Poradnik

Nowe przepisy dot. ochrony danych w e-sklepach

TRUSTED SHOPS

Treść

Wprowadzenie

25 maja 2018 r. zacznie obowiązywać RODO, czyli rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 (ogólne rozporządzenia o ochronie danych). Przetwarzanie danych osobowych będzie musiało zostać dostosowane do nowych wymogów prawnych. Warto zatem dobrze wykorzystać pozostający czas w celu jak najlepszego dopasowania własnego modelu biznesowego do nowych przepisów.

Prace nad nowym aktem prawnym, który ujednolica przepisy dotyczące ochrony danych osobowych dla wszystkich państw członkowskich Unii, trwały ponad 4 lata. Po długich negocjacjach, 4 maja 2016 r., w Dzienniku Urzędowym Unii Europejskiej opublikowano oficjalne teksty nowego rozporządzenia. Unijne rozporządzenie jest prawem bezpośrednio obowiązującym we wszystkich państwach członkowskich i nie wymaga implementacji do krajowych przepisów państw członkowskich.

Nowe przepisy dotyczą tak naprawdę wszystkich przedsiębiorców, którzy mają styczność z danymi osobowymi swoich klientów. Zasad określonych w RODO zobowiązane są przestrzegać zarówno wielkie korporacje, jak i mniejsze przedsiębiorstwa. Oczywiście również sklepy internetowe będą musiały dostosować swoją politykę prywatności i praktyki dotyczące przetwarzania danych osobowych.

RODO zostało uchwalone ze względu na konieczność wprowadzenia zmian wynikających z dynamicznego rozwoju technologii przetwarzania danych osobowych. Przepisy rozporządzenia są dość uniwersalne i elastyczne, co z jednej strony pomaga dostosować je do ciągłego i dynamicznego rozwoju nowych technologii, a z drugiej stanowi pewne trudności interpretacyjne. Unijny ustawodawca, dążąc do stworzenia przepisów niezależnych od rozwoju technologii, nie zawarł bowiem w rozporządzeniu żadnych konkretnych wytycznych, jak zabezpieczyć dane osobowe. Jest to zrozumiałe, gdyż wytyczne takie musiałyby być odmienne dla każdej branży, a ponadto ulegać ciągłym aktualizacjom pod kątem zmieniających się warunków i postępu technologicznego.

Mimo iż unijne rozporządzenia obowiązują bezpośrednio, polski ustawodawca zdecydował się na wdrożenie RODO poprzez stworzenie zupełnie nowej ustawy o ochronie danych osobowych. RODO oraz nowa krajowa ustawa dot. danych osobowych zastąpią obecną ustawę o ochronie danych osobowych oraz rozporządzenia wykonawcze wydane na jej podstawie. Projekt nowej ustawy jest dostępny na stronie Ministerstwa Cyfryzacji. Takie rozwiązanie umożliwi doprecyzowanie niektórych (w znacznej mierze mniej istotnych) kwestii poprzez krajowe przepisy. Unijne rozporządzenie o ochronie danych osobowych zawiera kilka tzw. otwartych klauzul, które pozostawiają niektóre kwestie do uregulowania lub doprecyzowania przez krajowe przepisy państw członkowskich.

RODO znacząco wpłynie na cały krajowy system ochrony danych osobowych. Administratorzy danych osobowych będą musieli sprostać nowym obowiązkom, takim jak np. uwzględnienie ochrony danych w fazie projektowania i domyślna ochrona danych, ocena skutków dla ochrony danych, rejestrowanie czynności przetwarzania, czy obowiązek zgłoszenia naruszenia ochrony danych organowi nadzorczemu oraz zawiadomienia podmiotu danych o naruszeniu ochrony danych osobowych. Z kolei osoby, których dane są przetwarzane, będą mogły korzystać z nowych uprawnień, takich jak prawo do przenoszenia danych czy prawo do bycia zapomnianym.

Kiedy można przetwarzać dane na gruncie RODO?

1

Rozporządzenie, które zacznie być stosowane od 25 maja 2018 r., nie wprowadza żadnej rewolucji w zakresie podstaw prawnych określających dopuszczalność przetwarzania danych osobowych. **Zachowany został podział na tzw. zwykłe dane osobowe i wrażliwe** (szczególna kategoria danych, np. dane ujawniające pochodzenie rasowe, przekonania religijne i światopoglądowe, poglądy polityczne, czy też dane genetyczne i biometryczne oraz dotyczące zdrowia lub seksualności i orientacji seksualnej, a także dane o wyrokach skazujących i przestępstwach).

Tego typu dane wrażliwe co do zasady nie są jednak przetwarzane przez sprzedawców internetowych. Dane przetwarzane przez sklepy internetowe, takie jak np. imię i nazwisko kupującego, adres dostawy, numer telefonu czy adres e-mail, to tzw. zwykłe dane osobowe. Ich przetwarzanie następuje najczęściej **w celu realizacji umowy** zawartej między sprzedawcą internetowym a kupującym (np. w celu realizacji zamówienia i wysłania produktu do kupującego) lub na podstawie **uprzednio udzielonej przez klienta zgody** (np. w celach marketingowych, otrzymywania newslettera). Taka zgoda musi zostać wyrażona w formie oświadczenia lub wyraźnego, jednoznacznego i świadomego działania osoby zezwalającej na przetwarzanie w określonym celu jej danych osobowych. Pozostałymi przesłankami legitymizującymi przetwarzanie tzw. zwykłych danych osobowych pozostają:

- niezbędność przetwarzania **do wypełnienia obowiązku prawnego** ciążącego na administratorze danych (właścicielu sklepu internetowego),

- niezbędność przetwarzania do **ochrony żywotnych interesów** osoby, której dane dotyczą, lub innej osoby fizycznej,

- niezbędność przetwarzania do **wykonania zadania realizowanego w interesie publicznym** lub w ramach sprawowania władzy publicznej powierzonej administratorowi,

- **niezbędność przetwarzania do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora** lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

Jeżeli przetwarzanie danych klientów następuje na podstawie uprzednio otrzymanej zgody, należy pamiętać o tym, iż zgoda taka musi być dobrowolna i jednoznaczna. W praktyce sprzedawcy internetowi zbierają zgody na przetwarzanie danych w celach marketingowych za pomocą tzw. checkboxów. Znajdujące się obok takiego checkboxu oświadczenie o zgodzie na przetwarzanie danych przez sprzedawcę internetowego powinno być sformułowane jasnym i prostym językiem oraz jednoznacznie określać cel przetwarzania danych. Należy pamiętać, że jeżeli dane mają być przetwarzane w różnych celach, należy uzyskać zgodę na wszystkie te cele.

Ze względu na wymóg dobrowolności oraz udzielenia wyraźnej, jednoznacznej zgody checkboxy nie powinny być zaznaczone domyślnie. Sprzedawca powinien pozostawić puste pole, które klient e-sklepu musi następnie samodzielnie zaznaczyć, aby wyrazić zgodę na przetwarzanie danych w określonym przy checkboxie celu. Niedozwolone jest również „wymuszanie" zgody, np. poprzez uzależnienie możliwości złożenia zamówienia czy też założenia konta w sklepie od udzielenia zgody na marketing lub newsletter. W szczególności nie należy interpretować milczenia klienta jako przyzwolenia na przetwarzanie jego danych osobowych. Co ważne, udzielona zgoda może zostać w każdym czasie odwołana przez klienta e-sklepu. Sprzedawca internetowy musi umożliwić klientowi wycofanie udzielonej zgody w łatwy sposób. W praktyce sprzedawcy internetowi umieszczają w tym celu w wysyłanych wiadomościach specjalny link, którego kliknięcie przez odbiorcę jest równoznaczne z usunięciem jego adresu poczty elektronicznej z bazy danych sklepu i rezygnacją z dalszego otrzymywania informacji drogą elektroniczną.

Zgoda na otrzymywanie informacji marketingowych

☐ Wyrażam zgodę na otrzymywanie drogą elektroniczną od **[podmiot prowadzący sklep internetowy]** informacji handlowych dotyczących najnowszych ofert i promocji, zgodnie z ustawą z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2002 r. Nr 144, poz. 1204 z późn. zm.).

Mogą Państwo w każdej chwili cofnąć udzieloną zgodę. Aby to zrobić, wystarczy wysłać odpowiednią informację na adres **[dane kontaktowe].** Udzielenie niniejszej zgody jest dobrowolne.

W przypadku sporu lub skarg ciężar udowodnienia prawidłowego otrzymania zgody spoczywa na sprzedawcy internetowym. Dlatego zaleca się stosowanie tzw. metody „double opt-in", w ramach której po wpisaniu w formularzu danego adresu e-mail zostanie na niego wysłana automatycznie wygenerowana wiadomość z linkiem aktywacyjnym. Dopiero po kliknięciu na niego przez użytkownika adres e-mail zostanie aktywowany w bazie mailingowej sprzedawcy internetowego. Lista utworzona w ten sposób jest bardziej wartościowa i bezpieczna pod względem prawnym. Umożliwia sklepowi zachowanie oświadczeń zgody (potwierdzeń aktywacji linku) w celach dowodowych. W ten sposób sklep jest chroniony przed ewentualnymi zarzutami wysłania niezamówionych informacji handlowych (spamu). Dzięki takiemu rozwiązaniu sprzedawca ma również pewność, że osoba, która zapisała się do jego listy mailingowej, faktycznie ma dostęp do danego konta e-mail i że dodany adres e-mail rzeczywiście istnieje.

Na czym polega nowe podejście do przetwarzania danych osobowych?

2

Oprócz zwiększenia obowiązków informacyjnych i uprawnień osób, których dane osobowe są przetwarzane, RODO **zmienia przede wszystkim sposób, w jaki administrator danych osobowych musi myśleć o procesach dotyczących przetwarzania danych osobowych.**

O ile prawne podstawy nie ulegają dużym zmianom, o tyle przyjęta w unijnym rozporządzeniu koncepcja ich praktycznego stosowania jest już sporą nowością i wyzwaniem dla administratorów danych osobowych. RODO wprowadza nowe zasady w praktyce przetwarzania danych osobowych, takie jak **„zasada rozliczalności", „privacy by default", „privacy by design" i podejście oparte na ryzyku** („risk based approach") zakładające, że administrator danych osobowych (np. właściciel sklepu internetowego) musi za każdym razem, gdy zbiera i przetwarza dane osobowe, analizować związane z tym ryzyko dla prywatności osób, których dane są wykorzystywane. Analizę skutków dla ochrony danych w celu udokumentowania jej przeprowadzenia administrator danych będzie musiał wykonać w formie pisemnego dokumentu.

Z kolei **zasada „privacy by design"** nakazuje, aby ochrona danych osobowych była uwzględniana już na etapie samego projektowania przez przedsiębiorców nowych produktów lub usług. Dane oraz prywatność mają być chronione już od samego rozpoczęcia operacji biznesowych przez przedsiębiorcę. Powyższe oznacza, iż sprzedawca, który postanowi założyć sklep internetowy, jako administrator danych, zobowiązany będzie pomyśleć o rozwiązaniach dotyczących bezpieczeństwa danych osobowych i prywatności już na etapie przygotowywania biznes planu, opracowywania modelu funkcjonowania e-sklepu i wyboru dostawcy usług hostingowych. Koncepcja ta nie dąży do ochrony prywatności poprzez systemowe dodatki do już istniejących rozwiązań, lecz nakazuje włączenie ochrony prywatności jako elementarnej części każdego projektu, produktu czy usługi.

Ponadto prywatność ma być traktowana jako standardowe, domyślne ustawienie systemowe w ramach procesów przetwarzania danych przez administratora danych osobowych **(„zasada privacy by default").** Oznacza to, że administratorzy powinni przetwarzać domyślnie minimalną ilość informacji (minimalizacja danych), niezbędną do osiągnięcia konkretnego celu przetwarzania, a o wszelkim zwiększeniu ilości zbieranych danych czy zakresu ich przetwarzania decydować ma podmiot danych osobowych, czyli osoba, której dane dotyczą. Domyślność oznacza przy tym brak konieczności jakiejkolwiek aktywności ze strony osoby, której dane dotyczą, i to w kluczowym dla niej momencie przyłączenia się do danego systemu administratora danych (np. założenie konta użytkownika na portalu społecznościowym lub konta klienta w sklepie internetowym).

Rozporządzenie wprowadza również nową **„zasadę rozliczalności",** zgodnie z którą na każdym administratorze danych spoczywać będzie obowiązek wdrożenia odpowiednich środków technicznych i organizacyjnych zapewniających przetwarzanie danych osobowych w sposób zgodny z wymogami rozporządzenia. **Zasada rozliczalności wymaga również, aby administrator danych był w stanie wykazać, iż dane osobowe przetwarzane są w zgodzie z zasadami przyjętymi w RODO.** Administratorzy danych będą więc musieli udowodnić poprawne wdrożenie zasad określonych w unijnym rozporządzeniu (np. przeprowadzenie analizy skutków dla ochrony danych osobowych, wdrożenie zasad „privacy by design" oraz „privacy by default").

Podstawową trudność z tym związaną upatruje się w fakcie, iż rozporządzenie nie mówi zbyt wiele o tym, w jaki sposób administrator danych powinien w praktyce zrealizować stawiane mu wymagania, i nie określa żadnych minimalnych standardów technicznych czy konkretnych przykładów najlepszych rozwiązań. Od 25 maja 2018 r., w związku z rozpoczęciem stosowania przepisów RODO, przestanie

obowiązywać również rozporządzenie MSWiA określające warunki techniczne i organizacyjne, jakie muszą spełniać urządzenia i systemy informatyczne wykorzystywane do przetwarzania danych osobowych. Administratorzy danych, uwzględniając specyfikę swojej działalności biznesowej, charakter, zakres, kontekst i cel przetwarzania danych oraz związane z tym ryzyko dla prywatności osób, których dane będą przetwarzane (podejście oparte na ryzyku), będą musieli samodzielnie zdecydować o wdrożeniu możliwie najlepszych i adekwatnych środków oraz procedur ochrony danych osobowych. Decyzje te podejmować będą musieli już na etapie projektowania swoich usług biznesowych (zasada „privacy by default").

Dość daleko idące zwiększenie samodzielności, ale i też odpowiedzialności administratorów danych za procesy przetwarzania danych osobowych jest konsekwencją przyjętego przez europejskiego ustawodawcę kierunku stworzenia ram prawnych niezależnych od ciągłego i dynamicznego postępu technologicznego. Przepisy RODO mają być, w założeniu ustawodawcy, technologicznie neutralne. Określają obowiązki administratora, pozostawiając mu jednocześnie bardzo dużą swobodę w wyborze odpowiednich rozwiązań gwarantujących ich spełnienie i zachowanie należytego standardu ochrony prywatności.

Obowiązki administratora danych osobowych – co się zmieni?

3

Nowe przepisy zmienią dotychczasowy zakres obowiązków. **Część zostanie zniesiona – w tym wiele tych najbardziej uciążliwych, jak np. obowiązek zgłaszania każdego zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych.** W miejsce GIODO powołany zostanie nowy państwowy organ kontrolny – Prezes Urzędu Ochrony Danych Osobowych. GIODO przestanie prowadzić jawny rejestr zbiorów danych. Zbiorów danych nie będzie trzeba zgłaszać do rejestracji niezależnie od tego, czy przetwarzane będą dane zwykle czy wrażliwe. **Administrator danych nie będzie również musiał nadawać na piśmie uprawnień do przetwarzania danych osobowych i prowadzić ewidencji osób upoważnionych do ich przetwarzania.**

W związku z rozpoczęciem stosowania przepisów RODO przestanie obowiązywać również wspomniane już rozporządzenie MSWiA określające warunki techniczne i organizacyjne, jakie musza spełniać urządzenia i systemy informatyczne wykorzystywane do przetwarzania danych osobowych. Administratorzy nie będą więc musieli zapewniać określonych w tym rozporządzeniu wymagań techniczno-informatycznych. Każdy administrator danych będzie natomiast musiał samodzielnie wypracować właściwe dla jego działalności biznesowej oraz zakresu i rodzaju przetwarzanych danych rozwiązania techniczne i środki zabezpieczeń. Przepisy przestaną konkretyzować, w jaki sposób należy to uczynić.

W konsekwencji zmieni się również sposób prowadzenia dokumentacji dotyczącej ochrony danych osobowych. Administratorzy nie będą już zobowiązani do opracowania i wdrożenia dotychczas obowiązkowych dokumentów takich jak:

- polityka bezpieczeństwa,
- instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

Nie oznacza to jednak, iż po 25 maja 2018 r. administrator danych nie będzie musiał w żaden sposób dokumentować procesu przetwarzania danych osobowych. Przepisy RODO nakładają na niemalże każdego administratora danych **obowiązek prowadzenia rejestru czynności przetwarzania danych osobowych** (art. 30). Opis informacji, jakie administrator musi zamieścić w takim rejestrze, zamieszczony został w dalszej części poradnika.

Ponadto przepisy RODO zobowiązują każdego administratora danych do wdrożenia odpowiednich środków technicznych i organizacyjnych zapewnianiających bezpieczeństwo przetwarzania danych osobowych. W razie potrzeby środki te muszą być poddawane przeglądowi i uaktualniane. Co więcej muszą one również umożliwiać administratorowi danych wykazanie (np. na wypadek kontroli), iż dane osobowe są przetwarzane zgodnie z unijnym rozporządzeniem (art. 24). Nowością na gruncie RODO są również wspomniane obowiązki uwzględnienia ochrony danych w fazie projektowania („privacy by design") oraz obowiązek realizowania domyślnej ochrony danych osobowych („privacy by default") określone w art. 25 rozporządzenia.

Przepisy rozporządzenia nie zawierają przy tym żadnych konkretnych wytycznych dla administratora w zakresie środków, jakie należy wdrożyć, by spełnić te wymogi. **Wybór odpowiednich środków został w całości pozostawiony administratorowi danych.** Dokonując wyboru środków technicznych i organizacyjnych, administrator powinien uprzednio dokonać rzetelnej analizy ryzyka i na jej podstawie ocenić, czy środki te będą w stanie zapewnić poziom bezpieczeństwa adekwatny do stopnia ryzyka wiążącego się z przetwarzaniem danych osobowych.

Ocena ryzyka oraz dobór odpowiednich środków bezpieczeństwa powinny być dokonywane przy uwzględnieniu wskazanych w art. 32 rozporządzenia kryteriów takich jak:

- aktualny stan wiedzy technicznej,
- koszt wdrożenia danego środka,
- charakter, zakres, kontekst i cele przetwarzania,
- wynikające z przetwarzania ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia.

Rozporządzenie wskazuje również przykładowe środki bezpieczeństwa, które w pewnych przypadkach mogą zapewnić stosowny poziom ochrony danych osobowych:

- pseudonimizację i szyfrowanie danych osobowych,
- środki zdolne do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,
- środki zdolne do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego,
- regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

Podkreślić należy, iż jest to jedynie przykładowe wyliczenie środków, a ich stosowanie nie jest obligatoryjne. To, czy środki te będą wystarczające lub niewystarczające do zapewnienia odpowiedniego bezpieczeństwa ochrony danych, zależeć będzie w indywidualnym przypadku od rodzaju działalności biznesowej prowadzonej przez administratora danych, charakteru, zakresu oraz kontekstu i celu przetwarzania danych osobowych, a także od wiążącego się z tym poziomu ryzyka naruszenia prywatności osób, których dane dotyczą. Zupełnie inne środki ochrony danych osobowych niż te stosowane w sklepie internetowym muszą bowiem wdrożyć wielkie instytucje finansowe, takie jak np. banki czy międzynarodowe korporacje.

Obowiązki informacyjne administratora względem osób, których dane są przetwarzane, oraz ich prawa

4

Osoby, których dane są przetwarzane, mają bardzo szeroko rozumiane prawo do informacji. Przepisy RODO rozszerzają obowiązki informacyjne administratora danych względem tych osób. W porównaniu do obecnego stanu prawnego rozporządzenie zwiększa również ich uprawnienia. Nowością jest np. prawo do żądania od administratora danych ich przeniesienia bezpośrednio na podmiot danych lub do innego administratora danych wskazanego przez osobę, której dane dotyczą. Takiego przeniesienia (przekazania) administrator będzie musiał dokonać w ustrukturyzowanym i powszechnie używanym formacie, tak aby dane te były możliwe do późniejszego odczytu. Dzięki RODO każda osoba, której dane będą przetwarzane, będzie mogła także – w ramach prawa dostępu do danych – zwrócić się do administratora z żądaniem wydania jej kopii wszystkich jej danych osobowych, jakie są przetwarzane przez tego administratora.

Już na etapie pozyskiwania danych osobowych administrator ma obowiązek przekazać osobom, od których dane te pozyskuje, rzetelnych informacji o:

- swojej tożsamość i danych kontaktowych oraz, gdy ma to zastosowanie, danych kontaktowych inspektora ochrony danych,
- celu przetwarzania danych oraz prawnej podstawie ich przetwarzania,
- prawnie uzasadnionych interesach realizowanych przez administratora (obowiązek ten dotyczy sytuacji, gdy administrator danych za podstawę prawną przetwarzania danych przyjmuje niezbędność takiego przetwarzania do celów wynikających z realizowanych przez siebie prawnie uzasadnionych interesów, art. 6 ust. 1 lit. f),
- odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli tacy istnieją,
- o zamiarze przekazania danych osobowych do państwa spoza UE lub organizacji międzynarodowej, jeżeli ma to zastosowanie.

Poza powyższymi informacjami administrator danych zobowiązany jest również poinformować o:

- okresie, przez który dane osobowe będą przetwarzane, a gdy nie jest to możliwe, kryteriach ustalania tego okresu,
- tym, czy podanie danych osobowych jest wymogiem ustawowym, umownym lub warunkiem niezbędnym do zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje ich niepodania,
- tym, czy administrator stosuje zautomatyzowane podejmowanie decyzji, w tym profilowanie (jeśli tak, przedstawić należy informacje o zasadach podejmowania decyzji oraz tryb działania profilowania, a także poinformować o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą),
- przysługującym użytkownikowi prawie do żądania od administratora dostępu do swoich danych osobowych, a także prawie do ich sprostowania, usunięcia lub ograniczenia przetwarzania,
- prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych,
- prawie do cofnięcia w dowolnym momencie zgody na przetwarzanie danych osobowych, gdy w danej sytuacji jest ona podstawą prawną przetwarzania,
- prawie do wniesienia skargi do organu nadzorczego.

Co istotne, wszystkie wyszczególnione powyżej informacje muszą zostać przekazane przez administratora danych jasnym i prostym językiem, w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie (art. 12 rozporządzenia). **W ramach prawa dostępu do danych każda osoba jest uprawniona do uzyskania od administratora (np. w drodze zapytania wysłanego pocztą e-mail) informacji, czy przetwarza on jej dane osobowe.** Jeżeli tak, wówczas osoba ta może również żądać od administratora informacji o:

- celu przetwarzania jej danych osobowych i tym, czy w oparciu o te dane podejmowane są zautomatyzowane decyzje takie jak np. profilowanie,
- odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione,
- okresie przechowywania danych.

Poza tym administrator danych zobowiązany jest przekazać takiej osobie informacje dotyczące przysługującego jej prawa do sprostowania, usunięcia, ograniczenia przetwarzania, wniesienia sprzeciwu, przeniesienia danych i złożenia skargi do organu nadzorczego, a także informacje o źródle pozyskania danych w przypadku, gdy administrator nie uzyskał danych osobowych od osoby, której dane dotyczą.

Osoba, której dane są przetwarzane, może żądać usunięcia jej danych osobowych (tzw. prawo do bycia zapomnianym) w następujących sytuacjach:

- Dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetworzone.
- Osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie, i nie ma innej podstawy prawnej przetwarzania.
- Osoba, której dane dotyczą, wniosła sprzeciw wobec przetwarzania i nie występują nadrzędne, prawnie uzasadnione podstawy przetwarzania.
- Dane osobowe były przetwarzane niezgodnie z prawem.
- Dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator.
- Dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego (np. portale społecznościowe czy aplikacje mobilne).

Gdy osoba, której dotyczą dane, żąda ich usunięcia i gdy występuje choć jedna z wskazanych powyżej okoliczności, administrator ma obowiązek usunąć dane osobowe bez zbędnej zwłoki.

Najlepszym sposobem na spełnienie przez administratora danych rozległych obowiązków informacyjnych względem osób, których dane są przetwarzane, pozostaje **polityka prywatności.** Dotyczy to oczywiście również sprzedawców internetowych, którzy w związku z realizacją zamówienia czy działaniami marketingowymi przetwarzają dane osobowe swoich klientów. RODO zwiększa zakres informacji, jaki należy przekazać osobom, których dane osobowe są przetwarzane. W związku z tym sklepy internetowe będą musiały zaktualizować informacje zawarte w swoich politykach prywatności tak, aby od 25 maja 2018 r. były one zgodne z zakresem wymagań przewidzianych w rozporządzeniu.

Profilowanie w sklepie internetowym

5

Profilowanie jest już dość powszechną praktyką w e-commerce. Sklepy internetowe coraz częściej stosują to narzędzie i przedstawiają kupującym online oferty dopasowane do ich potrzeb, bazując np. na historii ich wcześniejszych zakupów czy rodzaju przeglądanych na stronie produktów. Dotychczas w polskim prawie brakowało regulacji dotyczących profilowania. Sytuację tę zmieniło RODO, które wprowadza profilowanie jako nowe pojęcie prawne w systemie ochrony danych osobowych.

Zgodnie z definicją zawartą w rozporządzeniu **profilowanie oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych,** które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych człowieka, w szczególności do analizy lub prognozy aspektów dotyczących efektów jego pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się. Chodzi więc o zautomatyzowany proces polegający na wnioskowaniu o posiadaniu przez człowieka określonych cech czy zainteresowań i podejmowaniu na tej podstawie odpowiednich decyzji, np. poprzez tworzenie dedykowanych ofert dopasowanych do preferencji, zainteresowań i profilu danej osoby.

Dokonując określonej w RODO analizy skutków dla ochrony danych osobowych w kontekście profilowania, sprzedawcy internetowi będą musieli wybrać m.in. podstawę prawną takiego przetwarzania danych, wdrożyć adekwatne środki zabezpieczeń technicznych oraz spełnić obowiązki informacyjne. **Profilowanie klientów e-sklepu można będzie opierać na uprzednio otrzymanej zgodzie osoby profilowanej lub na prawnie uzasadnionych interesach realizowanych przez administratora (właściciela sklepu internetowego).** Oparcie profilowania na zgodach otrzymywanych poprzez zaznaczanie odpowiedniego checkboxu w modelu double opt-in może być czasochłonne i w dodatku nieskuteczne. Spora część klientów może nie wyrazić swojej zgody. W kontekście profilowania wydaje się to być mało praktyczny sposób. Drugą przesłanką prawną, na której sprzedawca internetowy może oprzeć stosowanie profilowania, jest wspomniana realizacja uzasadnionego interesu realizowanego przez administratora danych (sklep internetowy). Przy czym ów uzasadniony interes musi zostać skonkretyzowany i jednoznacznie opisany np. w polityce prywatności. Osoba, której dane będą przetwarzane, przykładowo poprzez stosowanie mechanizmu profilowania, musi uzyskać informacje o tym, jakie cele są w ten sposób realizowane przez administratora danych. Za taki uzasadniony interes należy uznać m.in. marketing bezpośredni własnych produktów i usług. Taka przesłanka pozwala dokonywać zautomatyzowanej oceny danej osoby (profilowania) bez konieczności pozyskania jej zgody.

Należy jednak zadbać przy tym o wdrożenie odpowiednich do zagrożeń zabezpieczeń oraz zagwarantowanie wszystkich praw osobom, których dane są przetwarzane. W szczególności należy zapewnić klientom e-sklepu możliwość wyrażenia w dowolnym czasie i w łatwy sposób sprzeciwu wobec profilowania oraz spełnić wszystkie obowiązki informacyjne. Sklepy internetowe będą więc musiały informować o stosowaniu zautomatyzowanego podejmowania decyzji, w tym profilowania, a także o trybie jego działania, znaczeniu oraz przewidywanych konsekwencjach takiej formy przetwarzania danych osobowych. Użytkownikom e-sklepów trzeba będzie również przekazywać informacje o przysługującym im prawie do sprzeciwu wobec przetwarzania danych osobowych przy użyciu mechanizmów profilowania. **W przypadku profilowania stosowanego w celach marketingowych, sprzedawca internetowy zawsze będzie musiał taki sprzeciw uszanować i zaprzestać dalszego profilowania.** W konsekwencji sprzedawcy będą musieli wdrożyć odpowiednie systemy i rozwiązania techniczne umożliwiające im realizacje przewidzianych w RODO obowiązków i uprawnień osób, których dane dotyczą. Wszystkich wymaganych

informacji dotyczących profilowania sprzedawca internetowy będzie mógł udzielić np. w polityce prywatności zamieszczonej w widocznym i łatwo dostępnym miejscu na stronie e-sklepu. Również link do polityki prywatności powinien zostać udostępniony, np. w podsumowaniu zamówienia.

W kontekście prawnych aspektów profilowania klientów sklepu internetowego uwzględnienia wymaga jeszcze jedna okoliczność. O ile stosowanie samego profilowania w celach marketingowych (np. sprofilowanie grupy klientów w celu przedstawienia odpowiednio dopasowanej do tej grupy oferty handlowej czy akcji promocyjnej) możliwe będzie bez konieczności uzyskiwania uprzedniej zgody, o tyle samo wysłanie drogą elektroniczną takiej sprofilowanej oferty (informacji handlowej) lub mailingu z informacją o akcji promocyjnej takiej zgody już oczywiście wymaga.

Jak prowadzić rejestr czynności przetwarzania i wykazać prawidłowość przetwarzania danych?

6

RODO rezygnuje z obowiązku rejestrowania zbiorów danych oraz prowadzenia ich wykazu jako elementu polityki bezpieczeństwa –obowiązkowego dotychczas dokumentu.

Dotychczasowa, dość obszerna dokumentacja ochrony danych osobowych zastąpiona zostanie obowiązkiem prowadzenia **rejestru czynności przetwarzania danych.** Rejestry muszą mieć formę pisemną (może to być również dokument w formie elektronicznej). Muszą znaleźć się w nich m. in następujące, wskazane w rozporządzeniu (art. 30) informacje:

- imię i nazwisko lub nazwa oraz dane kontaktowe administratora i wszelkich współadministratorów, a także (gdy ma to zastosowanie) przedstawiciela administratora i inspektora ochrony danych,
- cele przetwarzania,
- opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych,
- kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych,
- gdy ma to zastosowanie, informacje o przekazywaniu danych osobowych do państwa trzeciego lub organizacji międzynarodowej ze wskazaniem tych państw lub organizacji oraz udokumentowaniem stosowania odpowiednich zabezpieczeń,
- jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych,
- jeżeli jest to możliwe, ogólny opis technicznych i organizacyjny środków bezpieczeństwa stosowanych w celu zapewnienia ochrony danych osobowych.

W przypadku ewentualnej kontroli rejestr będzie trzeba udostępnić państwowemu organowi nadzorczemu. Wprawdzie rozporządzenie przewiduje również wyjątek od wymogu prowadzenia rejestru czynności przetwarzania w przypadku podmiotów zatrudniających mniej niż 250 osób, jednak wyjątek ten nie znajduje zastosowania w sytuacji, gdy przetwarzanie danych nie ma charakteru tymczasowego lub gdy dotyczy danych wrażliwych albo może powodować ryzyko naruszenia praw i wolności osób, których dane dotyczą. W praktyce dane rzadko kiedy przetwarzane są wyłącznie sporadycznie, a to w konsekwencji prowadzi do znacznego ograniczenia kręgu podmiotów, które będą mogły skutecznie powołać się na ten wyjątek. Z pewnością nie będą mogły tego uczynić sklepy internetowe, które w ramach swojej działalności regularnie przetwarzają dane osobowe klientów, choćby w celu realizacji umowy (wysłania towaru i dokonania płatności).

Wprowadzając zasadę rozliczalności, unijne rozporządzenie kładzie duży nacisk na dokumentowanie czynności związanych z przetwarzaniem danych osobowych oraz prowadzeniem oceny skutków dla ochrony danych. Administratorzy będą musieli być w stanie wykazać, iż przetwarzają dane osobowe zgodnie z przepisami zawartymi w RODO. Dlatego w rejestrze czynności przetwarzania powinny znajdować się również informacje wskazujące podstawę prawną przetwarzania, sposób, w jaki administrator spełnił obowiązki informacyjne, oraz to, komu i kiedy udostępnia dane. W praktyce bardzo ważnym dokumentem pozostanie polityka prywatności, w której administrator danych powinien spełnić wszystkie obowiązki informacyjne oraz opisać prawa osób, których dane są przetwarzane.

Wykazanie prawidłowości przetwarzania danych będzie ułatwione w przypadku stosowania zatwierdzonych przez krajowy organ nadzorczy kodeksów postępowania lub mechanizmów certyfikacji, czyli uzyskania stosownych certyfikatów i znaków jakości świadczących o zgodności przetwarzania danych z przepisami RODO. Certyfikacja będzie dobrowolna, a szczegółowe zasady akredytacji podmiotów certyfikujących określać będzie nowa ustawa o ochronie danych osobowych.

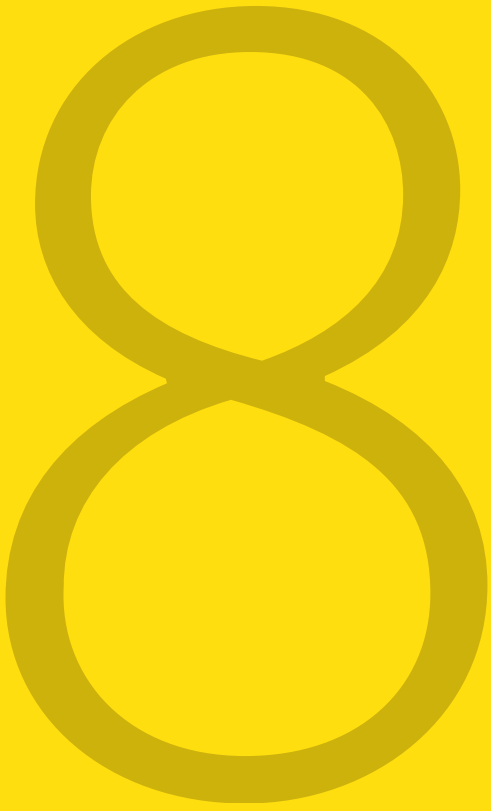
Inspektor ochrony danych osobowych (aktualnie ABI)

7

Po wejściu w życie w dniu 25 maja 2018 r. przepisów ogólnego rozporządzenia o ochronie danych rolę fachowego wsparcia dla administratorów danych i podmiotów przetwarzających pełnić będą inspektorzy ochrony danych (zwani również „DPO" od „data protection oficer"). Ich podstawowe zadania polegające na działaniu na rzecz zgodnego z przepisami o ochronie danych przetwarzania danych pokrywać będą się z dotychczasowymi zadaniami administratorów bezpieczeństwa informacji (ABI). Osoba pełniąca taką funkcję będzie musiała posiadać specjalistyczną wiedzę na temat prawa i praktyk w dziedzinie ochrony danych osobowych. Musi mieć zapewnione niezbędne środki oraz swobodę działania i podlegać bezpośrednio najwyższemu kierownictwu.

W przeciwieństwie do aktualnych regulacji przepisy RODO wprowadzają w określonych sytuacjach wymóg zatrudnienia inspektora ochrony danych (np. gdy administrator danych jest organem lub podmiotem publicznym lub gdy główna działalność administratora polega na przetwarzaniu na dużą skalę danych wrażliwych). **W przypadku przedsiębiorcy prowadzącego sklep internetowy powołanie inspektora ochrony danych osobowych (obecnie ABI) pozostanie oczywiście w dalszym ciągu dobrowolne.**

Urząd Ochrony Danych Osobowych w miejsce GIODO



Projekt nowej ustawy o ochronie danych osobowych, która ma zapewnić stosowanie przepisów RODO, zakłada powołanie w miejsce obecnego Generalnego Inspektora Ochrony Danych Osobowych **Prezesa Urzędu Ochrony Danych Osobowych.** Zmiana nazwy wymuszona została rozporządzeniem unijnym (RODO), które wprowadza instytucję inspektora ochrony danych. Inspektorem może być osoba dysponująca wiedzą ekspercką w zakresie ochrony danych osobowych, wyznaczona do tego zadania w organizacji administratora danych, np. odpowiednio przeszkolony pracownik administratora. Przyjęcie dla państwowego organu kontrolnego dotychczasowej nazwy (Generalny Inspektor Ochrony Danych Osobowych) wprowadzałoby więc w błąd i prowadziło do ustanowienia w polskim systemie ochrony danych osobowych dwóch kategorii inspektorów. Mając na uwadze powyższe, w projekcie ustawy odstąpiono również od nazywania pracowników państwowego organu nadzorczego „inspektorami" na rzecz określenia „kontrolujący".

Sankcje za naruszenia ochrony danych

9

Naruszenie ochrony danych oznacza naruszenie bezpieczeństwa i prywatności prowadzące np. do niezgodnego z prawem, nieuprawnionego ujawnienia lub dostępu do danych, ich zniszczenia, utracenia lub zmodyfikowania. Do tej pory organ nadzorczy o naruszeniach ochrony danych osobowych dowiadywał się głównie przy okazji kontroli lub na skutek skarg osób, których dane były przetwarzane w sposób nieprawidłowy.

Rozporządzenie wprowadza obowiązek poinformowania organu nadzorczego (od 25 maja 2018 r. organem tym będzie Urząd Ochrony Danych Osobowych) o naruszeniu zasad przetwarzania danych w przypadku, gdy może ono skutkować ryzykiem naruszenia praw i wolności osób, tj. np. jeśli może prowadzić do kradzieży lub fałszowania tożsamości, starty finansowej, naruszenia dobrego imienia czy też naruszenia tajemnic prawnie chronionych. Tego rodzaju naruszenia administrator danych będzie musiał zgłosić w ciągu 72 godzin od ich wykrycia. Jeżeli zgłoszenie nastąpi później, administrator będzie musiał dołączyć pisemne wyjaśnienie przyczyn opóźnienia. Administrator powinien również bez zbędnej zwłoki zawiadomić o takim naruszeniu osobę, której dane dotyczą.

Niezgłoszenie naruszenia do Urzędu Ochrony Danych Osobowych może skutkować nałożeniem przez organ nadzorczy bardzo dotkliwej kary finansowej. Oczywiście możliwe będzie również nałożenie kary już za samo naruszenie ochrony danych. Przepisy RODO przewidują surowsze niż dotychczas konsekwencje niezgodnego z prawem przetwarzania danych osobowych. Obok uprawnień naprawczych, w ramach których organ nadzorczy może wydawać ostrzeżenia i upomnienia oraz nakazywać administratorom podjęcie określonych czynności, Urząd Ochrony Danych Osobowych będzie mógł wymierzać również administracyjne kary pieniężne.

W przypadku przedsiębiorstw kary finansowe mogą wynosić maksymalnie 20 mln euro lub 4% całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego (zastosowanie ma kwota wyższa). Przepisy nie przewidują taryfikatora określającego wysokość kar za poszczególne naruszenia. Wymierzając karę pieniężną, organ nadzorczy będzie analizował każdy przypadek indywidualnie w zależności od okoliczności danej sprawy. Uwzględnieniu podlegać będą następujące okoliczności:

- charakter (umyślny lub nieumyślny), waga i czas trwania naruszenia przy uwzględnieniu liczby poszkodowanych osób, których dane dotyczą, oraz rozmiaru poniesionej przez nie szkody,
- działania podjęte przez administratora lub podmiot przetwarzający w celu zminimalizowania szkody poniesionej przez osoby, których dane dotyczą,
- stopień odpowiedzialności administratora lub podmiotu przetwarzającego z uwzględnieniem wdrożonych przez nich środków technicznych i organizacyjnych,
- historia ewentualnych wcześniejszych naruszeń ze strony administratora lub podmiotu przetwarzającego,
- stopień współpracy z organem nadzorczym w celu usunięcia naruszenia oraz złagodzenia jego ewentualnych negatywnych skutków,
- kategorie danych osobowych, których dotyczyło naruszenie,
- sposób, w jaki organ nadzorczy dowiedział się o naruszeniu, w szczególności czy i w jakim zakresie administrator lub podmiot przetwarzający zgłosił naruszenie,
- stopień wdrożenia środków nakazanych wcześniej przez organ nadzorczy w ramach jego uprawnień naprawczych,
- stosowanie mechanizmów certyfikacji lub kodeksów postępowania.

Katalog okoliczności, jakie zostaną wzięte pod uwagę przez urząd przy ustalaniu wysokości kary finansowej, jest otwarty. Oznacza to, iż organ nadzorczy może uwzględnić wszelkie okoliczności obciążające lub łagodzące, jakie uzna za istotne w konkretnym przypadku.

Przygotuj się na wejście RODO!

Politykę prywatności wraz z aktualizacjami w przypadku zmian prawa znajdziesz w pakiecie Trusted Shops.

Dowiedz się więcej:

sprzedaz@trustedshops.pl

Informacja o autorze
Marcin Jedrzejak, Legal Expert
Marcin Jędrzejak: absolwent wydziału Prawa i Administracji Uniwersytetu im. Adama Mickiewicza w Poznaniu oraz polsko-niemieckich studiów prawniczych Master of German and Polish Law na wydziale Prawa Uniwersytetu Europejskiego Viadrina we Frankfurcie nad Odrą. Ukończył również podyplomowe studia menedżerskie organizowane przez Wyższą Szkołę Bankową w Poznaniu oraz kurs administratora bezpieczeństwa informacji i posiada certyfikat ABI wydany przez TÜV SÜD Polska. Pierwsze doświadczenia zawodowe pozyskał pracując dla startupów z branży e-commerce. Następnie pracował w kancelarii Rödl & Partner w Gliwicach. Obecnie w Trusted Shops pełni funkcję specjalisty do spraw polskiego prawa.

201707_pl-PL_MKT-1052

Chcesz dowiedzieć się więcej o Trusted Shops?

Skontaktuj się z naszym konsultantem:

+48 22 462 64 00

sprzedaz@trustedshops.pl