RODO - przewodnik dla małych firm,

które nie robią nic szczególnego z danymi...

Tomasz Bienias
wersja z 2018-03-27

Od 25 maja 2018 r. każda firma działającą w UE, również osoby prowadzące działalność gospodarczą muszą stosować zasady unijnego rozporządzenia RODO / GDPR. Bez względu na to, gdzie przetwarzają dane.

Co w związku z tym trzeba wiedzieć?
- Jakie są prawa klientów (czyli również nasze prawa)
- Jakie są obowiązki firm
- Jak nie zrobić nic niepotrzebnie i nie przepłacić za dostosowanie

Niektórym lektura tego przewodnika wystarczy, by odnaleźć się w nowych warunkach, innym powinna ułatwić rozmowy z prawnikami.

Czy to mnie dotyczy?

Prowadzisz szkolenia, kursy jogi, uczysz angielskiego, masz salon kosmetyczny, wynajmujesz kwatery wakacyjne. Zbierasz kontakty - nazwiska, maile i telefony osób? Ten przewodnik jest dla Ciebie.

Jeśli robisz z danymi coś więcej niż podpisywanie umów i wystawianie faktur, np. prowadzisz marketing wysyłając klientom maile - przeczytaj ten przewodnik, ale zapoznaj się z RODO dokładniej.

Dużo w związku z RODO będzie nieporozumień. Warto ich uniknąć. To prawo jest trudne i zła interpretacja może oznaczać, że zrobisz nie to, co trzeba. Np. zrobisz za dużo, bo ktoś powie Ci, że na wszystko musisz zbierać zgody.

Co gorsza, jeśli jesteś małą firmą, nie znajdziesz prawnika, który rozumie rozporządzenie i na którego będzie Cię stać. Dziś wielki problem z RODO mają duże firmy i dobrzy prawnicy są bardzo zajęci pracując dla nich.

Kary

Za dużo się o nich mówi. Nie grożą Ci kary, jeśli nie zrobisz nic złego (celowo lub przez nieodpowiedzialność i beztroskę). Nie grożą Ci, jeśli zachowasz minimum przyzwoitości starając się poznać prawo i je stosować.

Większym problemem niż kary będzie biurokracja, zamieszanie i nieuzasadnione żądania od osób, które "coś słyszały". Warto wiedzieć, które oczekiwania klientów musimy spełniać, a których nie.

Przetwarzanie danych - co to jest?

Jeśli zbieramy dane o ludziach i przechowujemy je w uporządkowany sposób - przetwarzamy dane osobowe. Nie musi się to odbywać w komputerze. Nazwiska i adresy mogą być w naszych zbiorach "przy okazji" - np. na fakturach.

Bałagan, w którym tylko my możemy coś znaleźć, trudno nazwać przetwarzaniem. Podobnie jest z kartonem wizytówek, notesem czy wydrukami umów. Jeśli są na nich dane osób, to w związku z RODO trzeba zadbać, by nikt nieupoważniony nie miał do nich dostępu.

Gdy mamy uporządkowaną kartotekę papierową, zaczyna się przetwarzanie. Każdy taki zbiór trzeba

zabezpieczać. Przede wszystkim - cokolwiek robisz, musisz się troszczyć o to, żeby dane nie wpadły w niepowołane ręce. O tym jest to prawo - o szanowaniu danych osób (również pracowników).

Czego nie dotyczy RODO? Najkrócej:
- Zbiorów nieuporządkowanych
- Danych przetwarzanych w celach czysto prywatnych
- Danych kontaktowych firm i organizacji (osób prawnych)

Kiedy trzeba się RODO zainteresować dokładniej:
- Gdy zbieramy dane ludzi, do których wysyłamy informacje marketingowe
- Gdy zbieramy dane wrażliwe (np. o karalności, zdrowiu)
- Gdy przekazujemy dane innym firmom (choćby księgowej)
- Jeśli używamy systemu informatycznego, w którym są informacje o ludziach (cokolwiek bardziej zaawansowanego niż poczta)

Za dane odpowiada ich administrator. Jest to osoba prowadząca działalność lub spółka (nie jej pracownik). Przetwarzanie to wszystko co z danymi robimy: • zbieranie • przechowywanie • usuwanie • opracowywanie • udostępnianie.

Zgody - czy są potrzebne?

Jeśli ktoś powie wam, że w związku z RODO od wszystkich klientów musicie zbierać zgody na przetwarzanie danych, poślijcie go na drzewo. Kropka.

Jeśli jednej rzeczy mielibyście się tu dowiedzieć, niech to będzie właśnie to. Ze zgodami będzie najwięcej zamieszania. Zostaniemy zawaleni niepotrzebnymi komunikatami - nie dokładajmy się do tego.

Wg nowego prawa, w większości sytuacji zamiast zgody wystarczy normalne działanie. Może nim być np. podanie namiarów, w tym telefonu i adresu e-mail w formularzu internetowym. Dla przedsiębiorcy ważne jest, by pytać tylko o niezbędne dane. Wyłącznie to, co potrzebne, by wyświadczyć usługę lub odpowiedzieć na pytanie.

Gdy ktoś do nas dzwoni i umawia się na usługę, robi to świadomie i zwykle wie z kim rozmawia. Jeśli zbieramy zgłoszenia na kurs, czy wynajem noclegów za pomocą strony internetowej, przyda się na niej prosty komunikat "Zgodnie z RODO zbieramy Państwa dane dla potrzeb realizacji usługi". Powinna też być łatwo dostępna informacja o tym, kto prowadzi działalność (nazwa firmy i adres, lub nazwisko prowadzącego działalność).

Choć jest to przetwarzanie danych osobowych, nadal będziemy mogli trzymać dane klientów i informacje o tym czy zapłacili. Jednak wiedząc, po co je trzymamy i trzymając nie dłużej niż potrzeba.

Schody zaczynają się, gdy chcemy np. wysyłać osobom oferty i informacje o usługach. W przewodniku MPiT przeczytacie, że marketing własnych produktów i usług jest uzasadnionym interesem administratora i nie wymaga zgód. Tu jednak zdania prawników bywają podzielone. Na wszelki wypadek zawsze warto zadać sobie pytanie - czy tego spodziewają się klienci? Minimum to poinformować, że mogą dostać informacje o nowościach i naszych ofertach. Oraz dać im łatwą możliwość np. wypisania się z mailingu. Ważne by potem pilnować, żeby tym osobom naprawdę nic nie wysyłać!

Powtórzmy: zgody zazwyczaj nie są potrzebne.

Po pierwsze: nie ma konieczności ich zbierania.

Po drugie: lepiej ich nie zbierać. Dlaczego? Zbieranie zgód ma konsekwencje. Np. trzeba umożliwić ich łatwe cofanie. Każdy formularz musi działać w dwie strony, a to zwykle jest bardziej kosztowne i zawodne.

Zgoda oznacza też, że mamy jakąś bazę, w której są dane. Upraszczając, że jest jakieś rozwiązanie informatyczne, które pozwala na przeszukiwanie zbioru informacji wg określonych kryteriów. RODO narzuca dla każdej takiej bazy wymagania. Osoba, od której pozyskacie dane do bazy, ma np. prawo zażądać byście przekazali jej kopię wszystkiego co o niej macie. To kosztuje i trzeba się tym dodatkowo zajmować, więc lepiej tego nie robić.

Ważne: móc udowodnić, że się staramy

Nigdzie nie przeczytacie co dokładnie trzeba w związku z RODO zrobić. Przedsiębiorca powinien sam określić, jakie zabezpieczenia będą dla jego zbiorów wystarczające. Prawo każe nam tu dołożyć starań, w związku z czym warto udokumentować moment dokładania starań.

Jak to zrobić? Najpóźniej w maju przygotować prostą "analizę przetwarzania danych". Wydrukować, podpisać i trzymać ją na wypadek kontroli. Ważne by powstał dokument z datą i byli świadkowie. Przy okazji można przemyśleć to, co się robi. Można to zrobić z partnerem biznesowym lub z prawnikiem.

Tylko upewnijcie się, że ten prawnik rozumie to prawo. Możecie np. zadać mu pytania o rzeczy z tego poradnika. Oczywiście jest to wyzwanie, może nawet trudniejsze niż spotkanie z nieznanym mechanikiem samochodowym.

Wersja minimum tej analizy może być tabelą identyfikującą zbiory danych jakie mamy. Tworząc ją trzeba upewnić się, że nic nie zbieramy niepotrzebnie. W kolejnych kolumnach można zawrzeć następujące informacje (podaję punkty z przykładami dla ilustracji):

1. Nazwa zbioru. Np. *"kontakty w poczcie elektronicznej konto@nazwafirmy.pl'*
2. Co to za ludzie? Np. *"Klienci, kontrahenci, zainteresowaniu usługami"*
3. Po co nam ten zbiór - jakie są cele przetwarzania. Np. "*Prowadzenie korespondencji biznesowej'*
4. Podstawa prawna. Zwykle art. 6. RODO (niżej odniesienie).
5. Co z tym zbiorem robimy - jak dodajemy dane, kiedy usuwamy (ustalone terminy lub czas usunięcia danych).
6. Kto ma dostęp. Imię i nazwisko oraz dane kontaktowe administratora oraz informacje kto ma dostęp (np. imię nazwisko asystentki, księgowej i Pana Marka od komputerów).

I tyle.

Osoby, które mają dostęp do danych, muszą otrzymać prostą instrukcję, która każe im dbać o poufność danych.

RODO każe zrobić opis technicznych i organizacyjnych środków bezpieczeństwa danych. Brzmi strasznie, ale niech to będą spisane zasady działania dla nas i pracowników z dostępem. Z podkreśleniem, żeby:

- Nikomu nie przekazywać danych
- Chronić je przed dostępem innych ludzi
- Usuwać w terminach (nie trzymać, gdy niepotrzebne)
- Mieć opisaną procedurę alarmową (punkt niżej)

W małych firmach będzie to trochę dmuchanie na zimne. Jeśli jednak mamy wielu świadomych klientów, warto.

Przekazywanie danych np. księgowej

Czasem przekazujemy dane zewnętrznemu podmiotowi. Tak jest np. w związku z prowadzeniem księgowości, ale tylko gdy na naszych fakturach pojawiają się nazwiska ludzi - odbiorców lub wykonawców. Wtedy należy się upewnić, że nasza księgowa stosuje RODO.

To ważne, mamy obowiązek wyboru podmiotu, który przestrzega RODO. To on za to odpowiada, ale rozporządzenie nie pozwala nam na beztroskę.

Gdy komuś przekazujemy dane, nie ograniczajmy się do działania na podstawie tego przewodnika. W szczególności warto zadbać o umowę powierzenia danych. Warto znaleźć dobry wzór takiej umowy, lub sięgnąć po pomoc kogoś, kto dobrze zna temat.

Jednak uwaga, tu też można przesadzić, np. wymyślając, że przetwarzanie danych w poczcie jest przekazaniem ich np. do Google (w przypadku skrzynki Gmail). Znajdziecie tego typu rady w internecie. Naprawdę nie o to chodzi w tym prawie.

Najważniejsze: Alarmować

Najważniejsze to dbać, by dane osobowe klientów i partnerów, nie wpadły w niepowołane ręce.

Jeśli do tego dojdzie, trzeba szybko poinformować zainteresowanych oraz urząd. Może tak być, gdy zgubimy nośnik z danymi, lub gdy ktoś włamie się na nasze konto z dostępem do danych. Wtedy informujemy, że miał miejsce "wyciek danych".

Rozwiązania, które warto rozważyć

Tyle na temat rozporządzenia. Uzupełnieniem niech będą propozycje rozwiązań zwiększających bezpieczeństwo danych. Może ich być wiele, niżej podstawowe działania. Powinniście je stosować bez względu na to czy jest RODO czy nie. Jest jednak tak, że zwykle o tym nie myślimy:

- Założenie osobnej skrzynki pocztowej (poza prywatną) do korespondencji firmowej. Warto się upewnić, że jest bezpieczna i szyfrowana. Sami musimy zadbać o bezpieczne regularnie zmieniane hasło.

- Rozważyć przeniesienie części relacji biznesowych na bezpieczną platformę upewniwszy się, że stosuje RODO. Korespondencję biznesową i kontakty w wersji minimum można utrzymywać np. na GoldenLine czy LinkedIn. Rekrutacje prowadzić wyłącznie np. na Goldenline czy HRlink.

- W telefonie przedsiębiorcy są kontakty prywatne i biznesowe. Nie można nie mieć ustawionego hasła / kodu dostępu do telefonu. Jeśli jakimś cudem jeszcze tego nie macie: wasz telefon powinien się blokować po krótkiej bezczynności a dostęp do niego musi być chroniony hasłem lub odciskiem palca.

- Jeśli dane trzymacie w komputerze, profil nie może nie być zahasłowany. Zróbcie też tak, by profil biznesowy nie był profilem z prawami administratora na komputerze. To trochę wyższy poziom bezpieczeństwa.

- Dane papierowe należy trzymać w miejscu, do którego nie ma dostępu nikt nieupoważniony. Na pewno nie na biurku w recepcji, przez którą przewijają się dziesiątki osób, w niezamykanych pomieszczeniach publicznych, otwartych szafkach itp… Obowiązują nas tu elementarne zasady bezpieczeństwa.

Ważne zastrzeżenia

Gdybym był prawnikiem nie mógłbym tego przewodnika napisać tak wprost. Uprościłem temat najlepiej jak potrafię, mam nadzieję, że dzięki temu wiesz o co chodzi lub wiesz o co pytać dalej. Mam też nadzieję, że z czasem pojawi się coraz więcej klarownych publikacji, napisanych ludzkim językiem.

Nawiasem mówiąc - wymaga tego RODO. Motyw 39 Rozporządzenia mówi "Zasada przejrzystości wymaga, by wszelkie informacje i wszelkie komunikaty związane z przetwarzaniem tych danych osobowych były łatwo

dostępne i zrozumiałe oraz sformułowane jasnym i prostym językiem". Dziś większość publikacji, w tym poradników tworzonych przez urzędy, nie spełnia tego warunku - podaję to tylko jako przykład paranoi do jakiej można dojść w zasadzie z każdym zapisem tego prawa.

Nie znajdziesz poradnika o RODO, którego autor nie zastrzega, że to co napisał nie jest oficjalną wykładnią. Podobnie jest z tym poradnikiem. Nie jestem więc prawnikiem, ale poznałem dobrze temat. Dołożyłem wszystkich starań oraz pokazałem ten tekst znajomym prawnikom (takim zajętym, bardzo dobrym, przejrzeli to, bo dobrzy są nie tylko merytorycznie).

Pamiętaj jednak, że robisz, to co robisz, na własną odpowiedzialność.

Źródła - gdzie szukać dodatkowych informacji?

Proste poradniki
- Przewodnik Ministerstwa Przedsiębiorczosci i Technologii - plik PDF
- Legal Geek - Przewodnik prawny dla przetwarzających dane osobowe
- Poradniki i materiały Panoptykon, np. Rodo na tacy,

Treść RODO
Pełny tekst
Uwaga: Rodo zanim na dobre się zacznie ma 173 "motywy" - punkty opatrzone tekstem "a także mając na uwadze, co następuje:". Są pasjonujące, ale zostawmy je prawnikom - żeby zrozumieć jak to złożone, lepiej przeczytać te parę artykułów.
W szczególności spojrzeć na:
art. 6. "Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach..." "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;"
art. 9 "Przetwarzanie szczególnych kategorii danych osobowych"
art. 12 "Przejrzyste informowanie i przejrzysta komunikacja oraz tryb wykonywania praw przez osobę, której dane dotyczą"
art. 13 'Informacje podawane w przypadku zbierania danych od osoby, której dane dotyczą".

Lektury uzupełniające (warto poznać, by zrozumieć skalę problemów):
Większośc prawników pisząc o RODO zabezpiecza się zawalając teksty odniesieniami do paragrafów. Dlatego nieprzyzwyczajonym do takiej publicystyki ludziom trudno się w tym rozeznać. Ciekawym polecam wyróżniające się klarownością publikacje:
Coraz bliżej RODO
O zgodzie i braku zgody na marketing w internecie