Elavon

Czas na zmiany

Przewodnik po Ogólnym Rozporządzeniu o Ochronie Danych Osobowych (RODO)

elavon.pl

Ogólne Rozporządzenie o Ochronie Danych Osobowych (RODO) będzie regulowało kwestie w zakresie prywatności oraz przetwarzania danych osobowych osób na terenie Unii Europejskiej (UE). Przewodnik ten wyjaśnia, co to oznacza, jak wpłynie na osoby i firmy, takie jak Państwa, oraz przekazuje wszelkie informacje na temat nowego prawa.

Podsumowanie RODO

Kiedy nowe rozporządzenie wchodzi w życie?

25 maja 2018 r.

Co się zmieni?

Wprowadzone zostaną nowe prawa dotyczące dostępu osób do informacji przechowywanych na ich temat przez firmy, a także obowiązki w zakresie lepszego zarządzania danymi przez firmy oraz nowe postanowienia w zakresie kar

Co to jest RODO?

W styczniu 2012 r. Komisja Europejska stworzyła plany reformy w zakresie ochrony danych w całej Unii Europejskiej, co miało „przygotować Europę na erę cyfrową". Niemal cztery lata później uzgodniono, co taka reforma powinna obejmować i jak przepisy dotyczące tej reformy będą egzekwowane.

Jednym z głównych elementów reform jest wprowadzenie Ogólnego Rozporządzenia o Ochronie Danych Osobowych. Te nowe zasady UE dotyczą organizacji działających we wszystkich krajach członkowskich oraz firm na całym świecie, które współpracują z osobami z UE.

RODO to zasadniczo nowy zestaw reguł opracowanych, by zapewnić ludziom więcej kontroli nad ich danymi. Jego celem jest uproszczenie otoczenia regulacyjnego prowadzenia działalności, aby zarówno ludzie, jak i firmy mogli w pełni korzystać z cyfrowej gospodarki.

Reformy te mają za zadanie odzwierciedlać świat, w którym obecnie żyjemy, oraz ustanowić prawa i obowiązki na terenie Europy w odpowiedzi na postęp technologiczny.

Zasadniczo niemalże każdy aspekt naszego życia opiera się na danych. Od firm mediów społecznościowych, po banki, sklepy i rządy – niemalże każda usługa, z jakiej korzystamy, zbiera i analizuje nasze dane osobowe. Państwa imię i nazwisko, adres, numer karty płatniczej oraz inne dane są zbierane, analizowane oraz, co prawdopodobnie najważniejsze, przechowywane przez organizacje. Celem RODO jest harmonizacja regulacji w Europie, co ma być odpowiedzią na dzisiejsze wymogi związane z wymianą danych.

Co to oznacza dla mojej organizacji?

RODO będzie obowiązywało organizację lub osobę przetwarzającą jakiekolwiek dane osobowe osób w UE. Oznacza to, że firmy oraz osoby spoza UE, sprzedające towary lub usługi osobom mieszkającym w UE, również będą musiały przestrzegać nowego prawa. Ostatecznie oznacza to, że niemal każda wielka korporacja na świecie będzie musiała być przygotowana na wejście w życie RODO oraz musi zacząć pracować nad swoją strategią zgodności z tym rozporządzeniem. RODO dotyczy administratorów, współadministratorów oraz podmiotów przetwarzających dane, jednak ważne jest ich rozróżnienie, gdyż obowiązki każdego z nich są różne.

Czy są Państwo administratorem, czy podmiotem przetwarzającym dane?

Różne terminy

Nie każdy podmiot przetwarzający dane osobowe osób jest taki sam, a prawa w zakresie ochrony danych umożliwiają to, określając trzy różne kategorie: Administrator, współadministrator i podmiot przetwarzający dane. Oto, co oznaczają:

Administrator

Administrator to podmiot (osoba bądź firma) określający cel i sposób przetwarzania danych osobowych.

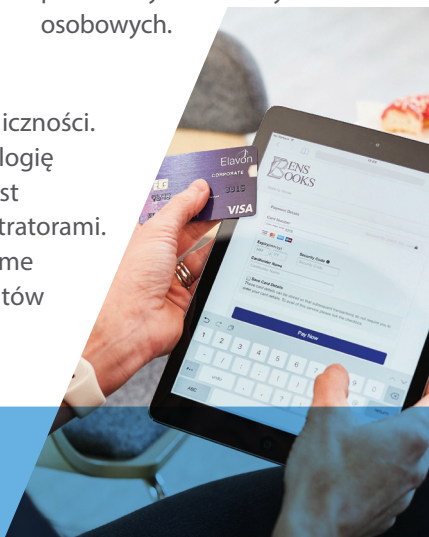
Współadministrator

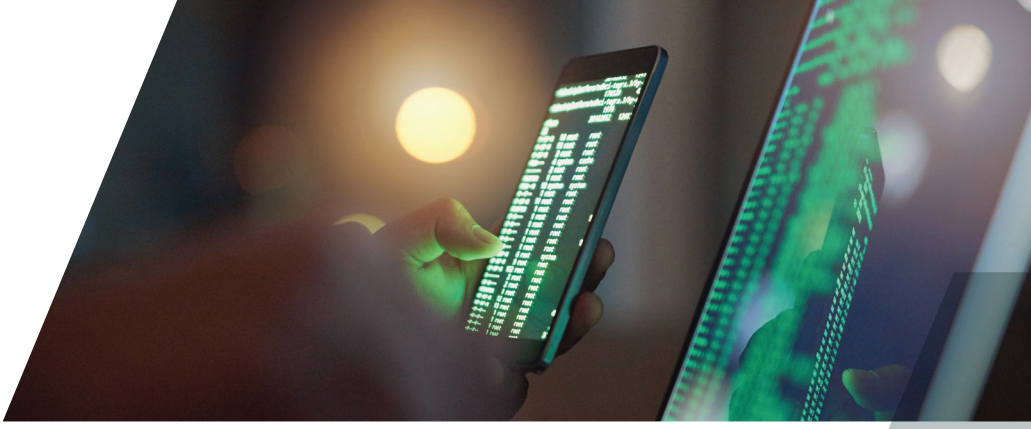
Jeśli dwie lub więcej firm wspólnie określa cel i sposób przetwarzania danych osobowych, np. wspólnie decyduje o przeznaczeniu/ powodach, okazji, naturze, zakresie oraz celach przetwarzania danych.

Podmiot przetwarzający dane

Osoba lub grupa przetwarzająca dane w imieniu administratora. Przetwarzanie oznacza zbieranie, zapisywanie, dostosowywanie lub przechowywanie danych osobowych.

Ten sam podmiot może być zarówno administratorem, jak i podmiotem przetwarzającym, w zależności od okoliczności. Na przykład firma technologiczna dostarczająca technologię przetwarzania płatności sprzedawcom internetowym jest podmiotem przetwarzającym, a sprzedawcy są administratorami. Jednakże, jeśli ta firma technologiczna wykorzysta te same dane osobowe, by dostarczać docelowe segmenty klientów reklamodawcom, działa wtedy jako administrator.





RODO ostatecznie nakłada obowiązki prawne na podmiot przetwarzający, by ten prowadził dokumentację danych osobowych i tego, w jaki sposób te dane są przetwarzane, zapewniając o wiele wyższy poziom odpowiedzialności prawnej w przypadku naruszenia bezpieczeństwa danych w firmie.

Administratorzy będą również zmuszeni zapewnić, by wszystkie kontrakty z Podmiotami przetwarzającymi dane spełniały wymogi RODO.

Czym są dane osobowe i wrażliwe dane osobowe?

Typy danych uważanych za dane osobowe w ramach obecnej legislacji obejmują imię i nazwisko, adres, zdjęcia i numer PESEL. RODO rozszerza definicję danych osobowych, by w niektórych okolicznościach danymi osobowymi można było uznać np. adres IP. Obejmuje to także wrażliwe dane osobowe, takie jak dane genetyczne i biometryczne, które można przetwarzać, by w unikalny sposób zidentyfikować osobę.

Dane osobowe

Dane związane z żyjącą osobą, którą można zidentyfikować bezpośrednio lub pośrednio, np.:

- Imię i nazwisko
- Numer telefonu
- Adres e-mail
- PESEL

Wrażliwe dane osobowe

Dane osobowe składające się z informacji, takich jak:

- Pochodzenie rasowe bądź etniczne osoby, której dotyczą dane
- Poglądy polityczne
- Wyznanie bądź inne wierzenia
- Ewentualne członkostwo w związku zawodowym
- Stan zdrowia fizycznego lub psychicznego
- Życie seksualne

Co ustanawia RODO

RODO składa się z 99 artykułów. W ich zakres wchodzą postanowienia ogólne, obowiązki administratora, współadministratora i podmiotu przetwarzającego dane, a także współpraca z władzami nadzorczymi.

Istotne zmiany, które mogą wpłynąć na Państwa organizację, to:

- **Zasada uwzględniania ochrony danych w fazie projektowania** – Ochrona danych musi być wbudowana w procesy oraz systemy biznesowe od początku i musi być zapewniana na etapie projektowania
- **Prawo do bycia zapomnianym** – Użytkownicy mogą poprosić, by ich dane zostały usunięte; mogą również poprosić, by ich kopia została przesłana do podmiotu trzeciego
- **Obowiązkowe powiadomienie o naruszeniu danych** – Niektóre naruszenia danych osobowych muszą być teraz niezwłocznie zgłaszane do osób, których te dane dotyczą, oraz do władz w ciągu 72 godzin
- **Kary za nieprzestrzeganie wymogów** – RODO przewiduje kary do 20 milionów EUR lub 4% rocznego globalnego obrotu firmy, w zależności od tego, która kwota jest wyższa

Jak wygląda zgodność z RODO?

Nie istnieje uniwersalne podejście do przygotowania się do RODO.

Każda firma będzie musiała określić, co dokładnie należy zrobić, aby spełniać te wymogi. Ważne, by wiedzieć, czy jest się podmiotem przetwarzającym dane, czy administratorem danych. Większość firm prawdopodobnie będzie pełnić obie role, w zależności od konkretnych otrzymywanych danych.

Jak się przygotować

- Rozpocząć od zrozumienia, jakie dane osobowe są przechowywane i kto ma do nich dostęp
- Ograniczyć dostęp w oparciu o potrzebę biznesową oraz wprowadzić monitoring, by wykryć wszelkie przypadki nieuprawnionego dostępu
- Przeprowadzić ocenę tego, jakie środki kontrolne w zakresie zgodności i bezpieczeństwa stosują Państwo do zbierania i ochrony danych, na ile są one skuteczne oraz gdzie znajdują się luki
- Opracować plan poprawy swojego programu bezpieczeństwa, przyglądając się osobom, procesom i technologii
- Wprowadzić proces powiadomień o naruszeniach danych, w tym możliwości wykrywania incydentów oraz reakcji na nie
- Niektóre organizacje muszą również mieć Inspektora ds. ochrony danych (*Data Protection Officer*, DPO)

Ramy PCI DSS wspierają zgodność w zakresie bezpieczeństwa RODO

RODO nie ustanawia szczegółowo ram w zakresie zgodności/bezpieczeństwa. Jednakże Standard Bezpieczeństwa Danych Branży Kart Płatniczych (*Payment Card Industry Data Security Standard*, PCI DSS) zapewnia użyteczny punkt wyjścia programu zgodności w zakresie zarządzania danymi osobowymi. Zmiana jednego określenia (z danych „posiadaczy kart" na dane „osobowe") w ramach 12 głównych wymogów PCI DSS zapewni logiczną strukturę dla kategorii „płatniczej" i „osobowej" w zakresie zgodności z RODO:

Cele	Wymagania
Stworzyć i utrzymać bezpieczną sieć	1. Zainstalować i utrzymywać konfigurację zapory sieciowej, by chronić dane **osobowe** 2. Nie stosować dostarczonych przez sprzedawców domyślnych haseł systemowych i innych parametrów bezpieczeństwa
Chronić dane posiadaczy kart	3. Chronić przechowywane dane **osobowe** 4. Szyfrować transmisję danych **osobowych** w otwartych, publicznych sieciach
Utrzymywać program zarządzania słabymi punktami w zabezpieczeniach	5. Stosować i regularnie uaktualniać oprogramowanie antywirusowe 6. Opracowywać i utrzymywać bezpieczne systemy i aplikacje
Wprowadzić silne środki kontroli dostępu	7. Ograniczać dostęp do danych **osobowych** do potrzeby biznesowej 8. Przydzielić unikalny identyfikator każdej osobie mającej dostęp do komputera 9. Ograniczać fizyczny dostęp do danych **osobowych**
Regularnie monitorować i testować sieci	10. Śledzić i monitorować wszelki dostęp do zasobów sieciowych oraz danych **osobowych** 11. Regularnie testować systemy bezpieczeństwa oraz procesy
Utrzymywać Politykę bezpieczeństwa informacji	12. Utrzymywać politykę dotyczącą bezpieczeństwa informacji dla całego personelu

Jeśli zachowana jest zgodność z PCI DSS i wszelkie dane osobowe/istotne dane traktowane są w taki sam sposób, jak dane posiadaczy kart, nie ma powodów do zmartwień. Co ważniejsze, PCI DSS nie obejmuje wszystkich wymogów ustanowionych przez RODO, lecz zapewnia użyteczny punkt wyjścia w zakresie bezpieczeństwa danych (Artykuł 32 RODO dla UE – „Bezpieczeństwo przetwarzania danych").

Lista kontrolna przygotowań do zapewnienia zgodności z RODO

- Ustanowić program pracy, co pozwoli sporządzić spójny spis procesów związanych z danymi osobowymi.
- Oceniać stopień ryzyka swoich danych według przyjętego procesu.
- Wiedzieć, gdzie i jak przekazywane są dane osobowe podmiotom zewnętrznym oraz zapewnić posiadanie prawidłowych kontraktów w celu utrzymywania zgodności z RODO.
- Ocenić swój program bezpieczeństwa w zakresie informacji, związany z danymi osobowymi, biorąc pod uwagę strony trzecie, którym przekazują Państwo dane.
- Przestrzeganie Standardu Bezpieczeństwa Danych Branży Kart Płatniczych dla podstawowego bezpieczeństwa danych osobowych oraz danych posiadaczy kart.
- W razie potrzeby należy zapewnić, że informacje oraz treść udzielanej przez klienta zgody lub zgód, przekazywane do podpisu klientom, są przejrzyste, wyraźne, jednoznaczne i napisane prostym językiem.
- Nakreślić plan zgodności w zakresie bardziej kompleksowych praw podmiotu, którego dotyczą dane, w tym praw dostępu, do zmiany i nanoszenia poprawek, do przeniesienia danych oraz do ich usunięcia.
- Ustanowić mechanizm identyfikacji tego, czy, kiedy i gdzie mają miejsce naruszenia i jak będzie się na nie reagować.
- Mieć audytora śledczego CI (*PCI Forensic Investigator*, PFI) w gotowości w przypadku naruszenia danych posiadaczy kart.

Jakie są konsekwencje nieposiadania statusu zgodności z wymogami bezpieczeństwa danych ?

Firmy, które nie podjęły kroków w celu zapewnienia, by ich działania w zakresie przetwarzania danych osobowych spełniały nowe obowiązki w ramach RODO, mogą podlegać karom za nieposiadanie statusu zgodności z wymogami bezpieczeństwa danych. Kary te mogą zostać nałożone zarówno na administratorów danych, jak i na podmioty przetwarzające dane.

Niezgodność z RODO może skutkować karą w wysokości do 20 milionów EUR lub 4% rocznego globalnego obrotu firmy macierzystej, co dla niektórych firm może oznaczać milionowe straty lub bankructwo.

Kary będą zależały od tego, jak poważne było naruszenie bezpieczeństwa danych oraz od tego, czy uzna się, że firma wystarczająco poważnie podeszła do zgodności oraz wymogów w zakresie bezpieczeństwa.

Maksymalna kara w wysokości 20 milionów EUR lub 4% obrotu na całym świecie, w zależności od tego, która kwota jest wyższa, nakładana jest za naruszenia praw podmiotów, których dotyczą dane, nieuprawniony międzynarodowy transfer danych osobowych oraz niewprowadzenie procedur bądź ignorowanie próśb podmiotu, którego dotyczą dane, o dostęp do swoich danych.

Niższy limit 10 milionów EUR lub 2% obrotów na całym świecie zostanie zastosowany w przypadku firm, które w inny nieprawidłowy sposób obchodzą się z danymi. Obejmuje to m.in. niezgłoszenie naruszenia bezpieczeństwa danych, niewprowadzenie wbudowanej prywatności oraz niezapewnienie, by ochronę danych stosować na pierwszym etapie projektu, oraz zgodności poprzez wyznaczenie Inspektora ds. ochrony danych (jeśli dotyczy).

W jaki sposób Elavon może pomóc?

Pytania, z którymi mogą Państwo się zmagać:

- Jak uzyskać zgodę pracowników?
- Co dokładnie należy dokumentować w ramach działań związanych z przetwarzaniem danych?
- Czy jesteśmy administratorem danych w zakresie danych pracowników, jakie przekazujemy usługodawcom w zakresie emerytur i świadczeń zdrowotnych?
- Jaki ma z tym wszystkim związek PCI DSS i czy jest to pomocne?
- Czy potrzebujemy Inspektora ds. ochrony danych?
- Co mamy robić ze wszystkimi naszymi danymi marketingowymi?

Aby pomóc klientom w radzeniu sobie z tymi zapytaniami, firma Elavon nawiązała stosunki z wieloma wiodącymi firmami zajmującymi się bezpieczeństwem danych. Wraz z naszymi partnerami firma Elavon może Państwu pomóc w zakresie wszelkich pytań dotyczących PCI i RODO, oferując usługi takie jak audyt, konsulting, analiza luk, planowanie gotowości na incydenty, a także zarządzane usługi związane z bezpieczeństwem.

Proszę skontaktować się z nami teraz pod adresem **PCIEurope@elavon.com**, aby uzyskać więcej informacji.

Współpraca

Proszę się z nami skontaktować, by sprawdzić, jak możemy pomóc Państwu w przygotowaniach do uzyskania zgodności ze standardami PCI DSS oraz RODO.

My stwarzamy możliwości. Państwo z nich korzystają.

PCIEurope@elavon.com

elavon.pl/strefa-klienta/zabezpieczswojafirme/pcicompliance

Elavon Financial Services Designated Activity Company (Spółka z Ograniczoną Odpowiedzialnością o Wyznaczonym Przedmiocie Działalności) Oddział w Polsce z siedzibą w Warszawie, ul. Puławska 17, 02-515 Warszawa, zarejestrowany w rejestrze przedsiębiorców Krajowego Rejestru Sądowego prowadzonym przez Sąd Rejonowy dla m.st. Warszawy w Warszawie, XIII Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS 287836, numer REGON 300649197, NIP 2090000825, kapitał zakładowy Elavon Financial Services Designated Activity Company 6.400.001,00 euro. Elavon Financial Services DAC prowadzi działalność gospodarczą pod nazwą Elavon Merchant Services i podlega nadzorowi Centralnego Banku Irlandii. Y2633v10118