- związania celem przetwarzania - zabronione jest przetwarzanie danych osobowych niezgodne z celem, dla którego zostały zebrane;
- merytorycznej poprawności - obowiązkiem administratora jest dbanie o to, by przetwarzane przez niego dane osobowe były prawdziwe i aktualne;
- adekwatności - zakres przetwarzanych danych osobowych musi być adekwatny do celu, w jakim są one przetwarzane; zabronione jest przetwarzanie danych osobowych w zakresie szerszym, niż jest to niezbędne dla realizacji celu przetwarzania;
- ograniczonego czasu przetwarzania - dane osobowe mogą być przetwarzane tylko przez czas niezbędny do realizacji celu ich przetwarzania; gdy cel ten wygasa, konieczne jest usunięcie danych.

Obowiązek zabezpieczenia danych

Administrator danych osobowych ma obowiązek zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. W celu realizacji tego obowiązku, musi on stosować środki techniczne i organizacyjne odpowiednie do kategorii przetwarzanych danych oraz występujących zagrożeń.

Realizacja wskazanego obowiązku opiera się przede wszystkim na technicznym zabezpieczeniu danych osobowych, dbaniu o to, żeby do ich przetwarzania dopuszczone były wyłącznie osoby posiadające nadane przez administratora danych upoważnienia oraz kontrolowaniu tego jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone, a także komu są przekazywane.

Szczegółowe regulacje dotyczące bezpieczeństwa przetwarzania danych osobowych zawiera rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. 2004, Nr 100, poz. 1024).

4. Podstawy przetwarzania danych osobowych - przesłanki legalizujące przetwarzanie

Podmiot pragnący przetwarzać dane osobowe musi zadbać, aby zachodziła któraś z określonych w ustawie o ochronie danych osobowych przesłanek legalizujących przetwarzanie. W ustawie wskazano dwa zamknięte katalogi przesłanek - jeden wskazujący sytuacje, w których dopuszczalne jest przetwarzanie tzw. danych osobowych zwykłych oraz drugi, dotyczący danych osobowych wrażliwych.

Co do zasady przetwarzanie danych osobowych jest dopuszczalne tylko wtedy, gdy zachodzi co najmniej jedna z następujących przesłanek:
- osoba, której dane dotyczą wyraziła zgodę na przetwarzanie jej danych - zgoda musi być wyraźna i wyrażona świadomie, nie może ona być domniemana lub dorozumiana z oświadczenia woli o innej treści (zgoda nie jest konieczna jedynie do usunięcia danych osobowych);
- przetwarzanie odbywa się na podstawie przepisu prawa, ustanawiającego uprawnienia lub obowiązki;
- jest to konieczne do realizacji umowy, której osoba, której dane dotyczą, jest stroną lub też do podjęcia działań przed zawarciem umowy na żądanie tej osoby;
- 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 (prawnie usprawiedliwione cele to, m.in. marketing bezpośredni własnych produktów lub usług administratora danych oraz dochodzenie roszczeń z tytułu prowadzonej działalności gospodarczej), a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.

Przesłanki przetwarzania danych osobowych określanych mianem wrażliwych są bardziej rygorystyczne, niż przesłanki pozwalające na przetwarzanie innych kategorii danych osobowych.

Co do zasady przetwarzanie danych osobowych wrażliwych jest zabronione, a dopuszczalne jedynie w następujących okolicznościach:

- jeśli osoba, której dane dotyczą, wyraziła na to zgodę (chyba że chodzi o usunięcie dotyczących jej danych) - należy pamiętać, że w przypadku danych wrażliwych zgodna musi być udzielona w formie pisemnej;
- przepis prawa (ustawy innej niż ustawa o ochronie danych osobowych) zezwala na przetwarzanie danych bez zgody osoby, której dane dotyczą, a ponadto stwarza dodatkowe, pełne gwarancje ochrony takich danych osobowych;
- przetwarzanie danych jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby (gdy osoba, której dane dotyczą, nie jest fizycznie lub prawnie zdolna do wyrażenia zgody - do czasu ustanowienia opiekuna prawnego lub kuratora);
- jest to niezbędne do wykonywania statutowych zadań kościołów i związków wyznaniowych, stowarzyszeń, fundacji lub innych niezarobkowych organizacji lub instytucji o celach politycznych, naukowych, religijnych, filozoficznych lub związkowych - oparcie przetwarzania na tej przesłance jest możliwe wyłącznie w odniesieniu do członków tych organizacji lub instytucji albo osób utrzymujących z nimi stałe kontakty w związku z ich działalnością; konieczne jest ponadto zapewnienie pełnych gwarancji ochrony przetwarzanych danych osobowych;
- przetwarzanie dotyczy danych osobowych, które są niezbędne do dochodzenia praw przed sądem;
- przetwarzanie jest niezbędne do wykonania zadań administratora danych osobowych odnoszących się do zatrudnienia pracowników i innych osób, a zakres przetwarzanych danych jest określony w ustawie;
- przetwarzanie jest prowadzone w celu ochrony stanu zdrowia, świadczenia usług medycznych lub leczenia pacjentów przez osoby trudniące się zawodowo leczeniem lub świadczeniem innych usług medycznych, zarządzania udzielaniem usług medycznych i są stworzone pełne gwarancje ochrony danych osobowych;
- przetwarzanie dotyczy danych osobowych, które zostały podane do wiadomości publicznej przez osobę, której dane dotyczą;
- jest to niezbędne do prowadzenia badań naukowych, w tym do przygotowania rozprawy wymaganej do uzyskania dyplomu ukończenia szkoły wyższej lub stopnia naukowego; publikowanie wyników badań naukowych nie może następować w sposób umożliwiający identyfikację osób, których dane zostały przetworzone (konieczna anonimizacja wyników);
- przetwarzanie danych jest prowadzone przez stronę w celu realizacji praw i obowiązków wynikających z orzeczenia wydanego w postępowaniu sądowym lub administracyjnym.

5. Dokumenty administratora danych osobowych

Przetwarzanie danych osobowych wiąże się z koniecznością prowadzenia przez administratora danych odpowiedniej dokumentacji. Zgodnie z ustawą o ochronie danych osobowych oraz rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, na dokumentację taką składają się:

- polityka bezpieczeństwa;

- instrukcja zarządzania systemem informatycznym;
- dokumenty związane z wyznaczeniem administratora bezpieczeństwa informacji;
- upoważnienia do przetwarzania danych osobowych;
- ewidencja osób upoważnionych do przetwarzania danych;
- dokumenty dotyczące rejestracji zbiorów danych.

Polityka bezpieczeństwa - jest to sporządzany w formie pisemnej dokument wdrażany przez administratora danych osobowych. Obowiązkowi jego sporządzenia podlegają wszyscy administratorzy danych, bez względu na sposób w jaki przetwarzają oni dane osobowe, tj. zarówno przetwarzający dane tradycyjnie jak i w systemach informatycznych.

Prawidłowo sporządzona polityka bezpieczeństwa powinna zawierać m.in.:
- 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 - obowiązkowi sporządzenia instrukcji zarządzania systemem informatycznym podlegają wyłączne administratorzy przetwarzający dane w systemach informatycznych. Instrukcja ta, podobnie jak polityka bezpieczeństwa, powinna zostać sporządzona w formie pisemnej.

Instrukcja powinna opisywać w szczególności:
- procedury nadawania uprawnień do przetwarzania danych osobowych 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 systemu;
- 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, kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania, sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego;
- sposób w jaki zapewnia się, że system odnotowuje informacje o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia;
- procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

Dokumenty związane z wyznaczeniem administratora bezpieczeństwa informacji - administrator danych osobowych może powołać administratora bezpieczeństwa informacji, jest on odpowiedzialny za bezpieczeństwo przetwarzanych danych osobowych oraz uprawniony do nadzorowania przestrzegania ustalonych przez administratora danych zasad dotyczących ochrony danych osobowych. Administrator bezpieczeństwa informacji jest odpowiedzialny za sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowywanie w tym zakresie sprawozdania dla administratora danych oraz prowadzi jawny rejestr danych

przetwarzanych przez administratora danych. Administrator danych może powierzyć administratorowi bezpieczeństwa informacji wykonywanie innych obowiązków. Administrator danych osobowych, który wyznaczył administratora bezpieczeństwa informacji, powinien posiadać dokumenty poświadczające ten fakt.

Administrator bezpieczeństwa informacji musi być osobą fizyczną, dlatego też administrator danych osobowych niebędący osoba fizyczną nie może pełnić tej funkcji. W przypadku gdy administrator danych osobowych jest osobą fizyczną, ma on możliwość wyboru, czy wyznaczać administratora bezpieczeństwa informacji, czy też samemu wykonywać jego zadania.

W przepisach prawa nie określono, w jakim stosunku powinien pozostawać administrator bezpieczeństwa informacji do administratora danych osobowych. Z uwagi na powyższe przyjmuje się, że może on być zarówno pracownikiem administratora danych osobowych, jak i podmiotem zewnętrznym wobec niego.

Obowiązkiem administratora danych osobowych jest zapewnienie środków i organizacyjnej odrębności administratora bezpieczeństwa informacji niezbędnej do niezależnego wykonywania przez niego zadań, Administrator danych jest obowiązany zgłosić do rejestracji Generalnemu Inspektorowi powołanie i odwołanie administratora bezpieczeństwa informacji w terminie 30 dni od dnia jego powołania lub odwołania.

Upoważnienia do przetwarzania danych - administrator danych osobowych jest zobowiązany zapewnić, że do danych osobowych nie mają dostępu osoby nieupoważnione. Dostęp taki powinny mieć tylko osoby wyznaczone przez administratora, tj. posiadające nadane przez niego upoważnienia.

Przepisy nie określają formy nadania upoważnienia. Dla celów dowodowych rekomendowane jest nadanie go w formie pisemnej, przy czym dozwolone jest również skorzystanie w tym zakresie z wiadomości e-mail, a nawet formy ustnej (co jednak utrudnia ew. wykazanie, że upoważnienie faktycznie zostało udzielone). W praktyce, z upoważnieniami będziemy mieli do czynienia najczęściej np. gdy w u danego przedsiębiorcy - administratora danych osobowych - funkcjonuje np. dział HR czy księgowości.

Upoważnienie do przetwarzania danych osobowych powinno posiadać następujące cechy:
- dotyczyć konkretnej, wskazanej imieniem i nazwiskiem osoby;
- wskazywać nazwę i adres administratora danych;
- wskazywać datę nadania oraz datę ustania upoważnienia.

Podkreślenia wymaga, że ustawa nie przewiduje sytuacji, w której nadawanie upoważnień nie jest konieczne. Ponadto wskazać należy, że upoważnienie do przetwarzania danych osobowych nie może być wywodzone tylko z treści umowy o pracę, czy z zakresu obowiązków pracowniczych.

Ewidencja osób upoważnionych do przetwarzania danych - ewidencja jest dokumentem, do którego prowadzenia zobowiązany jest każdy administrator danych osobowych.
Powinna ona zawierać co najmniej:
- imiona i nazwiska osób upoważnionych przez administratora do przetwarzania danych osobowych;
- daty nadania i ustania ważności poszczególnych upoważnień;
- zakres każdego z upoważnień do przetwarzania danych osobowych;
- identyfikator użytkownika upoważnionego do przetwarzania danych osobowych (w przypadku gdy dane przetwarzane są w systemie informatycznym).

Dokumenty dotyczące rejestracji zbiorów danych
Administratorowi danych osobowych, który zgłosił do rejestru prowadzonego przez Generalnego Inspektora Danych Osobowych zbiór zawierający dane wrażliwe, jest wydawane z urzędu

zaświadczenie potwierdzające fakt rejestracji zbioru.

Fakt rejestracji zbiorów nie zawierających danych wrażliwych nie jest z urzędu potwierdzany wydawaniem zaświadczenia, jednakże administrator danych może złożyć wniosek o jego wydanie.

6. Powierzenie do przetwarzania

Administrator danych osobowych jest uprawniony do podejmowania decyzji dotyczących danych osobowych, którymi administruje, jednakże żaden przepis prawa nie wiąże z tym uprawnieniem obowiązku osobistego przetwarzania danych. Co więcej, w ustawie wyraźnie uregulowano możliwość przekazania czynności przetwarzania danych osobowych innemu podmiotowi - w drodze umowy o powierzenie do przetwarzania.

Administrator danych osobowych powierzający przetwarzanie danych zachowuje wszystkie swoje uprawnienia - wciąż jest wyłącznie uprawniony do decydowania o celach i środkach przetwarzania, może ponadto kontrolować podmiot, któremu powierzył dane. Podkreślić należy, że podmiot przetwarzający dane na podstawie umowy powierzenia sam nie staje się administratorem danych osobowych, jest on jedynie realizatorem woli administratora danych, całkowicie związanym jego wytycznymi.

Powierzenie danych osobowych do przetwarzania zależy wyłącznie od woli administratora danych osobowych. Osoba, której dane dotyczą nie musi wyrażać zgody na powierzenie jej danych do przetwarzania. Co więcej, nie musi ona być nawet informowana o fakcie powierzenia.

Umowa powierzenia danych do przetwarzania
Umowa powierzenia danych do przetwarzania musi spełniać trzy wymogi:
- być zawarta w formie pisemnej;
- określać zakres przekazywanych do przetwarzania danych (tzn. wskazywać jakie dane są przekazywane - np. imiona, nazwiska, adresy);
- wyraźnie wskazywać cel, w którym mają być przetwarzane przekazane dane (może to być jeden cel, np. pozyskiwanie danych czy przetwarzanie ich w celach marketingowych, ale możliwe jest również powierzenie wszystkich czynności przetwarzania danych osobowych - od ich zgromadzenia do usunięcia).

Może ona ponadto regulować inne zagadnienia dotyczące powierzenia danych do przetwarzania, np. wskazywać zasady przeprowadzania przez administratora danych osobowych kontroli przetwarzania danych, co z pewnością ułatwi współpracę stron w tym zakresie.

Odpowiedzialność podmiotu przetwarzającego dane osobowe na podstawie umowy powierzenia do przetwarzania
Na podmiocie tym ciążą dwa rodzaje odpowiedzialności - odpowiedzialność wynikająca z umowy zawartej z administratorem danych osobowych oraz odpowiedzialność ustawowa.

Odpowiedzialność umowna wiąże się ze związaniem podmiotu przetwarzającego dane wytycznymi administratora danych osobowych (w szczególności co do zakresu i celu przetwarzania danych osobowych). Podmiot przetwarzający dane osobowe, który nie stosuje się do wytycznych administratora danych, odpowiada wobec niego za przetwarzanie danych niezgodne z umową.

Na podmiocie przetwarzającym dane na podstawie umowy powierzenia ciążą ponadto obowiązki wskazane w ustawie - w szczególności obowiązek zabezpieczenia danych jeszcze przed rozpoczęciem ich przetwarzania. Oznacza to konieczność zastosowania środków technicznych i organizacyjnych zabezpieczających dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem, zmianą, utratą, uszkodzeniem, zniszczeniem lub przetwarzaniem niezgodnie z ustawą. W zakresie realizacji

powyższego obowiązku, podmiot przetwarzający dane na podstawie umowy powierzenia ponosi odpowiedzialność jak administrator danych osobowych, a jego działalność może być przedmiotem postępowania kontrolnego prowadzonego przez Generalnego Inspektora Ochrony Danych Osobowych. Podmiot ten może być także adresatem decyzji wydawanych przez Generalnego Inspektora.

Odpowiedzialność administratora danych osobowych
Administrator danych osobowych ponosi pełną odpowiedzialność za dane, które powierzył do przetwarzania - odpowiada tak, jakby sam je przetwarzał. Dlatego też tak ważne jest przysługujące mu uprawnienie do kontrolowania podmiotu, któremu powierzył dane oraz możliwość kierowania do niego wytycznych.

Administrator danych osobowych powierzający przetwarzanie danych ma ponadto obowiązek ujawnienia tego faktu w rejestrze prowadzonym przez Generalnego Inspektora Ochrony Danych Osobowych. Może to zrobić na etapie zgłaszania zbioru do rejestracji lub później, w zgłoszeniu aktualizacyjnym.

7. Rejestracja zbiorów danych

Administrator danych osobowych ma obowiązek zgłoszenia zbiorów, w których przetwarza dane osobowe, do rejestru prowadzonego przez Generalnego Inspektora Ochrony Danych Osobowych. Zgłoszenie takie musi nastąpić przed rozpoczęciem przetwarzania danych osobowych w zbiorze. Obowiązkowi rejestracji zbiorów danych osobowych, z wyjątkiem zbiorów zawierających dane wrażliwe nie podlega administrator danych, który powołał administratora bezpieczeństwa informacji i zgłosił go Generalnemu Inspektorowi do rejestracji. W takim wypadku, rejestr zbiorów danych jest prowadzony przez administratora bezpieczeństwa informacji.

Co do zasady przetwarzanie danych osobowych jest legalne od momentu zgłoszenia zbioru do rejestru, jednakże w przypadku danych wrażliwych jest ono możliwe dopiero od momentu rejestracji zbioru, potwierdzonego zaświadczeniem wydanym przez Generalnego Inspektora.

Zgłoszenie zbioru danych osobowych następuje za pomocą formularza, którego wzór określa rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz.U. 2008, Nr 229, poz. 1536). Formularz można złożyć w Biurze Generalnego Inspektora Ochrony Danych Osobowych mieszczącym się w Warszawie, przesłać pocztą lub drogą elektroniczną za pośrednictwem platformy e-GIODO (http://egiodo.giodo.gov.pl).

W ten sam sposób, w jaki zgłasza się zbiory danych osobowych, dokonuje się również ich aktualizacji, która powinna nastąpić w terminie 30 dni od daty dokonania zmiany (z wyłączeniem zbiorów zawierających dane wrażliwe, w których można dokonać zmian dopiero po ich zarejestrowaniu).

W ustawie o ochronie danych osobowych przewidziano liczne zwolnienia z obowiązku rejestracji, administratorzy danych osobowych nie muszą zgłaszać, m.in. zbiorów:
- w których dane przetwarzane są w związku z zatrudnieniem u nich oraz świadczeniem im usług na podstawie umów cywilnoprawnych;
- przetwarzanych wyłącznie w celu wystawienia faktury, rachunku lub prowadzenia sprawozdawczości finansowej;
- powszechnie dostępnych;
- przetwarzanych w zakresie drobnych bieżących spraw życia codziennego.

8. Generalny Inspektor Ochrony Danych Osobowych

Generalny Inspektor Ochrony Danych Osobowych jest organem, do którego zadań należy w szczególności kontrola przetwarzania danych osobowych, wydawanie decyzji administracyjnych i rozpatrywanie skarg oraz prowadzenie rejestru zbiorów danych osobowych oraz rejestru administratorów bezpieczeństwa informacji.

Generalny Inspektor prowadzi ponadto postępowania egzekucyjne, w toku których może nakładać m.in. grzywny - na osoby fizyczne jednorazowo do kwoty 10.000 zł (maksymalnie do 50.000 zł), na osoby prawne jednorazowo do kwoty 50.000 zł (maksymalnie do 200.000 zł).

Kontrole wykonywane są przez inspektorów Biura Generalnego Inspektora Ochrony Danych Osobowych. W toku czynności kontrolnych, inspektorzy zwracają uwagę w szczególności na:

- przetwarzanie danych osobowych zgodnie z prawem, w szczególności na spełnianie przewidzianych w ustawie przesłanek legalizujących przetwarzanie danych;
- zabezpieczenie przetwarzanych danych;
- zakres i cel przetwarzania danych osobowych;
- wypełnianie przez kontrolowany podmiot obowiązków informacyjnych wobec osób, których dane są przetwarzane;
- rejestrację zbioru danych osobowych.

Po zakończeniu czynności kontrolnych, sporządzany jest protokół kontroli. Podmiot kontrolowany otrzymuje jeden egzemplarz protokołu i ma prawo wniesienia umotywowanych uwag i zastrzeżeń odnośnie jego treści, a także prawo odmowy jego podpisania. Jeżeli w wyniku kontroli inspektor stwierdzi naruszenie przepisów dotyczących ochrony danych osobowych, występuje on do Generalnego Inspektora o wydanie decyzji zobowiązującej do usunięcia naruszeń.

9. Transfer danych za granicę

Zasady przekazywania danych osobowych poza granice Polski różnią się w zależności od tego, czy państwo odbiorcy danych należy do Europejskiego Obszaru Gospodarczego, czy też nie należy do tej grupy.

Przekazywanie danych osobowych do państw Europejskiego Obszaru Gospodarczego
Do Europejskiego Obszaru Gospodarczego należy obecnie 31 państw - państwa Unii Europejskiej oraz Islandia, Norwegia i Liechtenstein.

W ramach Europejskiego Obszaru Gospodarczego obowiązuje zasada swobodnego przepływu danych osobowych. Dlatego też przekazywanie danych osobowych do jego państw odbywa się na takich samych zasadach jak przekazywanie danych podmiotom mającym siedzibę na terenie Polski - wiąże się z koniecznością stosowania wymogów polskiej ustawy o ochronie danych osobowych.

Przekazywanie danych do państwa trzeciego - nienależącego do Europejskiego Obszaru Gospodarczego

Przekazanie danych osobowych do państwa trzeciego może nastąpić, jeżeli państwo docelowe zapewnia na swoim terytorium odpowiedni poziom ochrony danych osobowych. Odpowiedni poziom ochrony danych osobowych jest oceniany z uwzględnieniem wszystkich okoliczności dotyczących operacji przekazania danych, w szczególności biorąc pod uwagę charakter danych, cel i czas trwania proponowanych operacji przetwarzania danych, kraj pochodzenia i kraj ostatecznego przeznaczenia danych oraz przepisy prawa obowiązujące w danym państwie trzecim oraz stosowane w tym państwie środki bezpieczeństwa i zasady zawodowe.

Państwo trzecie nie musi dawać takich gwarancji ochrony, jeśli spełnione są przesłanki przewidziane w ustawie, np. osoba, której dane dotyczą, udzieliła na to zgody na piśmie, lub uzyskano zgodę Generalnego Inspektora Danych Osobowych (zgoda Generalnego Inspektora nie jest wymagana, jeżeli administrator danych zapewni odpowiednie zabezpieczenia w zakresie ochrony prywatności oraz praw i wolności osoby, której dane dotyczą poprzez - standardowe klauzule umowne ochrony danych osobowych, zatwierdzone przez Komisję Europejską lub przez reguły lub polityki ochrony danych osobowych zatwierdzone przez Generalnego Inspektora Danych Osobowych).

10. Odpowiedzialność za przetwarzanie danych niezgodne z ustawą o ochronie danych osobowych

Przetwarzanie danych osobowych niezgodne z przepisami ustawy o ochronie danych osobowych wiąże się z odpowiedzialnością karną, za:

- przetwarzanie danych osobowych przez nieuprawnionego;
- udostępnianie danych osobom nieuprawnionym lub umożliwianie dostępu do nich;
- naruszenie obowiązku zabezpieczenia danych osobowych;
- niezgłoszenie zbioru danych osobowych do rejestru prowadzonego przez Generalnego Inspektora Ochrony Danych Osobowych;
- niedopełnienie obowiązków informacyjnych wobec osoby, której dane dotyczą;
- utrudnianie wykonania czynności kontrolnej inspektorowie Biura Generalnego Inspektora Ochrony Danych Osobowych.

W każdym przypadku odpowiedzialność ponosi administrator danych osobowych, w niektórych przypadkach (np. za niezabezpieczenie danych osobowych) odpowiada także podmiot przetwarzający.

Materiał przygotowany i opracowany dla Polskiej Agencji Informacji i Inwestycji Zagranicznych S.A. przez:

Olesiński & Wspólnicy sp.k.
ul. Prosta 32
00-838 Warszawa
tel. (+48) 22 12 35 231
e-mail: olesinski@olesinski.com
www.olesinski.com

Olesiński & Wspólnicy to aktualnie ponad 80 doradców, 4 miasta w Polsce, 11 lat doświadczenia, stale rozwijająca się sieć relacji z Partnerami w kraju oraz Partnerami zagranicznymi.

Świadczymy usług Klientom z różnych sektorów gospodarki, oferując kompleksowe doradztwo prawne i podatkowe we wszystkich dziedzinach prawa. Staranna definicja oczekiwanych rezultatów, poszukiwanie rozwiązań i wdrażanie nowych odważnych pomysłów, a przy tym odpowiedzialność za rekomendowane rozwiązanie to podstawa naszego podejścia.
Kontakt:

Grzegorz Leśniewski, manager, adwokat

Manager w Olesiński & Wspólnicy sp. k. zarządzający warszawskim biurem spółki i kierujący pracami zespołu TMT. Odpowiada m. in. za strategiczne doradztwo dla przedsięwzięć opartych o takie technologie jak blockchain oraz cloud computing, w szczególności z uwzględnieniem zasad transgranicznego przepływu danych osobowych. Trener i prelegent, a także autor wielu publikacji z zakresu swojej specjalizacji, w szczególności współautor książki „Ochrona danych osobowych w

działach kadr. Odpowiedzi na 370 najtrudniejszych pytań" wydanej w 2014 r.

tel.:(+48) 22 12 35 237
e-mail: grzegorz.lesniewski@olesinski.com

Anna Chrobot, partner, adwokat

Z Olesiński & Wspólnicy związana od 2005 roku. Specjalizuje się w zagadnieniach związanych z obsługą podmiotów gospodarczych, przy czym główne obszary doradztwa związane są z obsługą podmiotów aktywnych w sferze zamówień publicznych oraz niezależnie obejmują pełny zakres prawa pracy ze szczególnym uwzględnieniem narzędzi prawnych dla działów HR, sporów zbiorowych oraz polityki związanej z restrukturyzacją zatrudnienia. Posiada wieloletnią praktykę zawodową obejmującą stałą obsługą podmiotów prawnych z kapitałem zagranicznym w zakresie prawa gospodarczego i podatkowego.

tel.: (+48) 71 75 00 702
e-mail: anna.chrobot@olesinski.com