RODOmapa

JAK KROK PO KROKU WDROŻYĆ
RODO W SOLOBIZNESIE

Aga Zalewska
legalnienaonlajnie.pl

Czy ja przetwarzam jakieś dane - czyli zrób audyt danych osobowych w swoim biznesie...

Znajdź chwilę w spokoju, w miejscu w którym zazwyczaj pracujesz i masz dostęp do swego komputera i dokumentów, z którymi masz kontakt w swojej pracy.

KROK 1. Zidentyfikuj dane osobowe, które przetwarzasz

Szukaj przede wszystkim danych osób fizycznych, ale i firm. Jeśli dane dotyczą tylko firmy (np. nazwa spółki zoo i dane kontaktowe), to nie będą to dane osobowe. Jeśli natomiast przy nazwie firmy pojawi się imię i nazwisko lub adres email, który pozwala na identyfikację konkretnej osoby - tak, to już są dane osobowe.

Szukaj tych danych zarówno w formie cyfrowej (np. zapisy na newsletter, dane klientów w sklepie internetowym), jak i "papierowej" (np. umowy z klientami, pracownikami, drukowane formularze zgód, karty pracy z klientem, etc.).

Nie zastanawiaj się, jak to wszystko grupować, czy porządkować - na razie wypisz sobie wszystko, co przychodzi Ci do głowy. To mogą być bardziej oczywiste rzeczy, jak lista mailingowa do newslettera lub klienci albo mniej oczywiste jak np. formularz drukowany, jakiś zapomniany Excel na dysku, gdzie są dane np. uczestników warsztatu, który organizowałaś 3 miesiące temu.

I jeszcze jedna ważna informacja. Identyfikując dane osobowe w swoim biznesie, szukasz tego, co już jest oraz bierzesz pod uwagę wszystko to, co dopiero zaplanowałaś, że wprowadzisz (jeśli to dotyczy niedalekiej przyszłości).

Czym są dane osobowe?

Dane osobowych - to informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (osobie, której dane dotyczą).

Możliwa do zidentyfikowania osoba fizyczna - to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

Przykłady: dane klientów, osób chętnych na newsletter, osób współpracujących z Tobą, osób, które biorą udział w organizowanych przez Ciebie konkursach i wyzwaniach, kandydaci do pracy, pracownicy, osoby logujące się do Twojej platformy e-learningowej, na której udostępniasz swoje produkty online , etc.

KROK 2. Zbiory danych osobowych

Jak RODO definiuje zbiór?

> *„zbiór danych" oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;*

W poprzednim kroku wypisałaś sobie wszystkie dane osobowe, jakie przetwarzasz. Teraz przyjrzyj się tym danym. Czy to są wyodrębnione zbiory, jak np .

- baza klientów
- baza subskrybentów newslettera
- baza pracowników i współpracowników (umowy o prace, umowy zlecenia, dzieło)
- baza potencjalnych klientów
- uczestnicy wyzwania lub konkursu
- uczestnicy grupy mastermind, którą organizujesz
- inne

Jeśli to nie są konkretne zbiory, to spróbuj to sobie je pogrupować. Pomocne w tym będą poniższe pytania:

- w jakim **celu** przetwarzasz te dane osobowe
  np. rekrutacja pracownika/osoby współpracującej na stanowisko wirtualnej asystentki, realizacja umowy, wysyłka newslettera
- jakie są **kategorie** osób, których dane przetwarzasz:
  np. osoby, które zgłosiły się do rekrutacji na stanowisko wirtualnej asystentki, osoby chętne, by otrzymywać newsletter
- na jakiej **podstawie** przetwarzasz dane (podstawa prawna)
  czyli co Cię do tego upoważnia, może to być:
  - zgoda na przetwarzanie danych w określonym celu wyrażona np. w formularzu newslettra,
  - może to tez być sama umowa (np. klient zamówił produkt online w Twoim sklepie internetowym),

I pamiętaj:

jeden cel przetwarzania to jeden zbiór danych

Przykłady: baza klientów, którzy chcą kupić ebooka w przedsprzedaży, baza klientów, którzy zakupili subskrypcję szkolenia online, baza subskrybentów newslettera, baza pracowników, baza współpracowników, baza podwykonawców, baza do windykacji należności , członkowie programu lojalnościowego, itd.

I jeszcze jedno. Kontakty do klientów w skrzynce email, dane tych klientów w sklepie internetowym oraz np. rejestr wysyłek zrealizowanych zamówień z danymi klientów - to wszystko będzie jeden zbiór - dane klientów.

KROK 3. Czy znasz źródło danych osobowych, czyli skąd dane pochodzą

Przy wszystkich zbiorach danych (nazywajmy je bazami danych) wypisz sobie, jakie jest ich źródło, czyli skąd te dane pochodzą, w jaki sposób je zgromadziłaś.

Przykłady: dane podane przez osoby zainteresowane w formularzu zapisu na newsletter, dane podane przez klientów w formularzu zamówienia w celu realizacji umowy, dane podane przez osoby zainteresowane w formularzu na stronie lądowania, dane kandydatów do pracy przesłane pocztą elektroniczną

KROK 4. Cel oraz podstawa prawna przetwarzania danych, czyli po co i dlaczego przetwarzam dane

Teraz już masz świadomość, gdzie i jakie dane osobowe są przetwarzane w Twoim biznesie. Danych osobowych nie można sobie przetwarzać ot tak sobie, trzeba się z tego umieć wytłumaczyć i do tego służy m.in.: wskazanie celu przetwarzania.
Mówi o tym Artykuł 5 ust. 1lit.b) RODO:

> *Dane osobowe muszą być:*
>
> *(...)zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami;*

Co to oznacza? Chodzi o to, że nie można przetwarzać danych w celu innym niż się je zebrało. Skoro poinformowałaś kogoś, że będziesz przetwarzać dane tylko w celu wysyłki newslettera, to nie można potem tych danych przetwarzać w innym celu. Wyjątek stanowi sytuacja, jeśli osoba, której dane chcemy przetwarzać, wyraziła odrębną zgodę na nowy cel przetwarzania.

Przykłady takich celów:

- zbieranie danych w celu wysyłki newslettera do osób zainteresowanych, które wyraziły na to zgodę
- zbieranie danych w celu umożliwienia uczestnikom udziału w wyzwaniu/obejrzenia webinaru, etc.
- zbieranie i przetwarzanie danych klientów w celu realizacji umowy
- zbieranie danych kandydatów do pracy w celu rekrutacji na stanowisko asystentki
- przetwarzanie danych w celu udostępnienia klientom materiałów szkoleniowych na platformie e-learningowej

I jeszcze dla przypomnienia definicja, co oznacza przetwarzanie danych. Zwróć uwagę, że RODO już samo zbieranie danych określa jako przetwarzanie.

Czym jest PRZETWARZANIE DANYCH?

to **każda operacja** 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.

Ok, to cel już mamy. Teraz czas na podstawę prawną.

Dane osobowe możemy przetwarzać, jeśli spełnimy jeden z warunków określonych w Art. 6 RODO. Te warunki to właśnie podstawy prawne. Nie mając podstawy prawnej, nie możesz przetwarzać danych osobowych. Dlatego tak ważne jest określenie tych podstaw. Bo na pewno będzie ich klika. Może być, że dane jednej osoby będziesz przetwarzać w różnych celach i na różniej podstawie.

Będzie to miało miejsce, gdy np. ta sama osoba będzie Twoim klientem i zapisze się na newsletter.

No dobra - to jakie to podstawy? Odpowiada na to pytanie Art. 6 RODO.

> *Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – spełniony jest co najmniej jeden z poniższych warunków:*
>
> *a) osoba, której dane dotyczą wyraziła **zgodę** na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;*
>
> *b) przetwarzanie jest niezbędne do wykonania **umowy**, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;*
>
> *c) przetwarzanie jest niezbędne do wypełnienia **obowiązku prawnego** ciążącego na administratorze;*
>
> *d) przetwarzanie jest niezbędne do ochrony **żywotnych interesów osoby**, której dane dotyczą, lub innej osoby fizycznej;(chcesz wiedzieć, jakie to mogą być interesy? Zajrzyj do Motywu ie 46)*
>
> *e) przetwarzanie jest niezbędne do wykonania **zadania realizowanego w interesie publicznym** lub w ramach sprawowania władzy publicznej powierzonej administratorowi;*
>
> *f) przetwarzanie jest niezbędne 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.*

Przykłady:

a) zgoda na przetwarzanie danych w celu wysyłki newslettera, zgoda na przetwarzanie danych w celach marketingowych
b) umowa sprzedaży zawarta przez stronę internetowa, sprzedaż podczas kiermaszu, warsztatów (to nadal umowa, nawet gdy nie masz jej na papierze), przygotowanie kalkulacji dla klienta zainteresowanego naszą usługą lub produktem (nawet, gdy do zawarcia umowy finalnie nie dojdzie)
c) obowiązki podatkowo-księgowe (np. konieczność przechowywania faktur dokumentujących sprzedaż)
d) poinformowanie bliskich osoby, która uległa wypadkowi; poinformowanie ratowników o danych osoby, która uległa wypadkowi
e) zadania dotyczące edukacji publicznej lub zdrowia publicznego
f) np. przetwarzanie danych osób, które zgłosiły się po informację o usługach lub produktach lub pytają o ofertę, np. korzystając z formularza kontaktu na stronie lub dzwoniąc

KROK 5. Zakres danych osobowych: czyli jakie dokładnie dane przetwarzam

Dane osobowe, jak już wiesz, to wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.

Jakie dane umożliwiają identyfikację danej osoby? Są to na przykład: imię i nazwisko, adres zamieszkania, numer NIP, adres email. Ale to tylko niektóre przykłady.

Jak określić zakres przetwarzanych danych?

Po prostu wypisz "pola" (tytuły kolumn), jakie masz w każdej bazie. W przypadku bazy do wysyłki newslettera, będą to: imię i adres email, w bazie klientów będą to: imię i nazwisko, adres wysyłki, adres email, numer NIP, dane do faktury, a w przypadku płatności elektronicznych: imię, nazwisko, adres e-mail, kwota.

Pamiętaj, że określasz swoją sytuację w biznesie, a nie szukasz uniwersalnej wskazówki, jakie dane możesz zbierać. To Ty to określasz jako Administrator, ale pamiętaj, że powinno to być adekwatne do celu przetwarzania i zgodne z zasadami RODO m.in.: zasadą minimalizmu.

ZASADA MINIMALIZMU

Artykuł art. 5 ust. 1 lit. c) RODO mówi, że dane osobowe muszą być:
- adekwatne,
- stosowne
- oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane.

Czyli inaczej mówiąc:
- nie możesz pytać o adres zamieszkania danej osoby, jeśli chcesz wysyłać do niej newsletter,
- nie będziesz pytać o PESEL, jeśli chcesz sprzedać ebooka; zapytasz o niego, jeśli masz wypożyczalnię aut i potrzebujesz nr PESEL do ubezpieczenia lub na wypadek ewentualnych roszczeń

KROK 6. Czas przetwarzania, czyli na jak długo potrzebne będą Ci te dane i jak długo je możesz przetwarzać

W tym punkcie określ, jak długo dane będą przetwarzane. Dlaczego to takie ważne? Danych nie możemy sobie przetwarzać, jak długo chcemy. Powinno się to odbywać nie dłużej niż jest to uzasadnione celem przetwarzania. Tę informację znajdziesz w Art. 5 ust. 1 lit f.:

> *przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, **przez okres nie dłuższy, niż jest to niezbędne do celów**, w których dane te są przetwarzane;*

Jak określić ten czas?

To może być konkretna data, ale jeśli nie jest to możliwe, to możesz to określić w sposób opisowy.

Przykłady:

- do chwili cofnięcia zgody na przetwarzanie lub zaprzestania wysyłki newslettera
- do czasu zakończenia wyzwania (określ, jakiego wyzwania)
- przez 3 miesiące od chwili zalogowania się do platformy e-learningowej
- do chwili zakończenia procesu rekrutacji i wyłonienia osoby na szukane stanowisko
- do czasu zakończenia realizacji umowy
- może to być konkretna data, jeśli jesteś w stanie ją określić

...wiesz już o danych osobowych, które przetwarzasz, całkiem dużo - to sprawdź, na ile te dane są u Ciebie bezpieczne

KROK 7. Analiza ryzyka

Przeprowadź analizę ryzyka. Możesz to nazwać szacowaniem. To konieczne, by móc potem wdrożyć odpowiednie rozwiązania, które pomogą Ci zapewnić bezpieczeństwo danych, które przetwarzasz.

I jeszcze wyjaśnienie: **analiza ryzyka** a **ocena skutków dla ochrony danych** (DPiA). DPIA to po prostu sformalizowana analiza ryzyka. Przeprowadza się ją wg warunków wskazanych w RODO, jeżeli ryzyko przetwarzania danych jest wysokie. Kto ma obowiązek przeprowadzenia DPiA? Odpowiedź znajdziesz w Art. 35 ust. 3.

Czy do przeprowadzenia "zwykłej" analizy ryzyka potrzebne jest skomplikowane narzędzie? W przypadku działalności Soloprenerki - nie. Za to niezbędna jest wiedza o danych osobowych, jakie przetwarzasz.

Trochę jeszcze o samym o ryzyku

Co na to RODO?
Motyw 83 (motyw to punkt z preambuły, czyli rozbudowanego wstępu, do RODO)

> *W celu zachowania bezpieczeństwa i zapobiegania przetwarzaniu niezgodnemu z niniejszym rozporządzeniem administrator lub podmiot przetwarzający powinni **oszacować ryzyko właściwe dla przetwarzania** oraz **wdrożyć środki** – takie jak szyfrowanie – minimalizujące to ryzyko. Środki takie powinny zapewnić **odpowiedni poziom bezpieczeństwa**, w tym poufność, oraz uwzględniać **stan wiedzy technicznej oraz koszty ich wdrożenia w stosunku do ryzyka i charakteru danych** osobowych podlegających ochronie (...).*

Zaznaczyłam w powyższym tekście niektóre elementy. Zwróć na nie uwagę. To kilka wskazówek, które dotyczą od czego zacząć, jeśli chcemy zanalizować ryzyko naruszenia danych w naszym biznesie oraz zadbać o odpowiedni poziom bezpieczeństwa.

Po pierwsze. Analizujemy nie jakieś abstrakcyjne ryzyko, ale "właściwe dla przetwarzania" dla naszego biznesu. Tu nie chodzi o wzór z Sèvres (to taka gmina na południowo-zachodnich przedmieściach Paryża, gdzie się znajduje Międzynarodowe Biuro Miar i Wag i tam przechowuje się różne wzorce miar, np. wzorzec metra, takiego do mierzenia oczywiście). Tu chodzi o zanalizowanie sytuacji, którą Ty masz u siebie. Jeśli ryzyka nie ma, albo jest bardzo niskie, zastosujesz inne zabezpieczenia i procedury niż ktoś, kto to ryzyko oszacował na dużo wyższe, gdzie istnieje ryzyko naruszenia nie tylko samych danych, ale w jego skutek, również praw i wolności osoby fizycznej.

O jakie ryzyko chodzi?

...i dalej Motyw 83 mówi nam:

> *Oceniając ryzyko w zakresie bezpieczeństwa danych, należy wziąć pod uwagę ryzyko związane z przetwarzaniem danych osobowych – takie jak przypadkowe lub niezgodne z prawem **zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych** przesyłanych, przechowywanych lub w*

*inny sposób przetwarzanych – i mogące w szczególności prowadzić do **uszczerbku fizycznego, szkód majątkowych lub niemajątkowych**.*

A o jakie konkretnie szkody i uszczerbki może chodzić? Tu z pomocą idzie Motyw 75.
To może być na przykład:

- dyskryminacja, kradzież tożsamości lub oszustwo dotyczące tożsamości,
- strata finansowa,
- naruszenie dobrego imienia,
- naruszenie poufności danych osobowych chronionych tajemnicą zawodową,
- nieuprawnione odwrócenie pseudonimizacji
- lub wszelka inna znaczna szkoda gospodarcza lub społeczna;
- osoby, których dane dotyczą, mogą zostać pozbawione przysługujących im praw i wolności lub możliwości sprawowania kontroli nad swoimi danymi osobowymi
- naruszenie dotyczy danych wrażliwych (pochodzenie rasowe lub etniczne, poglądy polityczne, wyznanie lub przekonania światopoglądowe, lub przynależność do związków zawodowych oraz jeżeli przetwarzane są dane genetyczne, dane dotyczące zdrowia lub dane dotyczące seksualności lub wyroków skazujących i naruszeń prawa lub związanych z tym środków bezpieczeństwa;
- naruszenie dotyczy profilowania (ocena czynników osobowych, w szczególności analizowane lub prognozowane aspekty dotyczące efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się – w celu tworzenia lub wykorzystywania profili osobistych)
- naruszenie dotyczy danych osobowych osób wymagających szczególnej opieki, w szczególności dzieci;
- jeżeli naruszenie dotyczy danych przetwarzanych na dużą skalę

No to co teraz? Co robimy? Analizujemy...

Analiza ryzyka to po prostu obiektywna ocena sytuacji przetwarzania danych w naszym biznesie. Pamiętajmy, że przetwarzaniem jest już samo zbieranie danych i ich przechowywanie.

A bardziej konkretnie? Jak to zrobić? Podstawowy zakres tego, co mierzymy, to:

- **prawdopodobieństwo wydarzenia**
- **i ewentualny niekorzystny skutek wydarzenia**

Do oceny można przyjąć **5.stopniową skalę np. bardzo duże, duże, średnie, małe, bardzo małe.** To tyle o technicznej stronie, a w praktyce, można zrobić tak:

1. **zastanów się, co złego może się wydarzyć z danymi, w skutek ich przetwarzania (np. wyciek danych na zewnątrz, bo np. zgubiłaś pendriva lub został skradziony)**
2. **teraz postaraj się ocenić prawdopodobieństwo tych wydarzeń**
3. **I jak już wiesz te dwie rzeczy, to teraz czas pomyśleć, jak bardzo ucierpieć mogą osoby, których dane zostały naruszone wskutek wydarzenia (jednego z tych, które zidentyfikowałaś w pkt. 1)**

RZYKŁADY:

Nie masz zbyt wielu pomysłów na wydarzenia, które się mogą wydarzyć? To mogą być:

- zagrożenia fizyczne (np. pożar)
- naruszenie bezpieczeństwa informacji (np. kradzież urządzenia lub dokumentów, w których są dane)
- awaria techniczna (np. awaria urządzenia)
- nieautoryzowane działania (np. dostęp do danych przez osobę nieuprawnioną)
- naruszenia osobowe (np. działanie hackera, nie wyszkolone osoby wewnątrz)

Jeśli znasz ryzyko, to teraz pomyśl o bezpieczeństwie tych danych

KROK 8. System informatyczny, czyli za pomocą, jakich narzędzi przetwarzam

Wypisz sobie wszystkie programy, aplikacje i systemy informatyczne, strony internetowe i wtyczki do nich, w których przetwarzasz dane. Zwróć uwagę, że przetwarzanie danych może być automatyczne i nieautomatyczne. Nie musisz oglądać danych na własne oczy, by je przetwarzać.

Takim przykładem mogą być dane osób, które się zapisały na Twój newsletter, a Ty im go wysyłasz za pomocą programu do email marketingu (np. Mailer Lite). Piszesz treść newslettera i przyciskasz WYŚLIJ, a program sam wysyła go do bazy danych.

Przykłady: Wordpress (strona internetowa), Mailer Lite (program do email marketingu: newsletter, landing page), PayPal, Przelewy24 (programy do automatycznych płatności), iFirma (program do automatycznego wystawiania faktur), MS Excel (plik excel do ręcznego wystawiania faktur, plik excel z danymi kandydatów do pracy), program do rezerwacji wizyt itp.

Przy okazji systemu informatycznego przypomnij sobie też dane, które przetwarzasz poza nimi. Będą to wszystkie dane w formie "papierowej". Czy miejsca, gdzie je trzymasz są bezpieczne? Czy nie mają do nich dostępu osoby niepowołane?

Myśląc o bezpieczeństwie danych, zastanów się też nad tym, czy trwałość danych jest zachowana, tzn. czy zabezpieczasz je także przez zniszczeniem. I pytanie: czy pomyślałaś o backupach danych? A jeśli je robisz, to czy trzymasz je w innym miejscu niż źródło danych?

KROK 9. O bezpieczeństwie jeszcze trochę

Teraz, gdy wiesz, jakie dane i jak przetwarzasz oraz określiłaś już poziom ryzyka, zastanów się, jakie rozwiązania technologiczne i organizacyjne (czyli np. procedury) możesz wdrożyć, by zadbać o bezpieczeństwo danych. Pomyśl, jak maksymalnie obniżyć ryzyko przetwarzania tych danych.

Wybierając rozwiązania, zwróć uwagę na ich adekwatność. Co to oznacza? Mówi o tym art. 30 ust. 1, Który wymienia 11 takich elementów. Zapoznaj się z nimi.

Potrzebujesz przykładów, jakie środki bezpieczeństwa można zastosować? Proszę bardzo:

- narzędzia prawne (np. upoważnienia, oświadczenia o zachowaniu w poufności, umowa powierzenia)

- organizacyjne (np. procedury postępowania z danymi i urządzeniami, na których znajdują się dane)
- fizyczne (np. kontrola dostępu do pomieszczeń)
- informatyczne (np. oprogramowanie antywirusowe, kontrolowany dostęp do programów i aplikacji, unikalne loginy i hasła)

Pamiętaj to mogą być dowolne rozwiązania, które w Twojej ocenie zabezpieczą dane, w odpowiedni do zidentyfikowanego ryzyka, sposób. Nie przesadzaj z budowaniem twierdzy nie do zdobycia, jeśli to ryzyko jest u Ciebie niskie. Ale pamiętaj też, że to Ty jako administrator jesteś odpowiedzialna na to, co wybierzesz i efekt tych zabezpieczeń. Zatem też nie lekceważ tematu.

Ok, to mniej więcej wiesz już, jak się mają dane u Ciebie. A może komuś umożliwiasz dostęp do nich? Ha, to pytanie retoryczne. Na pewno tak. Nie jesteś pewna? Przejdź do następnego kroku.

KROK 10. Powierzenia, upoważnienia, udostępnienia, czyli komu umożliwiasz dostęp do danych, które przetwarzasz

UDOSTĘPNIENIE

Udostępnienie danych osobowych innemu administratorowi oznacza faktyczne przekazanie danych osobowych. Skutkiem udostępnienia danych osobowych jest faktyczne przekazanie danych osobowych, w wyniku **którego nowy administrator będzie decydował o celach i środkach przetwarzania danych oraz ponosił odpowiedzialność w zakresie przewidzianym dla administratora**. Podmiot, któremu udostępniasz dane staje się niezależnym administratorem tych danych.

POWIERZENIE

W tym przypadku nie przekazujesz faktycznie danych osobowych, ale jedynie umożliwiasz do nich dostęp w określonym celu i zakresie. I to Ty jesteś tą osobą, która określa cel i zakres przetwarzania. Podmiot, który otrzymał w drodze powierzenia dane osobowe nie może wyjść poza to, co zostało określone w umowie powierzenia. Podmiot ten staje się jedynie procesorem danych, a Ty jesteś nadal ich administratorem.

UPOWAŻNIENIE

Art. 29 RODO: Podmiot przetwarzający oraz każda osoba działająca z upoważnienia administratora lub podmiotu przetwarzającego i mająca dostęp do danych osobowych przetwarzają je **wyłącznie na polecenie administratora**, chyba że wymaga tego prawo Unii lub prawo państwa członkowskiego.

Jeśli chcesz by np. Twój pracownik miał dostęp do danych Twoich klientów, powinnaś wystawić mu upoważnienie dostępu do danych. Potem taka osoba nie może zrobić nic więcej poza ty, do czego została upoważniona.

Upoważnienie podpiszesz np. ze swoją asystentką lub specjalistą ds. obsługi klienta, jeśli zatrudniasz ich na umowę o pracę lub zlecenie.

Przypadków udostępnienia danych oraz upoważnienia do przetwarzania danych będzie niewiele w Twojej firmie.

RODO przewiduje tylko kilka przypadków udostępnienia danych. I są to:

- wyraźna zgoda osoby, której dane dotyczą
  (np. zgoda na udostępnienie innym podmiotom w celach marketingowych)
- na podstawie przepisów prawa
  (np. udostępnienie danych policji, prokuraturze, sądom)
- innemu administratorowi, jeżeli przetwarzanie jest niezbędne 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 (dochodzenie roszczeń, zapobieganie oszustwom, marketing bezpośredni).

Natomiast przypadków powierzeń będzie zdecydowanie więcej.

Jeśli korzystasz w swojej firmie z podwykonawców na zasadzie B2B lub inaczej mówiąc, outsourcujesz cześć usług na zewnątrz (np. księgowa, obsługa informatyczna, obsługa klienta), powinnaś wiedzieć, czym jest powierzenie i jak powinna wyglądać umowa powierzenia.

Więcej przykładów? Będą to firmy, którym powierzasz dane osobowe, bo konieczne jest to do realizacji usługi dla Twoje firmy

- np. firma, która dostarcza Ci automatyczny system płatności
- firma, która dostarcza Ci automatyczny system do fakturowania
- firma, która zapewnia Ci hosting
- firma, która dostarcza Ci narzędzie do email marketingu np, Mailer Lite, Mail Chimp
- usługi księgowe dla Twojej firmy
- firmy, które świadczą dla Twojej firmy usługi kurierskie (jeśli nie znajdują się w Rejestrze operatów pocztowych prowadzonej przez Urząd Komunikacji Elektronicznej)
- firmy, które udostępniają platformy do sprzedaży Twoich produktów

Powierzenie może się odbywać na podstawie umowy powierzenia lub innego instrumentu prawnego np. regulaminu usługodawcy.

Przykład:

- formularz na stronie internetowej Mail Chimp, który umożliwia zawarcie umowy powierzenia, zapisy w regulaminie
- hostingodawcy, umowa powierzenia podpisana w formie papierowej z księgową, umowa powierzenia podpisana
- z wykorzystaniem poczty elektronicznej z informatykiem

Jakie elementy powinna zawierać umowa powierzenia?
Zajrzyj do Art. 28. Tam znajdziesz przydatne wskazówki.

Bezpieczeństwo danych, to także zadbanie o prawa osób, których dane przetwarzasz

KROK 11. Obowiązek informacyjny

Obowiązek ten wynika z art. 13 RODO. Znajduje się tam cała lista informacji, jakie należy przekazać osobie, której dane chcemy przetwarzać. Skoro chcemy przetwarzać czyjeś dane osobowe, to ta osoba powinna wiedzieć, kim jesteśmy oraz jak i gdzie te dane będą przetwarzane. Obowiązek informacyjny możemy umieścić w tzw. klauzuli informacyjnej lub w polityce prywatności. Niezależnie od formy i treści takiej informacji, należy poinformować o :

- tożsamości i danych kontaktowych administratora,
- danych kontaktowych inspektora ochrony danych, jeśli został powołany w Twojej firmie,
- **celach** przetwarzania oraz podstawie prawnej,
- jeśli podstawą prawną przetwarzania jest prawnie uzasadniony interes administratora, to należy wskazać, jaki jest to interes,
- **o odbiorcach danych** osobowych lub o kategoriach odbiorców, jeżeli istnieją (czyli np. komu powierzać będziemy dane),
- o zamiarze **przekazania danych osobowych** do państwa trzeciego lub organizacji międzynarodowej (jeśli Cię to dotyczy)
- **okresie przetwarzania**, a gdy nie jest możliwe wskazanie konkretnego terminu, podajemy **kryteria** ustalania tego okresu,
- **PRAWACH**, które mają osoby, których dane chcemy przetwarzać i są to: prawo do żądania dostępu do danych dot. osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania , prawo do wniesienia sprzeciwu wobec przetwarzania, a także prawo do przenoszenia danych oraz prawo wniesienia skargi do organu nadzorczego,
- o prawie do **cofnięcia zgody** w dowolnym momencie , jeśli taka zgoda została wcześniej wyrażona,
- o tym, czy podanie danych osobowych jest **wymogiem ustawowym lub umownym albo warunkiem zawarcia umowy** oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;
- o **zautomatyzowanym** podejmowaniu decyzji, w tym o profilowaniu (jeśli jest stosowane)

Jeżeli jako administrator planujesz dalej przetwarzać dane osobowe **w celu innym niż cel, w którym dane osobowe zebrałaś**, przed takim dalszym przetwarzaniem poinformuj osobę, której dane dotyczą, o tym innym celu oraz udziel jej wszelkich innych stosownych informacji, które zostały wymienione powyżej.

Kiedy spełnić obowiązek informacyjny? Oczywiście zanim zaczniemy przetwarzać dane lub tak szybko, jak to jest możliwe.

KROK 12. RODO na stronie internetowej

Zadbałaś o to, co w środku? Teraz czas na to, co widoczne najbardziej - czyli Twoją stronę internetową. Będziesz potrzebowała:

- Polityki prywatności i plików cookies
- komunikatu o ciasteczkach
- klauzul informacyjnych przy formularzach na stornie (kontaktowym, zamówienia, zapisu na newsletter, innym)

Stwórz na swojej stronie internetowej podstronę pt. Polityka prywatności i wklej tam uzupełnioną Twoimi danymi treść Polityki prywatności i plików cookies. Podstrona ta może być dostępna np. z menu dolnego lub górnego strony (nie musi być w menu głównym). To może być też plik w pdf. Pamiętaj, że sposób udostępnienia powinien być wygodny i czytelny dla użytkownika.

Pamiętaj, że w polityce prywatności spełniasz obowiązek informacyjny, więc jej nie chowaj. Daj do niej łatwy dostęp osobie, wobec której spełniasz ten obowiązek. Nie zapomnij o linkach do Polityki z formularzy, czy komunikatu o ciasteczkach.

Pamiętaj również, że podstawa przetwarzania danych zbieranych za pośrednictwem strony internetowej może być różna, np. :

- formularz zamówienia - umowa
- formularz zapisu na newsletter - zgoda (nie zapomnij o nią zapytać)
- formularz kontaktowy - prawnie uzasadniony interes administratora

CHECKLISTA. Dokumenty

Dokumenty, jakie będą Ci niezbędne do wdrożenia RODO w swoim biznesie lub przydatne, by wykazać stosowanie zasady rozliczalności (czyli wykazania, że dane przetwarzane są zgodnie z RODO)

- Dokument potwierdzający przeprowadzenie analizy ryzyka
- Polityka prywatności i plików cookies dla Twojej strony internetowej
- Polityka bezpieczeństwa w zakresie ochrony danych osobowych (a w niej m.in.: wykaz obszaru przetwarzania, wykaz zbiorów danych , opis struktury danych, sposób przepływu danych, wykaz środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności)
- Instrukcja zarządzania systemem informatycznym
- Rejestr czynności przetwarzania
- Rejestr kategorii przetwarzania, jeśli dane przetwarzasz jako procesor
- Wzór Umowy powierzenia
- Rejestr umów powierzenia
- Wzór Upoważnienia do przetwarzania
- Oświadczenie o poufności
- Rejestr osób upoważnionych do przetwarzania danych osobowych
- Rejestr udostępnień danych osobowych podmiotom zewnętrznych (jeśli do tego dochodzi)
- Wzór Raportu z naruszenia ochrony danych osobowych (tak na wszelki wypadek)
- Rejestr naruszeń (tak na wszelki wypadek)

Co jeszcze warto wiedzieć

Polecam Ci lekturę Rozporządzenia RODO (ogólne rozporządzenie o ochronie danych osobowych). Nie jest to najbardziej porywająca lektura, ale ma kilka ciekawych fragmentów. Oprócz tego, o czym wspomniałam w tej RODOmapie, zwróć uwagę jeszcze na:

Artykuł 4 - Definicje

Artykuł 5 - Znajdziesz tam zasady dotyczące przetwarzana danych osobowych - jeśli będziesz o nich pamiętać, albo wiedzieć, gdzie ich szukać, pozwoli Ci to łatwiej podejmować decyzje dotyczące danych osobowych w Twoim biznesie

Artykuł 6 - Zgodność przetwarzania z prawem

Artykuł 7 - Warunki wyrażenia zgody (czyli, jak to powinno wyglądać)

Artykuł 9 - Dane wrażliwe

Artykuły 12 do 22 - Prawa osoby, której dane dotyczą

Artykuł 24 - Obowiązki administratora

Artykuł 25 - zasada privacy by design i zasada privacy by default

Artykuł 32 - bezpieczeństwo przetwarzania

RODOmapa na pewno nie wyczerpuje tematu RODO. To jedynie garść wskazówek, które mają wyłonić choć trochę czytelniejszy obraz na początek. Ale nie martw się, jeśli przejdziesz przez RODOmapę, to powinnaś wiedzieć, co zrobić i ewentualnie, jaką wiedzę uzupełnić. To tylko na początku wydaje się być trudne.

Jeśli masz pytania, chcesz podzielić się swoim doświadczeniem lub potrzebujesz pomocy - to znajdziesz mnie tutaj:

Grupa na facebooku: **Legalnie na onlajnie**
Fanpage: **Legalnie na onlajnie Aga Zalewska**
Instagram: **legalnienaonlajnie.pl**
email: **aga@legalnienaonlajnie.pl**