RODO

BROSZURA DLA PRACOWNIKÓW

FUNDACJA ENTROPIA

Wstęp

Prawo do ochrony własnych danych osobowych jest jednym z podstawowych praw człowieka. Wywodzi się ono z prawa do poszanowania prywatności, szacunku do życia prywatnego.

RODO to inaczej Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (inaczej ogólne rozporządzenie o ochronie danych osobowych - RODO). **Od 25 maja 2018 r.** w Państwach Członkowskich UE zmieniają się wymogi dotyczące przetwarzania danych osobowych. Wdrożenie RODO wynika po pierwsze z konieczności dostosowania przepisów do rozwoju technologii, a po drugie – z potrzeby wprowadzenia jednolitych zasad ochrony danych osobowych we wszystkich państwach Unii Europejskiej.

Prawo do ochrony prywatności, a więc i danych osobowych, nie jest oczywiście prawem absolutnym. Konieczne jest wyważenie go z innymi prawami – przy poszanowaniu zasady, że w korzystaniu z niego niedopuszczalna jest ingerencja władzy publicznej, z wyjątkiem przypadków przewidzianych przez ustawę i koniecznych w demokratycznym społeczeństwie.

Ważne, żeby pamiętać, że prawo do ochrony danych osobowych przysługuje jedynie osobom żyjącym.

Każdy z nas ma styczność z danymi

Swego czasu głośno było o pozyskiwaniu danych na „ofertę pracy". Przestępcy zamieszczali w sieci ogłoszenia o pracę. W odpowiedzi na ogłoszenie, oprócz podania w miarę standardowych danych, kandydaci (dla – rzekomo – weryfikacji tożsamości) mieli przesyłać skany dowodów osobistych. Oferty pracy nigdy się nie konkretyzowały, kandydaci zapominali o sprawie do czasu, kiedy do ich drzwi pukała Policja. Oszustwo polegało na tym, że posługując się skanem dowodu przestępcy otwierali rachunki w banku i prowadzili szeroko zakrojoną, nieuczciwą działalność posługując się rachunkiem otwartym na nazwisko „byłego kandydata". Poszkodowani klienci oszustów zgłaszali sprawy na Policję, bo na przykład nie otrzymali zamówionego i opłaconego towaru. Policja kierowała się oczywiście do właściciela rachunku, którym był niczego nieświadomy kandydat do pracy.

Zdarza się, że sami nie dbamy wystarczająco o ochronę swoich danych osobowych, ale zdarza się też, że winne są instytucje, którym te dane udostępniamy.

RODO, czyli Rozporządzenie Ogólne o Ochronie Danych Osobowych to regulacje, które zwiększają nasze uprawnienia i bezpieczeństwo w zakresie ochrony danych osobowych każdego z nas. Aby nasze dane były bezpieczne, organizacje, którym je powierzamy muszą wdrożyć nowe rozwiązania i podlegają nowym obowiązkom. Każda organizacja przetwarza dane osobowe i każdy pracownik ma z takimi danymi kontakt. Dlatego **każdy z nas może przyczynić się do ochrony danych osobowych i może być przyczyną incydentów naruszających tą ochronę**.

Z tej broszury dowiesz się, jak możesz przyczynić się do ochrony danych osobowych w organizacji, jakie obowiązki nakładają nowe przepisy oraz jakie są Twoje osobiste uprawnienia w zakresie ochrony własnych osobistych danych osobowych.

Wprowadzenie do RODO

Cel wprowadzenia RODO

Podstawą RODO jest zamiar ujednolicenia zasad ochrony danych osobowych w całej Unii Europejskiej i położenie szczególnego nacisku na wzmocnienie ochrony osób fizycznych, których dane są przetwarzane. Jako osoba fizyczna każdy z nas jest tak zwanym podmiotem danych, czyli „osobą, której dane dotyczą". Wprowadzenie jednolitego standardu ochrony danych osobowych we wszystkich państwach UE jest niewątpliwą korzyścią, która wynika z RODO. Taka jednolitość wyklucza rozbieżności między zakresami i sposobami ochrony danych w poszczególnych państwach Unii. Zrozumiałe jest też, że gwarantuje swobodny przepływ danych osobowych między państwami. Dla każdego z nas ma to skutkować pewnością prawa dotyczącego danych osobowych.

Materialny zakres stosowania RODO

Materialny zakres stosowania RODO jest szeroki. RODO stosuje się bez względu na formę przetwarzania danych i bez względu na komercyjny albo niekomercyjny cel przetwarzania. Wyłączone spod RODO są jednak prywatne zbiory danych osobowych rodziny i znajomych, prowadzone dla celów domowych albo osobistych, zarówno te w formie tradycyjnej (np. w skorowidzach adresowych), jak i elektroniczne skrzynki kontaktów np. przykład w telefonie, na komputerze albo w chmurze internetowej.

Terytorialny zakres stosowania RODO

Terytorialny zakres stosowania RODO obejmuje przetwarzanie danych osobowych w związku z działalnością administratora albo procesora na terenie Unii Europejskiej.

Co ważne, administrator nie musi mieć siedziby w Unii. Wystarczy, że na jej terenie przetwarza dane osobowe. Oznacza to objęcie regulacją RODO dużych graczy internetowych, szczególnie portali społecznościowych i wyszukiwarek internetowych.

Uprawnienia i obowiązki wynikające z RODO

W RODO zebrano i skodyfikowano podstawowe uprawnienia podmiotów danych, czyli uprawnienia każdego z nas w stosunku do naszych danych osobowych. Są to:

- **prawo dostępu do danych i informacji**,
- **prawo żądania sprostowania i uzupełnienia danych,**
- **prawo sprzeciwu wobec przetwarzania danych,**
- **prawo do przeniesienia danych,**
- **prawo do bycia zapomnianym.**

Jeżeli każdemu z nas przysługują te uprawnienia, to organizacje, którym dane przekazujemy, muszą tak dostosować swoje systemy ochrony danych osobowych, aby zapewnić przestrzeganie naszych uprawnień.

Wyjaśnienie podstawowych pojęć

Czym są „dane osobowe”?

Dane osobowe to informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, czyli o "osobie, której dane dotyczą". Inaczej mówiąc, są to informacje, które umożliwiają identyfikację danej osoby, a także informacje o tej osobie.

Dla przykładu danymi osobowymi, które umożliwiają identyfikacje osoby, są:

- **imię i nazwisko**,
- **numer identyfikacyjny np. PESEL, NIP, numer karty miejskiej,**
- **dane o lokalizacji,**
- **identyfikator internetowy, czyli adres IP, identyfikatory plików cookie, protokoły generowane przez aplikacje albo narzędzia internetowe,**
- **jeden albo kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej na przykład kod DNA, wzór siatkówki, linie papilarne.**

Zwróć uwagę na to, że dana osoba jest możliwa do zidentyfikowania, jeżeli **bez nadmiernego wysiłku** można uzyskać informacje umożliwiające jej identyfikację, czyli identyfikacja nie wymaga nadmiernego nakładu czasu, kosztów lub pracy.

W zależności zatem od okoliczności ten sam rodzaj danych może stanowić dane osobowe, ponieważ pozwala na identyfikację konkretnej osoby, a w innych nie.

Doskonałym przykładem jest popularne w Polsce imię i nazwisko: Jan Nowak. Bez dodatkowych informacji, takich jak PESEL czy adres zamieszkania, to imię i nazwisko nie pozwala na identyfikację określonej osoby, ponieważ osób o identycznym imieniu i nazwisku jest w Polsce bardzo wiele.

Linie papilarne będą daną osobową dla tego podmiotu, który na podstawie posiadanych baz danych jest w stanie skojarzyć odbicie tych linii z konkretną osobą.

Numer karty miejskiej będzie daną osobową dla przewoźnika, bo ten w swoich zbiorach posiada informacje, które pozwalają skojarzyć unikatowy numer karty z konkretną osobą (określoną z imienia, nazwiska, adresu).

Dane zwykłe i „szczególne kategorie danych” tzw. dane wrażliwe.

RODO utrzymuje znany już podział na dane osobowe „zwykłe” i „szczególne kategorie danych”, czyli tak zwane dane wrażliwe.

Dane „zwykłe” to wszystkie te dane, co do których z reguły nie miewamy obiekcji, jeżeli żąda się od nas ich ujawnienia.

RODO wprowadza nowatorskie podejście do „szczególnych kategorii” danych - danych wrażliwych - czyli tych, których nie lubimy ujawniać, bo określają nasze pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne, dotyczące zdrowia, seksualności albo orientacji seksualnej.

Zasadą jest zakaz przetwarzania „szczególnych kategorii" danych osobowych. Od tej zasady możliwe są oczywiście wyjątki, jednak warunkiem przetwarzania takich danych jest jedna z następujących podstaw:

- zgoda osoby, której dane dotyczą,
- niezbędność dla ochrony żywotnych interesów osoby, której dane dotyczą,
- profilaktyka zdrowotna,
- ważny interes publiczny.

Zbiór danych osobowych

Kluczowe w dotychczasowym modelu pojęcie „zbioru danych osobowych" schodzi na dalszy plan. Na pierwszy plan wysuwa się natomiast pojęcie „ryzyka". Niemniej prawidłowe wydzielenie i zewidencjonowanie zbiorów danych jest podstawą wprowadzenia rzetelnego systemu ochrony danych. Zbiorem danych osobowych jest uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów. Nie ma znaczenia, czy zbiór jest scentralizowany, zdecentralizowany, rozproszony funkcjonalnie lub geograficznie. Odrębnymi zbiorami danych są na przykład:

- zbiór danych pracowników, czyli dane zebrane w związku z zatrudnieniem,
- zbiór danych kandydatów do pracy, czyli dane osób ubiegających się o przyjęcie do pracy,
- zbiór danych klientów i współpracowników,
- zbiór danych osób odwiedzających, czyli tzw. księga gości.

Nie każde zestawienie danych osobowych jest zbiorem danych. Zbiór danych musi cechować wewnętrzne uporządkowanie, umożliwiające wyszukiwanie wybranych danych poprzez określone kryterium, np. według wieku, stanowiska, daty transakcji itp.

Administrator

W dotychczasowej regulacji Administrator, albo – zgodnie z polską ustawą „Administrator danych" – zwany był ADO, Administratorem Danych Osobowych.

Administratorem w świetle RODO jest osoba fizyczna, osoba prawna, organ publiczny lub inny podmiot. Istotne jest, aby podmiot ten samodzielnie albo wspólnie z innymi administratorami ustalał cele i sposoby przetwarzania danych osobowych.

Administratorem jest zatem **Twój pracodawca**.

Administrator jest odpowiedzialny za prawidłowe i zgodne z RODO przetwarzanie danych zarówno przez siebie, jak i przez podmioty, którym powierzył przetwarzanie danych.

Przetwarzanie danych osobowych

Przetwarzaniem danych osobowych jest operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, w tym:

- 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.

Przetwarzaniem jest więc każda operacja na danych osobowych.

Do przetwarzania danych osobowych administrator musi posiadać podstawę prawną.

RODO przewiduje zamknięty katalog przesłanek legalizujących przetwarzanie danych osobowych. Przetwarzanie danych osobowych musi zatem znajdować oparcie w jednej z następujących podstaw:

1) w zgodzie osoby, której dane dotyczą, albo:
2) w wykonaniu albo zawarciu umowy, albo:
3) w konieczności wypełnienia obowiązku prawnego ciążącego na administratorze albo:
4) w związku z ochroną żywotnych interesów osoby, której dane dotyczą, albo:
5) w wykonaniu zadania realizowanego w interesie publicznym albo sprawowaniu władzy publicznej, albo:
6) w prawnie uzasadnionym interesie administratora.

Zauważ, że każda z tych podstaw ma samodzielny byt. Dlatego **nie musisz wyrażać zgody, jeżeli podajesz swoje dane osobowe w związku z zawieraniem umowy**.

Pseudonimizacja i anonimizacja

Pseudonimizacja, nowe pojęcie wprowadzone przez RODO, jest podstawową metodą zabezpieczenia danych. Proces pseudonimizacji oznacza w praktyce pozbawienie informacji o osobie tych elementów, które pozwalają na ustalenie jej tożsamości. Administrator zachowuje jednak narzędzia do ponownej identyfikacji tej osoby.

Pseudonimizacja nie jest tożsama z anonimizacją. Anonimizacja oznacza bowiem trwałe usunięcie z danych osobowych elementów identyfikujących osobę, tak aby ustalenie tożsamości osoby nie było możliwe, nawet przez administratora.

Dane spseudonimizowane są danymi osobowymi, ponieważ przy użyciu klucza administrator może je bez wysiłku „odkodować". Dane zanonimizowane nie są natomiast danymi osobowymi.

Kluczowe zasady przetwarzania danych osobowych

Zasada legalności, rzetelności i przejrzystości przetwarzania

Zasada legalności, rzetelności i przejrzystości przetwarzania to generalna zasada, która dotyczy przetwarzania danych osobowych. Jest ona nadrzędna w stosunku do innych. Podlega konkretyzacji w przepisach szczegółowych, orzecznictwie i w dobrych praktykach. Oznacza konieczność przetwarzania danych zgodnie z przepisami – od zebrania danych do ich usunięcia.

Naruszeniem zasady rzetelności będzie włączenie zgody marketingowej do pozostałych zgód, ponieważ może to wskazywać na celowe ukrycie lub wymuszenie wyrażenia takiej zgody.

Zasada celowości

Zasada celowości sprowadza się do konieczności precyzyjnego określenia i rzetelnego ograniczenia przez administratora celu przetwarzania danych osobowych. Cel przetwarzania musi być określony przez administratora i zakomunikowany osobie, której dotyczą dane jeszcze przed zebraniem danych. Administratora obowiązuje bezwzględny zakaz poddawania danych dalszemu przetwarzaniu sprzecznemu z wyznaczonymi wcześniej celami.

Zasada adekwatności

Zasada ta oznacza, że przetwarzane dane osobowe powinny być w odniesieniu do ich treści adekwatne do celu przetwarzania. Niedopuszczalne jest przetwarzanie danych osobowych w zakresie szerszym, niż konieczny, czyli w zakresie wykraczającym poza niezbędny w stosunku do celu przetwarzania.

Dla przykładu, do celów marketingu drogą mailową nie jest adekwatne przetwarzanie takich danych osobowe, jak imiona rodziców adresata mailingu albo jego adres zamieszkania.

Zasada prawidłowości danych

Zasada prawidłowości danych oznacza, że administrator ma obowiązek zapewnić stałą prawidłowość, merytoryczną poprawność, zgodność ze stanem rzeczywistym, kompletność i aktualność przetwarzanych przez siebie danych. RODO wskazuje, że administrator powinien wziąć pod uwagę negatywne skutki błędnych danych dla osoby, której dane dotyczą.

Tym niemniej, administrator nie ma oczywiście obowiązku stałego, aktywnego monitorowania prawidłowości i aktualności wszelkich danych z własnej inicjatywy. Byłoby to zresztą niewykonalne. Administrator powinien jednak wdrożyć procedury korekty danych - natychmiastowej reakcji i poprawienia danych, jeżeli osoba, której dane dotyczą, zgłosi konieczność naniesienia korekt.

Zasada ograniczenia czasowego

Zasada ograniczenia czasowego, znana również pod pojęciem „retencji danych", oznacza zakaz przechowywania danych w formie, która umożliwia identyfikację osób, przez czas dłuższy niż jest to niezbędne do celów ich przetwarzania.

Jeżeli wyczerpią się cele przetwarzania danych, dane osobowe powinny być usunięte ze zbiorów administratora. Dane przechowywane w tym samym zbiorze mogą podlegać różnym okresom retencji. Administrator powinien wdrożyć procedurę okresowego przeglądu i usuwania zbędnych danych osobowych.

Zasada integralności i poufności danych

Zasada integralności i poufności danych oznacza, że dane osobowe muszą być przetwarzane za pomocą odpowiednich środków technicznych i organizacyjnych w sposób, który zapewnia odpowiednie bezpieczeństwo i poufność, w tym ochronę przed:

- niedozwolonym lub niezgodnym z prawem przetwarzaniem, nieuprawnionym dostępem do danych i do sprzętu służącego ich przetwarzaniu oraz przed nieuprawnionym korzystaniem z tych danych i z tego sprzętu,
- przypadkową utratą, zniszczeniem lub uszkodzeniem.

Zasada rozliczalności

Na administratorze spoczywa obowiązek wdrożenia odpowiednich rozwiązań, które zapewnią zgodność wewnętrznych procedur z RODO. Administrator musi wykazać, że stosowane przez niego metody przetwarzania danych osobowych są zgodne z RODO.

Z tego powodu zachowanie zgodności z RODO wymaga dobrego rozumienia wymogów RODO oraz rozumienia procesów przetwarzania danych osobowych nie tylko przez administratora, lecz także przez każdego pracownika, który styka się w swojej pracy z danymi osobowymi.

Podstawy prawne przetwarzania danych osobowych

Zgoda

Zgoda jest okazaniem woli:

- dobrowolnym,
- konkretnym,
- świadomym,
- jednoznacznym,

którym osoba, której dane dotyczą, zezwala na przetwarzanie dotyczących jej danych osobowych. Administrator musi być w stanie wykazać fakt uzyskania zgody. Konieczne jest zatem odpowiednie jej utrwalenie i przechowywanie.

Zapytanie o zgodę kierowane do osoby, której dane dotyczą, powinno być:

- napisane jasnym i prostym językiem,

- sformułowane przez administratora w zrozumiałej i łatwo dostępnej formie.

Zapytanie o zgodę skierowane do adresata w stronie czynnej np.:

„Zbieramy Twoje dane osobowe, żeby przesyłać Ci mailem informacje o promocjach i rabatach"

jest znacznie bardziej czytelne od zapytania sformułowanego w stronie biernej „Dane osobowe zbierane są w celu przetwarzania ich dla potrzeb marketingowych".

RODO wyklucza sytuację, w której zapytanie o zgodę jest sformułowane zawiłym, niejasnym językiem. Istotna jest również graficzna czytelność przekazu: wielkość czcionki, przejrzysty układ graficzny, jednoznaczność sformułowań itp.

Zgoda uzyskana nieprawidłowo, a więc z naruszeniem powyższych zasad, jest nieważna z mocy prawa.

Zgodę można wycofać w dowolnym momencie.

Wykonanie albo zawarcie umowy

Niezbędność danych osobowych do wykonania umowy jest samodzielną podstawą przetwarzania. W tym przypadku ewentualna dodatkowa zgoda nie jest wymagana. Warunkiem jest jednak to, że przetwarzanie danych i ich zakres muszą być niezbędne dla wykonania umowy.

Przykład: zawarcie umowy z operatorem telefonii komórkowej uprawnia operatora do przetwarzania naszych danych osobowych w zakresie imienia, nazwiska i adresu, ale z całą pewnością nie w zakresie imion naszych rodziców, numeru dowodu osobistego czy adresu email, o ile nie wyraziliśmy zgody na przesyłanie nam faktur elektronicznych.

Prawnie uzasadniony interes administratora

Jest to przesłanka elastyczna, ponieważ katalog „prawnych interesów" jest otwarty. Przesłanka ta jednak nie legalizuje każdego rodzaju przetwarzania danych. Przykładem przetwarzania danych na podstawie przesłanki „prawnie uzasadnionego interesu administratora" jest monitoring wizyjny instalowany w celu zwiększenia bezpieczeństwa. Zastosowanie tej przesłanki jako podstawy przetwarzania danych zawsze wymaga wyważenia interesu administratora i praw osoby, której dane dotyczą, przy czym interesy osoby mają priorytet.

Tego typu przetwarzanie danych nie wymaga ani odrębnej zgody osoby, której dane dotyczą, ani jakiejkolwiek umowy pomiędzy powierzającym a przetwarzającym dane. Musisz jedynie zostać poinformowany, np. za pomocą piktogramów, że znajdujesz się na obszarze monitorowanym.

Incydenty bezpieczeństwa

Incydentem bezpieczeństwa nazywamy każde naruszenie bezpieczeństwa danych osobowych. Incydentem jest włamanie się hakera do systemu informatycznego, ale i włamanie się złodzieja do biura. Incydent bezpieczeństwa stanowi utracenie danych osobowych przez przypadek, np. zgubienie ich albo kradzież, jest

nim też dopuszczenie do danych osobowych osób nieuprawnionych, np. jeżeli sprzęt komputerowy zostanie oddany do serwisu bez usunięcia z niego tychże danych.

Incydent

Incydent to każda sytuacja, w której zagrożone jest bezpieczeństwo przetwarzanych danych. Incydentem może być niezgodne z prawem: utracenie, zmodyfikowanie, ujawnienie danych osobowych albo umożliwienie dostępu do nich osobom nieupoważnionym.

Przykładem incydentu jest wysłanie mailem do wszystkich swoich pracowników listy płac albo zaadresowanie maila do otwartej wiadomości wszystkich swoich klientów.

Incydentem może być też pozostawienie w tramwaju firmowych dokumentów, które zawierają dane osobowe.

Incydent ma miejsce, jeśli nie zniszczysz przed wyrzuceniem do śmieci swojego kalendarza, w którym zapisane były dane adresowe klientów.

Incydentem może być również sprzedaż firmowego sprzętu, smartfonu, laptopa, przed wyczyszczeniem go z danych osobowych.

Co robić?

Na incydent bezpieczeństwa powinieneś oczywiście zareagować. Twoja reakcja jest niezbędna w co najmniej trzech przypadkach.

Po pierwsze, w sytuacji, w której do incydentu bezpieczeństwa doszło w wyniku Twojego działania, nawet niezamierzonego. Na przykład zostawiłeś teczkę z dokumentami w przedziale pociągu czy w tramwaju. Incydent ma miejsce nawet wtedy, gdy po jakimś czasie dokumenty odnajdziesz. Pamiętaj, przez czas, kiedy nie miałeś dokumentów pod nadzorem, ktoś nieuprawniony mógł się z nimi zapoznać, albo nawet je skopiować. Statystyki wskazują, że nie jest to wcale rzadki przypadek.

Po drugie – reaguj w sytuacji, w której stwierdzisz incydent w swoim otoczeniu, np. zauważysz dokumenty z danymi osobowymi, które leżą obok kserokopiarki.

Po trzecie, reaguj wtedy, gdy widzisz w swoim otoczeniu ryzyko wystąpienia incydentu, np. zauważasz, że pracownicze teczki osobowe są przechowywane w ogólnodostępnym pomieszczeniu, na otwartych regałach, bez drzwi.

Jeżeli stwierdzisz wystąpienie incydentu albo ryzyko jego wystąpienia, to natychmiast przekaż tę informację osobie odpowiedzialnej za ochronę danych osobowych w organizacji. Możliwe jest również zgłoszenie incydentu bezpośredniemu przełożonemu.

Konsekwencje wystąpienia incydentów

Jeżeli incydent bezpieczeństwa już wystąpił, RODO nakłada na administratora, bezwzględny obowiązek zgłoszenia go organowi nadzorczemu. W Polsce jest nim Prezes Urzędu Ochrony Danych Osobowych (PUODO). Administrator ma jedynie 72 godziny od stwierdzenia naruszenia na taką notyfikację. Jeżeli się spóźni, musi dołączyć stosowne wyjaśnienia przyczyn opóźnienia. To zupełnie nowy obowiązek, nieznany dotychczasowym przepisom.

W zgłoszeniu incydentu bezpieczeństwa administrator musi opisać, między innymi:

- charakter naruszenia danych i przybliżoną liczbę osób, których dane dotyczą,
- możliwe konsekwencje naruszenia ochrony danych,
- zastosowane środki zaradcze.

Dobre nawyki w ochronie danych

RODO nie zawiera gotowych rozwiązań dotyczących ochrony danych osobowych. Każdy administrator musi wypracować własne mechanizmy ochrony danych osobowych, które są ściśle dostosowane do specyfiki działalności czy charakteru przetwarzanych danych.

Pewne „dobre nawyki" są jednak wspólne.

1. Wszystkie zbędne dokumenty, zawierające dane osobowe, np. życiorysy kandydatów do pracy, którzy odpadli w rekrutacji, błędnie wydrukowane faktury albo umowy, od razu niszcz w niszczarce. Nie składuj makulatury, która zawiera dane osobowe! Nie wykorzystuj ich ponownie!
2. Stosuj zasadę „czystego biurka". Przed końcem dnia pracy uporządkuj swoje stanowisko, schowaj wszystkie dokumenty w zamykanych szafach, a klucz zdeponuj w miejscu do tego przeznaczonym. Zadbaj o to, aby dane osobowe, z którymi masz styczność, były odpowiednio zabezpieczone i żeby osoby nieupoważnione, na przykład pracownicy serwisu sprzątającego, nie miały do nich dostępu.
3. Gdy wysyłasz email do wielu odbiorców, np. do grupy współpracowników albo klientów, upewnij się, że ukrywasz widoczność adresów mailowych odbiorców wiadomości. Adresy email pozostałych odbiorców nie mogą być widoczne dla adresata maila. Służy temu opcja UDW lub BCC w polu adresata.
4. Korzystaj z prawa do bycia zapomnianym, jeśli po zmianie usługodawcy nie chcesz otrzymywać ofert od poprzedniego.
5. Gdy oddajesz telefon, tablet lub laptopa do serwisu, usuń z niego wszystkie dane osobowe. W ten sposób unikniesz ryzyka ujawnienia swoich danych osobom nieupoważnionym.

Kary

RODO pozostawia organizacjom wiele swobody w kształtowaniu wewnętrznych systemów ochrony danych osobowych i przenosi odpowiedzialność za właściwie ukształtowanie takiego systemu bezpośrednio na administratorów.

Jednocześnie przewiduje się możliwość nakładania na administratorów kar za nieprzestrzeganie regulacji RODO. Kary za najpoważniejsze naruszenia mogą sięgać 20 mln euro albo 4% rocznego światowego obrotu organizacji, przy czym zawsze zastosowanie znajdzie wyższa z tych kwot.

Kary nakładane są przez lokalne organy nadzorcze. W Polsce – przez Prezesa Urzędu Ochrony Danych Osobowych (PUODO).

MIEJSCE NA NOTATKI