Komisja Europejska

# Siedem kroków, jakie mogą podjąć przedsiębiorstwa,

# aby przygotować się na wejście w życie ogólnego rozporządzenia o ochronie danych

*Sprawiedliwość i konsumenci*

# Do kogo skierowany jest ten dokument?

**Niniejszy przewodnik ma pomóc firmom, które nie obsługują danych osobowych w ramach swojej podstawowej działalności, takim jak małe i średnie przedsiębiorstwa (MŚP) przetwarzające głównie dane osobowe swoich pracowników lub listy klientów i kontrahentów. Dotyczy to na przykład handlowców lub sklepów, takich jak piekarnie czy sklepy mięsne, bądź usługodawców, takich jak architekci. W niniejszym przewodniku wymieniono kilka kroków, które należy podjąć, aby przygotować się do wejścia w życie RODO.**

Dane osobowe oznaczają wszelkie informacje odnoszące się do rzeczywistej, żyjącej osoby fizycznej (w odróżnieniu od osoby prawnej). Zaliczają się do nich na przykład: imię, nazwisko, adres domowy, adres e-mail lub dane o lokalizacji pochodzące z mapy w telefonie komórkowym. Zazwyczaj dotyczy to danych pracowników, klientów lub dostawców przechowywanych przez przedsiębiorstwo.

**Im mniejsze jest ryzyko szkodliwego wpływu działań przedsiębiorcy na dane osobowe, tym mniejszy jest zakres jego obowiązków**

## Przestrzegaj podstawowych zasad:

- **zbieraj dane osobowe w jasno określonym celu i nie używaj ich do innych celów** (jeśli poprosisz klienta o jego adres e-mail, aby przesyłać mu nowe oferty lub promocje, nie możesz użyć tego adresu e-mail do żadnego innego celu ani sprzedać go innej firmie).
- **nie zbieraj danych, których nie potrzebujesz** (jeśli świadczysz usługi dostawy do domu, potrzebujesz np. adresu lub nazwiska na domofonie, ale nie musisz wiedzieć, czy dana osoba pozostaje w związku małżeńskim czy nie) — zwracaj uwagę na to, jakie dane osobowe pozostają pod Twoją kontrolą.

## KROK 1 — SPRAWDŹ DANE OSOBOWE, KTÓRE GROMADZISZ I PRZETWARZASZ, CEL, W JAKIM TO ROBISZ ORAZ PODSTAWĘ PRAWNĄ

Zatrudniasz **pracowników**; przetwarzasz ich dane osobowe w oparciu o umowę o pracę i na podstawie zobowiązań prawnych (takich jak składanie sprawozdań do organów podatkowych/systemu ubezpieczeń społecznych).

Możesz zarządzać listą **indywidualnych klientów**, na przykład wysyłać im powiadomienia o specjalnych ofertach/reklamach, jeśli uzyskasz zgodę tych klientów.

Nie zawsze potrzebujesz zgody. W niektórych przypadkach osoby fizyczne oczekują, że ich dane zostaną przetworzone. Przykładowo jako sprzedawca pizzy możesz przetwarzać dane dotyczące adresu dostawy, aby zareklamować jeden z nowych produktów. Taki cel jest nazywany uzasadnionym interesem. Musisz poinformować osoby fizyczne o zamierzonym celu wykorzystania danych i przerwać ich przetwarzanie na prośbę tych osób.

Jeśli zarządzasz listą **dostawców** lub **klientów biznesowych**, robisz to na podstawie zawartych z nimi umów. Umowy te nie muszą być sporządzone na piśmie.

## KROK 2 — POINFORMUJ KLIENTÓW, PRACOWNIKÓW I INNE OSOBY FIZYCZNE, JEŻELI GROMADZISZ ICH DANE OSOBOWE

Osoby fizyczne muszą wiedzieć, że przetwarzasz ich dane osobowe oraz w jakim celu.

Informowanie nie jest wymagane, gdy osoby fizyczne posiadają informacje o sposobie wykorzystania danych, na przykład gdy klient prosi o dostawę towaru do domu.

Na żądanie przedsiębiorca ma obowiązek poinformować osobę fizyczną, jakie dane osobowe na jej temat przechowuje, a także udostępnić jej te dane. Gromadzone dane powinny być uporządkowane, aby móc je bez problemu udostępnić, np. gdy pracownik zapyta pracodawcę o rodzaj przechowywanych danych osobowych.

## KROK 3 — PRZECHOWUJ DANE OSOBOWE NIE DŁUŻEJ, NIŻ JEST TO KONIECZNE

**Dane dotyczące Twoich pracowników:** przez cały okres obowiązywania stosunku pracy i związanych z tym zobowiązań prawnych.

**Dane dotyczące klientów:** przez cały czas trwania relacji z klientem i związanych z tym zobowiązań prawnych (na przykład do celów podatkowych).

**Usuń dane, które nie są już potrzebne do celów, do których je zebrano.**

## KROK 4 — ZABEZPIECZ PRZETWARZANE DANE OSOBOWE

Jeśli przechowujesz te dane w **systemie informatycznym**, ogranicz dostęp do plików zawierających dane, np. za pomocą hasła. Regularnie aktualizuj ustawienia zabezpieczeń swojego systemu.

*(Uwaga: RODO nie nakazuje stosowania żadnego konkretnego systemu informatycznego)*

Jeśli przechowujesz fizyczne dokumenty zawierające dane osobowe, upewnij się, że nie są dostępne dla osób nieuprawnionych; zamknij je w sejfie lub szafce.

## KROK 5 — PRZECHOWUJ DOKUMENTACJĘ DOTYCZĄCĄ PRZETWARZANIA DANYCH

Przygotuj krótki dokument wyjaśniający, jakie dane osobowe przechowujesz i w jakim celu. Może być konieczne udostępnienie dokumentacji krajowemu organowi ochrony danych, gdy tego zażąda.

Takie dokumenty powinny zawierać informacje wymienione poniżej.

| INFORMACJE | PRZYKŁADY |
|---|---|
| Cel przetwarzania danych | Informowanie klientów o ofertach specjalnych / świadczenie usług dostawy do domu; płacenie dostawcom; wypłacanie wynagrodzenia i odprowadzanie składek na ubezpieczenie społeczne pracowników |
| Rodzaje danych osobowych | Dane kontaktowe klientów; dane kontaktowe dostawców; dane pracowników |
| Kategorie osób, których dotyczą dane | Pracownicy; klienci; dostawcy |
| Kategorie odbiorców | Organy administracji pracy; organy podatkowe |
| Okresy przechowywania | Dane osobowe pracowników — do końca okresu obowiązywania umowy o pracę (i związanych z nią zobowiązań prawnych); dane osobowe klientów — do czasu zakończenia relacji/stosunku umownego z klientem |
| Techniczne i organizacyjne środki bezpieczeństwa w celu ochrony danych osobowych | Regularne aktualizacje systemów informatycznych; zamknięta szafka/sejf |
| Informacja, czy dane osobowe są przekazywane odbiorcom spoza UE | Korzystanie z usług podmiotu przetwarzającego dane spoza UE (np. na potrzeby przechowywania danych w chmurze) |

## KROK 6 — UPEWNIJ SIĘ, ŻE TWOI PODWYKONAWCY PRZESTRZEGAJĄ ZASAD

Jeżeli zlecasz przetwarzanie danych osobowych innej firmie, korzystaj wyłącznie z usług dostawcy, który gwarantuje przetwarzanie zgodnie z wymogami RODO (na przykład środki bezpieczeństwa). Przed podpisaniem umowy sprawdź, czy podwykonawca wprowadził już odpowiednie zmiany i dostosował się do wymogów RODO. Zamieść to w umowie.

## KROK 7 — SPRAWDŹ, CZY PONIŻSZE ZAPISY MAJĄ ZASTOSOWANIE DO TWOJEJ DZIAŁALNOŚCI

> Aby lepiej chronić dane osobowe, organizacje mogą być zmuszone do wyznaczenia inspektora ochrony danych. **Nie musisz jednak wyznaczać inspektora ochrony danych**, jeśli przetwarzanie danych osobowych nie należy do głównej działalności Twojej firmy, nie jest uznawane za ryzykowne, a Ty nie prowadzisz działalności na dużą skalę.

Przykładowo jeśli Twoja firma zbiera wyłącznie dane o klientach na potrzeby dostawy towarów do domu, nie musisz wyznaczać inspektora ochrony danych.

Nawet jeśli potrzebujesz wsparcia inspektora ochrony danych, możesz przypisać dodatkowe obowiązki jednemu z Twoich istniejących pracowników. Możesz również skorzystać z usług zewnętrznego konsultanta, tak jak wiele organizacji korzysta z usług zewnętrznych księgowych.

> **Zazwyczaj nie jest konieczne przeprowadzanie oceny skutków dla ochrony danych**

Taka ocena skutków jest przeprowadzana w przedsiębiorstwach, w przypadku których ryzyko niewłaściwego wykorzystania danych osobowych jest większe, na przykład w firmach świadczących usługi monitorowania publicznie dostępnych obszarów na dużą skalę (np. nadzór wideo).

Małe przedsiębiorstwa przechowujące dane osobowe na potrzeby zarządzania wynagrodzeniami pracowników i listami klientów nie muszą przeprowadzać oceny skutków dla ochrony danych w przypadku tych operacji przetwarzania.

## Grzywny

Organy nadzorcze ds. ochrony danych są uprawnione do karania naruszeń przepisów o ochronie danych. Mogą stosować środki naprawcze (takie jak nakaz lub tymczasowe zawieszenie przetwarzania) i/lub nakładać grzywny.

Decyzja o nałożeniu grzywny musi być proporcjonalna i oparta na ocenie wszystkich okoliczności danego przypadku.

Jeżeli organ zdecyduje się na nałożenie grzywny, wysokość grzywny zależy również od okoliczności sprawy, w tym wagi naruszenia lub faktu, czy naruszenie było umyślne czy powstało poprzez zaniedbanie. Uwzględni też nastawienie i intencje osoby winnej naruszenia.

# Aby uzyskać więcej informacji:

**1. Zapoznaj się z wytycznymi Komisji Europejskiej dotyczącymi reformy unijnych przepisów o ochronie danych — są one dostępne online we wszystkich językach UE:**

https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_pl

**2. Skonsultuj się z krajowym organem ochrony danych:**

http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612080

## WAŻNA INFORMACJA

Informacje zawarte w tym przewodniku mają pomóc w lepszym zrozumieniu unijnych przepisów dotyczących ochrony danych.

Przewodnik stanowi jedynie wytyczne — tylko tekst ogólnego rozporządzenia o ochronie danych osobowych (RODO) ma moc prawną. W związku z tym wyłącznie zapisy RODO prowadzą do powstania praw i obowiązków 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 pozostają 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 informacji zawartych w niniejszym przewodniku.

Zważywszy, że niniejszy dokument odzwierciedla stan faktyczny na moment jego sporządzenia, powinien być traktowany jako „żywe narzędzie", które można doskonalić, a jego treść może być modyfikowana bez powiadomienia.

Urząd Publikacji

Luksemburg: Urząd Publikacji Unii Europejskiej, 2018



| Print | PDF |
| --- | --- |
| ISBN 978-92-79-85406-4 | ISBN 978-92-79-85405-7 |
| doi:10.2838/797616 | doi:10.2838/39947 |
| DS-02-18-544-PL-C | DS-02-18-544-PL-N |