Przedsiębiorco, wchodzi RODO – przetwarzanie danych osobowych

Z tego poradnika dowiesz się:

- czym jest RODO,
- jakie nowe obowiązki związane z ochroną danych osobowych czekają przedsiębiorców,
- jak przygotować się do zmian związanych z RODO.

Podstawy prawne przetwarzania danych osobowych
Od 25 maja 2018 r. podstawą przetwarzania danych osobowych będzie RODO, czyli rozporządzenie Parlamentu Europejskiego i Rady nr 2016/679 z dnia 14 kwietnia 2016 r. w sprawie ochrony danych osobowych, które zastępuje dotychczasową ustawę krajową, czyli ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Pomimo tego, że jest to akt unijny, będzie on również bezpośrednio stosowany w Polsce. Każdy podmiot, który posiada lub przetwarza dane osobowe, będzie musiał go przestrzegać.
Na poziomie krajowym powstanie ustawa, która będzie regulować m.in.:

- zasady powoływania Prezesa Urzędu Ochrony Danych Osobowych (PUODO), zastępującego GIODO,
- podmioty obowiązane do wyznaczenia inspektora ochrony danych oraz tryb zawiadamiania o wyznaczaniu,
- postępowanie kontrolne,
- odpowiedzialność cywilną, przepisy karne oraz administracyjne kary pieniężne za naruszenie przepisów o ochronie danych osobowych.

Dane osobowe według RODO
Podobnie jak dzisiaj, również RODO dzieli dane osobowe na:

- zwykłe dane osobowe,
- szczególne dane osobowe (dawniej wrażliwe).

Do szczególnych danych osobowych zalicza się dane, które ujawniają:

- pochodzenie rasowe lub etniczne,
- poglądy polityczne, przekonania religijne, światopoglądowe,
- przynależność do związków zawodowych,
- dane genetyczne lub biometryczne,
- dane dotyczące zdrowia lub orientacji seksualnej.

Jak przetwarzać dane osobowe
Przetwarzanie danych osobowych to czynność, która obejmuje m.in.:

- zbieranie, utrwalanie,
- organizowanie, porządkowanie,
- przechowywanie, adaptowanie lub modyfikowanie,
- pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie,
- rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie albo
- łączenie, ograniczanie, usuwanie lub niszczenie.

Czynności te mogą być wykonywane w sposób zautomatyzowany lub niezautomatyzowany.

Szczególną formą przetwarzania danych jest ich profilowanie. Jest to nowa instytucja, która ma na celu ocenę osoby fizycznej i jej przewidywane zachowanie. Chodzi na przykład o podanie daty urodzenia lub wieku w celu ustalenia dla danej osoby jej zdolności kredytowej albo propozycji sprzedaży usług medycznych. Osoby starsze

zazwyczaj mają ograniczony dostęp do kredytów, natomiast są potencjalnymi klientami usług medycznych. Ustalenie tego przed złożeniem oferty będzie miało istotne znaczenie dla sprzedawcy, wymaga jednak uzyskania zgody potencjalnego klienta. Rozróżnia się profilowanie zwykłe (z udziałem czynnika ludzkiego) oraz zautomatyzowane (gdzie cały proces oceny kończy się podjęciem zautomatyzowanej decyzji).

Dane osobowe muszą być:

- przetwarzane zgodnie z prawem (zgodność z prawem, rzetelność i przejrzystość),
- zbierane w konkretnym celu (ograniczenie celu),
- adekwatne (minimalizacja danych),
- prawidłowe i w razie potrzeby aktualizowane lub usuwane (prawidłowość),
- przechowywane nie dłużej niż jest to konieczne do celu przetwarzania (ograniczenie przechowywania),
- odpowiednio zabezpieczone (integralność i poufność).

Kiedy można przetwarzać dane osobowe
Możesz przetwarzać dane osobowe, gdy:

- posiadasz zgodę osoby, której dane chcesz przetwarzać,
- ich przetwarzanie jest niezbędne do przygotowania lub wykonania umowy z osobą, której dotyczą (np. sporządzanie umowy sprzedaży, wystawienie faktury),
- przetwarzanie jest niezbędne do wykonania obowiązku prawnego (np. przetwarzanie danych w celach związanych z księgami rachunkowymi, których prowadzenie wynika z ustawy o rachunkowości),
- przetwarzanie jest niezbędne do realizacji prawnie uzasadnionych interesów (np. skierowanie pozwu o zapłatę przeciwko nieuczciwemu klientowi).

Zgoda i wyraźna zgoda na przetwarzanie
W RODO występują dwa rodzaje zgody:

- zgoda i
- wyraźna zgoda.

Zgoda wyraźna wymagana jest przy przetwarzaniu szczególnych kategorii danych osobowych. Pojawia się przy zautomatyzowanym podejmowaniu decyzji w indywidualnych przypadkach, w tym profilowaniu.
Odbierając zgodę na przetwarzanie danych osobowych przygotuj formularz, w którym odbierzesz zgodę na każdy cel przetwarzania oddzielnie. Nie możesz łączyć celów przetwarzania, czyli odbierać tzw. zgód ogólnych. Nie nadużywaj przesłanki „zgody” jako podstawy przetwarzania danych osobowych. Osoba, której dane dotyczą, może wycofać zgodę w dowolnym momencie, równie łatwo jak ją wyraziła.
Jeżeli będzie chciała skorzystać z tego prawa, to administrator musi zakończyć przetwarzanie jej danych. Jeżeli przetwarzanie było związane z wykonaniem obowiązku nałożonego przez prawo, to administrator nie będzie mógł zrealizować żądania tej osoby.

Przestrzeganie zasad ochrony danych osobowych
Ochrona danych osobowych jest obowiązkiem:

- urzędów państwowych (np. urzędów skarbowych),
- urzędów samorządu terytorialnego (np. urzędów miast lub gmin),
- każdego przedsiębiorcy.

Jeżeli urząd lub przedsiębiorca będzie przetwarzał dane osobowe, to może występować jako:

- administrator danych (np. pracodawca w stosunku do danych osobowych swoich pracowników, sprzedawca w sklepie internetowym w stosunku do danych osobowych swoich klientów),
- podmiot przetwarzający dane na zlecenie, czyli powierzone do przetwarzania przez administratora, który decyduje o celach i środkach (np. biuro rachunkowe, które przetwarza dane osobowe klientów, firma IT, która obsługując daną firmę utrzymuje jej serwery lub zakłada konta e-mailowe pracowników).

Podmiot przetwarzający dane na zlecenie powinien zawrzeć z administratorem danych pisemną umowę powierzenia, w której trzeba określić zasady przetwarzania danych osobowych. W praktyce w firmie dane osobowe przetwarzają konkretni pracownicy lub współpracownicy. Takie osoby powinny posiadać upoważnienie do przetwarzania danych osobowych.

Inspektor Ochrony Danych (IOD)
Będziesz musiał powołać Inspektora Ochrony Danych (IOD), jeśli:

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

Inspektor musi być powołany także w przypadku, gdy dane będą przetwarzane przez jednostki sektora publicznego (urzędy).

Inspektor danych osobowych to nowa instytucja, która zastąpi dotychczasowego Administratora Bezpieczeństwa Informacji - ABI. Do zadań IOD będzie też należało:

- informowanie pracowników o ich obowiązkach wynikających z RODO oraz doradzanie im i szkolenie,
- monitorowanie przestrzegania przepisów,
- współpraca z UODO oraz pełnienie roli punktu kontaktowego,
- udzielanie zaleceń co do oceny skutków dla ochrony danych,
- opiniowanie i doradzanie w kwestii wdrażania zasad przetwarzania danych.

Są to nowe zasady wprowadzone przez RODO.
Więcej na ten temat przeczytasz w dalszej części poradnika.

Ocena skutków dla ochrony danych osobowych
Nowością w RODO jest odejście od obowiązku rejestracji zbiorów danych osobowych. Zamiast tego wprowadza się procedurę tzw. oceny skutków dla ochrony danych osobowych.
Ocena skutków jest związana przede wszystkim z opisem procesu przetwarzania i ma pomóc w zarządzaniu ryzykiem naruszenia praw osób, których dane są przetwarzane. Ocenę przeprowadza się w sytuacji, kiedy przetwarzanie danych osobowych może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych. Obowiązkowo należy dokonać oceny przy przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa albo danych pochodzących z miejsc systematycznie monitorowanych na duża skalę (np. kamery w miejscach publicznych) czy profilowaniu.

Jeżeli będziesz mieć wątpliwości, czy musisz prowadzić ocenę skutków, to skonsultuj się z Urzędem Ochrony Danych Osobowych.

Prawa osób, których dane są przetwarzane
RODO daje także nowe prawa osobom, których dane dotyczą:

- prawo do bycia zapomnianym - czyli możliwość żądania przez osobę, której dane dotyczą, usunięcia jej danych osobowych przez administratora (przedsiębiorcę) lub żądanie powiadomienia o tym innych administratorów, którym udostępniono te dane (wyjątkiem jest przetwarzanie na podstawie prawa),
- prawo do ograniczenia przetwarzania,
- prawo sprzeciwu wobec przetwarzania danych,
- prawo do przenoszenia danych - czyli prawo do otrzymania od administratora (przedsiębiorcy) swoich danych osobowych lub przesłania tych danych innemu administratorowi.

Uwaga! Dotyczy to danych, które przetwarza się elektronicznie i nie obejmuje tradycyjnych, papierowych zbiorów danych.

Incydent bezpieczeństwa
RODO wprowadza także obowiązek zgłaszania naruszeń ochrony danych osobowych (incydent bezpieczeństwa).

Zgłoszenie powinno być skierowane do UODO w ciągu 72 godzin i powinno obejmować wszystkie zdarzenia, które mogły:

- skutkować ryzykiem naruszenia praw lub wolności osób fizycznych
- doprowadzić lub doprowadziły do „wycieku” albo utraty danych osobowych.

Zgłoszenia dokonuje administrator danych.

Przeczytaj też jak przygotować się do RODO.