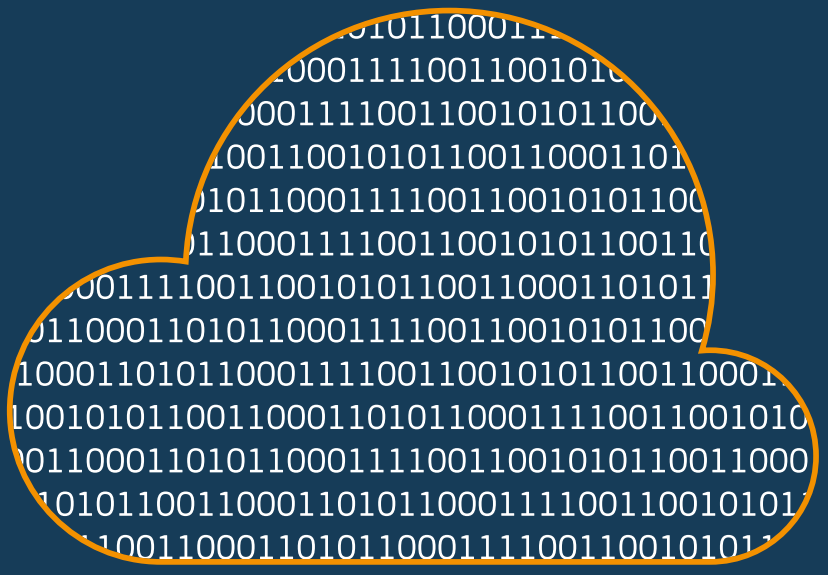
Komisja Europejska

RODO: nowe możliwości, nowe obowiązki



Wszystko, co każdy przedsiębiorca powinien wiedzieć o ogólnym rozporządzeniu UE o ochronie danych

Sprawiedliwość i konsumenci

Printed by Bietlot in Belgium

Luksemburg: Urząd Publikacji Unii Europejskiej, 2018

Print	ISBN 978-92-79-79411-7	doi:10.2838/915427	DS-01-18-082-PL-C
PDF	ISBN 978-92-79-79436-0	doi:10.2838/030304	DS-01-18-082-PL-N

SPIS TREŚCI

ROZDZIAŁ 1

MOŻLIWOŚCI GOSPODARCZE

RODO reguluje sposób, w jaki przedsiębiorstwa przetwarzają dane osobowe i zarządzają nimi. Począwszy od 25 maja 2018 r. nowe rozporządzenie będzie mieć zastosowanie do wszystkich przedsiębiorstw i organizacji (np. szpitali, organów administracji publicznej itd.). Stanowi zarazem największą od 20 lat zmianę w unijnych przepisach dotyczących ochrony danych.

RODO zawiera przepisy, które nie tylko dają obywatelom większą kontrolę nad tym, w jaki sposób wykorzystywane są ich dane osobowe, ale też istotnie wpływają na usprawnienie otoczenia regulacyjnego, w jakim działają firmy. Jest to możliwe dzięki ustanowieniu jednolitych ram prawnych dla przepisów w zakresie ochrony danych stosowanych na terenie całej UE. Innymi słowy oznacza to, że w miejsce przepisów o ochronie danych obowiązujących w poszczególnych krajach wprowadzone zostanie jedno rozporządzenie, któremu będzie podlegać cała Unia. W efekcie przedsiębiorstwa prowadzące działalność na terenie różnych krajów nie będą już podlegać wielu – często różniącym się od siebie – zbiorom przepisów. Zamiast tego, aby móc oferować swoje usługi w dowolnym kraju UE, będą musiały przestrzegać jedynie przepisów RODO.

Korzyści dla Twojej firmy płynące z RODO

- **Jedna Unia, jedno prawo:** wspólny zbiór przepisów oznacza łatwiejszy i oszczędniejszy sposób prowadzenia działalności na terenie UE.
- **Kompleksowa współpraca:** w większości przypadków firmy kontaktują się tylko z jednym organem ochrony danych.
- **Europejskie przepisy na europejskiej ziemi:** jeśli firma z siedzibą poza UE oferuje swoje towary lub usługi osobom fizycznym w UE, ma obowiązek przestrzegać tych samych przepisów co firmy europejskie.
- **Podejście oparte na ryzyku:** w miejsce uciążliwych i uniwersalnych obowiązków prawnych RODO wprowadza wymogi odpowiednio dostosowane do poszczególnych rodzajów i poziomów ryzyka.
- **Zasady na miarę innowacji:** przepisy RODO są neutralne pod względem technologii.

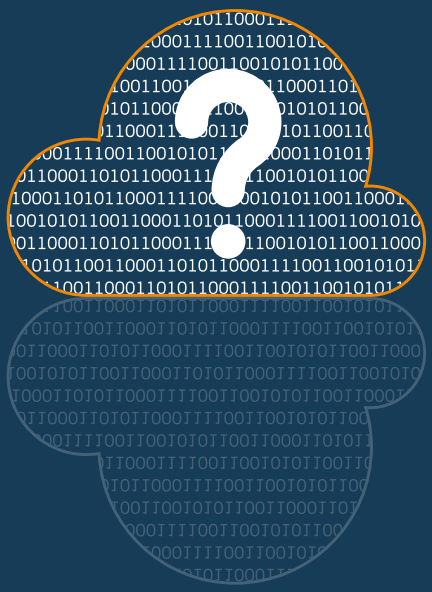
Chodzi o zaufanie

Ochrona danych osobowych jest istotną kwestią dla obywateli. Stąd tak niski poziom zaufania do środowisk cyfrowych. Z badania Eurobarometru wynika, iż:

- 80 proc. obywateli ma poczucie, że nie ma pełnej kontroli nad swoimi danymi osobowymi;
- 60 proc. twierdzi, że nie ma zaufania do firm internetowych;
- ponad 90 proc. Europejczyków chce, aby w całej UE przysługiwały im te same prawa w zakresie ochrony danych.

RODO daje nowe możliwości, dzięki którym firmy mogą budować zaufanie konsumentów poprzez zarządzanie danymi osobowymi w oparciu o analizę ryzyka.

„Jeśli dane przedsiębiorstwo nie zapewni odpowiedniej ochrony danych osobowych osób fizycznych, może utracić zaufanie konsumentów, które jest przecież niezbędne do tego, by ich zachęcać do korzystania z nowych produktów lub usług”.



ROZDZIAŁ 2

INTERPRETACJA PRZEPISÓW RODO

Czy moja firma podlega przepisom RODO?

W skrócie, RODO ma zastosowanie do ***każdego*** przedsiębiorstwa, które:

przetwarza dane osobowe w sposób **zautomatyzowany** lub **ręczny** (jeśli dane uporządkowane są według określonych kryteriów).

Nawet jeśli Twoja firma zajmuje się przetwarzaniem danych w imieniu innych firm, musi przestrzegać tych samych przepisów.

RODO ma zastosowanie w przypadku, gdy:

- przedsiębiorstwo przetwarza dane osobowe i ma siedzibę w UE, niezależnie od miejsca przetwarzania danych; lub
- przedsiębiorstwo posiada siedzibę poza UE, ale oferuje towary lub usługi osobom fizycznym na terenie UE bądź zajmuje się monitorowaniem ich zachowania.

Czym są dane osobowe?

Dane osobowe to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania żyjącej osoby fizycznej. Mogą to być na przykład:

- imię i nazwisko
- adres i numer telefonu
- lokalizacja
- dokumentacja dotycząca zdrowia
- dochody i dane bankowe
- preferencje kulturowe
- ...i inne.

Dane osobowe, które zostały pozbawione elementów pozwalających na identyfikację lub poddane pseudonimizacji, ale które mogą prowadzić do ponownej identyfikacji osoby fizycznej, pozostają danymi osobowymi objętymi zakresem RODO. Za dane osobowe nie uważa się jednak danych osobowych zanonimizowanych w taki sposób, że osób, których dane dotyczą, nie można już zidentyfikować. Wówczas takie dane nie są objęte RODO.

Rozporządzenie jest neutralne pod względem technologii, a więc zapewnia ochronę danych osobowych niezależnie od rodzaju technologii użytej do przetwarzania czy sposobu przechowywania danych osobowych. Ponadto nie ma znaczenia, czy firma przetwarza i przechowuje dane osobowe w złożonym systemie IT czy w formie papierowej – we wszystkich tych przypadkach podlega wymogom określonym w RODO.

„Nie ma znaczenia, czy firma przetwarza i przechowuje dane osobowe w złożonym systemie IT czy w formie papierowej – we wszystkich tych przypadkach podlega wymogom określonym w RODO”.

Zachowaj większą ostrożność w przypadku szczególnych (wrażliwych) kategorii danych osobowych

Wszelkie gromadzone dane osobowe zawierające informacje dotyczące zdrowia, rasy, orientacji seksualnej, religii, poglądów politycznych lub przynależności do związków zawodowych są uznawane za dane wrażliwe. Takie dane można przetwarzać wyłącznie pod ściśle określonymi warunkami, i prawdopodobnie Twoja firma będzie musiała stosować dodatkowe zabezpieczenia, takie jak szyfrowanie.

Czym jest przetwarzanie danych osobowych?

Zgodnie z RODO wszystkie czynności takie jak gromadzenie, wykorzystywanie i usuwanie danych osobowych mieszczą się w definicji przetwarzania danych osobowych.

Czy na terenie swojego przedsiębiorstwa stosujesz monitoring w systemie CCTV? Czy na potrzeby działalności korzystasz z bazy danych zawierającej dane osobowe? Czy wysyłasz promocyjne wiadomości e-mail? Czy zajmujesz się usuwaniem plików (cyfrowych) dotyczących pracowników lub niszczeniem dokumentów? Czy może chcesz umieścić zdjęcie innej osoby na swojej stronie internetowej lub na portalu społecznościowym?

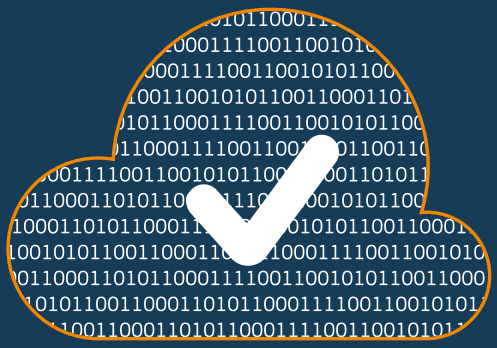
Jeśli na co najmniej jedno pytanie Twoja odpowiedź brzmi „tak”, to Twoja firma z całą pewnością przetwarza dane osobowe.

W jaki sposób RODO przyczynia się do obniżania kosztów?

Przy tworzeniu przepisów RODO wzięto pod uwagę potrzeby przedsiębiorców. Świadczy o tym między innymi fakt, że celem rozporządzenia jest wyeliminowanie wymogów administracyjnych, aby obniżyć koszty i zmniejszyć do minimum obciążenie administracyjne:

- **Zniesienie wymogu wcześniejszego powiadamiania**: reforma w większości przypadków znosi wymóg wcześniejszego powiadamiania organów nadzorczych, a co za tym idzie – ponoszenia związanych z tym kosztów.
- **Inspektorzy ochrony danych**: przedsiębiorstwa przeważnie mają obowiązek powołać inspektora ochrony danych (IOD), jeśli ich główną działalność stanowi przetwarzanie danych wrażliwych na dużą skalę lub regularne i systematyczne monitorowanie osób na dużą skalę. Organy administracji publicznej mają obowiązek powołania IOD.
- **Ocena skutków dla ochrony danych**: przedsiębiorstwa mają obowiązek dokonywania oceny skutków dla ochrony danych tylko wtedy, gdy proponowane przetwarzanie danych wiąże się z wysokim ryzykiem dla praw i wolności osób fizycznych.
- **Prowadzenie rejestrów**: przedsiębiorstwa zatrudniające mniej niż 250 pracowników nie mają obowiązku prowadzenia rejestrów, o ile przetwarzanie danych ma charakter incydentalny lub gdy nie dotyczy danych wrażliwych.

„Celem rozporządzenia jest wyeliminowanie wymogów administracyjnych, aby obniżyć koszty i zmniejszyć do minimum obciążenie administracyjne”.



ROZDZIAŁ 3

TWOJE OBOWIĄZKI WYNIKAJĄCE Z RODO

W myśl przepisów RODO na przedsiębiorstwa z całej UE nałożone zostały bezpośrednie obowiązki w zakresie przetwarzania danych. Zgodnie z RODO firmy mogą przetwarzać dane osobowe *wyłącznie* pod ściśle określonymi warunkami. Przetwarzanie powinno się odbywać, między innymi, w sprawiedliwy i przejrzysty sposób, w jasno określonych i uzasadnionych celach, a ponadto powinno być ograniczone do danych, które są niezbędne do osiągnięcia tych celów. Poza tym musi być oparte na jednej z poniższych podstaw prawnych.

- **Zgoda** osoby, której dane są przetwarzane.
- **Zobowiązanie umowne** zawarte pomiędzy firmą a daną osobą.
- Wypełnianie **obowiązku prawnego**.
- Ochrona żywotnych interesów danej osoby.
- Realizacja **zadania w interesie publicznym**.
- **Prawnie uzasadnione interesy** firmy, ale z wyjątkiem sytuacji, w których ma to poważne skutki dla podstawowych praw i wolności osoby, której dane są przetwarzane. Jeśli prawa przysługujące osobie, której dane dotyczą, są nadrzędne wobec Twoich interesów, nie możesz przetwarzać tych danych.

Więcej o uzyskaniu zgody na wykorzystanie danych osobowych

RODO przewiduje rygorystyczne przepisy w zakresie przetwarzania danych na podstawie zgody. Celem tych przepisów jest gwarancja, że osoby zainteresowane będą rozumiały, czego dotyczy udzielona przez nie zgoda. Oznacza to, że zgoda powinna być **wyrażona w sposób dobrowolny, konkretny, świadomy** i **jednoznaczny** oraz uzyskana na podstawie zapytania o zgodę sformułowanego jasnym i prostym językiem. Ponadto powinna być wyrażona za pomocą **działania potwierdzającego**, jak na przykład zaznaczenie okienka online lub podpisanie formularza.

W przypadku danych osobowych dotyczących **dziecka**, przetwarzanych na podstawie zgody, wymagane jest uzyskanie zgody rodzicielskiej. Jednak z uwagi na to, że w zależności od kraju UE granica wieku wynosi od 13 do 16 lat, zalecamy zapoznanie się z krajowymi przepisami prawa w tym zakresie.

Pamiętaj! Gdy dana osoba zgadza się na przetwarzanie swoich danych osobowych, Twoja firma może przetwarzać te dane wyłącznie do celów, których dotyczy zgoda. Ponadto musisz dać osobie, której dane dotyczą, możliwość wycofania wcześniej wyrażonej zgody.

Określając swoją rolę, określisz swoją odpowiedzialność

Jeśli z Twoich ustaleń wynika, że Twoja firma zajmuje się przetwarzaniem danych osobowych i podlega przepisom RODO, kolejnym krokiem będzie zdefiniowanie roli, jaką pełnisz w związku z przetwarzaniem.

Przepisy o ochronie danych wprowadzają rozróżnienie między administratorem danych a podmiotem przetwarzającym dane, co niesie ze sobą różne obowiązki. Administrator danych ustala cele, do których dane osobowe są przetwarzane, oraz sposoby ich przetwarzania, natomiast podmiot przetwarzający dane dokonuje przetwarzania danych osobowych wyłącznie w imieniu administratora. Nie oznacza to jednak, że podmiot przetwarzający może się po prostu schować za plecami administratora danych.

Na mocy RODO od administratora danych wymaga się, aby zatrudniał wyłącznie te podmioty przetwarzające dane, które są w stanie zapewnić wystarczające gwarancje. Gwarancje powinny być częścią pisemnej umowy zawartej pomiędzy administratorem danych a podmiotem przetwarzającym. Umowa taka powinna nadto zawierać szereg obowiązkowych klauzul, w tym na przykład klauzulę stwierdzającą, iż podmiot przetwarzający dane będzie przetwarzał dane osobowe wyłącznie na podstawie udokumentowanego polecenia administratora danych.

Obowiązki mające na celu ochronę poszczególnych praw

RODO określa szereg wymogów, które mają chronić prawa obywateli do kontrolowania ich własnych danych osobowych.

Twój obowiązek: zapewnianie przejrzystych informacji

Firmy muszą przekazywać osobom, których dotyczą dane, informacje o tym, kto przetwarza jakie dane i dlaczego. Minimum informacji musi wyraźnie określać:

- kto zbiera dane;
- dlaczego dane są przetwarzane;
- co jest podstawą prawną przetwarzania;
- komu będą przekazane dane (w stosownych przypadkach).

W niektórych wypadkach informacje muszą dodatkowo określać:

- dane kontaktowe IOD;
- prawnie uzasadniony interes (jeśli jest on podstawą prawną uzasadniającą przetwarzanie);
- podstawę uzasadniającą przekazanie danych do kraju spoza UE;
- jak długo dane będą przechowywane;
- prawa ochrony danych przysługujące osobom fizycznym (czyli prawa do dostępu, sprostowania, usuwania, ograniczania, sprzeciwu, przenoszenia itd.);
- w jaki sposób można wycofać zgodę (w przypadku gdy zgoda stanowi podstawę prawną przetwarzania);
- czy przekazanie danych stanowi obowiązek ustawowy lub umowny;
- w przypadku zautomatyzowanego podejmowania decyzji – informacje o zasadach, znaczeniu i konsekwencjach takiej decyzji.

„Firmy muszą przekazywać osobom, których dotyczą dane, informacje o tym, kto przetwarza jakie dane i dlaczego”.

Twój obowiązek: prawo dostępu i prawo do przenoszenia danych

Osoby fizyczne mają prawo zażądać dostępu do swoich danych osobowych, bez żadnych opłat, a także otrzymać ich kopię w powszechnie dostępnym formacie. Gdy otrzymasz takie żądanie, masz obowiązek:

- poinformować daną osobę o tym, czy przetwarzasz jej dane osobowe;
- udzielić informacji o procesie przetwarzania (między innymi o celach przetwarzania, kategoriach przetwarzanych danych osobowych, odbiorcach tych danych itd.);
- udostępnić kopię przetwarzanych danych osobowych dotyczących tej osoby.

Ponadto, jeżeli przetwarzanie odbywa się na podstawie zgody lub umowy, osoba fizyczna może poprosić o zwrot jej danych osobowych lub o przekazanie ich innej firmie. To uprawnienie nazywane jest prawem do przenoszenia danych. Dane powinny zostać dostarczone w powszechnie używanym i nadającym się do odczytu maszynowego formacie.

Pomimo że powyższe prawa są ze sobą ściśle powiązane, to stanowią dwa odrębne prawa. Dlatego też musisz dołożyć starań, aby nie mieszać ich ze sobą i aby udzielać osobom zainteresowanym właściwych informacji.

Twój obowiązek: prawo do usunięcia danych (prawo do bycia zapomnianym)

W pewnych okolicznościach, na przykład gdy dane nie są już potrzebne do celów, w jakich zostały zgromadzone, zainteresowana osoba fizyczna może zwrócić się do administratora z żądaniem usunięcia jej danych osobowych. Niemniej jednak Twoja firma nie jest zobowiązana do spełnienia żądania danej osoby w przypadku, gdy:

- przetwarzanie danych jest niezbędne do zapewnienia wolności wypowiedzi i prawa do informacji innych osób;
- dalsze przechowywanie danych osobowych jest uzasadnione wymogami prawnymi;
- istnieją inne względy interesu publicznego, na podstawie których dane osobowe muszą być przechowywane, na przykład do celów związanych ze zdrowiem publicznym lub badaniami naukowymi i historycznymi;
- przechowywane dane potrzebne są do ustalenia roszczeń.

Twój obowiązek: prawo do sprostowania danych i prawo do sprzeciwu

Jeżeli osoba, której dane dotyczą, uzna, że jej dane osobowe są niepoprawne, niekompletne lub niedokładne, ma wówczas prawo do ich sprostowania lub uzupełnienia bez zbędnej zwłoki.

W przypadku gdy przetwarzanie odbywa się na podstawie prawnie uzasadnionego interesu firmy albo w ramach zadania realizowanego w interesie publicznym, osoba, której dane dotyczą, może w dowolnym momencie sprzeciwić się przetwarzaniu jej danych osobowych w określonym celu. Wówczas musisz zaprzestać przetwarzania danych osobowych, chyba że Twój uzasadniony interes przeważa nad interesem tej osoby. Na tej samej zasadzie, dopóki nie zostanie ustalone, czy uzasadniony interes firmy przeważa nad interesem osoby, której dane dotyczą, może ona poprosić o ograniczenie przetwarzania jej danych osobowych. Jednak w przypadku marketingu bezpośredniego firmy zawsze mają obowiązek zaprzestania przetwarzania danych osobowych na żądanie zainteresowanej osoby.

Przestroga dotycząca zautomatyzowanego podejmowania decyzji i profilowania

Osoby fizyczne mają prawo do tego, by nie podlegać decyzji opartej wyłącznie na zautomatyzowanym przetwarzaniu. Istnieją jednak wyjątki od tej reguły, a mianowicie gdy dana osoba udzieliła wyraźnej zgody na zautomatyzowane podejmowanie decyzji. Poza wyjątkowymi sytuacjami, w których zautomatyzowana decyzja została podjęta zgodnie z prawem, Twoja firma ma obowiązek:

- poinformować daną osobę o zautomatyzowanym podejmowaniu decyzji;
- dać jej prawo do tego, by zautomatyzowana decyzja została zweryfikowana przez człowieka;
- dać jej możliwość wniesienia sprzeciwu wobec zautomatyzowanej decyzji.

Przykładowo, jeżeli bank w sposób zautomatyzowany podejmuje decyzję o przyznaniu lub nieprzyznaniu kredytu zainteresowanej osobie, wówczas ta osoba powinna zostać poinformowana o tym, że decyzja w jej sprawie zapadła w sposób zautomatyzowany oraz że przysługuje jej prawo do wniesienia sprzeciwu wobec tej decyzji i zażądania interwencji człowieka.

Obowiązki wynikające z analizy ryzyka

Poza wymogami mającymi chronić prawa osób fizycznych RODO przewiduje także szereg wymogów, których stosowanie zależy od analizy ryzyka.

Twój obowiązek: powołanie inspektora ochrony danych (IOD)

Inspektor ochrony danych jest odpowiedzialny za monitorowanie zgodności z przepisami RODO. Jednym z głównych zadań należących do IOD jest dostarczanie informacji i doradzanie pracownikom zajmującym się faktycznym przetwarzaniem danych osobowych na temat ich obowiązków. Ponadto IOD współpracuje z organem ochrony danych, pełniąc rolę punktu kontaktowego zarówno dla organu ochrony danych, jak i osób fizycznych.

Twoja firma jest zobowiązana do wyznaczenia IOD w przypadku, gdy:

- zajmuje się regularnym lub systematycznym monitorowaniem osób bądź przetwarzaniem szczególnych kategorii danych;
- przetwarzanie stanowi główną działalność gospodarczą; oraz
- odbywa się na dużą skalę.

Na przykład, jeżeli przetwarzasz dane osobowe na potrzeby kierowania reklam za pośrednictwem wyszukiwarek internetowych w oparciu o zachowanie użytkowników w środowisku online, zgodnie z RODO musisz powołać IOD. Jeśli jednak raz do roku rozsyłasz materiały promocyjne do swoich klientów, nie potrzebujesz usług IOD. Podobnie gdy jesteś lekarzem, który gromadzi dane dotyczące zdrowia pacjentów. W takim wypadku prawdopodobnie nie potrzebujesz usług IOD. Jeśli jednak przetwarzasz dane osobowe dotyczące genetyki i zdrowia na rzecz szpitala, wówczas ustanowienie IOD jest wymagane.

Twój obowiązek: ochrona danych w fazie projektowania oraz domyślna ochrona danych

Na mocy RODO wprowadzone zostają dwie nowe zasady: ochrona danych w fazie projektowania oraz domyślna ochrona danych.

Ochrona danych w fazie projektowania ma pomóc w zapewnieniu, aby firmy uwzględniały ochronę danych już na wczesnych etapach planowania nowych metod przetwarzania danych osobowych. Zgodnie z tą zasadą administrator danych musi podjąć wszelkie środki techniczne i organizacyjne, które są niezbędne do stosowania przepisów ochrony danych i zabezpieczenia praw osób fizycznych. Mogą to być takie środki, jak na przykład pseudonimizacja.

Ochrona danych w fazie projektowania ma na celu zminimalizowanie ryzyka, a jednocześnie zwiększenie zaufania. Uwzględnienie ochrony danych jako jednego z podstawowych elementów rozwijania nowych produktów lub usług pomoże już na wczesnym etapie uniknąć wszelkich możliwych problemów związanych z ochroną danych. Ponadto taka praktyka przyczynia się do podnoszenia świadomości w zakresie ochrony danych wśród pracowników wszystkich działów i na każdym szczeblu przedsiębiorstwa.

Domyślna ochrona danych jest zasadą, zgodnie z którą firmy zawsze muszą zapewniać użytkownikom jak najwyższy stopień prywatności w ramach ustawień domyślnych. Jeśli na przykład możliwe są dwa rodzaje ustawień i jedno z nich blokuje innym osobom dostęp do danych osobowych, właśnie to ustawienie powinno być ustawieniem domyślnym.

„Ochrona danych w fazie projektowania ma na celu zminimalizowanie ryzyka, a jednocześnie zwiększenie zaufania”.

„Domyślna ochrona danych jest zasadą, zgodnie z którą firmy zawsze muszą zapewniać użytkownikom jak najwyższy stopień prywatności w ramach ustawień domyślnych”.

Twój obowiązek: odpowiednie powiadomienie w przypadku naruszenia ochrony danych

Naruszenie ochrony danych występuje, gdy dane, za które odpowiedzialny jest podmiot, zostały przypadkowo albo niezgodnie z prawem ujawnione nieuprawnionym odbiorcom lub gdy zostały zmodyfikowane bądź są czasowo niedostępne.

Kluczowe dla firmy jest wdrożenie odpowiednich środków technicznych i organizacyjnych zapobiegających możliwym naruszeniom ochrony danych. Jeśli jednak miało miejsce naruszenie ochrony danych i stwarza ono ryzyko dla praw i wolności osób fizycznych, Twoja firma powinna zgłosić je do swojego organu ochrony danych w ciągu 72 godzin od stwierdzenia naruszenia.

W zależności od tego, czy naruszenie ochrony danych powoduje *wysokie* ryzyko dla osób poszkodowanych, firma może mieć też obowiązek poinformowania o tym wszystkich osób poszkodowanych wskutek tego naruszenia.

Przekazujesz dane osobowe poza UE?

RODO ma zastosowanie do Europejskiego Obszaru Gospodarczego (EOG), który obejmuje wszystkie kraje UE oraz Islandię, Liechtenstein i Norwegię. W momencie gdy dane są przekazywane poza strefę EOG, ochrona zapewniana przez RODO powinna przemieszczać się wraz z danymi. Oznacza to, że aby móc wysyłać dane za granicę, przedsiębiorstwa muszą stosować określone zabezpieczenia.

RODO oferuje zróżnicowany zestaw narzędzi do stosowania w przypadku przekazywania danych do krajów trzecich. Zgodnie z RODO taki transfer danych jest dozwolony pod warunkiem, że:

1. środki ochrony w danym kraju zostały uznane przez UE za odpowiednie; lub
2. Twoja firma podejmuje niezbędne działania, aby zapewnić odpowiednie zabezpieczenia, takie jak na przykład umieszczenie specjalnych klauzul w umowie zawartej z podmiotem spoza Europy importującym dane osobowe; lub
3. Twoja firma przekazuje dane na przykład w oparciu o szczególne podstawy (zwane „wyjątkami"), takie jak zgoda osoby fizycznej.

Aby uzyskać więcej informacji na temat przepisów obowiązujących w przypadku międzynarodowych przepływów danych, należy zapoznać się z komunikatem Komisji Europejskiej w sprawie wymiany i ochrony danych osobowych w zglobalizowanym świecie: http://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52017DC0007&from=PL

Kiedy należy dokonać oceny skutków dla ochrony danych?

Ocena skutków dla ochrony danych jest wymagana w każdym przypadku, gdy planowane operacje przetwarzania danych mogą stanowić wysokie ryzyko naruszenia praw lub wolności osób fizycznych. Odnosi się to na przykład do korzystania z nowych technologii.

Zgodnie z RODO wysokie ryzyko dotyczy co najmniej poniższych sytuacji:

- mechanizmy zautomatyzowanego przetwarzania i profilowania są wykorzystywane do systematycznej i wszechstronnej oceny osób;
- obszar dostępny publicznie jest systematycznie monitorowany na dużą skalę (np. CCTV);
- dane wrażliwe są przetwarzane na dużą skalę (np. dane dotyczące zdrowia).

Celem oceny skutków dla ochrony danych jest ustalenie potencjalnych zagrożeń dla praw i wolności osób fizycznych jeszcze przed rozpoczęciem przetwarzania danych osobowych i pojawieniem się ryzyka. Zapobiegając pojawianiu się ryzyka, można uniknąć szkód i zminimalizować koszty.

Jeśli środki wskazane w ocenie skutków dla ochrony danych nie wyeliminują wszystkich wykrytych czynników wysokiego ryzyka, przed rozpoczęciem planowanego przetwarzania danych należy je skonsultować z organem ochrony danych.

„Ocena skutków dla ochrony danych jest wymagana w każdym przypadku, gdy planowane operacje przetwarzania danych mogą stanowić wysokie ryzyko naruszenia praw lub wolności osób fizycznych”.

Co należy zrobić

Udzielanie odpowiedzi na żądania

Jeśli Twoja firma otrzymała wniosek osoby fizycznej, która chce skorzystać z przysługujących jej praw, należy odpowiedzieć na jej żądanie bez zbędnej zwłoki, a w każdym razie w ciągu 1 miesiąca od otrzymania wniosku. Termin udzielenia odpowiedzi może zostać jednak wydłużony o 2 miesiące w przypadku skomplikowanych spraw lub dużej ilości wniosków, o ile zainteresowana osoba została o tym wydłużeniu terminu poinformowana. Ponadto żądania powinny być rozpatrywane **bezpłatnie**. Jeśli odrzucisz żądanie, musisz poinformować zainteresowaną osobę o powodach odrzucenia, a także o przysługującym jej prawie do wniesienia skargi do organu ochrony danych.

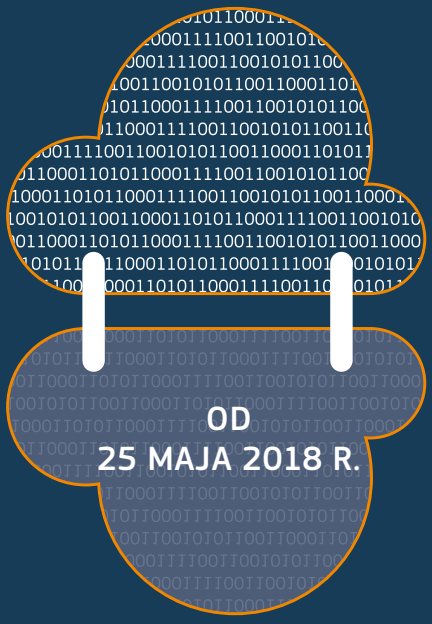
Wykaż zgodność z przepisami i prowadź rejestry!

Jedną z podstawowych zasad, na których opiera się RODO, jest zadbanie o to, aby przedsiębiorstwa mogły wykazać, że przestrzegają przepisów. Oznacza to, że Twoja firma musi udowodnić, iż działa zgodnie z RODO i spełnia wszystkie obowiązujące wymogi, w szczególności na żądanie lub podczas kontroli prowadzonej przez organ ochrony danych.

Jednym ze sposobów na wykazanie zgodności jest prowadzenie rejestrów zawierających poniższe informacje:

- nazwa i dane teleadresowe firmy zajmującej się przetwarzaniem danych;
- powody przetwarzania danych osobowych;
- opis kategorii osób udostępniających dane osobowe;
- podział organizacji otrzymujących dane osobowe na kategorie;
- informacje o transferze danych osobowych do innych krajów lub organizacji;
- okres przechowywania danych osobowych;
- opis środków ochrony stosowanych przy przetwarzaniu danych osobowych.

Dodatkowo Twoja firma powinna posiadać – i regularnie aktualizować – pisemne procedury i wytyczne, które są udostępniane także pracownikom firmy.



ROZDZIAŁ 4

PEŁNA GOTOWOŚĆ NA STOSOWANIE RODO

RODO pozostawia przetwarzanie danych osobowych w Twoich rękach. Pierwszym krokiem, jaki musisz wykonać, jest zdefiniowanie bieżących operacji przetwarzania danych i dokonanie ponownej oceny wewnętrznych procesów Twojego przedsiębiorstwa. Musisz w szczególności podjąć poniższe działania:

- określić, jakie dane posiadasz, do jakich celów je wykorzystujesz i w oparciu o jaką podstawę prawną;
- sprawdzić wszystkie obowiązujące umowy, zwłaszcza te zawarte pomiędzy administratorami a podmiotami przetwarzającymi dane;
- ocenić wszystkie dostępne szlaki międzynarodowych transferów danych; oraz
- dokonać przeglądu ogólnego zarządzania firmą (czyli sprawdzić, jakie posiadasz rozwiązania IT i środki organizacyjne), włącznie z ustaleniem, czy masz obowiązek lub chcesz powołać inspektora ochrony danych.

Istotnym elementem tego procesu jest zadbanie o to, aby najwyższe kierownictwo firmy brało udział we wspomnianych przeglądach i ustaleniach, dostarczało informacji oraz było na bieżąco z aktualnościami i zmianami w zakresie przepisów o ochronie danych.

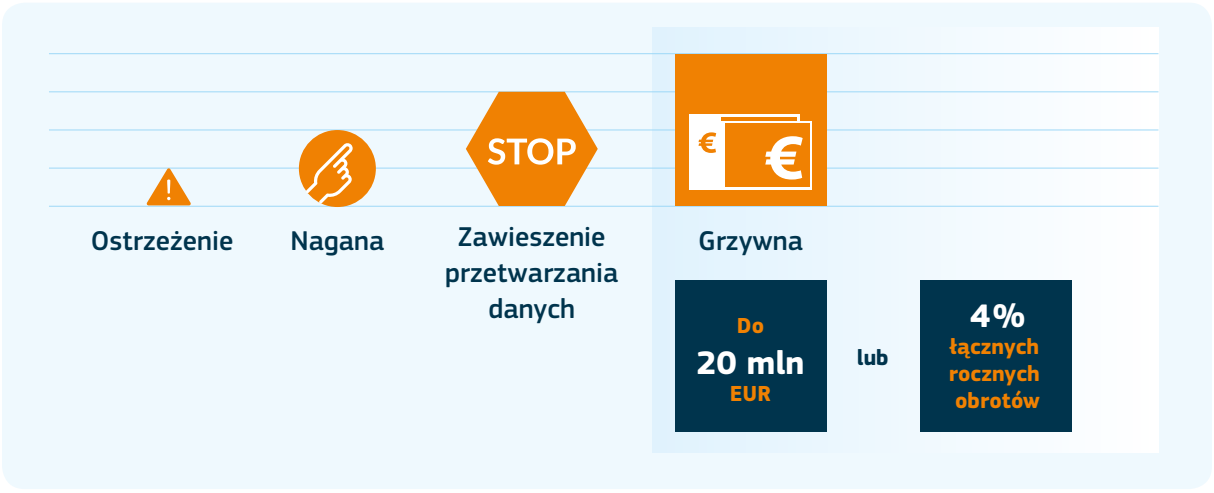
Przetwarzasz dane w różnych krajach?

W przypadku transgranicznego przetwarzania danych może się zdarzyć, że właściwym organem nie jest Twój krajowy organ ochrony danych, ale organ nadzorczy z innego kraju. Zazwyczaj jest to organ ochrony danych w kraju, w którym znajduje się główna jednostka organizacyjna Twojej firmy (czyli miejsce, gdzie zapadają decyzje dotyczące celów i sposobów przetwarzania) na terenie UE.

Ryzyko nieprzestrzegania przepisów

Nieprzestrzeganie przepisów RODO może skutkować nałożeniem znacznych kar finansowych – w wysokości do 20 mln EUR lub 4% całkowitych obrotów firmy za niektóre naruszenia. Organ ochrony danych może zastosować dodatkowe środki naprawcze, takie jak nakaz zaprzestania przetwarzania danych osobowych. Należy też wziąć pod uwagę utratę dobrego imienia wskutek nieprzestrzegania przepisów.

Cena niestosowania się do przepisów RODO jest ewidentnie dużo wyższa niż jakiekolwiek nakłady poniesione na przestrzeganie prawa.



Pytania? Wątpliwości? Prosimy o kontakt z krajowym organem ochrony danych.

Wyszukaj online organ ochrony danych w swoim kraju

http://ec.europa.eu/justice/data-protection/article-29/structure/data-protection-authorities/index_en.htm

WAŻNA INFORMACJA

Informacje i wskazówki zawarte na stronach niniejszej broszury mają na celu lepsze zrozumienie unijnych przepisów o ochronie danych.

Służą jedynie jako narzędzie informacyjne – moc prawną posiada wyłącznie treść ogólnego rozporządzenia o ochronie danych (RODO). W związku z tym wyłącznie przepisy RODO mogą rodzić prawa i obowiązki dla osób fizycznych. Niniejsze wytyczne nie skutkują żadnymi wykonalnymi prawami ani oczekiwaniami.

Wiążąca wykładnia aktów prawnych UE należy do wyłącznych kompetencji Trybunału Sprawiedliwości Unii Europejskiej. Opinie wyrażone w niniejszych wytycznych są bez uszczerbku dla stanowiska, jakie Komisja może przyjąć przed Trybunałem Sprawiedliwości.

Ani Komisja Europejska, ani żadna osoba działająca w imieniu Komisji Europejskiej nie jest odpowiedzialna za sposób wykorzystania niniejszych informacji.

Zważywszy, że niniejsze wytyczne odzwierciedlają stan wiedzy w momencie ich sporządzania, powinny być traktowane jako „rozwijające się narzędzie", które można doskonalić, a jego treść może być modyfikowana bez powiadomienia.

Jak skontaktować się z UE

Osobiście

W całej Unii Europejskiej istnieje kilkaset centrów informacyjnych Europe Direct. Adres najbliższego centrum można znaleźć na stronie: https://europa.eu/european-union/contact_pl.

Telefonicznie lub drogą mailową

Europe Direct to serwis informacyjny, który udziela odpowiedzi na pytania na temat Unii Europejskiej. Można się z nim skontaktować:

– dzwoniąc pod bezpłatny numer telefonu: 00 800 6 7 8 9 10 11 (niektórzy operatorzy mogą naliczać opłaty za te połączenia),
– dzwoniąc pod standardowy numer telefonu: +32 22999696,
– drogą mailową: https://europa.eu/european-union/contact_pl.

Wyszukiwanie informacji o UE

Online

Informacje o Unii Europejskiej są dostępne we wszystkich językach urzędowych UE w portalu Europa: https://europa.eu/european-union/index_pl.

Publikacje UE

Bezpłatne i odpłatne publikacje UE można pobrać lub zamówić w serwisie EU Bookshop: https://publications.europa.eu/bookshop. Większą liczbę egzemplarzy bezpłatnych publikacji można otrzymać, kontaktując się z serwisem Europe Direct lub z lokalnym centrum informacyjnym (zob. https://europa.eu/european-union/contact_pl).

Prawo UE i powiązane dokumenty

Informacje prawne dotyczące UE, w tym wszystkie unijne akty prawne od 1952 r., są dostępne we wszystkich językach urzędowych UE w portalu EUR-Lex: http://eur-lex.europa.eu.

Portal Otwartych Danych UE

Unijny portal otwartych danych (http://data.europa.eu/euodp/pl) umożliwia dostęp do zbiorów danych pochodzących z instytucji i innych organów UE. Dane można pobierać i wykorzystywać bezpłatnie, zarówno do celów komercyjnych, jak i niekomercyjnych.

DS-01-18-082-PL-C

Ogólne rozporządzenie o ochronie danych (RODO) reguluje sposób, w jaki przedsiębiorstwa przetwarzają dane osobowe i zarządzają nimi. Dzięki jednolitemu europejskiemu prawu w zakresie ochrony danych osobowych Twoja firma, oferując towary i usługi w dowolnym kraju UE, podlega przede wszystkim wspólnym przepisom o ochronie danych.

Upraszczając otoczenie regulacyjne, w jakim działają firmy, RODO jest źródłem nowych możliwości, dzięki którym przedsiębiorstwa mogą skuteczniej zarządzać danymi osobowymi, co w rezultacie prowadzi do zwiększenia zaufania konsumentów.

Niniejsza broszura poświęcona jest obowiązkom Twojej firmy wynikającym z RODO.

europa.eu/dataprotection/pl

Urząd Publikacji

ISBN 978-92-79-79411-7