PayU

Poradnik:
RODO

Co oznacza RODO dla e-biznesu?

SPIS TREŚCI:

1 Co zmienia RODO w e-biznesie

Czym jest RODO i jaki ma wpływ na Twój e-biznes?

RODO to nowe unijne rozporządzenie dotyczące ochrony danych osobowych nakładające na przedsiębiorców, również internetowych, dodatkowe obowiązki. Jesteś na nie gotowy? Czas na dostosowanie się do nowych przepisów mija 25 maja 2018 roku.

Ochrona danych osobowych to drażliwy temat. I skomplikowany, zwłaszcza, jeśli prowadzi się działalność w wielu krajach. Teraz tę sferę czeka wiele zmian, bo po kilku latach burzliwych dyskusji i przygotowań w 2016 r. Parlament Europejski i Rada Unii Europejskiej przyjęły Rozporządzenie Ogólne o Ochronie Danych Osobowych (RODO), zwane także „GDPR" lub „Ogólnym Rozporządzeniem o Ochronie Danych". Chodzi o nowe wytyczne dla prowadzących działalność gospodarczą, dotyczące tego, w jaki sposób mają chronić dane osobowe użytkowników.

Regulacje musiały być uwspółcześnione, bo obowiązujące do tej pory przepisy zostały ustanowione w 1995 roku – trzy lata przed powstaniem Google. To właśnie rewolucja technologiczna w największym stopniu wymusiła reformę przepisów dotyczących danych osobowych. Rozporządzenie od 25 maja 2018 r. będzie bezpośrednio stosowane we wszystkich krajach członkowskich UE.

– RODO, wbrew obawom nie wprowadzi całkowitej rewolucji w zasadach przetwarzania danych. Już teraz musisz przestrzegać wielu wymogów z tym związanych, prowadząc sklep internetowy, ale z pewnością teraz stanie się to bardziej skomplikowane – ostrzega Teresa Grabowska, ekspert w dziedzinie ochrony danych osobowych, ECDP ODO.
Do tej pory musiałeś bowiem wykazać tylko zgodność

stosowanych zabezpieczeń z listą zawartą w rozporządzeniu o środkach zabezpieczających z 2004 roku. – Teraz sytuacja diametralnie się zmieni – to Ty musisz samodzielnie ocenić adekwatność zabezpieczenia danych swoich pracowników czy klientów – dodaje ekspertka.

Czy nowe przepisy dotyczą każdego e-przedsiębiorcy?

Nowe prawo będzie dotyczyć praktycznie wszystkich, którzy przetwarzają lub przechowują dane osobowe. Czyli zarówno podmiotów publicznych, jak i przedsiębiorców – a także osób fizycznych prowadzących działalność gospodarczą na niewielką skalę, jeśli przetwarzają dane innych osób fizycznych, w tym głównie:

- pracowników,
- kandydatów do pracy,
- klientów,
- kontrahentów,
- współpracowników.

Jakie dane podlegają ochronie?

Zgodnie z definicją RODO dane osobowe to wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, a w szczególności:

- imię i nazwisko,
- PESEL,
- wizerunek (czyli zdjęcie, film...),
- dane o lokalizacji (miejsce zamieszkania lub przebywania),
- identyfikator internetowy (adresy IP, identyfikatory plików cookies),
- wszystko to, co określa fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, czy kulturową lub społeczną tożsamość (czyli np. płeć, wygląd, zarobki, stan cywilny itp.).

Musisz ustalić indywidualnie konkretne sposoby zabezpieczania tych danych w swojej firmie. Nowe regulacje nie wprowadzają bowiem sztywnych rozwiązań. Po to m.in. by uwzględnić specyfikę każdej działalności i nie tworzyć zbędnej biurokracji. Co może być zarówno plusem, jak i minusem...

RODO nie daje bowiem żadnych konkretnych wskazówek technicznych ani organizacyjnych, w jaki sposób chronić dane, aby je w pełni zabezpieczyć. Czyli zapewnić im tzw. pseudomizację, szyfrowanie, poufność, integralność, jak i szybkie przywrócenie dostępności w przypadku np. awarii Twojego sprzętu IT.

> Pseudomizacja to nowy środek zabezpieczenia danych, którego dotychczasowe przepisy w ogóle nie przewidywały. To użycie zamiast np. imienia i nazwiska rzeczywistej osoby – liczby. Wszystko po to, by nie można ich było przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji. Jest to proces odwracalny.

Większa niż obecnie będzie zatem rola administratora danych (o czym więcej w Rozdziale III). I odpowiedzialność, bo nie dostosowanie się do przepisów, co może wyjść na jaw w trakcie np. dostania się danych klientów w nieupoważnione ręce, naraża Cię na spore kary (o czym więcej w Rozdziale IV).

Tworząc zabezpieczenia dotyczące danych swoich klientów czy pracowników, będziesz musiał oczywiście uwzględnić określone prawem wytyczne. Jak również stworzyć lub dostosować do RODO dotychczasową dokumentację z zakresu danych osobowych. Będą to prawdopodobnie dokumenty bardziej rozbudowane niż te, które stosowałeś dotychczas – zgodnie z przepisami krajowymi.

Zmiany dotyczą m.in.:

- zgody na przetwarzanie danych osobowych,
- ewidencji osób upoważnionych do przetwarzania danych,
- upoważnień osób do przetwarzania danych osobowych,
- rejestru czynności przetwarzania danych osobowych,
- rejestru naruszeń ochrony danych osobowych,
- umowy powierzenia danych (jeśli je stosujesz).

SKUTKI WPROWADZENIA RODO DLA TWOJEJ FIRMY

Zniknie obowiązek rejestracji zbiorów danych osobowych w GIODO. Administratora Bezpieczeństwa Informacji będą musiały powoływać jedynie firmy zatrudniające powyżej 250 osób, przetwarzające dane na dużą skalę (np. w celach marketingowych) oraz te podmioty, które dysponują danymi osobowymi ws. wyroków skazujących i naruszeń prawa.

Zgoda na przetwarzanie danych osobowych musi być: jawna, świadoma, dobrowolna, potwierdzona.

Klient będzie mógł nie zgodzić się na wyświetlanie reklam utworzonych na podstawie jego zachowań w sieci.

„Prawo do bycia zapomnianym". Klient może zażądać, abyś usunął jego dane z bazy.

Każda umowa między firmami będzie musiała zawierać zapis dotyczący ochrony danych osobowych.

Firmy będą mieć obowiązek zgłaszania, w ciągu 72 godzin, do Prezesa Urzędu Ochrony Danych Osobowych wszystkich incydentów, w wyniku których dojdzie do wycieku danych.

2 Nowe obowiązki wobec klientów

Jakie uprawnienia zyskują klienci i jak trzeba będzie przetwarzać ich dane?

Dzięki RODO klienci będą mieć większy wpływ na to, co dzieje się z ich danymi osobowymi. Zyskają m.in. prawo do bycia zapomnianym, będą mogli również wyrazić sprzeciw wobec profilowania zwykłego, czyli wykorzystywania ich danych przy targetowaniu i reklamach kontekstowych. Co to oznacza dla e-sklepów?

Klient musi wiedzieć, po co zbierasz jego dane

Zgodnie z RODO dane osobowe będziesz mógł zbierać tylko w konkretnym, wyraźnym i prawnie uzasadnionym celu, z którym musisz klienta dokładnie zaznajomić. Nie możesz np. poinformować go, że jego dane są potrzebne do złożenia zamówienia, a potem wykorzystywać je do wyświetlania mu reklam na Facebooku.

Cel zbierania danych musi być konkretny

Twój klient musi wiedzieć, do czego konkretnie jego dane zostaną wykorzystane. Określenia typu „cele marketingowe" są zbyt ogólnikowe. Musisz w tym przypadku przynajmniej podać administratora (podmiot), który będzie te cele realizował, np.:

> Twoje dane będą przetwarzane dla celów marketingowych TWÓJ E-SKLEP Sp. z o.o., aby przesyłać Ci informacje o aktualnościach i promocjach oraz spersonalizowane oferty.

Jeżeli jednak np. prowadzisz informacyjny serwis internetowy lub bloga i chcesz dane swoich czytelników przekazać swoim reklamodawcom, aby oni także mogli przesyłać informacje handlowe, musisz użytkowników odwiedzających Twoją stronę

szczegółowo o tym poinformować, stosując sformułowania typu:

> Jeśli zgodzisz się otrzymywać od nas (NAZWA SPÓŁKI) oraz naszych reklamodawców oferty handlowe, będziesz mógł korzystać z tego serwisu bez opłat i ograniczeń.

Wysyłasz do swoich klientów newsletter? Zapewne też analizujesz odbiorców – ich płeć, zainteresowania – oraz ich działania – co i kiedy najchętniej czytają lub kupują. Oczywiście robisz to, by przesyłać im potem spersonalizowane oferty. Zgodnie z nowymi przepisami musisz poinformować klienta, do czego służy mailing. Możesz to zrobić np. w taki sposób:

> Jeśli subskrybujesz nasz newsletter, będziemy przetwarzali Twoje dane osobowe (WYMIEŃ JAKIE, np. imię, e-mail, historię otwieralności wiadomości) w celu przesyłania Ci informacji handlowych. Jeśli jesteś naszym klientem, będziemy analizowali historię Twoich zakupów, aby dostarczać Ci w newsletterze treści najbardziej dostosowane do Twoich zainteresowań.

Klient musi się na to wyraźnie zgodzić...

Zgoda klienta na przetwarzanie danych musi być dobrowolna. Co to oznacza? Że nie możesz od niej uzależniać np. wykonania umowy, w tym świadczenia usługi, jeśli przetwarzanie danych nie jest niezbędne do wykonania tej umowy.

Uwaga! Nie wystarczy już jeden przycisk („checkbox"), po wciśnięciu którego klient zezwalał na przetwarzania jego danych w celach marketingowych oraz udostępnianie ich podmiotom trzecim. Zgoda nie może być też ukryta w regulaminie, czy schowana w jakikolwiek inny sposób.

Klient, zapisując się na newsletter, musi wyrazić:

- zgodę na przetwarzanie danych osobowych do celów marketingowych,
- zgodę na przesyłanie informacji handlowych środkami komunikacji elektronicznej.

Jak ją uzyskać? Możesz zastosować np. model double opt-in. Polega on na wysłaniu na podany przy zapisie adres mailowy wiadomości z prośbą o potwierdzenie subskrypcji. Dopiero, gdy potencjalny subskrybent kliknie w link, e-mail zostaje zapisany w bazie. Wówczas komunikacja może być kontynuowana.

Pamiętaj: musisz być w stanie wykazać, że dana osoba faktycznie wyraziła stosowną zgodę – np. rejestrować w bazie danych kto, kiedy i w jaki sposób wyraził zgodę.

Według RODO zgoda jest tylko jedną z podstaw do przetwarzania danych osobowych klientów. Jeśli Twój e-sklep zawiera umowę z klientem na sprzedaż towaru, czy świadczenie usługi drogą elektroniczną, może się okazać, że już sama umowa stanowi podstawę i przesłankę do przetwarzania danych klienta. W praktyce może to oznaczać, że zamieszczanie zgody na przetwarzanie danych osobowych klienta w e-sklepie nie będzie konieczne.

Zobacz, jak wygląda umowa uwzględniająca wymogi RODO na przykładzie umowy o świadczenie usług z firmą Microsoft.

O zgodę na przetwarzanie danych musisz też poprosić przed rozmową telefoniczną z klientem lub w trakcie rozmowy poprzez chata. W tym ostatnim przypadku chatbot może wykonać robotę za Ciebie, bazując na rozwiązaniach sztucznej inteligencji.

Zgodnie z RODO możesz przetwarzać dane osób, które ukończyły 16 lat. W przypadku młodszych dzieci zgodę musi wyrazić rodzic lub opiekun. To na Tobie leży obowiązek sprawdzenia, czy zgodę wyraziła odpowiednia osoba.

Klient może zostać „zapomniany"

Zgodnie z RODO użytkownik ma prawo dostępu do swoich danych, poprawiania ich. Może także zażądać, abyś przestał przetwarzać jego dane. Na przykład abyś usunął go z bazy mailingowej. Będziesz wówczas musiał poinformować innych administratorów, którzy przetwarzają dane osobowe tego klienta, o usunięciu wszelkich łączy do tych danych, kopii lub ich replikacji.
Dla e-sklepów oznacza to konieczność ustalenia procedury związanej z przyjmowaniem i rozpatrywaniem wniosków klientów w terminie określonym przez RODO („bez zbędnej zwłoki, nie później niż 30 dni").

Ponadto, jeśli korzystasz z rozwiązań technicznych dostarczanych przez podmioty trzecie, będziesz musiał zapewnić w umowie z dostawcą, aby ten np. usunął dane klienta z systemu, jeśli kupujący zażąda, aby być „zapomnianym".

> Zgoda na przetwarzanie danych może być przez klienta w każdym momencie wycofana w równie prosty sposób, w jaki sposób została udzielona. Nie możesz więc np. wymagać od klienta, który wyraził zgodę online, aby cofnął ją, wysyłając list polecony.

W jaki sposób klienci będą mogli w praktyce domagać się od Ciebie usunięcia swoich danych?

– RODO nakłada na przedsiębiorców bardzo szczegółowe obowiązki, aby w kompleksowy sposób traktowali prośby i żądania klientów o usunięcie. W mojej ocenie na każdą prośbę, która zostanie w jakikolwiek sposób utrwalona, trzeba będzie odpowiednio zareagować – mówi Bartosz Berestecki, członek zarządu PayU.

Wszystkie firmy, które posiadają call center i kontaktują się z klientami przez telefon, mają obowiązek nagrywania tych

rozmów. W warunkach obowiązywania RODO trudno sobie wyobrazić, żeby firma mogła zignorować prośbę tylko dlatego, że została złożona telefonicznie.

– Wydaje mi się, że w niedalekiej przyszłości dojdziemy do takiej praktyki, że każdy e-mail czy telefon, który zostanie nagrany i w którym zostanie jasno wyrażone żądanie, będzie musiał być potraktowany w sposób poważny – dodaje Bartosz Berestecki.

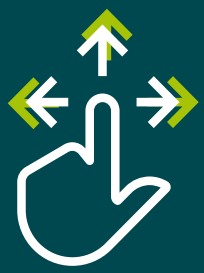
Cały wywiad z Bartoszem Beresteckim o wyzwaniach związanych z RODO przeczytaj tutaj.

Źródło: PGBS

NOWE PRAWA TWOJEGO KLIENTA

Prawo dostępu do swoich danych

Prawo do sprzeciwu wobec profilowania: Klient może zabronić Ci „targetowania" reklam poprzez pliki cookies



Prawo do przenoszenia danych

Privacy by design: Musisz uwzględnić ochronę danych klienta już na etapie projektowania, np. tworzenia aplikacji, witryny e-sklepu, czy serwisu

Privacy by default: Możesz domyślnie przetwarzać tylko te dane osobowe, które są niezbędne do osiągniecia zakomunikowanego klientowi celu przetwarzania

Prawo do „bycia zapomnianym" Klient może zażądać usunięcia go np. z bazy mailingowej. Wyjątek stanowią dane zawarte w umowach kredytowych, ubezpieczeniowych czy dotyczących roszczeń. Ich nie można usunąć

3 Jak wdrożyć RODO w swojej firmie

Jakie uprawnienia zyskują klienci i jak trzeba będzie przetwarzać ich dane?

RODO nie jest zbiorem gotowych do zastosowania rozwiązań, określa tylko wytyczne. Dlatego musisz sam stworzyć swój indywidualny system ochrony danych, które gromadzisz.

RODO niewiele narzuca, raczej daje wskazówki i jest neutralne technologicznie. Dzięki temu przepisy, nawet za kilka lat, mają być odpowiednie zarówno dla jednoosobowego sklepu internetowego, jak i ogromnego serwisu.

To na administratorze danych spoczywa obowiązek wdrożenia odpowiednich mechanizmów chroniących dane, zgromadzone m.in. poprzez:

- adresy IP,
- pliki cookies,
- informacje biometryczne,
- e-mail, dokumenty na komputerach, nagrania głosu, czy pen drive.

Zbiorów danych osobowych nie trzeba już będzie rejestrować w GIODO. W trzech przypadkach trzeba będzie natomiast wyznaczyć inspektora ochrony danych:

1. Gdy przetwarzania dokonuje organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości.
2. Gdy główna działalność administratora czy podmiotu przetwarzającego polega na operacjach przetwarzania, które wymagają regularnego i systematycznego monitorowania danych osób, których dane dotyczą, na dużą skalę (dotyczy to np. zakładów opieki zdrowotnej czy banków).

3. Gdy główna działalność administratora lub procesora polega na przetwarzaniu, na dużą skalę, szczególnych kategorii danych osobowych (RODO – art. 9 ust. 1) oraz danych dotyczących wyroków skazujących i naruszeń prawa (RODO – art. 10).

Rozporządzenie RODO dopuszcza także jednego wspólnego inspektora dla:

1. grupy przedsiębiorstw – pod warunkiem, że łatwo będzie można nawiązać z nim kontakt z każdej jednostki organizacyjnej;
2. kilku organów lub podmiotów publicznych – z uwzględnieniem ich struktury organizacyjnej i wielkości;
3. zrzeszeń lub innych podmiotów reprezentujących określone kategorie administratorów.

Musisz też zdecydować, czy wszystko zrobisz sam, czy zlecisz całość lub część procesu firmie zewnętrznej. Bez względu na to wdrożenie RODO powinno mieć podobny przebieg:

Wdrożenie RODO krok po kroku

1. Powołanie zespołu wdrożeniowego

2. Analiza zgodności

- Jakie dane przetwarzasz?
- Jaka jest podstawa prawna przetwarzania?
- Gdzie i przez kogo są przetwarzane?
- Jak długo mają być przechowywane?
- Czy dane są przekazywane innym podmiotom?
- Jak zabezpieczony jest proces przetwarzania danych?
- Czy jesteś w stanie realizować nowe prawa podmiotów danych?

3. Szczegółowy harmonogram wdrożenia RODO

- Audyt prawny: treść klauzul, zgód, polityk, procedur, umów powierzenia. Przygotowanie raportu i zaleceń
- Audyt informatyczny: zabezpieczenia i funkcjonalność systemów informatycznych pod względem możliwości realizacji praw właścicieli danych. Przygotowanie raportu i zaleceń

- DPIA (Data Protection Impact Assesment): ocena skutków przetwarzania dla ochrony danych
- Analiza ryzyka dla zasobów uczestniczących w operacjach przetwarzania danych

4. Zaprojektowanie działań zgodnych z RODO i ich wdrożenie

- Przygotowanie dokumentacji przetwarzania danych osobowych, zawierającej wymagane prawem elementy
- Dostosowanie systemów informatycznych
- Wdrożenie nowych rozwiązań prawnych i informatycznych zgodnie z RODO
- Monitoring i stałe zapewnienie zgodności
- Szkolenia pracowników

> **Pamiętaj**, że jako administrator danych sam odpowiadasz za proces przetwarzania danych osobowych i ich ochrony, ponieważ to administrator decyduje o środkach i celach przetwarzania. Nawet, jeśli Twoja firma zleci wdrożenie RODO zewnętrznej firmie.

Do czego potrzebny jest audyt?

Audyt to kontrola obecnego stanu zarządzania danymi i procedur postępowania. Ma pomóc Ci sprawdzić:

- czy masz wszystkie zgody na przetwarzanie danych,
- czy zawarte są odpowiednie umowy wskazujące odpowiedzialnych za zarządzanie danymi,
- czy umowy zlecające usługi na zewnątrz gwarantują bezpieczeństwo przepływu danych.

Musisz też sprawdzić samą procedurę przepływu informacji wewnątrz firmy.

Ile to kosztuje?

Ile taki audyt będzie Cię kosztować? Widełki kosztów mogą być bardzo szerokie. Audyt procedur może kosztować od

1 tysiąca złotych (np. w małym e-sklepie, gdzie trzeba jedynie skonsultować umowy), po kilkadziesiąt tysięcy złotych w dużej korporacji, zatrudniającej dziesiątki lub setki osób i operującej danymi na terenie Unii Europejskiej, czy nawet na całym świecie.

Podobnie duże różnice w kosztach mogą wystąpić przy zamówieniu inwentaryzacji danych. W lokalnej firmie z dużą bazą, ale nie rozproszoną na serwerach po świecie, może to kosztować 2 tysiące złotych. W takiej, gdzie dane są rozsiane globalnie, firmy doradcze mogą zażądać nawet 20 tys. złotych.

W dłuższej perspektywie może Ci się to jednak opłacić. Jeśli na przykład klient zażąda usunięcia swoich danych, musisz je usunąć ze wszystkich lokalizacji, a więc z archiwum z umowami, z cyfrowej bazy danych, z bazy handlowej itd. Gdy tego nie zrobisz, grożą Ci bardzo wysokie kary (patrz Rozdział IV).

Jakie informacje musi podawać administrator danych osobowych (ADO)?

Zanim skonstruujesz komunikat, w którym poprosisz o zgodę na przetwarzanie danych osobowych, pamiętaj, że jako administrator tych danych musisz podać do publicznej wiadomości:

- Twoją tożsamość (nazwę firmy) oraz dane kontaktowe inspektora ochrony danych;
- cele przetwarzania danych osobowych oraz podstawę prawną przetwarzania;
- informacje o odbiorcach danych;
- informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej;
- okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
- informacje o prawach do usunięcia danych, ograniczenia ich przetwarzania oraz do przenoszenia danych; informacje o prawie do cofnięcia zgody w dowolnym momencie;
- informacje o prawie wniesienia skargi do organu nadzorczego;

- informacje, czy podanie danych osobowych wynika z przepisów, czy tylko z zawartej umowy oraz jakie są ewentualne konsekwencje ich niepodania;
- informacje o zautomatyzowanym podejmowaniu decyzji (np. automatyczne odrzucenie elektronicznego wniosku kredytowego czy elektroniczne metody rekrutacji bez udziału człowieka) o profilowaniu oraz o konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

Jak taki komunikat może wyglądać w praktyce?

Prosimy o zapoznanie się z poniższymi informacjami oraz wyrażenie zgody poprzez zaznaczenie pola „zgadzam się". Pamiętaj, że zawsze możesz wycofać zgodę.

25 maja 2018 roku zacznie obowiązywać Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 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 (określane jako „RODO", „ORODO", „GDPR" lub „Ogólne Rozporządzenie o Ochronie Danych").
W związku z tym chcielibyśmy poinformować o przetwarzaniu Twoich danych oraz zasadach, na jakich będzie się to odbywało po dniu 25 maja 2018 roku. Chodzi o dane osobowe, które są zbierane w ramach korzystania przeze Ciebie z naszego serwisu internetowego, w tym zapisywanych w plikach cookies. Kto będzie administratorem Twoich danych? Administratorami Twoich danych będziemy my: E-FIRMA SPÓŁKA SP. O.O.

W związku z powyższym, zgadzam się na przetwarzanie w celach marketingowych, w tym profilowanie oraz celach analitycznych, moich danych osobowych zbieranych w ramach korzystania przeze mnie z serwisu XXX, w tym zapisywanych w plikach cookies przez E-FIRMĘ SP. Z O.O.

Wyrażenie tej zgody jest dobrowolne i możesz ją dowolnym momencie wycofać, z tym, że wycofanie zgody nie będzie miało wpływu na zgodność z prawem przetwarzania na podstawie zgody, przed jej wycofaniem.

Zamiast zgłaszania zbiorów – prowadzenie rejestru czynności przetwarzania danych

Od momentu rozpoczęcia stosowania RODO nie trzeba będzie zgłaszać zbiorów danych do rejestracji u odpowiedniego organu (obecnie GIODO).

Będziesz musiał za to prowadzić rejestr czynności przetwarzania danych osobowych, w którym podać trzeba takie informacje, jak:

- imię i nazwisko lub nazwę oraz dane kontaktowe administratora;
- cele przetwarzania (np. świadczenie e-usługi);
- opis kategorii osób, których dane dotyczą (np. klienci sklepu lub użytkownicy aplikacji);
- opis kategorii danych osobowych (np. adresy e-mail);
- kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione;
- jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;
- jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.

Przedsiębiorcy zatrudniający poniżej 250 pracowników nie muszą prowadzić takiego rejestru, ale pod warunkiem, że przetwarzanie:

- nie powoduje ryzyka naruszenia praw lub wolności osób, których dane dotyczą;
- nie ma charakteru sporadycznego lub
- obejmuje szczególne kategorie danych osobowych (np. dane ujawniające pochodzenie rasowe lub etniczne, czy poglądy polityczne) lub dane osobowe dotyczące wyroków skazujących i naruszeń prawa.

Pamiętaj, że samo przechowywanie danych jest już równoznaczne z ich przetwarzaniem. A zatem jeśli prowadzisz e-sklep i przechowujesz dane klientów, oznacza to, że nie przetwarzasz ich sporadycznie i powinieneś prowadzić ewidencję. Można ją prowadzić w formie elektronicznej.

Uwaga! To Twój wewnętrzny dokument i nie możesz umieszczać go na stronie internetowej dostępnej dla użytkowników.

4 Incydenty i sankcje

Regulator zyskał dzięki RODO potężny bat na firmy nie wystarczająco chroniące dane osobowe. Nowe przepisy zakładają wysokie kary za łamanie prawa. Mogą one sięgnąć aż 20 mln euro lub 4 proc. całkowitego rocznego obrotu spółki.

Jako administrator danych osobowych masz kolejny ważny obowiązek. Musisz najpóźniej w terminie 72 godzin zgłosić właściwemu organowi nadzorczemu (UODO – Urząd Ochrony Danych Osobowych) jakikolwiek incydent, który mógł doprowadzić do naruszenia danych osobowych, np.:

- ujawnienie informacji osobom nieupoważnionym,
- udostępnianie hasła i loginu innym użytkownikom,
- złamanie zasad polityki bezpieczeństwa informacji,
- awaria zasilania,
- uszkodzenie informacji,
- kradzież systemów (laptop, urządzenie przenośne),
- kradzież oprogramowania,
- podejrzenie kradzieży danych.

W zgłoszeniu musisz opisać okoliczności naruszenia ochrony danych (np. wysłałeś do jednego z dostawców listę wszystkich swoich klientów z ich danymi adresowymi), informacje o skutkach i o tym, jakie podjąłeś działania zaradcze (np. dane zostały zaszyfrowane). Jeśli przekroczysz termin 72 godzin, musisz dołączyć do swojego zgłoszenia wyjaśnienie przyczyn opóźnienia.

> Każda osoba, która poniosła szkodę majątkową lub niemajątkową z powodu naruszenia swoich danych osobowych, może domagać się od Ciebie odszkodowania za poniesione szkody.

Co grozi za niedostateczną ochronę danych?

Nieprzestrzeganie RODO może jednak mieć dużo poważniejsze skutki. Prezes Urzędu Ochrony Danych Osobowych (który zastąpi GIODO) będzie miał miesiąc na skontrolowanie firmy. Jeśli uzna, że narusza ona czyjąś prywatność, wymierzy jej karę finansową.

Kary do **10 mln euro** lub **2%** całkowitego rocznego obrotu:

- powierzenia danych bez zapewnienia wysokiej ochrony danych przez podmioty je przetwarzające, w szczególności bez umowy określającej prawa i obowiązki;
- niezgłoszenia naruszenia ochrony danych w ciągu 72 h od jego wykrycia, jeśli w danej sytuacji podmiot byłby do tego zobowiązany lub braku współpracy z organem nadzorczym;
- niewyznaczenia inspektora ochrony danych, jeśli jest się do tego zobowiązanym.

Kary do **20 mln euro** lub **4%** całkowitego rocznego obrotu za nieprzestrzeganie przepisów w zakresie m.in. takich spraw, jak:

- podstawowe zasady przetwarzania danych, w tym niezapewnienie warunków udzielenia świadomej i dobrowolnej zgody;
- prawa osób, których dane dotyczą, w tym prawa do przenoszenia danych i bycia zapomnianym;
- przekazywania danych odbiorcy w państwie trzecim, bez uwzględnienia odpowiednich regulacji prawnych.

Jeśli PUODO (Prezes Urzędu Ochrony Danych Osobowych) uzna, że dalsze przetwarzanie danych może spowodować poważne i trudne do usunięcia skutki, może zakazać dalszego przetwarzania danych. Co to oznacza w praktyce? Sklep internetowy, któremu PUODO zakaże przetwarzania danych klientów, straci możliwość prowadzenia sprzedaży.

> Decyzje PUODO będą podlegać kontroli sądów administracyjnych, które mogą się nie zgodzić ze stanowiskiem organu.

W projekcie ustawy o ochronie danych osobowych Ministerstwo Cyfryzacji przewidziało również dwa przepisy karne:

- Za udaremnienie lub utrudnianie kontrolującemu prowadzenie kontroli przestrzegania przepisów o ochronie danych osobowych będzie groziła grzywna, kara ograniczenia wolności lub pozbawienia wolności do lat dwóch.
- Za przetwarzanie szczególnych kategorii danych (ujawniających np. pochodzenie rasowe czy poglądy polityczne) bez podstawy prawnej będzie groziła grzywna, kara ograniczenia wolności, albo pozbawienia wolności do roku.

Spokojnie, nie od razu w przypadku naruszeń będziesz płacił milionowe kary, czy trafisz do więzienia. Przepisy przewidują, że wcześniej możesz otrzymać ostrzeżenia, upomnienia oraz decyzje niezawierające kar. Poza tym wiele zależy od tego, czy i jak współpracujesz z urzędnikami.

Instytucje akredytowane przez Prezesa Urzędu Ochrony Danych Osobowych będą mogły wydawać certyfikację dla firm. Certyfikat będzie oznaczał zgodność określonego rozwiązania narzędzi/systemów IT z wymogami RODO. Certyfikat może obejmować wszystkie procesy przetwarzania danych osobowych w całej firmie, bądź też wybrane procesy (np. w kontekście zatrudnienia), produkty lub usługi. Certyfikacja w zakresie zgodności z RODO będzie też miała znaczenie w przypadku wprowadzania nowych produktów (np. aplikacji, programów).

Jeżeli zdobędziesz certyfikat, będziesz bardziej wiarygodny w kontekście zgodności z nowymi przepisami o ochronie danych. Posiadanie certyfikatu może mieć również wpływ na wysokość ewentualnej kary finansowej. Certyfikat jest ważny 3 lata.

Decyzja o ukaraniu jest zarezerwowana dla najbardziej opornych, czyli tych, którzy nie będą reagować na upomnienia, czy naprawiać tego, co zostało uznane przez kontrolerów za niezgodne z RODO.

Materiał powstał we współpracy z ECDP ODO - spółką wyspecjalizowaną w ochronie danych osobowych w Grupie ECDP.

business consulting

Szukasz aktualnych wiadomości i przydatnych porad ze świata e-commerce?
Czytaj bloga PayU: https://www.payu.pl/blog