




INSTYTUT
AKTYWIZACJI
REGIONÓW

Podstawowe zasady przetwarzania danych osobowych RODO

Niniejszy informator ma na celu przedstawienie podstawowych zagadnień związanych z przywołanym tematem i powstał w ramach realizacji zadania edukacji prawnej realizowanej w 2023 roku przez Instytut Aktywizacji Regionów



RODO to unijne rozporządzenie o ochronie danych osobowych (tj. Rozporządzenie Parlamentu Europejskiego i Rady UE 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE). RODO obowiązuje od 25 maja 2018 roku.

Przepisy RODO stosuje się, kiedy organizacja przetwarza dane osobowe obywateli Unii Europejskiej na całym świecie. Przepisy RODO nie dotyczą działalności osobistej lub domowej, czyli przetwarzania danych osobowych w celach prywatnych, np. wysyłanie kartek świątecznych do rodziny (dane są przetwarzane w innych celach, niż tych związanych z działalnością handlową, gospodarczą lub zawodową osoby przetwarzającej dane).

RODO chroni tylko osoby żyjące, przepisy nie dotyczą zmarłych. RODO to przepis prawa obowiązujący w całej Unii Europejskiej. Może on jednak w niektórych obszarach zostać uzupełniony przepisami prawa krajowego. Organizacje spoza Unii Europejskiej również podlegają nowym przepisom – w przypadku, kiedy oferują towary i usługi na terenie Unii Europejskiej lub jeżeli monitorują zachowanie osoby, której dane dotyczą w UE.

RODO dzieli dane osobowe na:

1. zwykłe dane osobowe,
2. szczególne dane osobowe (dawniej dane wrażliwe takie jak pochodzenie, przynależność religijna, związkowa, dane dotyczące zdrowia, dane genetyczne itp.)

Pierwsza to dane, mówiąc potocznie - zwykłe. Są to dane, którymi dysponujemy w normalnych relacjach gospodarczo-społecznych. Do tej kategorii zalicza się między innymi: imię, nazwisko, adres, dane wynikające z ewidencji ludności czy numeru dokumentów. Dane zwykłe podajemy na przykład w przypadku zakupów online czy podpisywania różnego rodzaju umów.

Druga płaszczyzna przetwarzania danych osobowych to dane szczególnie chronione – tak zwane wrażliwe. Do tej grupy należą m.in. przede wszystkim informacje o naszym

stanie zdrowia, ale nie tylko. Wszelkie informacje dotyczące naszych poglądów politycznych, przynależności do grup wyznaniowych, czy dane biometryczne. Dla potrzeb ułatwienia wyliczeń do danych szczególnych można zaliczyć informacje dotyczące wyroków. Chociaż te zostały ujęte osobno w RODO.

Przetwarzanie danych osobowych obejmuje:

1. zbieranie, utrwalanie,
2. organizowanie, porządkowanie,
3. przechowywanie, adaptowanie lub modyfikowanie,
4. pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie,
5. rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie albo
6. łączenie, ograniczanie, usuwanie lub niszczenie

W jakim charakterze można przetwarzać dane osobowe?

Będąc przedsiębiorcą można przetwarzać dane osobowe jako:

- administrator danych,
- podmiot przetwarzający dane

Administrator danych to podmiot, który decyduje o tym, po co (cele) i jak (środki, sposoby) przetwarzać dane osobowe. Administratorem może więc być:

- zakład pracy w stosunku do danych osobowych swoich pracowników,
- właściciel strony internetowej w stosunku do danych osób, które zaprenumerowały

Newsletter Natomiast podmiotem przetwarzającym dane osobowe może być:

- administrator, który sam przetwarza dane,
- przetwarzający dane, który jako podmiot zewnętrzny będzie przetwarzał dane w imieniu i na rzecz administratora i na podstawie zawartej z nim pisemnej umowy

Przetwarzającym dane może być:

- biuro rachunkowe, które przetwarza dane osobowe klientów przedsiębiorstwa/instytucji współpracującej z nim,
- przedsiębiorstwo IT zajmujące się profesjonalnie przechowywaniem lub niszczeniem danych osobowych dostarczonych przez klientów

W roli administratora lub podmiotu przetwarzającego dane osobowe zawsze występuje firma, a nie jej pracownik. Pracownik, który zajmuje się przetwarzaniem danych osobowych w firmie, powinien być upoważniony do czynności w tym zakresie. Inspektor Ochrony Danych (IOD) Należy powołać Inspektora Ochrony Danych (IOD), jeśli:

- w danej firmie przetwarzane są dane na dużą skalę (należy samodzielnie ocenić, czy przetwarzane są dane na dużą skalę; takie przetwarzanie dotyczy m.in. banków i firm ubezpieczeniowych),
- dotyczy to przetwarzania szczególnych kategorii danych (np. szpitale) lub wymaga ciągłego monitorowania osób na dużą skalę.

Inspektor musi być powołany także w przypadku, gdy dane będą przetwarzane przez jednostki sektora publicznego (urzędy). Kiedy można przetwarzać dane Aby przetwarzać dane, musi istnieć do tego podstawa. W przypadku zwykłych danych podstawą do przetwarzania jest:

1. zgoda osoby, której dane są przetwarzane,
2. sytuacja, w której przetwarzanie danych jest niezbędne do wykonania umowy z osobą, której dane dotyczą (dane do przygotowania umowy cywilnej sprzedaży),
3. sytuacja, w której przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze (np. wpisywanie danych klienta do ksiąg rachunkowych, których prowadzenie jest narzucone przepisami prawa o rachunkowości),
4. sytuacja, w której przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora (np. złożenie pozwu do sądu o zapłatę przeciwko nieuczciwemu klientowi). W przypadku szczególnych kategorii danych (wyznanie, orientacja seksualna, poglądy polityczne, pochodzenie) podstawą do przetwarzania danych są:

- wyraźna zgoda osoby, której dane dotyczą,
- sytuacja, w której przetwarzanie danych jest niezbędne do wykonania zadań związanych z zatrudnieniem czy ubezpieczeniem społecznym pracowników,
- sytuacja, w której przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, a także do oceny zdolności pracownika do pracy,

□ sytuacja, w której przetwarzanie danych jest niezbędne w celu dochodzenia praw przed sądem Jako administrator zawsze należy wykazać, że posiada się odpowiednią podstawę do ich przetwarzania (tzw. rozliczalność).

Zgoda na przetwarzanie danych

Każda zgoda na przetwarzanie danych powinna być:

1. dobrowolna – zgoda może być ważna tylko wtedy, gdy osoba, której dane dotyczą, wyrazi ją bez przymusu,
2. konkretna – aby zgoda była ważna, musi dokładnie określać cel przetwarzania i być wyrażona oddzielnie dla każdego celu,
3. jednoznaczna – zgoda musi mieć charakter wyraźny, a nie domniemany

Aby uzyskać zgodę na gromadzenie danych, należy przekazać osobie, której dane dotyczą, informacje o:

1. celach i podstawie przetwarzania danych,
 2. odbiorcach danych osobowych lub o kategoriach odbiorców,
 3. zamiarze przekazania danych osobowych do państwa trzeciego,
 4. prawie do żądania od administratora dostępu do danych osobowych, ich sprostowania, usunięcia lub o prawie do wniesienia sprzeciwu wobec przetwarzania,
 5. prawie do cofnięcia zgody w dowolnym momencie lub wniesienia skargi do UODO
- Tak rozbudowane obowiązki informacyjne w przypadku zgody na przetwarzanie danych osobowych mają najczęściej postać:

1. tzw. klauzuli zgody na przetwarzanie danych wpisywanej do umowy o współpracy,
2. formularza internetowego (udzielenie zgody na przetwarzanie poprzez zaznaczenie odpowiedniego pola w formularzu) Zgodnie z zasadą minimalizmu można przetwarzać wyłącznie takie dane osobowe, które są niezbędne do osiągnięcia celu ich przetwarzania. Należy więc ograniczyć przetwarzanie do takich danych, bez których nie można osiągnąć tego celu.

Profilowanie

Profilowanie to szczególny rodzaj przetwarzania danych osobowych, który:

1. odbywa się automatycznie,
2. ma na celu ocenę osoby fizycznej lub przewidywanie jej zachowania

Może to być na przykład podanie daty urodzenia lub wieku w celu ustalenia dla danej osoby jej zdolności kredytowej lub propozycji sprzedaży usług medycznych. Innym przykładem profilowania jest automatyczny dobór reklam na stronie internetowej w oparciu o wcześniejszą aktywność osoby na tej stronie. Aby wykonywać profilowanie, należy zawsze poinformować o tym osoby, których to dotyczy i uzyskać na tę czynność ich zgodę wyraźną.

Rejestrowanie czynności przetwarzania

Rejestr czynności przetwarzania danych osobowych jest elementem dokumentacji ochrony danych. Taki rejestr muszą prowadzić administrator danych oraz podmiot przetwarzający dane. Rejestr można prowadzić w formie pisemnej i elektronicznej.

Administrator danych musi odnotować w rejestrze:

1. imię i nazwisko lub nazwę oraz dane kontaktowe administratora, przedstawiciela administratora oraz inspektora danych osobowych IOD,
2. cele przetwarzania,
3. opis kategorii osób, których dane dotyczą oraz kategorii danych osobowych,
4. kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione,
5. przekazanie danych osobowych do państwa trzeciego - jeśli do niego doszło,
6. planowane terminy usunięcia poszczególnych kategorii danych - jeżeli jest to możliwe,
7. ogólny opis technicznych i organizacyjnych środków bezpieczeństwa danych - jeżeli jest to możliwe

Z kolei podmiot przetwarzający musi umieścić w rejestrze:

1. imię i nazwisko lub nazwę oraz dane kontaktowe podmiotu przetwarzającego oraz każdego administratora, w imieniu którego działa podmiot przetwarzający

2. rodzaj przetwarzań dokonywanych w imieniu każdego z administratorów
3. przekazania danych osobowych do państwa trzeciego - jeśli do niego doszło
4. ogólny opis technicznych i organizacyjnych środków bezpieczeństwa danych - jeżeli jest to Możliwe Inne zasady przetwarzania danych osobowych

Jeśli jest się posiadaczem lub przetwarza się dane należące do konkretnych osób fizycznych, to należy pamiętać o ich uprawnieniach. Osoby te mogą korzystać z prawa:

1. do bycia zapomnianym,
2. do przenoszenia danych,
3. do ograniczenia przetwarzania,
4. sprzeciwu wobec przetwarzania danych

Prawo do bycia zapomnianym

Prawo do bycia zapomnianym pozwala osobom, których danymi się dysponuje, na żądanie ich usunięcia i poinformowania o tym również innych przedsiębiorców, którym te dane są przekazywane. Jest zazwyczaj konsekwencją odwołania wcześniejszej zgody klienta na przetwarzanie jego danych lub złożenia przez niego sprzeciwu. Usunięcie danych osobowych w tym trybie dotyczy także przypadków, gdy dalsze przetwarzanie danych jest już zbędne lub gdy do przetwarzania doszło z naruszeniem prawa. Jeśli osoba fizyczna skorzysta z prawa do bycia zapomnianym, należy natychmiast przestać przetwarzać dane i zlikwidować je z własnych zasobów. Prawo to nie obejmuje sytuacji, gdy:

1. prawo - wbrew oczekiwaniom danej osoby - nakazuje przetwarzanie jej danych (np. wystawioną jej fakturę zaksięgowano w ewidencjach podatkowych, które trzeba przechowywać przez 5 lat),
2. przetwarzanie danych jest niezbędne do dochodzenia lub obrony roszczeń (np. złożenie pozwu do sądu przeciwko dłużnikowi)

Prawo do przenoszenia danych to z kolei prawo, w ramach którego klient może:

- chcieć uzyskać swoje dane,
- domagać się ich przesłania innemu administratorowi

Prawo do przenoszenia danych możesz realizować wyłącznie wtedy, gdy przetwarzane są dane na podstawie zgody lub w celu wykonania umowy. Można je wykonać tylko wtedy, gdy przetwarza się dane elektronicznie. Prawo to bowiem obejmuje tylko te dane osobowe, które przetwarza się elektronicznie i nie ma zastosowania do tradycyjnych, czyli papierowych zbiorów danych.

Prawo sprzeciwu

Natomiast prawo sprzeciwu pozwala klientom domagać się zaprzestania przetwarzania ich danych osobowych. Od tego momentu nie można tych danych używać ani przekazywać innym podmiotom przetwarzającym je na zlecenie (np. biuro rachunkowe), chyba że zostanie wykazane, iż przemawia za tym interes nadrzędny tego klienta.

Do czasu wyjaśnienia tej kwestii obowiązuje jednak ograniczenie przetwarzania danych. Innym powodem ograniczenia przetwarzania danych może być sytuacja, gdy nie potrzebuje się już danych osobowych, ale są one niezbędne do dochodzenia lub obrony twoich roszczeń. Skarga dotycząca naruszenia przepisów o ochronie danych osobowych Naruszenie danych osobowych klientów skutkuje, możliwością złożenia przez nich skargi do Prezesa UODO.

Może to dotyczyć sytuacji, gdy np. zamieści się nazwisko klienta lub jego adresu bez jego zgody w ogólnodostępnym miejscu. Skargę można złożyć również, gdy nasze dane lub dane naszych pracowników zostały naruszone w podobny sposób.