Ochrona danych osobowych w Rainbow English

Szkolenie podstawowe

Wersja wrzesień 2019

DO UŻYTKU WEWNĘTRZNEGO

Pewnie słyszałeś o RODO

RODO to Rozporządzenie Unii Europejskiej regulujące zasady ochrony danych osobowych obywateli UE.

To najważniejszy akt prawny w Europie na ten temat.

Oficjalna nazwa to:

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 (ogólne rozporządzenie o ochronie danych)

RODO obowiązuje wszystkie podmioty, które przetwarzają dane osób z Unii Europejskiej.

Zasady są bardzo podobne we wszystkich krajach UE. Różnice wynikają z prawa krajowego i podejścia regulatorów.

Główne cele RODO

- Zapewnienie lepszej ochrony osób fizycznych poprzez ochronę ich danych – o ryzykach przeczytasz na następnym slajdzie
- Zapewnienie większych praw do prywatności dla obywateli UE
- Ułatwienie kontroli nad własnymi danymi. Konieczność zachowania transparentności

Ryzyka naruszenia praw lub wolności osób

RODO ma minimalizować ryzyka wynikające z niewłaściwego przetwarzania danych osobowych, które może doprowadzić między innymi do:

- uszczerbku fizycznego - *np. zaginięcie dokumentacji medycznej*
- szkód majątkowych lub niemajątkowych, - *np. ujawnienie danych karty kredytowej*
- dyskryminacji, - *np. na podłożu rasowym, wyznaniowym*
- kradzieży tożsamości lub oszustwa dotyczącego tożsamości, - *np. kradzież tożsamości skutkująca zaciągnięciem zobowiązań przez przestępcę w imieniu ofiary*
- naruszenia dobrego imienia – np. w wyniku kradzieży konta w social mediach

Kontekst przetwarzania może mieć wpływ na zwiększenie ryzyka.

Np. wyciek adresu email z bazy sklepu obuwniczego powoduje mniejsze ryzyko niż wyciek z bazy portalu dla osób chorych na AIDS

Mówiąc o ryzyku w przypadku RODO nie patrzymy na ryzyko ze strony firmy, tylko ze strony osoby, której dane dotyczą!

Podsumowując

RODO ma chronić osoby fizyczne poprzez ochronę ich danych przed ujawnieniem osobom nieupoważnionym, utratą lub nieupoważnioną zmianą.

Kluczowe pojęcia z RODO

Co to są dane osobowe

są to wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”).

Dane osobowe można podzielić na dane identyfikujące osobę np. imię i nazwisko, adres email, wizerunek, PESEL oraz wszelkie dane z nimi powiązane takie wiek, miejsce pracy, wykształcenie itp.

Prawo wskazuje jeszcze szczególne kategorie danych, które podlegają większej ochronie. Należą do nich:

- Pochodzenie rasowe lub etniczne,
- Poglądy polityczne,
- Przekonania religijne lub światopoglądowe,
- Przynależność do związków zawodowych,
- Dane genetyczne,
- Dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej,
- Dane dotyczące zdrowia, seksualności lub orientacji seksualnej osoby
- Informacje o karalności

Przetwarzanie szczególnych kategorii danych

Przetwarzanie szczególnych kategorii danych osobowych zwiększa ryzyko naruszenia praw lub wolności osób. W związku z tym RODO wprowadza ograniczenia w przetwarzaniu tych danych.

Obowiązuje zasada, że przetwarzanie takich danych jest zakazane chyba, że spełniona jest określona lista warunków.

W każdym wypadku przed rozpoczęciem przetwarzania tego typu danych powinieneś to skonsultować z Administratorem Danych Osobowych.

Przetwarzanie danych osobowych

„przetwarzanie” oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

Bardzo szerokie pojęcie.

Praktycznie wszystkie operacje na danych są uznawane za przetwarzanie.

Anonimizacja i pseudonimizacja

Anonimizacja i pseudonimizacja są metodami zabezpieczania danych osobowych

anonimizacja – oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie

nieodwracalna

Stosujemy, gdy nie potrzebujemy już danych osobowych, ale potrzebujemy np. statystyk.

Np.. Mamy dane dotyczące wejść na stronę www. Możemy usunąć adres IP i inne dane pozwalające na identyfikację. Reszta informacji pozwalających na śledzenie statystyk zostaje.

pseudonimizacja - oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej

odwracalna

Przykładem na pseudonimizację jest zastąpienie imienia i nazwiska numerem indeksu na liście wyników egzaminu

Administrator vs podmiot przetwarzający

Administrator to podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych

Możecie się też spotkać z angielską nazwą Controller

Przykładowo: Rainbow English będzie Administratorem, jeśli decyduje :

- Jakie kategorie danych zbiera i przetwarza
- W jakich celach dane są przetwarzane
- Jak długo dane są przechowywane
- Czy i komu dane są udostępniane

Tak jest w przypadku zbierania danych w procesach rekrutacyjnych, kadrowych, w ramach świadczenia usług etc.

Podmiot przetwarzający

Podmiot przetwarzający oznacza podmiot, który przetwarza dane osobowe w imieniu Administratora;

Możecie się też spotkać z angielską nazwą Processor

Przykłady, gdy Rainbow English jest Podmiotem przetwarzającym:

- Wykonujemy szkolenie dla pracowników klienta, przetwarzamy jego dane (np. lista osób uczestników)

Rainbow English ma też swoje podmioty przetwarzające: np. współpracujący z nami lektor, firma dostarczający nam obsługę księgową czy firma dostarczającą nam usługi hostingowe.

Ważne
Można korzystać wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.

Umowa powierzenia danych

Relacja między Administratorem, a Podmiotem przetwarzającym **musi** się odbywać się na **podstawie umowy** lub innego instrumentu prawnego, które:

- wiążą Podmiot przetwarzający i Administratora,
- określają przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, oraz
- obowiązki i prawa Administratora

To nie musi być oddzielna umowa. Można zapisy dotyczące przetwarzania danych zawrzeć w umowie głównej.

Jeśli korzystasz/chcesz skorzystać z podmiotów przetwarzających i chcesz przekazać im posiadane przez Rainbow English dane osobowe lub ktoś np. klient chce nam powierzyć przetwarzanie zgłoś się do Administratora Danych Osobowych biuro@rainbow-english.pl w celu przygotowania stosownych rozwiązań umownych

Administrator vs Podmiot przetwarzający - wymagania

Administrator

Przykładowe wymagania:

- Uczciwe, przejrzyste i bezpieczne zbieranie danych osobowych
- Może zbierać dane tylko w określonymi i zgodnymi z prawem celami
- Musi zapewnić dokładność i bezpieczeństwo przetwarzania
- Musi zapewnić uaktualnianie i czyszczenie danych
- Musi zapewnić przestrzeganie retencji danych i ich usuwania

Podmiot przetwarzający

Przykładowe wymagania:

- Musi przetwarzać dane wg udokumentowanych instrukcji Administratora
- Musi utrzymywać bezpieczeństwo danych i chronić je przed nieautoryzowanym dostępem, ujawnieniem lub utratą
- Musi informować Administratora o naruszeniu bezpieczeństwa danych

Przesłanki prawne przetwarzania danych osobowych

W celu zgodnego z prawem przetwarzania danych osobowych każdy Administrator musi mieć do tego co najmniej jedną podstawę prawną z niżej wymienionych

- **zgoda** – *dobrowolna, konkretna, świadoma, jednoznaczna*
- **niezbędność do wykonania umowy** – *do celów wykonania umowy np. umowy o pracę*
- **niezbędność do wypełnienia obowiązku prawnego** – *w celu wypełnienia obowiązku wynikającego z prawa np. prowadzenie ksiąg rachunkowych*
- **ochrona żywotnych interesów podmiotów danych** – *przetwarzanie konieczne do ochrony czyjegoś życia*
- **zadania realizowane w interesie publicznym** – *przetwarzanie konieczne do prawnie zdefiniowanych interesów publicznych jak podatki, zdrowie publiczne, opieka społeczna*
- **uzasadnione interesy realizowane przez Administratora** – *do celów prawnie usprawiedliwionych interesów Administratora z wyjątkiem sytuacji, gdy taki interes przeważa nad interesami, prawami podstawowymi osoby. Przetwarzanie takie nie powinno zaskakiwać lub być dotkliwe dla osoby.*

Cel przetwarzania

dane osobowe muszą być m.in.: zbierane w **konkretnych, wyraźnych i prawnie uzasadnionych celach** i nie mogą być przetwarzane dalej w sposób niezgodny z tymi celami

przykład zmiany celu

Jeśli dzwoni do nas klient, by zapytać o ofertę, zbieramy jego dane w postaci numeru telefonu w celu odpowiedzi na zapytanie.

Nie możemy takich numerów zbierać i sprzedawać firmie sprzedającej garnki. Nie w takim celu ta osoba nam swoje dane przekazała.

Przejrzystość

Podczas zbierania danych od osoby, której dane dotyczą należy poinformować tą osobę m.in. o

- danych Administratora;
- celach przetwarzania danych osobowych oraz podać podstawę prawną przetwarzania;
- informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;
- okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
- o prawach tej osoby

Przejrzystość - cd

Jeśli zbieramy dane w sposób inny niż od osoby, której dane dotyczą, także musimy wykonać obowiązek informacyjny.

Musimy to wykonać

a) w rozsądnym terminie po pozyskaniu danych osobowych – najpóźniej w ciągu miesiąca

b) jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą – najpóźniej przy pierwszej takiej komunikacji z osobą, której dane dotyczą; lub

c) jeżeli planuje się ujawnić dane osobowe innemu odbiorcy – najpóźniej przy ich pierwszym ujawnieniu

Naruszenia ochrony danych

naruszenie ochrony danych osobowych oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Jeśli jest prawdopodobne, że naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych, **jesteśmy zobowiązani zgłosić je do UODO** bez zbędnej zwłoki – w miarę możliwości, nie później niż **w terminie 72 godzin** po stwierdzeniu naruszenia.

Jeśli naruszenie dotknęło danych, które przetwarzamy jako Podmiot przetwarzający, musimy o nim poinformować Administratora danych, czyli firmę z którą współpracujemy. Tu w zależności od umowy mamy jeszcze mniej czasu.

Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.

Naruszenia ochrony danych cd.

Jeśli masz podejrzenia lub wykryjesz incydent związany z bezpieczeństwem danych osobowych **musisz natychmiast zgłosić** to Administratorowi Danych Osobowych (biuro@rainbow-english.pl)!

Prawa osób

Zgodnie z RODO każda osoba fizyczna ma prawo do żądania od Rainbow English

- Informacji o przetwarzaniu jej danych osobowych
- Otrzymania kopii danych
- Sprostowania danych
- Zaprzestania przetwarzania danych (prawo do sprzeciwu) w tym do celów marketingu bezpośredniego oraz profilowania
- Usunięcia danych („prawo do bycia zapomnianym”)
- Ograniczenia przetwarzania
- Przeniesienia danych

Jeśli wpłynie do Ciebie takie żądanie poinformuj bezzwłocznie Administratora Danych Osobowych, tak abyśmy mogli zrealizować je w przewidzianym prawem czasie (30 dni)

Ogólne zasady przetwarzania danych osobowych - podsumowanie

Dane osobowe muszą być:

- przetwarzane zgodnie z prawem, rzetelnie, w sposób przejrzysty
- zbierane w konkretnych, wyraźnych i uzasadnionych celach
- odpowiednie i ograniczone do niezbędnego minimum
- prawidłowe i w razie potrzeby, uaktualniane
- przechowywane do czasu, gdy jest to konieczne
- przetwarzane w sposób zapewniający bezpieczeństwo danych

Co jest wymagane od Ciebie?

Zadaj sobie pytania?

Dlaczego zbieram te dane? Czy naprawdę potrzebuję ich wszystkich?

Czy mogę zastosować anonimizację lub pseudonimizację, by zredukować ryzyko dla zainteresowanych osób i dla firmy?

- ✓ Zbieraj tylko to, co jest ci naprawdę potrzebne do wykonania zadania
- ✓ Używaj danych tylko w określonym wcześniej celu
- ✓ Dane zebrane w jednym celu nie mogą być używane w innym bez właściwej podstawy prawnej
- ✓ Bądź świadomy danych, jakie posiadasz i tego, jaki skutek może mieć ich ujawnienie
- ✓ Trzymaj się zasad retencji danych
- ✓ Anonimizuj lub pseudonimizuj dane, jeśli jest to wykonalne

- ❖ Nie trzymaj starych danych, nawet jeśli chcesz ich użyć ponownie. Jest prawdopodobne, że są już nieaktualne.
- ❖ Nie trzymaj danych na wszelki wypadek
- ❖ Nie twórz wielu instancji danych. Unikaj posiadania wielu kopii tych samych danych.
- ❖ Nie przetwarzaj szczególnych kategorii danych

Co jest wymagane od Ciebie?

Zadaj sobie pytania?

Czy dostęp do danych jest ograniczony wedle zasady *need to know*?

Czy dane są przechowywane bezpiecznie?

Jaki jest najlepszy sposób przesyłania danych?

- ✓ Udostępniaj dane tylko tym, którzy tego potrzebują do pracy i są upoważnieni
- ✓ Wyczyść dane ze swojego dysku twardego
- ✓ Przesyłaj dane w postaci zaszyfrowanej (np. używaj zaszyfrowanych załączników)
- ✓ Przechowuj dane w formie papierowej w bezpieczny sposób. Zamykaj je w szafce, jeśli ich właśnie nie używasz.
- ✓ Natychmiast informuj ADO, jeśli utraciłeś swój sprzęt lub wysłałeś poufnego maila do niewłaściwej osoby
- ✓ Myśl, zanim klikniesz
- ✓ Upewnij się, że umowy z naszymi Twoimi procesorami są zgodne z wymaganiami

Co jest wymagane od Ciebie?

Zadaj sobie pytania?

Czy jest prawdopodobne, że osoba, której dane posiadam, może tego oczekiwać?

Czy mam pozwolenie/podstawę prawną, by używać tych danych, by wykonać inne zadanie/przetwarzać dane w inny, nowy sposób?

Czy działam w sposób przejrzysty?

- ✓ Bądź szczery i przejrzysty z pracownikami, klientami lub innymi osobami na temat sposobu, w jaki przetwarzamy ich dane

- ❖ Nie używaj danych w innych celach niż zamierzone
- ❖ Nie rób marketingu do osoby, która wyraziła sprzeciw
- ❖ Nie udostępniaj danych na zewnątrz, jeśli nie masz na to właściwych podstaw prawnych

Podsumowanie

Bezpieczeństwo danych osobowych to zmartwienie nie tylko Administratora Danych Osobowych, ale **odpowiedzialność wszystkich** pracowników i współpracowników Rainbow English.

Działania nas wszystkich mają wpływ na firmę, na jej rynkową wiarygodność i reputację.

Każdy ma obowiązek:

- Ukończyć szkolenie dotyczące ochrony danych oraz zdać test wiedzy
- Stosować polityki, standardy i wytyczne w zakresie ochrony danych, bezpieczeństwa
- Minimalizować ilość i zakres danych
- Traktować osoby, których dane przetwarzamy po partnersku. Wykorzystanie przez nas danych powinno być przez nich spodziewane.
- Zgłaszać do Administratora Danych Osobowych incydenty i żądania osób, których dane dotyczą.
- Konsultować – jeśli masz wątpliwości dzwoń / pisz. Kontakt na kolejnej stronie

Dane kontaktowe

Julia Budzowska
Administrator Danych Osobowych
m: + 48 509 611 918
julia.budzowska@gmail.com
biuro@rainbow-english.pl

ZAPRASZAM DO KONTAKTU!

Przejdź do testu